International Journal of Computer Sciences and Engineering
Vol.**12**, Issue.**2**, pp.**37-45**, February **2024**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Survey Article

Assessment of Phishing Websites Prediction using Machine Learning Approaches

Ankit Prajapati[1*], Chetan Agarwal[2], Pawan Meena[3]

[1,2,3]Dept. of CSE, Radharaman Institute of Technology & Science, Bhopal, India

**Corresponding Author: theankitprajapati@gmail.com*

Received: 27/Dec/2023; **Accepted**: 29/Jan/2024; **Published**: 29/Feb/2024. **DOI**: https://doi.org/10.26438/ijcse/v12i2.3745

Abstract: Phishing is a kind of cyberattack in which victims are tricked into divulging private information, including credit card numbers or passwords, by means of phoney emails or websites. Users may find it challenging to distinguish phishing websites from authentic websites due to their convincing appearance. This can lead to users entering their personal information on the phishing website, which can then be stolen by the attacker. An artificial intelligence technique called machine learning is used to train algorithms to find patterns in data. This can be used to create systems that automatically detect and alert users to potentially harmful websites, such as phishing website detection systems. The field of phishing website prediction currently faces some obstacles that require attention. The constant growth of phishing methods is one challenge. Artificial intelligence-based deep learning and machine learning techniques can identify phishing websites. Using machine learning techniques to predict phishing websites, we identify, monitor, and shield end users from monitoring based on phishing algorithms with respect to different publications. We present a machine learning method for phishing website identification in this research. Our method makes use of a number of characteristics, such as the URL structure, website content, and the existence of particular keywords or patterns, to discern between authentic and phishing websites. We test our method on a dataset of actual phishing websites, such as Google's PhishCorp, Kaggle, and PhishTank, and we obtain a greater accuracy than the earlier studies on the detection of phishing websites. Our results show that machine learning can be an effective method for spotting phishing websites. With a better prototype and increased accuracy, our method is simple to use and can shield users from phishing assaults.

Keywords: Phishing Websites, Machine Learning, A I, Accuracy, Precision, Error rate.

1. Introduction

Phishing is the technique of posing as a trustworthy organisation and sending mass emails designed to evade spam filters in an effort to get sensitive data, such as credit card numbers, login credentials, and passwords. Scammers often utilise emails purporting to be from banks, auction websites, IT administrators, or well-known social media platforms to deceive gullible people. It's a form of illicit dishonest social engineering.[1]

Digital operations gained importance as the world responded to the COVID-19 pandemic in 2020, and people began to rely on novel efforts likes cloud computing and mobile infrastructure. As a result, there are now more hacks like phishing. Machine learning can identify phishing websites by categorizing websites as real or fraudulent.

There are many different forms of cybercrime today. This is one of them. In this type of assail, an assailant pretends to be a representative of a reputable institution or organization via email, text message, advertisements, or any other method in order to obtain sensitive information. As a result, they lose personal and sensitive information like account numbers, social security numbers, credit card numbers, etc. Attacks including phishing have risen dramatically. Most innocent users lose their sensitive, unique, personal, important, and safe data and information as a result of this attack.

Many hackers are successful through phishing attacks, in which victims are duped into interacting with internet pages that falsely appear to be legitimate websites the Internet of Things (IoT), large data, and massive network connections globalization of technology, and the use of social media platforms and apps have created significant issues for both institutional and personal security. The traditional security system frequently falls short of offering cyber security[2] to organizations and people. With its high adaptability and intelligence, artificial intelligence (AI) can manage the unstable cyber security environment. Access control, user authentication, behavior analysis, spam, malware, and botnet detection all benefit from the usage of AI.[3]

Computer programmes called scraping bots or scrapers automatically retrieve data from the Internet. To gain

advantage, some e-commerce stores illegally copy and paste product prices into their websites. Numerous web traffic studies re veal that almost half of all website passage is generated by automated programmers. However, despite a huge increase in E-commerce development, there are still numerous security concerns with regard to websites that conduct business online. Regarding rival websites, pricing scraping is one of the most destructive attacks on e-commerce companies.

Information on users' internet browsing habits has been gathered and correlated through the use of third-party tracking. A new method known as CNAME masking was introduced by tracking overhaul providers in reaction to the growing prevalence of third-party tracking ramparts and ad-blocking. This subdomain trickes Web browsers into believing that a request for it is coming from the website being viewed, even though it utilises a CNAME to link to a tracking-related third-party province. Consequently, this approach circumvents the privacy limitations on third-party targeting.[4]

Recently, a lot of individuals have become interested in the arena of AI in web development. AI is still developing and growing, and it's becoming more and more significant in the web-app development diligence. The underlying machineries continue to be more important when it comes to creating cutting-edge and complex online apps. With the internet becoming more and further integrated into our daily lives, businesses in specific are benefiting from AI.

The format of the paper is as follows. The several forms of phishing assaults are acknowledged in Section II. Section III, here and overview of how machine learning is applied in phishing detection. In section IV, provides comprehensive overview of previous studies which are interrelated to our work in phishing detection system. In section V, when I come across multiple papers we found the phishing websites aim to deceive users by masquerading as legitimate entities and tricking them into divulging sensitive information. Here I discussed about the various problem statements. At the end of the paper VII, we conclude the paper.

2. Phishing Attacks & Types

Phishing attacks are malicious attacks that are designed to trick users into revealing susceptible information such as passwords, credit card details, or personal information. Figure 1. Here we demonstrate how the attacker or hackers steal the information from victim. These websites typically mimic justifiable websites, such as banking or social media platforms; in order to deceive users into thinking they are providing their information to a trustworthy source. Phishing attacks are a prevalent type of cybercrime that may result in financial loss, identity theft, or unapproved access to personal accounts.[5]

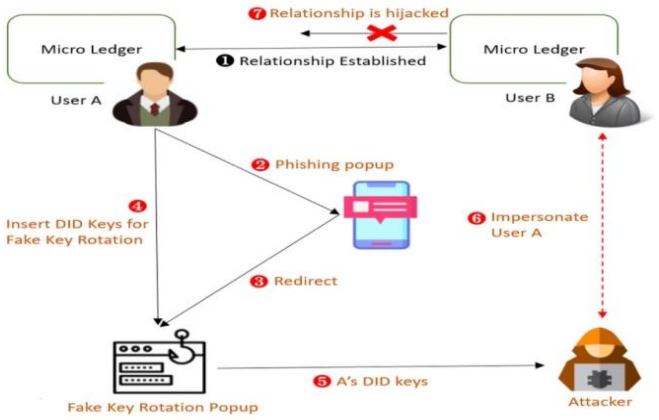

Fig1. Execution of Phishing attacks

Phishing attacks are a kind of cyberattack where the attacker uses deception to get people to divulge sensitive information, like credit card numbers, passwords, or personal information. Figure 2. We divided up a few common phishing attack types into smaller categories.

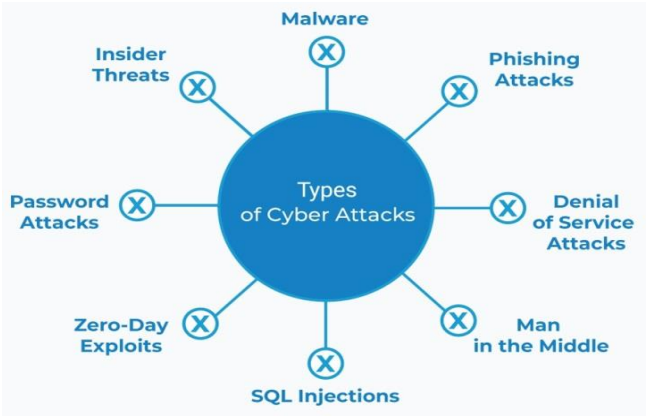

Fig2. Types of Phishing Attacks

Here are some common types of phishing attacks:

A. Deceptive Phishing: This type involves the careless distribution of a single phishing email to hundreds or even thousands of recipients. A tiny number of users clicking on the malicious link and disclosing their personal information on the bogus website is what the hacker is hoping for.

B. **Spear Phishing:** This kind of attack is more individualised and focused. After gathering information about their targets through research, attackers create emails that seem to be from people the target knows or trusts, like a business partner, friend, or coworker. The intention is to trick the receiver into divulging private information or carrying out particular behaviours.

C. **Whaling:** High-profile people with access to important information or decision-making power, including CEOs or senior executives, are the targets of whaling assaults. Perpetrators frequently adapt their strategies to match the target and employ social engineering methods to trick victims into disclosing private information or carrying out acts that further the attackers' interests.

D. **Pharming:** Phishing attacks include the manipulation of DNS (Domain Name System) settings or router

compromises to secretly steer users to phoney websites. The victim is tricked into thinking they are accessing reputable websites, and they can unintentionally divulge important information.

E. **Email Phishing:** Attackers send phoney emails that seem to be from reputable companies, such banks, social networking sites, or internet service providers. These emails try to deceive recipients into disclosing personal information by including links to harmful attachments or phoney websites.
F. **Smishing:** Smishing attacks involve the use of text messages, or SMS, rather than emails, to trick victims. They pose as reputable companies, like banks, in text messages they send, requesting victims to click on harmful links or divulge personal information.
G. **Vishing:** Phone calls are used in phishing attempts as opposed to emails. Attackers utilise social engineering tactics to deceive victims into divulging their personal information over the phone by posing as reputable companies, such as banks or government agencies.
H. **Man-in-the-Middle (MitM) Attacks:** In MitM attacks include the placement of the attacker between the target and the intended communication channel, with the intention of intercepting and perhaps changing the information that is transferred. This makes it possible for attackers to get private information without the victim's awareness.

To detect and identify phishing websites using Python, you can leverage various techniques. Here's a high-level approach to get you started:

Extract URL features: Begin by extracting relevant features from the URL of a website. Phishing websites often contain suspicious elements. You can use Python libraries like urllib or tldextract to extract domain names, subdomains, and other URL components.

Analyze SSL certificates: Phishing websites often use fake or expired SSL certificates. You can utilize the requests library in Python to retrieve SSL certificate information from a website and examine its validity, expiration date, and issuer. Suspicious or mismatched certificates may indicate a phishing attempt.

Check for redirects: Phishing websites often use URL redirects to hide the actual destination from users. Python's requests library can help you follow these redirects and inspect the final URL. If the final URL doesn't match the expected domain or if it redirects to an unexpected location, it could be a red flag.

Analyze page content: Use Python libraries like BeautifulSoup or html.parser to parse the HTML content of the website. Look for specific elements that are commonly found in phishing websites, such as forms that request sensitive information or hidden iframes that load content from other domains.

Compare with blacklists: There are public databases and blacklists that maintain records of known phishing websites. You can use Python to query these databases and compare the extracted features or domain names against the blacklisted entries. Some popular databases include Google Safe Browsing API or PhishTank.

Machine learning-based approaches: Another advanced technique involves training machine learning models to classify websites as legitimate or phishing based on historical data. This approach requires a labeled dataset of phishing and legitimate websites. Python libraries like scikit-learn or TensorFlow can be used for training and deploying machine learning models.

In the following subsections, we describe the various types of phishing attacks and also discussed about the various techniques such as extract URL features, analyze SSL certificates, checked for redirects, compare with blacklists, machine learning-based approaches. It's important to stay updated with the latest phishing techniques and continuously improve detection algorithms to combat evolving threats.

3. Machine Learning in Phishing Detection

Machine learning prediction is the process of using trained models to make predictions or estimates about future or unseen data based on patterns and relationships learned from historical data. Figure 3. In this figure, shows the standard flow diagram of detection algorithms. It is a fundamental aspect of machine learning and has applications in multiple domains, having financed, healthcare, marketing, and more. Machine learning techniques are commonly used in phishing detection to analyse and predict whether a given email, website, or communication is likely to be a phishing attempt.[6]

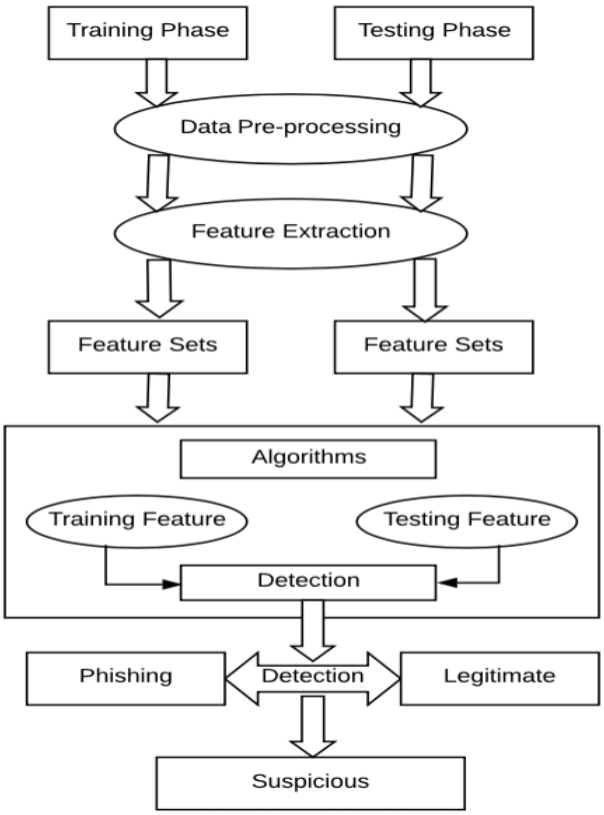

Fig3. Flowchart of The Machine Learning System in Phishing Detection

Here's an overview of how machine learning is applied in phishing detection:

Feature Extraction: Machine learning models rely on relevant features extracted from phishing-related data to make predictions. For example, features can include email header information (sender, subject line, etc.), URL characteristics, webpage content, and user behaviour patterns.

Training Data Collection: A labeled dataset is needed to train the machine learning model. This dataset consists of examples of both legitimate and phishing instances, where each instance is associated with a class label (legitimate or phishing).

Feature Selection and Preprocessing: Relevant features are selected, and data preprocessing techniques are applied to prepare the dataset for training. This can involve removing irrelevant or redundant features, handling missing data, and normalizing or transforming the data.[7]

Model Training: MitM attacks include the attacker putting himself in the way of the victim and the intended communication channel in order to intercept and maybe modify the conveyed data. Because of this, attackers may obtain confidential data without the victim's knowledge.

Model Evaluation: The performance of the trained model is assessed using independent testing data. Evaluation criteria that are often used include F1 score, recall, accuracy, and precision. The model's performance is fine-tuned if necessary, and different algorithms or configurations may be compared to select the best-performing model.

Concurrent Phishing Detection: The model may be utilised for real-time phishing detection after it has been trained and assessed. When an email or website is encountered, the model analyses the relevant features and predicts whether it is likely to be a phishing attempt or not. The model's prediction can be used to warn or block suspicious emails or websites.[9]

Continuous Improvement: Phishing techniques and patterns evolve over time, so it's crucial to continuously update and improve the machine learning model. Regularly collecting new training data and retraining the model helps it stay up to date with emerging phishing threats.

It's important to note that while machine learning is a powerful tool for phishing detection, it is not foolproof. Attackers constantly adapt their techniques, making it necessary to combine machine learning with other security measures, such as user education, domain reputation checks, and blacklisting known phishing sources, to create a robust defense against phishing attacks.

4. Literature Survey

The information provided is based on the knowledge available up to September 2021, and there may be more recent studies beyond that:

"Phishing Detection: A Machine Learning Approach" by Fatima Salahdine, and Naima Kaabouch (2022): This study proposes a phishing website detection system using machine learning algorithms. Values such as URL length, domain age, SSL certificate information, and page content are used. Classifiers like decision trees, Naive Bayes, k-Nearest Neighbors, and Support Vector Machines (SVM) are employed. The study achieves high accurateness in detecting phishing websites and compares the performance of different classifiers.[10]

"Phishing Websites Classification using Random Forest Algorithm" by Dr. G Ramesh, R.B. Lokitha (2023): This work focuses on using the Random Forest algorithm for phishing website classification. Features like URL-based, HTML-based, and domain-based features are used for training the classifier. The study demonstrates that the Random Forest algorithm achieves good performance in detecting phishing websites.[11]

"Phishing Detection using RDF and Random Forest" by Vamsee Muppavarapu Shriram Vasudevan**(2018):** The authors propose a phishing recognition system based on resource description framework and random forest algorithms. Features such as URL-based features, domain-based features, and content-based features are utilized. The learning shows that the proposed system achieves high exactness in detecting phishing websites.[12]

"Phishing Website Detection using Convolutional Neural Network" by Rundong Yang, Bin Wu and Chunhua Wu (2021): This research explores the use of Convolutional Neural Networks (CNN) for phishing website detection. The HTML content of web pages is converted into image representations, which are then fed into the CNN model. The study demonstrates the effectiveness of using CNNs in detecting phishing websites with high accuracy.[13]

"DeepPhish: A Deep Learning-Based Phishing Detection using CNN, LSTM, and LSTM-CNN " by Zainab Alshigiti, Kasif Saleem et al. (2023): The authors propose DeepPhish, an end-to-end deep neural network for phishing detection. The model combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. The study shows that DeepPhish achieves high accuracy and outperforms traditional machine learning methods.[14]

"PhishGuard: Phishing Website Detection using Machine Learning and Deep Learning" by Selvakumari M, Sneha Das et al. (2021): This work presents PhishGuard, an ensemble wisdom approach for phishing website detection. Multiple machine learning classifiers, including Random Forest, Naive Bayes, and SVM, are combined using voting. The study demonstrates the effectiveness of the ensemble approach in achieving improved detection accuracy. Optimistic techniques such as online learning and deep learning remain unexamined.[15]

"Phishing Detection: A Machine Learning Approach" by Kamalam, G.K. Suresh et al. (2022): This study proposes a machine learning-based phishing detection system and compares the performance of different classifiers. Features such as URL length, domain age, SSL certificate information, and page content are used. Decision trees, Naive Bayes, k-Nearest Neighbors, and Support Vector Machines (SVM) are evaluated as classifiers.[16]

"A Novel Approach for Phishing Websites Detection using Machine Learning Techniques" by Ashit Kumar Dutta (2021): This research proposes a novel approach for phishing website detection using machine learning techniques. Features such as URL-based, HTML-based, and domain-based characteristics are extracted and used as input. The authors experiment with various machine learning algorithms, including Decision Trees, Naive Bayes, and Random Forest. The study achieves high accuracy in predicting phishing websites and compares the performance of different classifiers.[5][17]

"Phishing Website Detection using Machine Learning Techniques: A Systematic Literature Review" by R. Pandey et al. (2020): This literature review provides an overview of machine learning techniques used for phishing website detection. The study explores various features, including URL-based, HTML-based, and domain-based features, commonly used in phishing detection. Different machine learning algorithms, such as Decision Trees, Random Forest, SVM, and Neural Networks, are reviewed.[18]

These are a few selected studies that highlight different machine learning approaches for phishing website prediction:

Table1. Comparative Analysis of Various Phishing Detection Techniques

References	Author	Methodology	Dataset	Results	Performance Measures
[10]	Fatima Salahdine, and Naima Kaabouch	Features Selections, Classification Techniques	Phishing and legitimate websites	Achieved an accuracy of 94.5% using ANN	Accuracy
[11]	G. Ramesh, R.B. Lokitha	Random Forest Algorithm	PhishTank and legitimate websites	Detected 97.14% of accuracy by using RFA	97.14% Accurate
[12]	Vamsee Muppavarapu, Shriram Vasudevan	Resource Description Framework and Random Forest Algorithm	PhishTank Website	Together, these two phases lower the quantity of false positives and raise the accuracy of the system.	Accuracy and Run-time efficiency
[13]	Randong Yang, Bin Wu and Chunhua Wu	Deep Learning (Convolutional Neural Networks) and Random Forest	Alexa and PhishTank Websites	Using a CNN-based classifier, phishing website classification accuracy on the dataset was 99.35%.	Precision, True positive rate,
[14]	Zainab Alshigiti, Kasif Saleem et al.	CNN, LSTM, and LSTM-CNN	UCI, PhishTank and Common Crawl datasets	LSTM obtained 96.8% prediction accuracy, while the LSTM–CNN algorithm earned the best accuracy at 99.2%.	computed the F1 score, recall, accuracy, and precision.
[15]	Selvakumari M, Sneha Das et al.	k-nearest neighbors (KNN), Random Forest, XG Boost and Decision Tree	Kaggle and Legitimate websites	Decision Tree – 96.13%	Some algorithms work quickly and efficiently, utilising several classifiers to make predictions.
[16]	Kamalam, G.K. Suresh et al.	Random Forest, Decision Tree, Linear model and Neural Network algorithms	UCI and FhishTank	Accuracy of RF 95.7%	When it comes to accuracy, error rate, and other factors, random forest performs better.
[5]	Ashit Kumar Dutta	SVN, KNN, RFC	AlexaRank and PhishTank	Achieved an accuracy of 97.4% using a combination of ML algorithms and URL-based features.	Limited to URL-based analysis and may struggle with detecting advanced phishing techniques
[18]	Rishikesh Mahajan, Irfan Siddavatam	Decision Tree Algorithm, Random Forest Algorithm, SVM	AlexaRank and PhishTank	Achieved 97.14% detection accuracy using random forest algorithm with lowest false positive rate.	Lowest false negative rate than decision tree and support vector machine algorithms.

They provide insights into feature selection, algorithm comparison, and the performance of various classifiers. However, it's vital to note that the arena of phishing website prediction is continuously evolving, and new research is being published regularly. It's recommended to explore recent literature and stay updated with the most recent innovations in the field.

Datasets for Phishing Detection

A data set is a group of related data. It is a group or collection of facts that is essentially arranged in a tabular format. You might also call it a set of data, where the row represents the contents of the set and the dataset represents one or more database tables. When it comes to tabular data, a data set is associated with one or more database tables; in these tables, each row corresponds to a particular record and each column to a particular variable.

Datasets can be used for a variety of purposes, such as: Data analysis, Machine learning, Data visualization, Statistical modelling and Research. Many datasets are available for research on phishing detection. The most well-liked datasets include:

Phishing Dataset for Machine Learning on Kaggle: This dataset holds 48 features extracted from 5000 phishing webpages and 5000 legitimate webpages.[19]

Web Page Phishing Detection Dataset on Kaggle: There are 11430 URLs in this dataset, and 87 characteristics have been extracted. The dataset is intended to serve as a standard for phishing detection systems that rely on machine learning.[20][19]

PhishTank Dataset on GitHub: This dataset contains over 1 million phishing URLs that have been collected by PhishTank, a community-based phishing detection service.

Malicious URL Dataset on UCI ML Repository: This dataset contains over 100,000 URLs that have been labeled as malicious or benign.

Google PhishCorp Dataset on Google AI Platform: This dataset contains over 100,000 phishing URLs that have been collected by Google's PhishCorp project.

In addition to these publicly available datasets, there are also a number of private datasets that are owned by organizations that specialize in phishing detection. These private datasets are typically more comprehensive and up-to-date than the public datasets, but they are not available to the general public.

5. Problem Statement

Phishing attacks pose a significant threat to individuals, organizations, and online security. Phishing websites aim to deceive users by masquerading as legitimate entities and tricking them into divulging superficial information such as login credentials, financial details, or subjective data. Detecting and preventing such attacks is crucial to safeguarding users' privacy and preventing financial losses.

Machine learning methods have demonstrated potential in detecting and categorising phishing websites according to their traits and tendencies. To increase the efficacy of machine learning-based phishing website identification, a number of issues must be resolved, though:

Imbalanced datasets: Phishing websites are often outnumbered by legitimate websites in real-world scenarios, resulting in imbalanced datasets for training machine learning models. This imbalance can lead to prejudiced classifiers that favor the majority class (legitimate websites) & struggle to accurately detect phishing websites. Developing techniques to handle imbalanced datasets and mitigate the bias is essential for improving detection performance.

Feature selection and representation: Choosing relevant and discriminative features for phishing website detection is crucial. Traditional features such as URL characteristics, domain attributes, and HTML content are commonly used, but they may not capture all the subtle indicators of phishing. Research is needed to explore more advanced feature selection and representation techniques, including text analysis, visual similarity, behavioral patterns, and network-based features, to improve the accuracy of detection models.

Generalization across evolving phishing techniques: Phishing attackers continuously adapt their strategies and employ new techniques to equivocate detection systems. Machine learning models proficient on existing phishing techniques may struggle to generalize well to unseen or evolving attack patterns. Developing robust and adaptive machine learning algorithms that can detect unknown or zero-day phishing attacks is essential for keeping pace with the ever-evolving threat landscape.

Interpretability and explain ability: When it comes to phishing website identification, machine learning models frequently function as "black boxes," making it difficult to decipher the logic behind their judgements. In critical applications, such as financial institutions or user-facing systems, interpretability and explain ability are crucial for building trust and enabling human oversight. Research is needed to develop interpretable models and methods that can provide explanations for their classification outcomes.

Real-time detection: Phishing attacks can occur in real-time, requiring detection systems to operate promptly and accurately. Machine learning models that require significant computational resources or have high inference time may not be suitable for real-time detection. Developing lightweight, efficient, and real-time machine learning approaches that can analyze website behavior, network traffic, or user interactions is essential for timely phishing detection.

Adversarial attacks and evasion techniques: Phishing attackers can employ adversarial techniques to manipulate features, obfuscate URLs, or mimic legitimate websites, aiming to deceive machine learning-based detection systems. Research is needed to investigate adversarial attacks specific to phishing detection and develop techniques that are resilient to such evasion attempts.

6. Research Gap

Phishing website detection research has made significant progress in recent years, but there are still several gaps that warrant further investigation. These research gaps highlight areas where additional efforts can enhance the effectiveness and robustness of phishing detection techniques. Here are some key research gaps in phishing website detection:

Evolving phishing techniques: Phishing attackers continuously adapt their strategies to bypass existing detection mechanisms. There is a need to study and understand emerging phishing techniques, such as homograph

attacks, image-based phishing, and advanced obfuscation methods.

Real-time detection: Many existing phishing detection approaches rely on static analysis of websites or URL-based features. However, phishing attacks can be dynamic and may involve time-based triggers or content changes. Research should focus on real-time detection techniques that can analyze website behavior, detect malicious activities, and adapt to dynamic phishing attacks.[21]

Multi-modal detection: Phishing attacks often employ multiple channels, including emails, websites, and mobile apps, to deceive users. Current research primarily focuses on website-based phishing detection, neglecting other potential attack vectors. Exploring multi-modal detection approaches that combine information from different sources (e.g., URLs, email headers, app behavior) can improve overall detection accuracy.

Zero-day phishing detection: Existing phishing detection methods often rely on blacklists or known phishing indicators. Zero-day phishing attacks, which exploit vulnerabilities before they are known, pose a significant challenge. Research should aim to develop proactive detection techniques that can identify zero-day phishing attacks based on behavioral analysis, anomaly detection, or machine learning algorithms.

User-centric detection: Users' susceptibility to phishing attacks remains a critical factor in successful exploitation. Incorporating user behavior, cognitive factors, and psychological aspects into detection systems can enhance their effectiveness. Investigating user-centric detection techniques, such as personalized risk assessment, user profiling, and adaptive warning mechanisms, can empower users to make informed decisions and improve overall security.

Adversarial attacks and evasion techniques: Phishing attackers can employ adversarial techniques to evade detection mechanisms. They may manipulate features, obfuscate URLs, or mimic legitimate websites to deceive detection systems. Research should focus on studying adversarial attacks specific to phishing detection and developing robust techniques that can withstand such evasion attempts.

Dataset diversity and scalability: The availability of diverse and large-scale datasets plays a crucial role in training and evaluating phishing detection models. However, there is a scarcity of publicly available datasets that cover a wide range of phishing techniques, target industries, and geographic regions. Researchers should work towards creating standardized and diverse datasets to facilitate fair comparison and benchmarking of detection methods.

Explain ability and interpretability: Phishing detection systems often rely on complex machine learning algorithms, making it challenging to interpret their decision-making processes. It is essential to develop transparent and interpretable models that can provide explanations for their detection outcomes. This can aid in building trust, understanding system limitations, and facilitating human-in-the-loop decision-making.

Generalization across contexts: Phishing attacks can vary across different contexts, such as languages, cultures, and user demographics. Existing detection techniques may not generalize well across diverse contexts due to variations in attack strategies, user behavior, or regional factors. Research should aim to develop context-aware detection models that can adapt to specific environments and mitigate the challenges posed by context-dependent phishing attacks.

7. Future Research Direction

The future research direction of phishing website detection is promising, with several key areas offering opportunities for advancement and innovation. Here are some potential future research directions in the field of phishing website detection:

Deep learning and advanced machine learning techniques: Further exploration and refinement of deep learning models, such as recurrent neural networks (RNNs), transformers, and graph neural networks (GNNs), can improve the accuracy and robustness of phishing detection systems. Investigating the effectiveness of transfer learning, domain adaptation, and ensemble methods can also enhance the generalization capabilities of these models.[8][15]

Behavioral analysis and anomaly detection: Incorporating behavioral analysis techniques, such as user interaction patterns, mouse movements, and click sequences, can provide valuable insights into distinguishing phishing websites from legitimate ones. Anomaly detection algorithms, including unsupervised learning and clustering techniques, can help identify novel and previously unseen phishing attacks.

Explainable AI and trustworthiness: Developing explainable AI techniques for phishing detection systems is essential to gain users' trust and foster transparency. Research should focus on creating interpretable models that can provide human-understandable explanations for their decisions. Additionally, exploring user-centered design principles and integrating user feedback can improve the usability and acceptance of detection systems.

Mobile and IoT phishing detection: Phishing attacks targeting mobile devices and the Internet of Things (IoT) are becoming more common as these platforms become more widely used. Future research should address the unique challenges posed by mobile and IoT phishing, including small screen sizes, limited resources, and diverse communication channels. Designing efficient and effective detection mechanisms specifically tailored to these contexts is crucial.

Multi-modal and multi-source analysis: Integrating information from multiple sources, such as URLs, email headers, website content, social media, and network traffic, can improve the accuracy and reliability of phishing detection systems. Investigating multi-modal fusion techniques, data

fusion approaches, and cross-domain analysis can enable comprehensive and holistic phishing detection across different attack vectors.[22]

Adversarial robustness and evasion techniques: Developing phishing detection systems that can withstand adversarial attacks and evasion techniques is a critical research direction. This includes studying adversarial machine learning methods, generating adversarial examples for evaluation, and designing robust defense mechanisms to mitigate the impact of adversarial attacks on detection performance.

User-centric approaches and awareness enhancement: Integrating user-centric approaches, such as personalized risk assessment, user behavior modeling, and educational interventions, can empower users to better identify and avoid phishing attacks. Research should focus on developing user-friendly interfaces, intuitive warning systems, and effective training programs to enhance users' awareness and resilience against phishing threats.

Real-world deployment and evaluation: Conducting large-scale field studies and evaluating phishing detection systems in real-world settings is crucial to assess their effectiveness and practicality. Collaboration with industry partners, cyber security organizations, and end-users can facilitate the deployment of detection systems in real-world environments and provide valuable insights for system improvement.

Collaborative approaches and data sharing: Collaboration among researchers, industry stakeholders, and law enforcement agencies is vital to combat phishing attacks effectively. Encouraging data sharing initiatives, establishing benchmark datasets, and promoting collaborative research efforts can facilitate the development of more robust and comprehensive phishing detection solutions.

8. Conclusion

Phishing poses a severe risk to security and can have catastrophic effects on both people and businesses. The identification of phishing websites appears to be a potential use of machine learning, since several research have demonstrated the high accuracy levels of these models.

The most recent developments in machine learning methods for identifying phishing websites have been examined in this survey article. We have covered the many machine learning methods that have been applied to phishing detection and spoken about the various feature kinds that may be utilised to train machine learning models. We've also spoken about the difficulties in identifying phishing websites and mentioned some interesting areas for further study.

The survey's findings indicate that machine learning is a viable method for identifying phishing websites. Nevertheless, before machine learning models are used in practical environments, a number of issues still need to be resolved. Developing strong machine learning models that can withstand evasion tactics, obtaining vast and high-quality datasets, and taking usability of machine learning-based phishing detection systems into account are some of these problems.

Notwithstanding these difficulties, we think machine learning has a lot of potential to contribute significantly to the battle against phishing. Phishers will find it harder to succeed if we keep researching and creating new machine learning approaches. This will help shield users from this grave security risk.
All things

References

[1] F. Yahva *et al*., "Detection of Phising Websites using Machine Learning Approaches," *2021 Int. Conf. Data Sci. Its Appl. ICoDSA 2021*, pp.**40–47, 2021,** doi: 10.1109/ICODSA53588.2021.9617482.

[2] S. M. Istiaque, M. T. Tahmid, A. I. Khan, Z. Al Hassan, and S. Waheed, "Artificial Intelligence Based Cybersecurity: Two-Step Suitability Test," *2021 IEEE Int. Conf. Serv. Oper. Logist. Informatics, SOLI 2021*, **2021**, doi: 10.1109/SOLI54607.2021.9672437.

[3] N. Megha, K. R. Remesh Babu, and E. Sherly, "An Intelligent System for Phishing Attack Detection and Prevention," *Proc. 4th Int. Conf. Commun. Electron. Syst. ICCES 2019*, Jul., pp.**1577–1582**, **2019.** doi: 10.1109/ICCES45898.2019.9002204.

[4] H. Dao, J. Mazel, and K. Fukuda, "CNAME Cloaking-Based Tracking on the Web: Characterization, Detection, and Protection," *IEEE Trans. Netw. Serv. Manag.*, Sep, Vol.**18**, No.**3**, pp.**3873–3888**, **2021**, doi: 10.1109/TNSM.2021.3072874.

[5] A. K. Dutta, "Detecting phishing websites using machine learning technique," *PLoS One*, October , Vol.**16**, No.**10**, pp.**1–17, 2021**, doi: 10.1371/journal.pone.0258361.

[6] E. Gandotra and D. Gupta, "An Efficient Approach for Phishing Detection using Machine Learning," pp.**239–253, 2021**, doi: 10.1007/978-981-15-8711-5_12.

[7] A. Joshi and P. T. R. Pattanshetti, "Phishing Attack Detection using Feature Selection Techniques," *SSRN Electron. J.*, Jul. **2019**, doi: 10.2139/SSRN.3418542.

[8] S. Jain and C. Gupta, "A Support Vector Machine Learning Technique for Detection of Phishing Websites," *2023 6th Int. Conf. Inf. Syst. Comput. Networks, ISCON 2023*, **2023**, doi: 10.1109/ISCON57294.2023.10111968.

[9] M. H. Alkawaz, S. J. Steven, A. I. Hajamydeen, and R. Ramli, "A comprehensive survey on identification and analysis of phishing website based on machine learning methods," *ISCAIE 2021 - IEEE 11th Symp. Comput. Appl. Ind. Electron.*, Apr., pp.**82–87, 2021**, doi: 10.1109/ISCAIE51753.2021.9431794.

[10] F. Salahdine, Z. El Mrabet, and N. Kaabouch, "2022 IEEE 13th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2022," *2022 IEEE 13th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2022*, **2022.**

[11] R. B. Lokitha, R. R. Monisha, N. S. Neha, T. Nadu, and T. Nadu, "Phishing Detection System using Random Forest Algorithm," vol. 8, no. 4, pp. 510–514, 2023.

[12] V. Muppavarapu, A. Rajendran, and S. K. Vasudevan, "Phishing detection using RDF and random forests," *Int. Arab J. Inf. Technol.*, Vol.**15**, No.**5**, pp.**817–824, 2018.**

[13] R. Yang, K. Zheng, B. Wu, C. Wu, and X. Wang, "Phishing website detection based on deep convolutional neural network and random forest ensemble learning," *Sensors*, Vol.**21**, No.**24**, pp.**1–18, 2021**, doi: 10.3390/s21248281.

[14] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E. U. Haq, K. Saleem, and M. H. Faheem, "A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN," *Electron.*, Vol.**12**, No.**1**, pp.**1–18, 2023**, doi: 10.3390/electronics12010232.

[15] M. Selvakumari, M. Sowjanya, S. Das, and S. Padmavathi,

"Retraction: Phishing website detection using machine learning and deep learning techniques," *J. Phys. Conf. Ser.*, Vol.**1916**, No.**1**, **2021**, doi: 10.1088/1742-6596/1916/1/012169.
[16] G. K. Kamalam, P. Suresh, R. Nivash, A. Ramya, and G. Raviprasath, "Detection of Phishing Websites Using Machine Learning," *2022 Int. Conf. Comput. Commun. Informatics, ICCCI 2022*, no. June, **2022**, doi: 10.1109/ICCCI54379.2022.9740763.
[17] I. Tyagi, J. Shad, S. Sharma, S. Gaur, and G. Kaur, "A Novel Machine Learning Approach to Detect Phishing Websites," *2018 5th Int. Conf. Signal Process. Integr. Networks, SPIN 2018*, Sep., pp.**425–430**, **2018**, doi: 10.1109/SPIN.2018.8474040.
[18] R. Mahajan and I. Siddavatam, "Phishing Website Detection using Machine Learning Algorithms," *Int. J. Comput. Appl.*, Vol.**181**, No. **23**, pp.**45–47, 2018**, doi: 10.5120/ijca2018918026.
[19] Shashwat Tiwari, "Phishing Dataset for Machine Learning | Kaggle," *Kaggle*, **2021**.
[20] "Kaggle: Your Home for Data Science." https://www.kaggle.com/datasets/isatish/phishing-dataset-uci-ml-csv?select=uci-ml-phishing-dataset.csv (accessed Jul. 27, 2023).
[21] Z. Fan, "Detecting and Classifying Phishing Websites by Machine Learning," Feb., pp.**48–51,** **2022**, doi: 10.1109/ICAML54311.2021.00018.
[22] N. B. M. Noh and M. Nazmi Bin M Basri, "Phishing Website Detection Using Random Forest and Support Vector Machine: A Comparison," *2021 2nd Int. Conf. Artif. Intell. Data Sci. AiDAS 2021*, Sep. **2021**, doi: 10.1109/AIDAS53897.2021.9574282.

AUTHORS PROFILE

Ankit Prajapati is pursuing Master of Technology in CSE and earned his B.Tech, Diploma in CSE from Rajiv Gandhi Proudyogiki Vishwavidyalaya in 2021, 2018 respectively. He achieved Best academic Performance Award in 2018. His research areas of interest are Algorithmic Mathematics, Artificial Intelligence, Machine Learning, Deep Learning, Cyber Security and Machine Level Programming & System Design.

Chetan Agrawal studied for his Master of Engineering in CSE at TRUBA Institute of Engineering & Information Technology Bhopal. He is currently pursuing a PhD in CSE at the University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya (UIT - RGPV), Bhopal. At the BANSAL Institute of Science & Technology Bhopal, he completed his studies for his Bachelor of Engineering in CSE. He is currently employed at the RADHARAMAN Institute of Technology & Science in Bhopal, Madhya Pradesh, India, as an assistant professor in the CSE department. Social network analysis, data analytics, machine learning, deep learning, network security, cloud computing, artificial intelligence, and cyber security are among his research interests**.**

Pawan Meena earned his B. Tech., M. Tech., and Ph.D. in computer science from RGPV Bhopal in 2007, 2012, and 2024, respectively. He has been working as an assistant professor in the Department of Computer Science and Engineering at RITS, Bhopal, since 2009. He has been a member of the IEEE since 2019. He has published more than 10 research papers in reputed international journals, including Thomson Reuters (SCI and Web of Science) and conferences, including IEEE, and they're also available online. His main research work focuses on social media minning, data analytics, query optimisation, and data mining. He has 10 years of teaching experience and 5 years of research experience.

