**PhishSecure: A Phishing Website Detection**

**using Machine learning**

**1.Abstract**

Cybersecurity is about protecting of computer systems, networks and information from harm, theft and unauthorized use from cyber threats such as phishing, malware, and hacking. This involves tools like firewalls, antivirus software, and detection systems to prevent unauthorized access and protect sensitive information. Among these threats, phishing is a common internet scam where attackers send fake messages pretending to be from trusted sources. These messages frequently contain URLs that when clicked, can steal personal information or infect systems with malware. Existing systems primarily focus on features, such as HTTPS presence and URL preprocessing, to identify phishing attacks. However, the proposed system emphasizes the lexical features of URLs in conjunction with machine-learning algorithms. In this approach, URLs received by users are analyzed using machine learning models to classify them as phishing or legitimate. Various algorithms, such as Support Vector Machines (SVM), Neural Networks, Random Forest, Decision Tree, and XG Boost, can be applied for this purpose. Among these, the gradient boosting classifier was selected for its robustness and accuracy. By extracting and comparing the key characteristics of legitimate and phishing URLs, the proposed system effectively identifies phishing websites in real-time. The results show that this method is accurate and effectively distinguishes safe websites from phishing ones, providing a reliable solution against phishing attacks.

**2.Introduction**

In today’s world internet is essential for our daily life, helping in banking, entertainment, online payments and education. These technologies help the people do tasks easily and quickly. Mobile and wireless networks have made this even better by providing internet access anytime and anywhere. However, many people are using digital platforms they face various security threats such as spam, phishing and fraud. Among this phishing is a cybercrime and very popular these days. Phishing is an internet scam sending fraudulent links that appear to come from the reputable sources. According to [1] IBM's 2019 "Cost of a Data Breach" report, the average cost of a data breach has risen 12% over the past 5 years and now costs $3.92 million on average. Additionally, [2] Cybersecurity Ventures predicts that global cybercrime costs will grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025. Among these attacks, phishing is one of the most widespread and critical, causing both financial losses and intangible damages.

The infection starts when a user unknowingly clicks on a phishing link or downloads a harmful attachment. This can result in malware being installed, stealing of login details, or direct theft of money. The Domain Name System (DNS) is crucial in phishing attacks because attackers use fake domains that look like real ones to trick users. DNS spoofing and cache poisoning are often used to send users to fake phishing websites. Attackers often change the structure of URLs to make them look real. They might replace characters (like "g00gle.com" instead of "google.com"), use subdomains to mimic trusted sites, or use HTTPS to seem secure. They also use certain top-level domains (TLDs) like .xyz or .info because they are cheaper and have fewer rules.

Traditional methods for detecting phishing are not enough to handle the changing threats. The blacklist method, which updates lists of bad URLs and IP addresses, doesn't work well against new phishing attacks. Attackers can easily avoid these lists by hiding URLs, changing them quickly, or creating new ones automatically. Heuristic-based detection methods, which look for common signs of phishing attacks, also have problems. These signs are not always there and can lead to many false alarms. These limitations show the need for better and more flexible phishing detection methods. This has led to exploring new approaches like machine learning-based solution.

As of 2022, the average cost of a data breach is $4.35 million (IBM) [5]. Phishing attacks account for 90% of all data breaches [3] (Verizon). Business Email Compromise (BEC) [4] scams resulted in losses of over $43 billion between 2016 and 2022 (FBI). Machine learning is used to detect phishing attacks because it can find patterns and unusual behavior in data, making detection more accurate. Traditional methods with fixed rules don't work well against new phishing tricks, but machine learning can adapt to new threats. Its ability to learn over time makes it a great solution.

This research proposes a novel approach to phishing detection by leveraging the lexical features of URLs in conjunction with machine learning algorithms. By analyzing the URL's linguistic characteristics, this approach aims to improve the accuracy and effectiveness of phishing detection. Through a comprehensive evaluation of prominent machine learning algorithms, including SVM, Neural Networks, Random Forest, Decision Tree, and XG Boost, this study seeks to identify the optimal solution for detecting phishing attacks and enhancing online security.

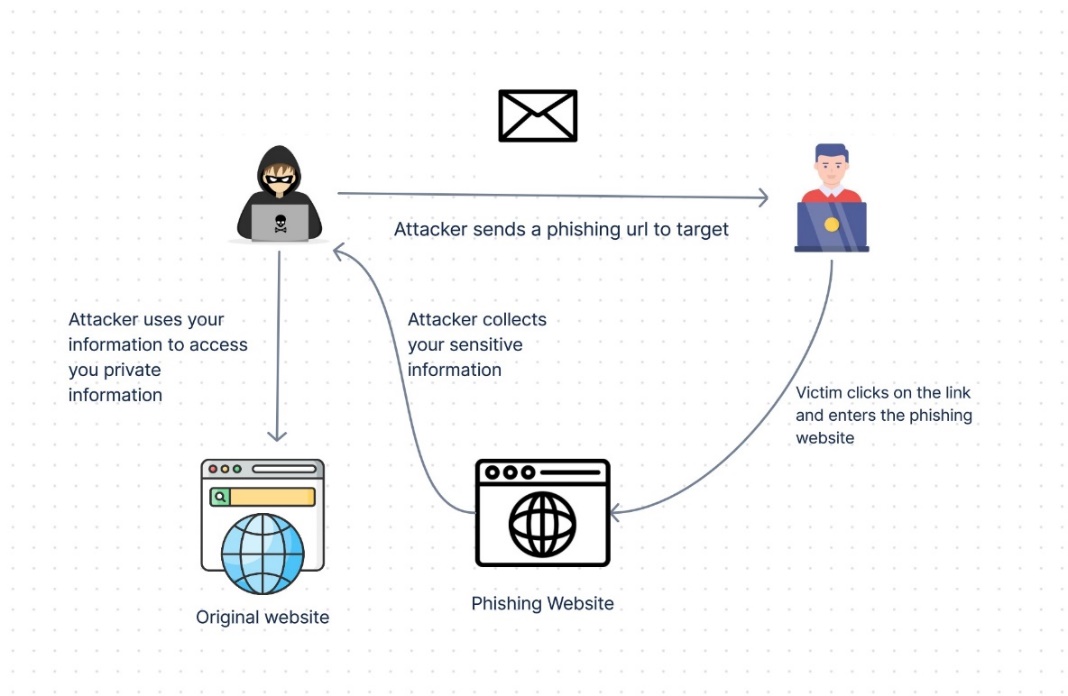


Fig 2.1 Life cycle of a phishing attack

**3.Literature Review**

In this section, existing system approach for phishing detection and their gaps and limitations are summarized.

1. *Traditional List-Based Phishing Detection*

List-based phishing detection uses blacklists of known phishing websites and whitelists of trusted websites. Whitelists have verified, legitimate websites and only allow access if the URL is on the list. Blacklists record known phishing websites and block access to those URLs. In [10] Researchers have found whitelists effective, as shown in studies where access is limited to websites on the whitelist. In [11] Blacklist-based systems are commonly used in tools like Google Safe Browsing API and PhishNet, as well as in research. However, they have major challenges. Small changes in a phishing URL can avoid detection, and new threats, called zero-day attacks, go unnoticed because the lists are updated reactively. These issues show the need for additional methods, like machine learning or heuristic analysis, to improve the effectiveness of list-based detection.

1. *Rule-Based detection*

Rules-based phishing detection systems identify harmful websites by using predefined rules to analyze features like URL structure, domain details, and webpage behavior[12] . They also flag behaviors such as hidden content in iframes, multiple redirects, or disabled right-clicks. While these systems are efficient and straightforward, they need constant updates to keep up with new threats. They can also produce false positives and struggle with advanced phishing tactics. Therefore, they work best when combined with dynamic methods like machine learning.

*c. Machine learning based detection*

Machine learning-based phishing detection systems use algorithms to analyze and classify websites based on patterns and features from data. These systems learn from past data, looking at key details like URL structure, domain age, HTTP usage, and webpage content. Algorithms such as Random Forest, Support Vector Machines (SVM), and Neural Networks are often used for these tasks. Machine learning is good at finding complex and subtle patterns that traditional methods might miss, making it effective at detecting new phishing attacks.

In [6] proposed a machine learning-based system for phishing detection using eight algorithms tested on three datasets, focusing on URL features. While the system achieved high accuracy, it had some gaps. It lacked diverse features, real-time performance testing, and a web application for users. It also didn't include adaptive learning or a detailed comparison of algorithm performance. These gaps show the need for systems that are accurate, user-friendly, adaptable, and capable of real-time detection.

The paper [7] proposes an efficient phishing detection method using machine learning, specifically with Support Vector Machine (SVM) classifiers. This method achieves 95.66% accuracy in identifying phishing websites using only 22.5% of new features. The authors compare their approach with standard phishing datasets and show promising results. However, the paper does not discuss optimizing feature selection or dealing with high computational costs and false positives in detail.

The research paper [8] suggests a Google Chrome extension to detect phishing websites using blacklisting and semantic analysis. It uses a database of known phishing sites and checks on-site data like text, links, and images to find patterns. The method was tested and compared with other methods, showing it works well. However, it depends on pre-collected databases, which might miss new phishing tricks. The approach combines blacklisting with semantic analysis and redirection detection to better prevent phishing.

In [9] The paper suggests a system to detect phishing URLs using machine learning, aiming to warn users about phishing attacks in real-time. It highlights the challenge of quickly changing phishing tactics. The main gap is the lack of an automated process for detecting phishing attacks. The method involves analyzing URLs for patterns and features that indicate phishing, allowing for the detection of multiple phishing attempts at once.

In the system outlined in [13], the researchers enhanced the number of NLP vectors and evaluated the performance of three machine learning algorithms to assess their accuracy. The algorithms tested were Random Forest, SMO (Sequential Minimal Optimization), and Naïve Bayes. Among these, the Random Forest algorithm outperformed the others, achieving the highest accuracy of 97.2% when used in a hybrid approach.