International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 06, 2024
www.ijirse.com
ISSN: 2454-9665

PHISHING URL DETECTION BY USING MACHINE LEARNING AND LEVERANGING PHISH GUARD

Ms. SHAIK RIZWANA[1], M. JEEVANA SINDHU[2], K. MOUNIKA REDDY[3], K. PRASANTHI[4], SK. LAL BASHA[5]

1, Assistant Professor, Dept Of Electronics And Communication Engineering, Tirumala Engineering College,

2,3,4,5, Ug Students, Dept Of Electronics And Communication Engineering, Tirumala Engineering College.

Narasaraopet, Palnadu Dist. Andhra Pradesh India, 522601

ABSTRACT

Phishing websites have proven to be a major security concern. Several cyberattacks risk the confidentiality, integrity, and availability of company and consumer data, and phishing is the beginning point for many of them. Many researchers have spent decades creating unique approaches to automatically detect phishing websites. While cutting-edge solutions can deliver better results, they need a lot of manual feature engineering and aren't good at identifying new phishing attacks. As a result, finding strategies that can automatically detect phishing websites and quickly manage zero-day phishing attempts is an open challenge in this field. The web page in the URL which hosts that contains a wealth of data that can be used to determine the web server's maliciousness. Machine Learning is an effective method for detecting phishing. Italso eliminates the disadvantages of the previous method. We conducted a thorough review ofthe literature and suggested a new method for detecting phishing websites using features extraction and a machine learning algorithm. The goal of this research is to use the dataset collected to train ML models and deep neural nets to anticipate phishing websites.

Key words: *URL, Algorithms, Feature extraction*

I. INTRODUCTION

Malicious URL, a.k.a. malicious website, is a common and serious threat to cybersecurity Malicious URLs host unsolicited content (spam, phishing, drive-by downloads, etc.) and

ISSN: 2454-9665

lureun suspecting users to become victims of scams (monetary loss, theft of private information and malware installation), and cause losses of billions of dollars every year. It is imperative to detect and act on such threats in a timely manner. Traditionally, this detection is done mostly through the usage of blacklists. However, blacklists cannot be exhaustive, and lack the abilityto detect newly generated malicious URLs. To improve the generality of malicious URL detectors, machine learning techniques have been explored with increasing attention in recent years. This article aims to provide a comprehensive survey and a structural understanding of Malicious URL Detection techniques using machine learning. We present the formal formulation of Malicious URL Detection as a machine learning task, and categorize and review the contributions of literature studies that addresses different dimensions of this problem (feature representation, algorithm design, etc.).

II LITERATURE SURVEY

Many scholars have done some sort of analysis on the statistics of phishing URLs. Our technique incorporates key concepts from past research. We review past work in the detectionof phishing sites using URL features, which inspired our current approach. Happy describe phishing as "one of the most dangerous ways for hackers to obtain users' accounts such as usernames, account numbers and passwords, without their awareness." A literature review of "Phishing URL Detection by Using Machine Learning and Leveraging Phish Guard" would involve summarizing and synthesizing existing research and publications related to the detection of phishing URLs, particularly focusing on the utilization of machine learning techniques and the integration of Phish Guard, a widely-known anti-phishing tool. Provide an overview of the importance of phishing URL detection in cybersecurity.

Introduce the specific focus of the literature review: the use of machine learning and Phish Guard for phishing URL detection. Machine Learning Techniques for Phishing URL Detection

Summarize existing research on the application of machine learning algorithms for phishing URL detection. Discuss the types of features used in machine learning models, such as URL structure, lexical features, host-based features, etc. Highlight different machine learning algorithms utilized, including decision trees, random forests, support vector machines, neural networks, etc. Evaluate the performance of various machine learning approaches in terms of accuracy, precision, recall, and other relevant metrics.

ISSN: 2454-9665

III. TYPES OF PHISHING

Phishing comes in various forms, each designed to trick individuals into revealing sensitive information or taking harmful actions. Here are some common types:

1. **Email Phishing:** This is the most common type, where attackers send fraudulent emails masquerading as legitimate entities like banks, government agencies, or businesses. These emails typically contain links to fake websites or attachments that install malware.
2. **Spear Phishing:** Similar to email phishing but more targeted. Attackers research their victims to personalize their messages, making them appear more authentic and increasing the likelihood of success.
3. **Vishing (Voice Phishing):** In this type, attackers use phone calls instead of emails. They often impersonate legitimate organizations or authorities, tricking victims into revealing personal or financial information over the phone.
4. **Smishing (SMS Phishing):** Attackers send text messages containing malicious links or prompts to download malware onto victims' devices. These messages often appear to be from trusted sources, like banks or delivery services.
5. **Whaling:** This target high-profile individuals or executives within organizations. Attackers tailor their phishing attempts to these individuals, aiming to gain access to sensitive corporate information or funds.
6. **Clone Phishing:** Attackers create a replica of a legitimate email that has already been sent, altering the content slightly to include malicious links or attachments. They then resend the modified email to the same or similar recipients, tricking them into thinking it's a legitimate follow- up.
7. **Pharming:** Instead of relying on email or messages, pharming involves redirecting victims to fake websites, even if they type the correct URL into their browsers. This is often achieved through DNS spoofing or malware.
8. **Search Engine Phishing**: Attackers create fake websites optimized to appear in search engine results for popular queries. When users visit these sites, they may unknowingly enter sensitive information, thinking they're on a legitimate page.
9. **Session Hijacking:** Also known as man- in-the-middle attacks, this involves intercepting communication between users and legitimate websites to steal their credentials or other sensitive information.

ISSN: 2454-9665

10. **Social Media Phishing:** Attackers use social media platforms to gather information about their targets or to spread phishing links and malware through messages, posts, or fake profiles.

IV. EXISTING SYSTEM

Anti-phishing strategies involve educating netizens and technical defense. In this paper, we mainly review the technical defense methodologies proposed in recent years. Identifying the phishing website is an efficient method in the whole process of deceiving user information Along with the development of machine learning techniques, various machine learning based methodologies have emerged for recognizing phishing websites to increase the performance of predictions. The primary purpose of this paper is to survey effective methods to prevent phishing attacks in a real-time environment.

V. PROPOSED SYSTEM

The most frequent type of phishing assault, in which a cybercriminal impersonates a well-known institution, domain, or organization to acquire sensitive personal information from the victim, such as login credentials, passwords, bank account information, credit card information, and so on. Emails containing malicious URLs in this sort of phishing email contain a lot of personalization information about the potential victim. To spear phish a "whale," here a top-level executive such as CEO, this sort of phishing targets corporate leaders such as CEOs and top- level management employees To infect the target, the fraudster or cyber-criminal employs a URL link.

Phishing is one of the most common and most dangerous attacks among cybercrimes. The aim of these attacks is to steal the information used by individuals and organizations to conduct transactions. Phishing websites contain various hints among their contents and web browser based information. The purpose of this study is to perform Extreme Learning Machine (ELM) based classification for 30 features including Phishing Websites Data in Machine Learning Repository database.

VI. SYSTEM ARCHITECTURE

The architecture of the system the URLs to be classified as legitimate or phishing is fed as input to the appropriate classifier. Then classifier that is being trained to classify URLs as

ISSN: 2454-9665

phishing or legitimate from the training dataset uses the pattern it recognized to classify the newly fed input.

The features such as IP address, URL length, domain, having favicon, etc. are extracted from the URL and a list of its values is generated. The list is fed to the classifiers such as KNN, kernel SVM, Decision tree and Random Forest classifier. These models' performance is then evaluated and an accuracy score is generated. The trained classifier using the generated list predicts if the URL is legitimate or phishing. The list contains values 1, 0 and -1 if the features exist, not applicable and if the features doesn't exist respectively. We are considering 30 features in the project.

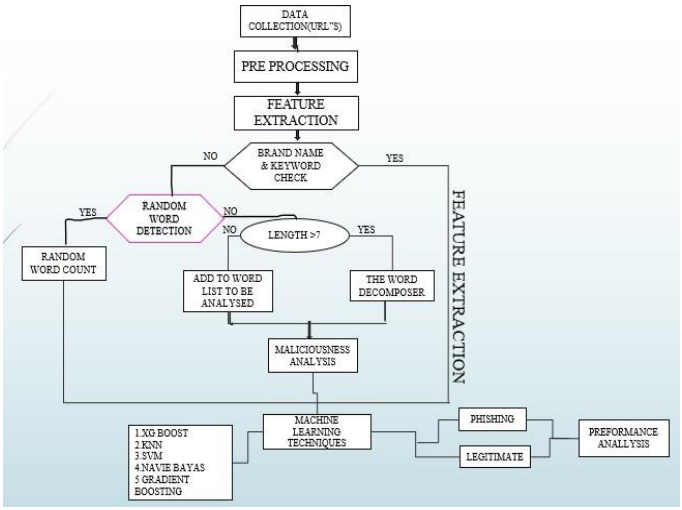


Figure: Block Diagram

VII. METHODOLOGY

A phishing website is a social engineering technique that imitates legitimate webpages and uniform resource locators (URLs). The Uniform Resource Locator (URL) is the most commonway for phishing assaults to occur. Phisher has complete control over the URL's sub-domains.The phisher can alter the URL because it contains file components and directories. This researchused the linear-sequential model, often known as the waterfall model. Although the waterfall approach is considered conventional, it works best in instances where there are few requirements. The application was divided into smaller components that were built using frameworks and hand-written code.

FUNCTIONAL REQUIREMENTS

Data Collection and Preprocessing: Gather a large dataset of both phishing and legitimate

ISSN: 2454-9665

URLs from various sources. Preprocess URLs to extract meaningful features that distinguish phishing from legitimate ones.

Feature Selection: Identifying the most impactful features for accurate detection. Streamline the model by removing less important ones.

Model Training: Training the chosen algorithm on the preprocessed dataset to learn patternsand relationships between features and phishing URLs. **Model Evaluation and Testing:** Evaluating the model's accuracy, precision, recall, F1-score, and other relevant metrics. Testing the model on a separate dataset to assess its ability to generalize to unseen data.

Real Time Detection: Enable the real-time analysis of new URLs for timely identification of phishing threats.

K-NEAREST NEIGHBOUR ALGORITHM:

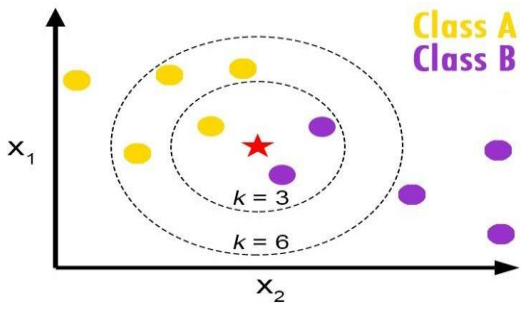


Figure: K-Nearest Neighbour classification

The k-nearest neighbours classifier is a basic, simple to-actualize administered ML algorithm that can be utilized to take care of both classification and regression issues. The KNN algorithm presumes that comparative things are real in closeness. As such, comparable things are close to one another. The KNN algorithm relies on the assumption that being authentic enough for the algorithm to be beneficial. KNN catches the possibility of similarity with computing the separation between focuses on a graph.

KERNEL SUPPORT VECTOR MACHINE:

The fundamental thought is that when a data set is indistinguishable in the present dimensions, include another dimension, perhaps that way the information will be distinct and This is called the kernel trick. Mapping to higher dimension is not blindly including an additional dimension. An example of mapping from 1D to 2D.

International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 06, 2024
www.ijirse.com
ISSN: 2454-9665

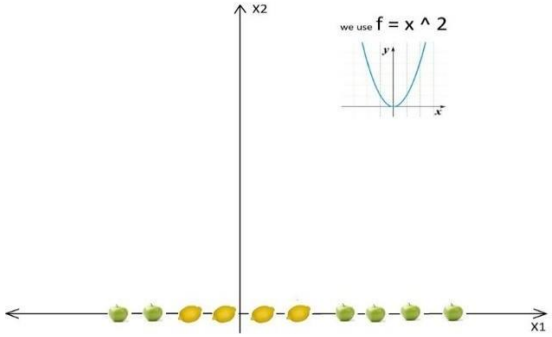


Figure: Initial graph

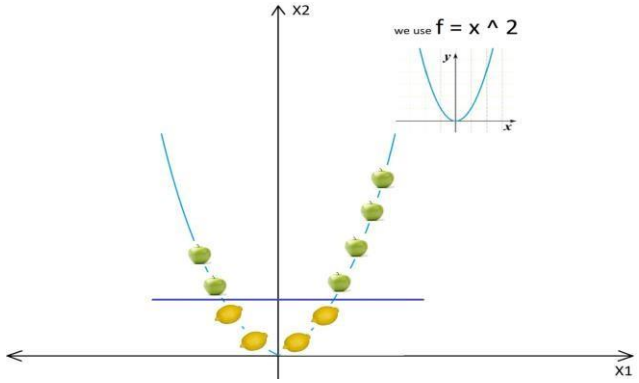


Figure: After using the kernel and after the Transformations

DATA FLOW DIAGRAMS:

DFDs are used to depict graphically the data flow in a system. It explains the processes involved in a system from the input to the report generation. It shows all possible paths from one entity to another of aa system. The detail of a data flow diagram can be represented in three different levels that are numbered 0, 1 and 2.

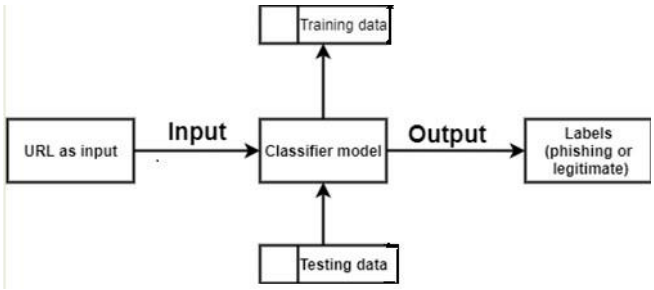


Figure : DFD – Level 0

International Journal of Innovative Research in Science and Engineering
Volume 10, Issue 06, 2024
www.ijirse.com
ISSN: 2454-9665

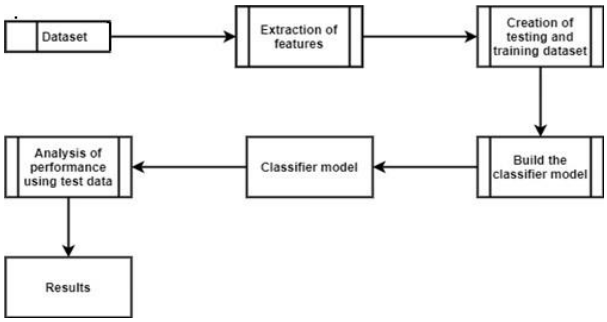


Figure: DFD - Level 1

VIII. RESULTS

EXPERIMENTAL ANALYSIS:

Confusion matrix (CM) is a graphical summary of the correct predictions and incorrect predictions that is made by a classifier that can be used to determine the performance.

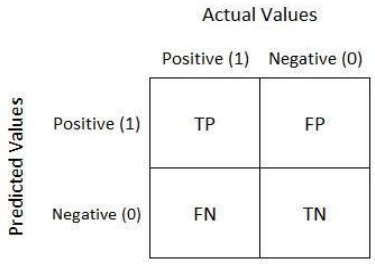


Figure : Confusion matrix

KNN:

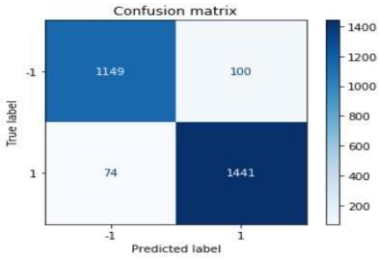


Figure : KNN - Confusion matrix KERNEL SVM:

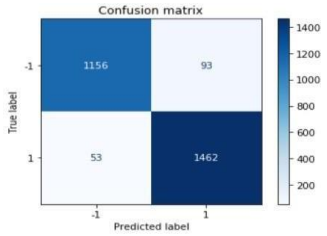


Figure : Kernel SVM - confusion matrix

ISSN: 2454-9665

DECISION TREE:

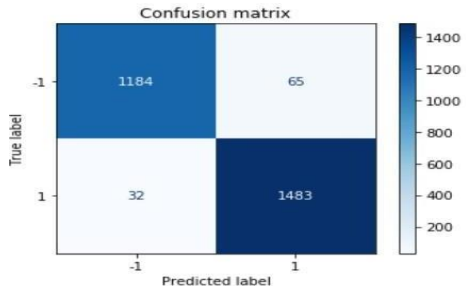


Figure : Decision Tree - confusion matrix F1 SCORE:

F1 score is calculated as the harmonic mean of precision and recall. The higher the F1 score, the better the model. Figure shows the formula for evaluating the F1 score.

$$F1 = \frac{2}{\frac{1}{precision} + \frac{1}{recall}} = \frac{2 * (precision * recall)}{precision + recall}$$

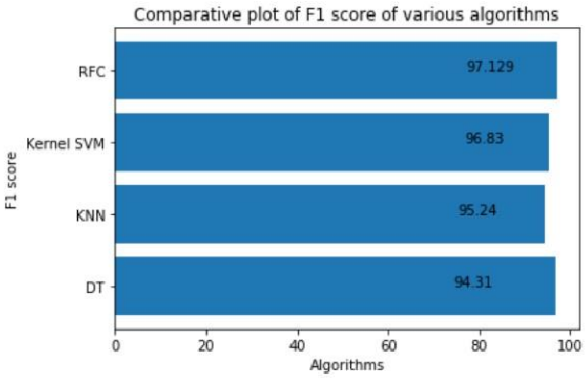


Figure: Comparative plot of F1 scores ACCURACY SCORE

The accuracy is the fraction of sample corrected correctly. The formula used for accuracy of the four algorithms namely; KNN, Kernel SVM, Decision tree and random forest classifier.

$$\text{Accuracy} = \text{Fraction predicted correctly} \quad \frac{TP + TN}{TP + TN + FP + FN}$$

ISSN: 2454-9665

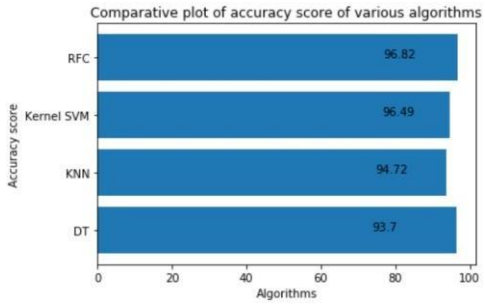


Figure: Comparative plot of accuracy scores

IX CONCLUSION

The survey presented various algorithms and approaches to detect phishing websites by several researchers in Machine Learning. On reviewing the papers, we came to a conclusion that most of the work done by using familiar machine learning algorithms like Naïve Bayesian, SVM, Decision Tree and Random Forest. Some authors proposed a new system like Phish Score and Phish Checker for detection. The combinations of features with regards to accuracy, precision, recall etc. were used. Experimentally successful techniques in detecting phishing website URLs were summarized. As phishing websites increases day by day, some features may be included or replaced with new ones to detect them.

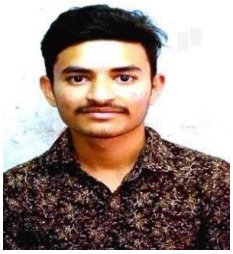
REFERENCES

1. 'APWG | Unifying The Global Response To Cybercrime' (n.d.) available: https://apwg.org/
2. 14 Types of Phishing Attacks That IT Administrators Should Watch For [online] 3.Lakshmanarao, A., Rao, P.S.P., Krishna, M.M.B. (2021) 'Phishing website detection using novel machine learning fusion approach', in 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Presented at the 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 1164–1169
4. H. Chapla, R. Kotak and M. Joiser, "A Machine Learning Approach for URL Based Web Phishing Using Fuzzy Logic as Classifier", 2019 International Conference on Communication and Electronics Systems (ICCES), pp. 383- 388, 2019, July
5. Microsoft, Microsoft Consumer safety report. https://news.microsoft.com/ensg/2014/02/11/microso ft- consumer safety-index-reveals- impact-of-poor- online-safety-behaviour

Singapore/sm.001xdu50tlxsej410r11kqvks u4nz.

ISSN: 2454-9665

XI. AUTHORS PROFILES

	Ms. Shaik. Rizwana is currently working as Assistant professor in Depa rtment of ECE, Tirumala Engineering College, Jonnalagadda, Narasaraopet, Palnadu (dt). She pursued her M. Tech in Narasaraopet Engineering College Narasaraopet. Her area of interest is Digital Systems & Computer electronics.
	Ms. M. Jeevana Sindhu is a studentcurrently pursuing B. Tech inthe stream of ECE in TirumalaEngineering College (TEC), Jonnalagadda, Narasaraopet, Palnadu (dt).
	Ms. K. Mounika Reddy is a studentcurrently pursuing B. Tech inthe stream of ECE in TirumalaEngineering College (TEC), Jonnalagadda, Narasaraopet, Palnadu (dt).
	Ms. K. Pra sa nthi is a studentcurrently pursuing B. Tech inthe stream of ECE in TirumalaEngineering College (TEC), Jonnalagadda, Narasaraopet, Palnadu (dt).
	Mr. Shaik Lal basha is a studentcurrently pursuing B. Tech in the stream of ECE in Tirumala Engineering College (TEC), Jonnalagadda, Narasaraopet, Palnadu (dt).