STM JOURNALS

Journal of
Microelectronics and Solid
State Devices

ISSN: 2455-3336
Volume 12, Issue 3, 2025
September–December
DOI (Journal): 10.37591/JoMSD

https://journals.stmjournals.com/jomsd

Review JoMSD

A Survey on Leveraging Machine Learning for Phishing Attack Prediction and Detection

D. Diana Julie[1,*], K. Dinesh Kanna[2], P. Thirumal[3], M.P. Victor Moses[4]

Abstract

Phishing is one of the biggest cybersecurity threats that exploits user trust by masquerading as a legitimate site or email to steal personal and sensitive information. This survey reviews state-of-the-art phishing detection systems, showcasing the evolution from traditional list-based techniques, including blacklisting and whitelisting, to machine learning and deep learning models. While list-based systems cannot evolve to detect new and zero-day attacks, ML algorithms such as Decision Tree, Random Forest, Support Vector Machine, and Neural Networks have been widely used for URL-based phishing attacks. Hybrid models combining multiple algorithms improve detection in terms of both accuracy and robustness, because detected weaknesses in single models can be mitigated. Recent advances in DL models, such as CNNs and LSTMs, have the ability to automatically learn complex features, which enhances detection capability. Nonetheless, evasion attacks continue to be a highly effective threat against ML classifiers. Defenses that highlight adversarial robust classification and feature learning are also reviewed. This survey focuses special attention on the continuous update and adaptation of phishing detection models for evolving attacker strategies and reliable protection in dynamic environments.

Keywords: Phishing detection, machine learning, hybrid models, URL features, cybersecurity, evasion attacks, random forest, support vector machine (SVM)

INTRODUCTION

Phishing is one of the most common cybercrimes, meaning that attackers can deceive a wide range of users by using malicious websites or emails to steal information. Attacks can be even more devious and frequent because most people and businesses around the world increasingly use digital platforms, thereby rendering the old idea of using list-based detection methods obsolete. Indeed, blacklists and whitelists have formed the first approach. Although fairly effective against a familiar threat, these conventional approaches prove deficient in detecting new or zero-day phishing attacks because they operate based upon predefined rules and static databases.

To overcome these drawbacks, ML and DL techniques have proven highly potent within the phishing detection arena, utilizing a variety of features extracted from URLs and web pages. ML models include Decision Trees, Support Vector Machines, and Random Forests that have greatly enhanced phishing identification. Hybrid models, composed of several algorithms, may provide improved prediction results and resist more

***Author for Correspondence**
D. Diana Julie
E-mail: vignesh.v@kce.ac.in

[1]Assistant Professor, Department of Artificial Intelligence and Data Science, KIT–Kalaignarkarunanidhi Institute of Technology, Kannampalayam, Coimbatore, Tamil Nadu, India
[2-4]Student, Department of Artificial Intelligence and Data Science, KIT–Kalaignarkarunanidhi Institute of Technology, Kannampalayam, Coimbatore, Tamil Nadu, India

Received Date: March 27, 2025
Accepted Date: April 16, 2025
Published Date: December 12, 2025

Citation: D. Diana Julie, K. Dinesh Kanna, P. Thirumal, M.P. Victor Moses. A Survey on Leveraging Machine Learning for Phishing Attack Prediction and Detection. Journal of Microelectronics and Solid State Devices. 2025; 12(3): 1–10p.

complex attacks. Additionally, deep learning models, such as CNN or RNN, have demonstrated enhanced prediction capabilities and better resistance to even more complex attacks by automatically learning abstract features.

This literature review aims to summarize the development of phishing detection methods, exhibit the strengths and weaknesses of current models, and comment on how more advanced ML/DL techniques may help overcome the current problems with evasion attacks and feature manipulation. The study explores the recent development trends to better understand the augmentation of modern approaches in improving phishing detection and in constructing more robust systems against those attacks.

LITERATURE REVIEW

Phishing Detection System Through Hybrid Machine Learning Based on URL

State-of-the-art literature in phishing detection has made tremendous improvements with the introduction of ML algorithms that allow for phishing attack identification and prevention. Phishing is a method of cybercrime where users are duped into revealing sensitive information by fake websites or emails, as more people acquire access to the internet. Advanced techniques for detecting phishing attacks initially involved list-based systems – specifically, blacklisting and whitelisting legitimate and phishing sites. However, these systems failed to detect newly developed, zero-day attacks due to their reliance on predefined lists that constantly needed updates.

Given the limitations of list-based systems, ML-based approaches emerged. Classification of phishing URLs can be carried out with algorithms like Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), Gradient Boosting Machine (GBM), Naive Bayes (NB), K-Nearest Neighbors (KNN), and Logistic Regression (LR). Models pick specific features from the structure of domain names, existence of HTTPS, and length of the URL to differentiate between a legitimate website and a phishing website. Decision Tree algorithms have proven to achieve accuracy as high as 95.41% in phishing webpage detection, while aggregated decision trees within Random Forest models provide accuracy up to 96.77%. Despite being much more simplistic, Naive Bayes models also led to almost 88.39% accuracy. It is appropriate to note that Support Vector Machine models, especially in phishing detection scenarios, perform exceptionally well for binary classification problems, with precision obtained at approximately 71.8%.

A hybrid model combining Logistic Regression (LR), Support Vector Machine (SVC), and Decision Tree (DT) through the implementation of both soft and hard voting mechanisms has been presented. This allows the proposed hybrid model to achieve an accuracy of 95.23% compared with any single algorithm. Techniques such as cross-fold validation and Grid Search Hyperparameter Optimization have further enhanced the model's efficiency. Hybrid models also overcome the main weaknesses: they enhance detection accuracy, give minimum false positives, and are more reliable compared to traditional single-algorithm models. This paper suggests that although individual ML algorithms offer various improvements over list-based techniques, hybrid models demonstrate impressive accuracy and robustness in phishing detection. The demonstrated accuracy and efficiency of the proposed hybrid model position it as an excellent solution to overcome security challenges caused by phishing attacks [1].

Intelligent Detection Designs of HTML URL Phishing Attacks

In recent days, phishing attacks have greatly increased and are waged against users by masquerading as fake websites or messages to steal personal information. In the past, several methods have been designed to detect attacks; however, most are based on URL and HTML features. The main development in this area lately has been dedicated to great advances in machine learning (ML) and deep learning (DL) models for automatic detection, thereby reducing human expertise. Most of the detection models rely on HTML and analyze both the structure and content of the web pages. Most cases were tackled using features such as URL length, domain age, and the presence of keywords,

employing techniques like Random Forest and Support Vector Machines (SVM). Such methods achieved moderate results but remain fragile against evasion attacks where attackers may manipulate some key features and yet keep a legitimate look.

These methods scan URL features such as domain reputation, character distribution, and hyperlink structure for URL-based detection. Jain et al. proposed a model for an evasion attack that concentrated on URL detectors by checking how adversarial examples can evade detection systems via alteration of minimal features in a URL. Chen et al. further added that small feature manipulations can reduce phishing detection rates to 30–50%, proving that classifiers are vulnerable to evasion attacks.

Recently, some deep learning models incorporating CNN and RNN have been proposed. Using these models is helpful for learning more abstract features, thus increasing detection accuracy. For example, with the help of URL patterns, CNN-based systems have achieved accuracy up to 98%. Similar performances have been achieved by hybrid models that are based on both URL and HTML features. Beyond these benefits, a generalized ability across multiple phishing attacks is another positive aspect for DL models, although at a huge computational cost. ML and DL-based approaches have excellent potential for effective phishing detection. However, some of the challenges faced are evasion attacks, feature manipulation, and scalability. Improvements in feature extraction, adversarial robustness, and the creation of models efficient to counter the ongoing menace of phishing are in demand [2].

Evasion Attacks and Defence Mechanisms for Machine Learning-Based Web Phishing Classifiers

Classification-based classifiers Machine learning-based classifiers offer hope for detecting phishing sites but are often defeated by evasion attacks. Evasion attacks supply adversarial samples that manipulate website functionality while keeping it intact to resemble the phishing sites under consideration. They utilize whitelist and blacklist approaches; however, initial techniques proved ineffective against new phishing sites, necessitating more advanced tactics. Jain et al. have shown that an evasion attack framework on machine learning-based phishing URL detectors can be achieved by generating adversarial URLs, highlighting the weakness of these systems. Chen et al. have shown that ML models are vulnerable to minor feature alterations; slight changes can reduce detection rates close to zero. Against this background, similarity analysis of phishing websites with their adversarial versions can lead to new defense mechanisms.

Metrics such as Mean Squared Error and DOM tree structure analysis are used, and they have proven effective in detecting adversarial manipulations. The defense mechanism was tested by using a couple of classifiers. Random Forest outperformed all others with the highest accuracy, while Logistic Regression yielded the lowest. This calls for detection systems that are immune to advanced evasion techniques without compromising the original functionality or beauty of websites [3].

Characteristics of Understanding URLs and Domain Names Features

The Detection of Phishing Websites With Machine Learning Methods. A number of research studies have utilized the implementation of machine learning techniques to establish phishing detection schemes. Ludl et al. used a decision tree algorithm, J48, to classify phishing sites according to their features, such as HTML and URL features, and they obtained an accuracy of 83.09%. Kulkarni et al. used Decision Tree, Naive Bayes, SVM, and Neural Networks with an accuracy of 90%. Fette et al. used SVM and implemented the PILFER algorithm, which obtained an accuracy of 92% on a phishing and legitimate dataset. Chiew et al. applied the Random Forest algorithm and achieved an accuracy of 94.6% on data from 5,000 URLs from PhishTank. Parekh et al. also employed Random Forest but achieved an accuracy of 95% for URL-based phishing detection. Hence, these approaches advance this process to the next level, demonstrating that the effectiveness of identifying phishing sites by machine learning methods is inevitable; however, such a move demands relentless improvement to keep track of ever-changing phishing strategies.

In surveying a great deal of literature on malicious URL detection techniques, which exist and have primarily been context-specific for IoT environments, this paper can thus be categorized into three major types of approaches: blacklist-based, content-based methods, and ML-based methods. These are the most traditional ones based on a list of known malicious URLs that crowdsourcing and antivirus groups collect in advance. However, in the case of static database dependency, they fail to detect newly created malicious URLs. Content-based approaches extract and analyze features from content that depicts the webpage's content in terms of HTML tags and CSS attributes. This is highly effective in the detection of malicious URLs embedded in the content; however, they tend to be computationally expensive and thus not practicable for real-time applications. The classification of URLs uses statistical and computational models based on machine learning. Techniques such as Support Vector Machines, Naïve Bayes, Decision Trees, and Deep Learning have demonstrated excellent detection accuracy. Though these models require considerable feature engineering and domain knowledge, they are not as dynamic compared to fast-changing threats. The literature has highlighted several critical limitations of the approaches presently followed: failure in identifying malicious URLs that have not been exposed to before, dependency on fixed features, and manual participation in the preparation of the knowledge base.

Rather than having direct use of the traditional knowledge-based approach, some recent research studies proposed deep learning models, such as GRN and LSTM networks, which can automatically learn to discover patterns from URL sequences without human involvement in feature extraction. However, all of them have some sort of limitations with respect to computational cost and real-time implementation. Therefore, the novelty that this proposed study brings forward is integrating the simulated expert system with KBS. The SE system works exactly like a human expert, learning always from experimental results so that novel malicious URL patterns get identified with no interference. This combination has improved the detection capability with a mere reduction in false positives and adapting to emerging threats. The authors try to demonstrate how Naïve Bayes performs well in this setup, with an accuracy of 95.8%, outperforming state-of-the-art ML algorithms in their category, both in terms of speed and precision.

Traditionally, phishing detection relies on list-based approaches that involve blacklists like Google Safe Browsing and PhishTank, comparing URLs to a database of known phishing sites. Since these systems work well against previously seen URLs, they perform poorly against phishing attempts as phishers constantly change URLs to evade detection. To counter list-based approaches, researchers explored various machine learning approaches to build an automated phishing detection scheme. Sahingoz et al. (2019) used 38 handcrafted features, including URL length, number of subdomains, and special characters. By making use of this NLP-based feature, they managed to attain a Random Forest classifier with an accuracy of 93.98%. In a similar manner, Jain and Gupta (2018) designed an anti-phishing system utilizing some URL-based features, such as WHOIS data, attaining a classification accuracy of 91.28% with an SVM classifier. Banik and Sarma (2020) optimized the feature selection process, which led to a much-reduced set of 9 descriptors; however, the classification accuracy improved to 95.57% with the Random Forest model.

Besides traditional machine learning methods, deep learning methods were also studied. In some works, CNNs and RNNs were used for automatic feature extraction at the character level of URLs. For example, Somesha et al. proposed a model based on an LSTM network, as it has the potential to retrieve results with 97.57% accuracy utilizing both URL and HTML features. Another important contribution was made by Aljofey et al. in 2020, where they used a character-level RCNN model that attains an immense accuracy of 95.02% for phishing URL classification. These trends reflect the general shift toward using automatic techniques for feature extraction to enhance detection in phishing mechanism identification.

The authors published their own solution to this paper from the reviewed set, using the PILU-90K dataset, which specifically focuses on phishing URL detection with a login page. Their best model,

logistic regression combined with Term Frequency–Inverse Document Frequency (TF-IDF), achieved an accuracy of 96.50%. This work, of course, illustrates the challenge of real-world phishing detection and underlines the need for continuously updated datasets for sustained accuracy over time [6].

Machine Learning Techniques for Cyber Security in the Last Decade

Unlike list-based techniques, detection of phishing relies heavily on blacklists, such as Google Safe Browsing, for previously known phishing URLs. These static methods fail in handling newly emerging phishing attacks since attackers change the URLs to bypass the filters. Hence, ML approaches have been widely sought after for the automatic detection of phishing URLs. Another interesting paper by Sahingoz et al. (2019) again used Random Forest classifiers with 38 features from URLs, like length, subdomain count, and special character presence. This resulted in an accuracy of 97.98%. However, it was very feature-engineering-intensive and not effective against dynamic or novel URLs. Jain and Gupta (2018) also established an SVM classifier with feature inclusion of WHOIS data and URL patterns and achieved 91.28% accuracy. Though SVMs are efficient, they are not scalable for big data and fast-changing phishing schemes.

Later advancements minimized feature engineering efforts through deep learning models that automatically learned URL patterns. For example, in their paper, Somesha et al. (2020) reported that the LSTM network achieved 99.57% accuracy, explicitly marking a shift toward employing deep learning models for phishing detection. These developments depict massive gains in terms of accuracy, and one would anticipate that with such advancement, it may be quite feasible to detect a phishing URL in a dynamic scenario [7].

LSTM based Phishing Detection for Big Email Data

Traditional phishing detection systems rely, by and large, on comparing URLs or email addresses to a known list of malicious or trusted ones. This method was not effective, primarily due to the dynamic nature of phishing attacks, where attackers constantly change addresses or URLs to evade detection. For example, Cao et al. (2008) proposed an anti-phishing approach based on domain name credibility. However, it could be easily bypassed simply by changing the sender IP or domain information; hence, its effectiveness in practice was low. New techniques in sandbox-based detection use more proactive analysis, in which email attachments are isolated and run in controlled environments to detect malicious behavior. Han et al. (2017) developed a new sandbox tool that proved highly effective in detecting unencrypted phishing attachments, but their systems were unable to efficiently deal with encrypted or obfuscated files, which have become typical in sophisticated phishing attacks.

With the use of machine learning, massive breakthroughs have been seen in the field of phishing detection. Techniques such as SVM and Random Forests have been used extensively for the classification of emails based on varied features such as sender reputation, domain structure, and attachment analysis. Saeed et al. relied on SVM to classify emails with moderate accuracy. Such methods face difficulties in feature extraction and generalization to more sophisticated phishing techniques.

However, with deep learning models, especially LSTMs, these limitations can be overcome; LSTM networks can handle much longer sequences than feedforward networks do. So, LSTMs have been proven successful in classifying phishing emails, which considers full-text email content rather than isolated features. LSTM networks improve the accuracy of phishing detection through the capture of patterns in the text of emails; they eradicate the gradient vanishing problem inherent in long email content and outperform all conventional machine learning techniques when dealing with large-scale datasets of phishing emails [8].

Phishing Web Page Detection Methods

URL and HTML Features Detection. This paper focused on detection approaches to phishing sites. The paper elaborated on the high frequency of such attacks and the need for effective detection

systems in real-world scenarios. The authors observe that phishing schemes often emulate legitimate websites to deceive users into divulging sensitive information. They discuss various methodologies, including machine learning techniques like SVM, Decision Trees, and Gaussian Naive Bayes, while noting that URL and HTML features – such as URL length, presence of sensitive keywords, and absence of SSL (HTTPS) – play a decisive role in detection. The research demonstrated that a rules-based approach can achieve 93.3% accuracy, in contrast to machine learning, which generates – a bit more accuracy of up to 96.8%. Therefore, the authors conclude with a hybrid approach where URL and HTML features are combined with rule-based detection, making phishing detection stable and efficient without the complexity involved in machine learning algorithms [9].

Detection of Phishing Attacks with Machine Learning Techniques in Cognitive Security Architecture

This paper investigates the application of a cognitive security framework to detect phishing attacks through machine learning. The authors mostly apply algorithms such as Logistic Regression (LR) and Artificial Neural Networks (ANNs) to classify URLs as legitimate, suspicious, or phishing, based on attributes such as URL length, subdomains, and Google indexing. Therefore, the Logistic Regression model was used for its simplicity and ability to handle large databases, whereas ANNs have been applied in more sophisticated ways to simulate human cognitive processes by learning from incomplete data.

The datasets were downloaded from Kaggle and provided numerous phishing examples. Logistic Regression obtained an accuracy level of about 80%, while ANNs showed promise but misclassified some legitimate URLs. This research concludes that when combined with cognitive security systems, machine learning improves real-time phishing detection but needs further iteration and refinement for more accurate use in algorithms and datasets. Thus, the system aims to reduce response time and the number of human interventions required by a cybersecurity practitioner [10].

LITERATURE SURVEY FINDINGS

Limitations of List-Based Detection

Traditional list-based approaches, such as blacklisting and whitelisting, fail against newly created phishing URLs and zero-day attacks because of their reliance on predefined lists.

Machine Learning Models

Promising algorithms, including DT, RF, SVM, LR, and NB, are used to identify phishing URLs by utilizing features such as URL structure, domain age, and HTTPS presence.

Hybrid Models

The use of ensembling among several ML models improves detection accuracy and reduces false positives compared to single models, making them more robust for phishing detection, as demonstrated by combinations such as LR+SVM+DT.

Feature Selection and Extraction

Proper reduction of feature sets to a minimal subset through efficient feature selection and automatic extraction of features from the data is highly useful in enhancing model efficiency and scalability.

Challenges in Real-World Application

Issues associated with dynamic real-world applications, due to the requirement of continuous updates for effective management of complex phishing schemes and dynamic attack patterns, make their implementation difficult.

Performance Trade-offs

Although the ML models possess high accuracy, deep learning techniques require significant computational power. Hybrid methods aim to balance accuracy, efficiency, and resource usage.

EXISTING SYSTEM

The internet has left much room for criminals to commit criminal activities such as online fraud, malware, viruses, ransomware, worms, intellectual property rights, denial-of-service attacks, money laundering, vandalism, electronic terrorism, and extortion. Hacking poses a significant threat to the internet, as individuals can compromise computer information and exploit it in various ways to cause harm. The misuse of information and the associated ethical concerns represent a significant problem, particularly for younger generations.

Detection of these websites, which may appear simple and secure, will help protect individuals. Therefore, awareness of these websites is also required. Viruses can damage an entire computer network and compromise confidential information by spreading to multiple computers. It is not advisable to use unauthorized websites on the internet.

PROPOSED SYSTEM

All these threats necessitate effective phishing detection to secure computer systems. Cybersecurity is one of the leading issues in the world today. Over the last decade, various anti-phishing detection mechanisms have been proposed. Studies have focused on the structure of Uniform Resource Locators (URLs) and feature selection methodologies for machine learning. We identify the most relevant features and reduce the dimensionality of the feature subset. These features are then utilized in the phishing detection process, employing feature ranking combined with Random Forest and XGBoost algorithms, alongside a correlation matrix visualized with a heatmap.

We ran the experimentation process of the implemented classifiers, and the best hybrid classifier comprised SVM, Decision Tree, Random Forest, and XGBoost, achieving enhanced accuracy. Our proposed hybrid classifier will help Internet users in validating the authenticity of websites, thereby reducing the chances of encountering phishing websites and enabling safer online usage.

The most effective features have been derived through feature ranking using machine learning, specifically the Random Forest and Logistic Regression algorithms; the dimensionality of a feature subset has been reduced, which can be used in phishing detection. We analyzed the performance of classifiers which have been implemented, and identified the Logistic Regression machine learning model as achieving the highest accuracy. Our proposed hybrid classifier will assist Internet users in identifying authentic websites, thereby eliminating phishing websites and fostering secure online usage. This project enhancement focuses on predicting whether a URL is phishing or not. The model leverages the relationship between features and labels for phishing prediction

Data Collection and Data Preprocessing

This process involves loading and exploratory data analysis of the dataset, including understanding its structure and outlining preprocessing steps.

- *Loaded Data:* The dataset was imported using pandas (`pd.read$_c$sv`), and the first few rows were displayed to understand its structure.
- *Summary of Data:* The commands `df.describe()` and `df.info()` were used to obtain summary statistics and information regarding the dataset.
- *Missing Values Handling:* Lines of code were used to identify and manipulate missing values, such as `df.isna().sum()`.
- *Data Transformation:* Categorical values were transformed into numerical representations. For example, 'status' labels were mapped to equivalent numerical values.

EDA (Exploratory Data Analysis)

Exploratory Data Analysis was performed to identify patterns and relationships within the data.

Correlation

The correlation matrix was calculated and plotted using `sns.heatmap` to examine relationships between features.

Feature Selection

A feature selection tool, `features electron correlation`, was designed to select only those features whose correlation with other features crosses a defined threshold.

Model Training and Evaluation

Model training involves the use of machine learning models such as the Random Forest Classifier and the Logistic Regression algorithm, along with their performance evaluation.

- *Data Splitting:* The dataset was divided into training and test sets using `train$_t$est$_s$plit`..
- *Model Training:* All models, including Random Forest, Deep Belief Network, and Restricted Boltzmann Machine, were trained using the scikit-learn library.
- *Model Evaluation:* A custom function (`custom$_a$ccuracy$_s$et`) was used to evaluate models on both training and testing data, based on confusion matrices and classification reports.

Model Comparison and Visualization

- *Model Comparison:* The training, testing, and cross-validation accuracies for each model were plotted using a bar chart.
- *Feature Importance Visualization:* A bar chart was plotted for the ML model to visualize feature importance.

Test Size and Cross-Validation Sensitivity

- *Test Size Sensitivity:* Different test sizes, such as 20%, 30%, 40%, and 50%, were explored to assess their impact on model accuracy.
- *Cross-Validation Scores:* Cross-validation scores were calculated and displayed for all models.

Prediction

The model was used to predict whether a given URL is a phishing attempt. The model predicts phishing status based on the relationship between features and labels. Accuracy is defined as the degree of correctness of the predicted value. The model's accuracy is predicted based on the algorithms used, varying features, and different train-test split sizes. A significant impact of training data size on model accuracy was observed. The larger the training size, the more accurate the model will be. The model employs multiple algorithms for phishing prediction, illustrating the impact of each attribute on the predicted outcome.

WORKFLOW DIAGRAM

1. *Data Extraction & Preprocessing:* Raw data is collected and preprocessed by filling missing values, encoding categorical variables, and normalizing features where necessary.
2. *Data Split:* The data is divided into training and validation test sets, which are used to determine the model's fitness on unseen data.
3. *Model Selection:* The appropriate machine learning algorithm or model type is determined based on the specific problem and dataset characteristics.
4. *Model Training:* The model is fitted using the training data, with subsequent adjustments to its parameters to reduce error.
5. *Model Evaluation & Deployment:* The model is evaluated based on defined metrics and deployed to a production environment if its performance is satisfactory.
6. *Real-Time Monitoring and Detection:* Monitor the model's performance in the live environment for drifts or anomalies (Figure 1).

CONCLUSION

This phishing detection survey reveals significant advancements in detecting and mitigating phishing attacks using diverse machine learning techniques and hybrid models. Traditional list-based methods, including blacklisting and whitelisting, proved effective for known threats but failed to detect zero-day attacks and new phishing tactics. Subsequently, different models like Decision Trees,

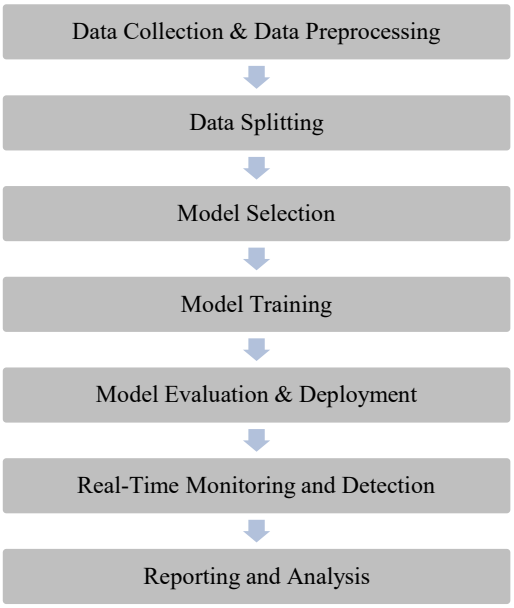

Figure 1. Work flow of the system.

Random Forests, Naïve Bayes, and Support Vector Machines significantly enhanced detection accuracy by analyzing complex features extracted from the URLs and HTML structure. However, an individual model was prone to high false positives and required extensive feature engineering. Thus, this indicates a recent trend toward using hybrid models and deep learning-based techniques, where the strengths of various algorithms can be combined to achieve greater accuracy and robustness. Hybrid models – that is, Logistic Regression, Support Vector Machines, and Decision Trees – exhibited fewer false positives and performed admirably.

Nevertheless, CNN and LSTM networks can automatically perform feature extraction with better generalization, albeit at a greater computational cost. Based on the literature survey, the most promising solutions for effective phishing detection involve hybrid models coupled with advanced deep learning techniques. However, there are always evasion attacks, issues of feature manipulations, and aspects regarding scalability that make it even more imperative to continuously research and develop to make the phishing detection system more robust and adaptive.

REFERENCES

1. Karim A, Shahroz M, Mustofa K, Belhaouari SB, Joga SR. Phishing detection system through hybrid machine learning based on URL. IEEE Access. 2023 Mar 3;11:36805–22.
2. Asiri S, Xiao Y, Alzahrani S, Li S, Li T. A survey of intelligent detection designs of HTML URL phishing attacks. IEEe Access. 2023 Jan 18;11:6421–43.
3. Pillai MJ, Remya S, Devika V, Ramasubbareddy S, Cho Y. Evasion attacks and defense mechanisms for machine learning-based web phishing classifiers. IEEE Access. 2023 Dec 14;12:19375–87.
4. Kara I, Ok M, Ozaday A. Characteristics of understanding URLs and domain names features: the detection of phishing websites with machine learning methods. IEEE Access. 2022 Nov 17;10:124420–8.
5. Anwar S, Al-Obeidat F, Tubaishat A, Din S, Ahmad A, Khan FA, Jeon G, Loo J. et al. Countering malicious URLs in internet of things using a knowledge-based approach and a simulated expert. IEEE Internet of Things Journal. 2019 Nov 21;7(5):4497–504.
6. WESAM M, GONZÁLEZ-CASTRO VÍ. Phishing URL detection: A real-case scenario through login URLs.
7. Shaukat K, Luo S, Varadharajan V, Hameed IA, Xu M. A survey on machine learning techniques

for cyber security in the last decade. IEEE access. 2020 Dec 2;8:222310–54.
8. Li Q, Cheng M, Wang J, Sun B. LSTM based phishing detection for big email data. IEEE transactions on big data. 2020 Mar 12;8(1):278–88.
9. Faris H, Yazid S. Phishing web page detection methods: URL and HTML features detection. In2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS). IEEE; 2021 Jan 27. pp. 167–171.
10. Contractor A, Mehta R, Menaria S. A Comprehensive Survey on Phishing Attack Detection, Smart Computing;2021,PP:22-32, DOI: https://doi.org/10.47531/SC.2022.05.

