


# Survey and comparative analysis of phishing detection techniques: current trends, challenges, and future directions

Ashvini Jadhav, Pankaj R. Chandre

Department of Computer Science and Engineering, MIT School of Computing, MIT Art Design and Technology University, Pune, India

Article Info	ABSTRACT
<p><b>Article history:</b></p> <p>Received May 10, 2024 Revised Nov 4, 2024 Accepted Nov 14, 2024</p> <hr/> <p><b>Keywords:</b></p> <p>Convolutional neural network K-nearest neighbor Machine learning Naive Bayes Random forest Recurrent neural network Support vector machine</p>	<p>In the age of digital communication, scams such as phishing continue to be a problem, necessitating the need for ever-more-advanced detection techniques to safeguard sensitive data. Examining several methods now in use, this review article groups them according to the application (email, web server, mail server, or browser-based). It explores the advantages and disadvantages of behavior-based, heuristic-based, machine learning (ML)-based, and signature-based techniques and offers a comparative evaluation of their efficacy. The essay delves deeper into the latest developments in phishing detection research, such as ML-powered social media exploration and real-time website analysis. The evaluation goes beyond just identifying detecting techniques; it also includes a data-driven analysis. In particular, random forest and support vector machines are ML algorithms that regularly produce results with high accuracy for detecting phishing attempts. Metrics like as recall, F1-score, and precision show how well these algorithms. Furthermore, specialised techniques such as heuristic-based and cantina-based approaches provide remarkable performance, underscoring the possibility of additional research in this field. Future research explores improved phishing detection through: better accuracy with ML, integrating new technologies, analyzing user behavior. A hybrid approach combining these techniques offers a stronger defense.</p> <p><i>This is an open access article under the <a href="#">CC BY-SA</a> license.</i></p> <div></div>

## Corresponding Author:

Ashvini Jadhav  
Department of Computer Science and Engineering, MIT School of Computing  
MIT Art Design and Technology University  
Loni, Pune, India  
Email: ashvinigadhav@gmail.com

## 1. INTRODUCTION

Phishing attacks pose significant threats to individuals, organizations, and cybersecurity systems globally. Strong phishing detection methods are becoming more and more important as these attacks continue to grow in complexity. In addition to examining current trends, addressing issues, and pointing out future directions in the field. This article undertakes a thorough review and comparative analysis of the available phishing detection techniques. Through an analysis of the advantages and disadvantages of different strategies, this study seeks to further the development of efficient defences against phishing attacks. This paper analyzes and compares existing phishing detection techniques to highlight their effectiveness and explore advancements in the field.

Phishing attacks have become one of the most prevalent and dangerous forms of cybercrime, with attackers continuously evolving their tactics to deceive users and bypass traditional security measures. These attacks, often disguised as legitimate communication, aim to steal sensitive information such as passwords, credit card numbers, and personal data. As phishing techniques grow in sophistication, there is an increasing

need for robust detection methods that can identify malicious activities before they result in significant damage. The development of such methods is a critical challenge, as phishing attacks can take various forms, such as spear-phishing, voice phishing (vishing), and email-based phishing, each requiring tailored detection strategies.

The current state of phishing detection involves a combination of techniques, including machine learning (ML)-based models, rule-based systems, and heuristics. ML methods have gained considerable attention due to their ability to analyze large datasets and identify patterns indicative of phishing behavior. These models are often trained on features such as URL characteristics, email content, sender information, and user interaction data. However, despite their effectiveness, ML models require continuous updates to remain accurate against emerging phishing tactics. On the other hand, rule-based systems, though simpler and more transparent, may struggle to keep up with new attack strategies due to their reliance on predefined rules. Therefore, combining multiple techniques in a hybrid approach has emerged as a promising solution to enhance detection accuracy and adaptability.

Looking ahead, the future of phishing detection will likely see significant advancements in the integration of artificial intelligence (AI) and natural language processing (NLP) to analyze and understand phishing attacks more deeply. AI models could be used to detect more subtle patterns in the communication, such as the tone or context of the message, that may indicate phishing. Additionally, integrating detection methods with real-time monitoring systems could provide more dynamic and proactive defense mechanisms. As phishing attacks continue to diversify and exploit new vulnerabilities, further research into adaptive learning models, continuous data collection, and user behavior analysis will be crucial in creating resilient systems capable of defending against evolving threats.

## **2. BACKGROUND ON PHISHING ATTACKS**

### **2.1. Overview of phishing attacks**

Phishing attacks are deceptive tactics employed by cybercriminals to trick individuals into disclosing sensitive information such as usernames, passwords, and financial details [1]. Usually, these assaults use phoney emails, texts, or websites that imitate reputable companies in order to trick victims into giving their personal information without realising it [2]. Phishing attacks make it difficult for users to distinguish between legitimate and malicious messages by taking use of social engineering techniques and human psychology to instill a sense of urgency or trust. Effective detection techniques are essential in the fight against these constantly evolving cyber dangers because of their widespread presence and the potential to cause severe financial and reputational harm.

Phishing attacks involve fraudulent attempts to deceive individuals into disclosing sensitive information such as passwords, financial data, or personal details [3]. These assaults typically take the shape of false emails, websites, or messages impersonating trustworthy organisations; they frequently have the goal of distributing malware or stealing login credentials [4]. Phishing attacks can take many different forms, such as spear phishing, which sends targeted, personalised emails to specific people or organisations, email phishing, which uses false emails to trick recipients into disclosing information, and pharming, which sends users to fraudulent websites without their knowledge or consent. Moreover, victims of vishing and smishing attacks are tricked into divulging private information through voice calls and SMS texts, respectively

### **2.2. Importance of phishing detection techniques**

Phishing attacks remain a prevalent and persistent threat to individuals, businesses, and organizations worldwide [5]. Robust phishing detection strategies are essential for protecting confidential data, averting financial losses, and maintaining confidence in online interactions. These methods enable people to make wise decisions and lessen their chance of falling for phishing scams by spotting phoney emails, webpages, and communications [6]. Furthermore, to remain ahead of hackers and safeguard digital ecosystems, ongoing research and innovation in detection techniques is crucial as phishing tactics develop and become more complex.

### **2.3. Purpose and scope of the paper**

The purpose of this paper is to provide a comprehensive survey and comparative analysis of existing phishing detection techniques. It attempts to examine the most recent developments in phishing detection, evaluate the difficulties these methods encounter, and suggest prospective lines of inquiry for further study and advancement. This study aims to improve cybersecurity measures by providing insights into the efficacy, constraints, and future developments in countering phishing attacks through an examination of multiple methodologies.

## 2.4. Research objectives

Phishing attacks have become a major concern for both individuals and organizations worldwide, and as these attacks grow in sophistication, the need for effective detection techniques has never been more critical. To combat phishing, researchers have developed a variety of detection methods, each with its own strengths, limitations, and areas of application. This research aims to explore and analyze the various techniques that have been implemented in the fight against phishing, offering a comprehensive understanding of their effectiveness and challenges. The following objectives guide this study in addressing key aspects of phishing detection:

- To offer a thorough analysis of the many phishing detection methods now in use, including behavior-based, heuristic-based, ML-based, signature-based, and hybrid approaches.
- To do a comparative analysis of these methods, assessing their suitability for different situations as well as their efficacy, strengths, and limits.
- To determine the most recent developments and new technologies in phishing detection research, as well as their possible effects on enhancing detection skills.
- To examine the difficulties encountered by current phishing detection techniques and provide future paths and viable fixes to improve detection efficiency, scalability, and accuracy in the fight against phishing attacks.

Phishing attacks are deceptive cybercrimes that aim to steal sensitive information such as usernames, passwords, and financial data by masquerading as legitimate entities. Phishing attacks are commonly conducted via email, websites, or instant messaging platforms. They frequently utilise social engineering techniques to deceive targets into disclosing personal information or clicking on harmful links. Serious repercussions from these attacks may include financial loss, identity theft, and compromise of private company information. Safeguarding individuals and organisations against these ubiquitous risks requires strong detection and mitigation solutions as phishing attempts continue to increase in sophistication and scale.

## 2.5. Common characteristics and tactics used by phishers

Phishing attacks often involve the use of phoney email content that imitates reliable sources like government agencies or financial institutions. These techniques use urgent or fear-inducing language to elicit a quick response; URLs or hyperlinks that lead to fraudulent websites intended to steal sensitive information. Additionally, phishing fakes spoofing sender addresses to appear authentic and social engineering techniques that take advantage of psychological weaknesses to trick victims into divulging personal or financial information.

## 2.6. Impact of phishing attacks on individuals and organizations

Phishing attacks pose significant threats to both individuals and organizations, exploiting human vulnerabilities and technological weaknesses to steal sensitive information or financial assets [7]. Individuals who fall prey to phishing scams may experience identity theft, financial loss, and compromised personal data, which may have long-term effects on their reputations and credit ratings [8]. Phishing attacks have the potential to seriously impair an organization's operations, compromise confidential information, and reveal critical corporate data, all of which can result in monetary losses, legal ramifications, and reputational harm. Successful phishing attempts can also reduce consumer loyalty and brand trust, which can affect an organization's long-term survival and capacity to compete in the market.

# 3. EXISTING PHISHING DETECTION TECHNIQUES

Current phishing detection techniques cover a wide range of methodologies, such as ML models that identify phishing attempts based on labelled datasets, heuristic-based techniques that analyse email content and sender characteristics, and signature-based methods that rely on known phishing patterns. Behavior-based detection systems keep an eye on how users interact with emails and webpages in order to spot any unusualities that could be signs of phishing. Furthermore, various detection techniques are used for improved accuracy in hybrid and multi-layered approaches. Notwithstanding developments, problems including changing phishing strategies, the complexity of identifying authentic emails, and scalability issues continue to exist, necessitating continued study and innovation in the area. Figure 1 depicts the phishing detection techniques model.

## 3.1. Signature-based detection methods

Signature-based detection methods in phishing involve comparing incoming emails or messages against a predefined list of known phishing signatures or patterns. Usually, these signatures are made up of particular terms, URLs, or patterns that are frequently connected to phishing attempts. If a match is discovered, the communication is marked as possibly harmful and is examined more closely or may be taken further [9]. Although signature-based detection works well for spotting known phishing attempts, it might

have trouble spotting novel or undiscovered phishing variations. Moreover, signature databases need to be updated often in order to remain effective against phishing schemes that change over time. Notwithstanding these drawbacks, signature-based detection is still an essential part of all-encompassing phishing defence plans, especially when paired with additional detection methods for increased coverage and accuracy.

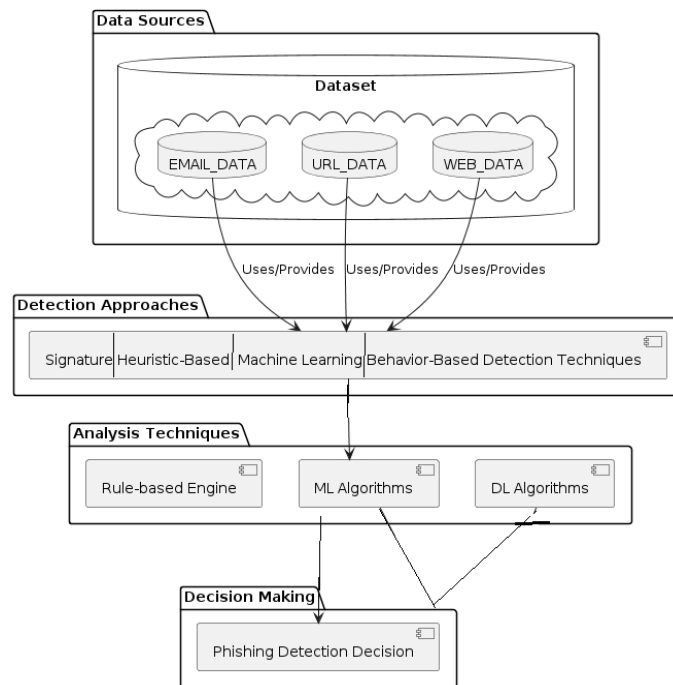


Figure 1. Phishing detection techniques model

### 3.2. Heuristic-based detection approaches

Heuristic-based detection approaches leverage predefined rules and patterns to identify potential phishing attacks. These methods look for unusual patterns suggestive of phishing by analysing different aspects of emails, URLs, and content [10]. Common heuristics include analysing the email address of the sender, verifying that domains are spelt correctly, evaluating the content of messages for urgency or threats, and closely inspecting embedded URLs to look for redirection or mismatched domains. Although heuristic methods are flexible and adaptable to changing phishing techniques, they might not be able to identify sophisticated attacks that avoid preset guidelines. Achieving a balance between detection accuracy and false positives is a challenge, as phishing strategies are always developing, necessitating ongoing development. Heuristic-based techniques for thwarting phishing threats can be made more effective by integrating them with other detecting techniques and technology.

### 3.3. Machine learning-based detection models

ML-based phishing detection models leverage algorithms to analyze various features extracted from emails, websites, or user behavior to identify phishing attempts. Frequently, these models employ supervised learning methodologies, including classification algorithms, to categorise emails or webpages as authentic or fraudulent [11]. With features like email content, sender information, URL characteristics, and user interactions, feature engineering is essential to these models. To increase detection accuracy, ensemble techniques like gradient boosting and random forests (RF) are frequently used. Managing adversarial attacks, class disparities, and changing phishing strategies are among the difficulties. Future directions include utilising anomaly detection methods to identify new phishing threats and investigating deep learning (DL) architectures for improved feature representation. Other areas of active study to improve the efficacy of ML-based phishing detection include the integration of contextual information and real-time analysis.

### 3.4. Behavior-based detection techniques

Behavior-based detection techniques in phishing involve analyzing the behavioral patterns of users to identify potential phishing attempts. These methods concentrate on tracking different user activities, like keystrokes, mouse movements, and browsing patterns, in order to identify departures from typical behaviour

that may be signs of phishing activity [12]. A baseline of acceptable user behaviour can be set up so that abnormalities can be identified and further examined for possible phishing attacks. Behavioural analysis has the ability to adjust to changing attack strategies and is advantageous in identifying phishing operations that have not been observed before. Nonetheless, obstacles consist of precisely distinguishing between authentic user conduct and dubious activities, in addition to managing privacy issues related to tracking user activities. The creation of strong behavior-based detection techniques is still essential for successful cybersecurity defence tactics as phishing attempts becoming more complex.

### 3.5. Hybrid and multi-layered detection systems

Hybrid and multi-layered detection systems leverage a combination of different detection techniques to enhance the accuracy and robustness of phishing detection. To provide a thorough defence against phishing assaults, these systems usually combine signature-based, heuristic-based, ML-based, and behavior-based techniques. They can effectively solve the shortcomings of individual techniques and produce more dependable detection results by integrating numerous detection methods. Because hybrid systems dynamically modify the weighting of various detection components in response to changing threat landscapes, they provide flexibility and adaptability [13]. By successively putting suspicious emails through several detection modules, multi-layered systems increase the likelihood of identifying sophisticated phishing attempts and provide an additional layer of protection. However, there are issues with system complexity, resource consumption, and maintenance overhead when integrating and coordinating various detection methods. Ongoing research aims to optimize the performance of hybrid and multi-layered systems while addressing scalability and efficiency concerns to keep pace with evolving phishing tactics.

Gupta *et al.* [14] introduces a novel ML-based approach for real-time phishing website detection, utilizing hybrid URL and hyperlink features to achieve high accuracy without relying on third-party systems. Due to their reliance on outside sources, such as search engines, traditional anti-phishing systems are unable to respond appropriately in real-time and struggle with zero-hour attacks. The suggested approach, which is fully client-side, uses the XGBoost technique to achieve an impressive 99.17% detection accuracy while extracting characteristics from URL and hyperlink data. The method, which just uses the website's address bar and source code, has a 98.81% true positive rate and a 0.49% false positive rate. It was validated using a recently created dataset. The paper makes a substantial contribution by combining hyperlink and URL data into a hybrid set in an efficient manner, which opens the door to improved phishing detection. However, the integration of more specific features may further improve accuracy, albeit at the cost of increased complexity, especially concerning mobile phishing, which poses a growing threat in the era of ubiquitous mobile devices.

Punia *et al.* [15] explore the use of various ML classification algorithms to convert unstructured data from social media networks, particularly Twitter, into structured information. They use supervised, unsupervised, and reinforcement learning methods, such as k-nearest neighbor (KNN), naive Bayes (NB), decision trees (DT), neural networks (NN), and support vector machines (SVM). They discover through their investigation that SVM has the best accuracy across a range of sensitivity settings, with NB coming in second. DT, NN, SVM, NB, and KNN all yielded average accuracy values of 0.3875, 0.4625, 0.6, 0.525, and 0.37, respectively. The study comes to the conclusion that SVM produces the best classification accuracies, and it makes recommendations for future enhancements by experimenting with different kernels and using RF with variable numbers of DT.

Liu *et al.* [16] focuses on the increasing cyber security threats posed by insiders within information communications technology systems. Insider risks are classified into three primary categories: traitor, masquerader, and inadvertent perpetrator. Additionally, early stage threats that could result in insider misconduct are taken into account. It examines numerous programmes and methods intended to identify and stop insider threats from a data analytics standpoint, classifying them according to audit data sources including host, network, or contextual data. Every task is evaluated based on how well it protects against insider threats, data extraction techniques, and algorithms that make decisions. A comparative study is presented, emphasising the advantages and disadvantages of various strategies. In order to encourage more contributions to the mitigation of insider risks in ICT systems, the survey ends by outlining research gaps and challenges.

Paliath *et al.* [17] explores phishing detection techniques by applying knowledge discovery principles and comparing machine-learning approaches. It presents two novel features and applies information gain to assess their efficacy in conjunction with current features. After comparing six classifiers, NN exhibit the highest accuracy, at 99.4%. Nonetheless, it observes a noteworthy 1.5% mean absolute error rate and a minor decline in classification efficiency. Future research attempts to improve detection by extending word embedding multi-classifier systems to better recognise novel phishing forms, and by adding new features like document frequency and inverse document frequency.

Gupta *et al.* [18] presents a novel ML-based phishing detection approach. Unlike previous methods requiring a plethora of features and significant processing power, our approach relies on just nine lexical

features, making it suitable for resource-constrained devices. Utilising the ISCXURL-2016 dataset, which includes 11,964 examples of both authentic and fraudulent URLs, our method utilised the RF technique to get a remarkable 99.57% accuracy. The paper gives a summary of phishing assaults, evaluates current detection techniques, and describes how our methodology was developed. It displays the distribution of lexical data in phishing and authentic URLs and describes the feature extraction strategies. A comparative study with alternative methods highlights the applicability of our method for integration into devices with limited resources. Future research will assess our methodology using sophisticated DL algorithms.

Paniagua *et al.* [19] proposes a novel method for detecting phishing websites through URL analysis, comparing ML and DL techniques. The authors include URLs from both index and login pages to better reflect real-world settings, in contrast to existing solutions that frequently remove login pages from the valid class. This reveals substantial false-positive rates with legitimate login URLs. By using more recent URLs for testing and training on older datasets, they show how the accuracy of the model deteriorates over time. To determine which phishing strategies are evolving, the authors do a frequency study of the most popular phishing domains. A new dataset called PILU-90K, consisting of 30 K phishing and 60 K valid URLs, is introduced. A logistic regression model using term frequency-inverse document frequency (TF-IDF) feature extraction is shown, and it can detect phishing login URLs with 96.50% accuracy. Their approach aims to enhance current blacklist methods, offering the PILU-90K dataset for researchers to train and test their approaches, providing a more representative scenario for real-world phishing detection.

Gerke *et al.* [20] addresses the prevalent issue of email phishing attacks within the context of cloud computing. It discusses the methodology employed to detect phishing emails using ML algorithms, including SVM, NB, and long short-term memory (LSTM). The classifiers attained high accuracy rates by using features that were retrieved from the dataset using NLP and regular expression. The SVM, NB, and LSTM classifiers achieved 99.62%, 97%, and 98% accuracy rates, respectively. The study emphasises the significance of efficient detection methods in protecting confidential information sent by email and suggests a framework for upcoming enhancements, like combining phishing and authentic email datasets to produce a more complete training set. The ultimate objective is to create strong systems that can consistently identify and counteract phishing attacks in order to shield users and businesses from possible security lapses. The existing methods provide a well-structured overview of various phishing detection techniques, including signature-based, heuristic-based. The Table 1 (see in Appendix) offers a valuable breakdown of detection methods across different categories.

The Figure 2 shows a concept of phishing detection infrastructure design packages. It outlines various methods to secure an organization from phishing attacks. Here are the methods explained in the image:

Network-based detection (focuses on network traffic):

- Web server logs analysis: Examining logs generated by web servers to identify suspicious activity related to phishing attempts. Imagine sifting through server logs like a detective searching for clues. These clues might indicate unusual access patterns or attempts to access sensitive information.
- Web application firewall (WAF) (Shield): Acting as a shield, a WAF filters incoming traffic to web applications. It blocks malicious requests that might be associated with phishing attacks. Think of it as a security checkpoint that only allows legitimate traffic to pass through.
- Mail server logs analysis: This involves analyzing logs from email servers to identify suspicious email patterns or activities indicative of phishing attempts. Similar to web server logs, this is looking for red flags within email server records, such as a sudden surge in emails from an unusual source.
- Anti-spoofing techniques: These methods prevent attackers from disguising their email addresses or websites to impersonate legitimate entities. Imagine putting a stop sign on email and website impersonation. These techniques help ensure emails and websites are who they claim to be.

Content-based detection (focuses on the content of emails and websites):

- Email filters (Sieve): Similar to a sieve that filters out unwanted objects, email filters analyze incoming emails based on pre-defined criteria to identify phishing attempts. These filters look for suspicious characteristics in emails, such as misspelled sender addresses, urgency tactics, or malicious attachments.
- Email content analysis: This involves a deep dive into the content of emails to uncover suspicious elements. Techniques analyze email content for linguistic cues used in phishing attempts, HTML anomalies that might indicate hidden content, or the presence of malicious attachments. It's like examining a crime scene to find evidence.
- Sender authentication (sender policy framework (SPF), domainkeys identified mail (DKIM), domain-based message authentication, reporting and conformance (DMARC)): These protocols act like ID checks for emails, ensuring they're coming from who they say they are (SPF, DKIM, and DMARC). These protocols verify the legitimacy of the sender's email address, helping to prevent email spoofing used in phishing attacks.

User education and awareness (teaches users to identify phishing attempts):

- User training and awareness: Equipping users with knowledge is key. These programs educate users about phishing tactics and how to identify and avoid phishing attempts. By empowering users to recognize phishing attempts, they become a stronger defense against these attacks.

Infrastructure and services (tools and services used for detection):

- Web servers (Apache, Nginx): While not directly involved in detection, secure configuration of web servers, the foundation upon which websites are built, can help mitigate vulnerabilities that might be exploited in phishing attacks. Think of them as the building blocks of websites, and keeping them secure helps prevent weaknesses that could be targeted.
- Browser extensions: Imagine a plus sign adding an extra layer of protection to your browser. These add-ons offer real-time phishing detection by analyzing URLs or warning users about suspicious websites. They provide an additional line of defense within your web browser.
- Safe browsing features: Built-in browser shields provide protection against potential phishing websites based on blacklists or real-time threat intelligence. These features act as a shield within your browser, automatically warning you about potentially dangerous websites.
- URL scanners: Imagine a magnifying glass used to examine a URL in detail. These tools analyze URLs to assess their legitimacy and identify potential phishing attempts. They provide a way to investigate the trustworthiness of a URL before you click on it.
- URL reputation analysis: These services act like historical investigators, checking the "history" of a URL to see if it's been flagged as suspicious before. They analyze the reputation of a URL based on various factors, including user reports, blacklists, and historical data.

Service providers (companies offering anti-phishing solutions):

- Email service providers (ESPs): The companies behind your email service can offer tools to fight phishing, like email filtering and sender authentication. They provide functionalities within your email service to help prevent phishing attacks.
- URL scanning services: These companies provide specialized tools for scanning URLs and assessing their safety. They offer dedicated services specifically designed to analyze URLs for suspicious activity.
- WAF providers (Shield): Similar to the WAF itself, these companies provide WAF solutions as a service, offering protection against phishing attempts on web applications. They offer WAF solutions that can be implemented to protect web applications.
- Browser extension developers: Imagine a person adding a plus sign, representing the developers who create browser extensions with phishing detection functionalities.
- Domain hosting providers: Heuristic methods can be used to analyze domain registration patterns

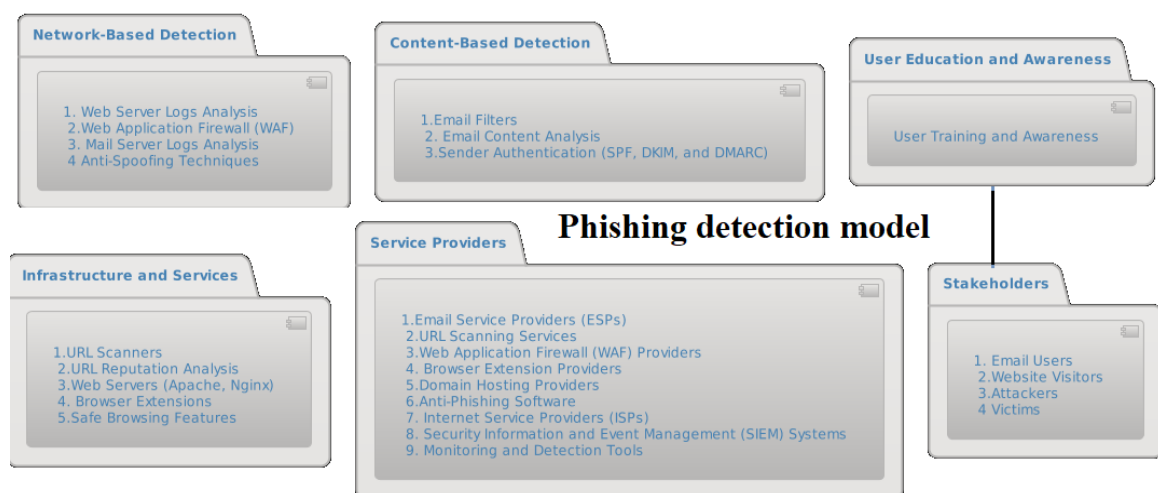


Figure 2. Multi-layered package phishing detection model

Table 2 presents a detailed comparison of various phishing detection models, highlighting their effectiveness, strengths, and limitations across different approaches. The table provides insights into the suitability of each model for specific phishing scenarios. This helps in the selection of the most appropriate detection method.

Table 2. Phishing models and its comparison

Criteria	V7Encase Forensic	FTK	MailXamine V4	eMailTrackerPro V10	Autopsy	Paraben EMX V8.6.5277	Aid4Mail v3.8
Language interface	English	English	English	English	English	English	Chinese, English
User interface	Requires training	Requires training	Easy to use	Easy to use	Easy to use	Easy to use	Easy to use
Programming language	Python	Java	Not specified	Python	Java	Java	Java
Creation of image file	Supports	Supports	Not specified	Not specified	Supports	Supports	Supports
Calculation of hash value	MD5 & SHA	MD5, SHA-1		MD5	MD5	MD5	Supports
Cost	Expensive	Expensive	Open Source	Expensive	Free	Open Source	Expensive
Regular expressions	✓	✓	✓	✓	✓	✓	✓
Header analysis tools	✓	✓	✓	✓	✓	✓	✓

#### 4. SURVEY OF CURRENT TRENDS IN PHISHING DETECTION

##### 4.1. Overview of recent advancements in phishing detection

Recent advancements in phishing detection have seen a significant shift towards more sophisticated and proactive approaches. AI and ML techniques are being used more and more to analyse enormous datasets and find minor trends that point to phishing efforts. More precise and adaptable detection techniques are now possible because to the development of behavioural analysis, anomaly detection, and NLP as major areas of concentration. Furthermore, there is potential to increase detection rates while lowering false positives through the integration of various data sources and the creation of hybrid detection systems that combine numerous methodologies. Moreover, developments in adaptive learning models and real-time analysis are improving the capacity to identify changing phishing strategies almost instantly, strengthening cybersecurity defences against phishing attempts overall.

##### 4.2. Analysis of key research papers and contributions

In this section, we will conduct an in-depth analysis of prominent research papers and contributions in the field of phishing detection. We'll look at the approaches, calculations, and assessment measures applied in these research. We will also note recurring patterns and recent advancements in phishing detection methods. By using a comparative lens, we hope to bring attention to the advantages and disadvantages of each strategy, illuminating the efficacy and relevance of different detection techniques. We want to offer significant guidance for future research areas and breakthroughs in phishing detection systems by combining ideas from these seminal research articles. Table 3 outlines the different methods and techniques used in phishing detection, categorizing them based on their approach, such as behavior-based, ML, and heuristic methods. This table provides a clear overview of the various strategies employed to identify and mitigate phishing attacks.

Table 3. Method used/techniques used in phishing

Paper	Method used/techniques/technology	Outcome	Limitation
[21]	KNN, DT, RF, genetic algorithms	High accuracy with ID3 and yet another generating genetic algorithm (YAGGA).	Relies on normalized features and excludes original URL.
[21]	RF	Achieved 99.33% accuracy.	Limited dataset size and computational cost.
[13]	Artificial neural networks	High accuracy.	Limited research and data size.
[21]	Visual similarity & DNS blacklist	Achieved 96.17% accuracy.	Limited dataset size
[22]	List-based, multistage detection with content, anchor, style, and environment (CASE) features	Efficient detection of known fraudulent websites.	Vulnerable to evasion tactics employed by sophisticated fraudsters
[18]	Detect phishing URLs in real-time, Lexical-based ML	Can detect websites mimicking legitimate ones.	Requires ongoing research and development to address evolving threats and improve accuracy.
[21]	Fuzzy set technique	Visual similarity	SVM, DT, NN
[13]	PART algorithm	List-based	including ML in some studies

#### 4.3. Identification of emerging techniques and technologies

In recent years, emerging techniques and technologies have significantly impacted the landscape of phishing detection. DL and ensemble techniques are two examples of advanced ML algorithms that are being used more and more to improve the efficiency and accuracy of detection. Furthermore, methods for behavioural analysis and anomaly detection are becoming more popular because of their capacity to spot minute patterns suggestive of phishing efforts. Furthermore, more advanced phishing content identification is made possible by the combination of semantic analysis and NLP. In addition to providing a secure means of channel verification and digital asset authentication, blockchain technology is also showing promise as a means of preventing phishing attacks. Lastly, the creation of more resilient and adaptable phishing detection systems is being made possible by developments in threat intelligence sharing platforms and cooperative efforts within cybersecurity communities.

### 5. COMPARATIVE ANALYSIS OF PHISHING DETECTION TECHNIQUES

Performance measurements for a range of ML classifiers from several studies are provided by the provided data. The models work well in general, frequently achieving accuracy, recall, F1-score, and precision above 90%. Notable classifiers with consistently good performance throughout investigations are RF and SVM. A few specialised methods, such as cantina based and heuristic-based, also demonstrate high accuracy rates of about 97% and 96%, respectively. Furthermore, ML-based methods, especially those based on RF and KNN, regularly perform well, with accuracy, recall, and precision reaching approximately 99%. All things considered, ML techniques, particularly ensemble techniques like RF, produce encouraging outcomes. Table 4 compares the performance of various phishing detection approaches, evaluating their accuracy, detection rate, and efficiency. The table highlights the strengths and limitations of each approach in real-world phishing scenarios, offering a comprehensive view of their effectiveness.

Table 4. Performance of various phishing detection approaches

Paper	Classifier	Precision (%) TP/(TP+FP)	Recall (%) TP/(TP+FN)	F1-Score (%) $2*((\text{Precision} * \text{Recall}) / (\text{Precision} + \text{Recall}))$	Accuracy (%) (TP+TN) / (TP+TN+FN+FP)
[17]	NN	99.76	98.55	99.15	99.44
	SVM	99.75	97.83	98.78	99.21
	NB	98.52	96.62	97.56	98.41
	Rule set (RS)	98.08	98.55	98.31	98.89
	RF	98.55	98.55	98.55	99.05
	Regression tree (RT)	98.31	98.31	98.31	98.89
	Heuristic based	96.00	97.56	96.76	96.76
[23]	Blacklist approach	-	-	-	84.36
	Fuzzy rule-based approach	-	-	-	100.00
	ML approach	98.39	N/A	N/A	98.4
	Cantina based approach	-	-	-	97
	Image based approach	-	-	-	98
[18]	RF	99.7	99.46	99.58	99.57
	KNN	98.67	99.45	99.06	99.04
	SVM	96.87	98.5	97.68	97.64
	Logistic regression	94.96	96.3	95.625	95.56
[19]	LightGBM	95.38	93.89	94.67	94.63
	XGBoost	95.21	93.99	94.63	94.59
	AdaBoost	94.18	91.72	93.03	92.93
	RF	91.57	94.25	94.42	94.4
	KNN	94.06	92.18	93.18	93.11
	SVM	94.15	92.95	93.59	93.55
	Logistic regression	93.57	90.91	92.33	92.22
	NB	93.84	80.73	87.72	86.79
	TF-IDF + N-gram	96.57	96.58	96.93	96.93

### 6. CHALLENGES IN PHISHING DETECTION

#### 6.1. Evolving tactics and strategies used by phishers

Phishers use complex email content, fake websites, and social engineering techniques to constantly modify and improve their methods in order to avoid discovery [24], [25]. Phishing detection systems face a big difficulty in keeping up with these changing tactics. In order to stay effective, they need to be updated and improved on a regular basis.

## **6.2. Difficulty in distinguishing legitimate from phishing emails**

Phishing emails frequently imitate official correspondence, making it difficult for both users and detection systems to distinguish between real and fake messages [26]. Phishers trick recipients by using a variety of strategies such as phony sender addresses, convincing logos, and compelling language, making it harder to identify them accurately. Additionally, phishing emails often exploit urgency or fear tactics, prompting recipients to act quickly without careful consideration. These psychological manipulations, combined with the increasing sophistication of phishing techniques, further complicate detection and response efforts.

## **6.3. Limited generalization of detection models**

Models for detecting phishing attempts that are trained on particular datasets or attributes may find it difficult to adapt successfully to brand-new, untested phishing efforts [27]. This inability to generalise might result in false positives or false negatives, which lowers the overall efficacy of detection systems and calls for constant optimisation and modification of detection algorithms. Moreover, the dynamic nature of phishing tactics, including changes in language patterns, attack vectors, and social engineering techniques, presents an ongoing challenge for detection models. As a result, continuous model retraining with updated data is essential to maintain high detection accuracy and to address emerging phishing strategies effectively.

## **6.4. Scalability and efficiency concerns in large-scale deployments**

The large-scale implementation of phishing detection technologies, especially in heterogeneous networks or huge organisations, presents resource allocation, computational efficiency, and system scalability problems [28], [29]. Effective deployment in large-scale contexts requires ensuring real-time detection and reaction capabilities while minimising resource overheads and operating costs. Furthermore, managing the diverse range of devices and systems across an organization or network can complicate the integration of phishing detection tools. Ensuring consistent and reliable performance across different environments, while maintaining security and privacy, adds another layer of complexity to large-scale deployment efforts.

# **7. FUTURE DIRECTIONS AND POTENTIAL SOLUTIONS**

## **7.1. Opportunities for improving detection accuracy and efficiency**

By improving ML algorithms, integrating real-time threat intelligence feeds, and honing feature selection strategies, there are chances to improve detection efficiency and accuracy [30], [31]. Furthermore, the utilisation of behavioural analysis and user profiling can yield significant insights into typical user behaviour, facilitating the detection of unusual behaviours suggestive of fraudulent attempts. Incorporating adaptive learning models that can evolve with changing phishing tactics will also enhance detection capabilities over time. Additionally, leveraging ensemble methods that combine multiple detection techniques could provide more robust protection against a wide range of phishing attacks.

## **7.2. Integration of emerging technologies in phishing detection**

Phishing detection capabilities can be strengthened by the incorporation of emerging technologies like blockchain, AI, and internet of things (IoT) devices. Blockchain's unchangeable ledger can improve communication channel security [32]–[34], and AI and IoT sensors can facilitate proactive monitoring and phishing attack detection on a variety of digital platforms. Moreover, AI-powered systems can analyze vast amounts of data in real-time, identifying patterns and anomalies that suggest phishing attempts. IoT devices, with their extensive network presence, can provide additional data points, enhancing the detection of suspicious activities and enabling faster responses to threats.

## **7.3. Role of artificial intelligence and machine learning in enhancing detection capabilities**

The creation of adaptive and self-learning detection models is made possible by AI and ML, which is crucial in improving phishing detection capabilities [35]–[37]. Large data sets can be analysed by these technologies to find patterns and trends that point to phishing attempts, making it possible to detect suspicious activity more quickly and accurately. Additionally, AI and ML algorithms can continuously update their models based on new data, allowing them to stay ahead of evolving phishing tactics. This ability to adapt in real-time significantly enhances the robustness and resilience of phishing detection systems.

## **7.4. Novel approaches for addressing persistent challenges**

To build a strong defense system against phishing assaults, the hybrid phishing detection architecture integrates heuristic, ML, and DL techniques [38]–[40]. It applies consistent preprocessing approaches and uses data from several sources, including phishing emails, real emails, and website metadata

[11], [21]. Heuristic list-based detection uses rule-based algorithms, such as blacklist matching, keyword matching, attachment analysis, and website examination, to identify emails and websites that have been linked to phishing schemes [10], [13]. The ML Model is trained on labelled data and uses algorithms like as RF, SVM, or XGBoost to assign probability scores to emails and websites that indicate the possibility of phishing. The DL model compares reconstructed authentic data against incoming data and uses autoencoders, or variational autoencoders (VAEs), to identify abnormalities. It then assigns higher scores to possible phishing efforts [1], [41].

User alerts, email blocking, and website warnings are made possible by the ultimate categorization of "phishing" or "legitimate," which is obtained through the integration of outputs from all levels using a weighted approach [42], [43]. A multi-layered defence system, increased precision in identifying simple and sophisticated phishing attempts, adaptability through retraining with fresh data, and a decrease in false positives are among the advantages. It is necessary to pay attention to issues like preserving data quality, allocating computational resources, and comprehending DL model decision-making. In the future, it will be important to investigate hybrid model training, include real-time threat intelligence, and analyse user behaviour to improve detection capabilities. All things considered, this hybrid design holds great promise for improving internet security against phishing scams. Finally, the architecture explores the potential of DL. Here, models like autoencoders or VAEs can reconstruct "normal" email patterns. Incoming data is compared against this reconstruction, and significant deviations trigger higher phishing scores. This approach helps identify sophisticated attempts that might bypass traditional methods. Heuristics catch common threats, ML offers adaptability through training, and DL tackles complex anomalies. This layered approach aims to achieve high accuracy in detecting both simple and sophisticated phishing attempts, while minimizing false positives.

While current phishing detection methods like ML and heuristics offer impressive accuracy, a critical gap exists in their ability to adapt to the ever-evolving tactics of phishers. This challenge stems from the potential limitation of ML models trained on specific datasets. These models may struggle to generalize effectively when encountering entirely new attack attempts, hindering their long-term effectiveness. This study highlights the significant promise of ML algorithms, particularly RF, in phishing detection. These algorithms achieve accuracy rates exceeding 90%, demonstrating their robust capabilities in identifying phishing attempts. The findings emphasize the need for a multi-faceted approach to phishing detection. While ML offers a powerful toolset, overcoming limitations like model generalizability is crucial for sustained effectiveness. This may involve incorporating additional techniques or exploring methods to enhance model adaptability. Large-scale deployments of phishing detection systems introduce scalability concerns related to resource allocation and computational efficiency.

## 8. CONCLUSION

This study provided a comprehensive examination of various methods used for phishing detection, categorizing them based on their application and exploring their advantages and disadvantages. From behavior-based to heuristic-based, ML-based and signature-based techniques, each approach offers unique strengths and limitations. Deeper into the latest developments in phishing detection research, highlighting the promising capabilities of ML-powered social media exploration and real-time website analysis. Specifically, ML algorithms like RF and SVM demonstrate high accuracy in detecting phishing attempts, while specialized techniques such as heuristic-based and cantina-based approaches show remarkable performance, indicating avenues for further research in the field. However the battle against phishing presents significant challenges. Phishers continuously evolve their strategies, employing social engineering tactics, phoney websites, and intricate email content. This necessitates regular updates and improvements to detection systems to keep pace with these changing tactics. Furthermore, the restricted generalizability of detection models, difficulties in scalability, and resource allocation pose additional hurdles in building effective defense systems against phishing assaults. To address these challenges, the hybrid phishing detection architecture offers a comprehensive solution by integrating heuristic, ML, and DL techniques. This multi-layered defense system combines the strengths of different approaches, providing increased precision in identifying both simple and sophisticated phishing attempts. However, challenges such as preserving data quality, allocating computational resources, and comprehending DL model decision-making require careful attention. Looking ahead, future research should focus on hybrid model training, real-time threat intelligence integration, and user behavior analysis to further enhance detection capabilities. Overall, the hybrid design holds great promise for improving internet security against phishing scams, underscoring the importance of ongoing innovation and collaboration in the field.

## APPENDIX

Table 1. Phishing category and technique analysis

Category and technique	Algorithm examples	Advantages	Disadvantages	Limitations
Email phishing detection	– Statistical analysis, keyword matching, regular expressions	– Rapid detection of known phishing emails	– Potential false positives	– Limited effectiveness against novel phishing tactics
– Email filters	– Logistic regression, NB	– Identifies phishing attempts based on content	– May miss sophisticated phishing techniques	– Requires frequent updates to stay effective
– Sender authentication (SPF, DKIM, and DMARC)	– Cryptographic hashing	– Verifies sender authenticity	– Ineffective against spoofing attacks	– Relies on sender cooperation and correct implementation
– User training and awareness	– Phishing simulations	– Educates users about phishing tactics	– Dependent on user behavior	– Requires training and reinforcement
Web server phishing detection	– Anomaly detection algorithms, traffic pattern analysis	– Identifies suspicious patterns in server logs (e.g., unusual access attempts)	– False positives	– May miss sophisticated attacks not reflected in logs
– Web server logs analysis	– Signature-based detection, anomaly detection	– Blocks malicious traffic in real-time based on pre-defined rules or patterns	– Reactive approach	– May introduce performance overhead
– WAF			– Configuration complexity	
Mail server phishing detection	Similar to web server logs analysis	Identifies suspicious email patterns (e.g., high volume from a single source)	Reactive approach	May miss sophisticated attacks not reflected in logs
– Mail server logs analysis				
Browser phishing detection	– Blacklist matching, heuristics	– Blocks access to known phishing sites	– Limited to specific browsers	– May introduce compatibility issues
– Browser extensions	– Blacklist matching, ML	– Warns users about potentially malicious sites based on browsing history and threat intelligence	– Limited to specific browsers	– Requires regular updates for effectiveness
– Safe browsing features				
Phishing detection methods (list-based)	– (List-based) Blacklists/whitelists	Simple and fast to implement	Static and requires frequent updates	Limited to known phishing URLs/domains
Heuristic-based	Rule-based engines	Effective for basic phishing attempts	Prone to false positives	May miss sophisticated phishing tactics
– Rule datasets				
Machine learning	Logistic regression, SVM, RF	Flexibility and adaptability to new attacks	Requires labeled data	May not handle complex phishing tactics
– Labeled phishing/non-phishing datasets				
Deep learning	Convolutional neural network (CNN) for images, recurrent neural network (RNN) for text	Captures complex patterns in data (visual elements, language style)	Requires large datasets for training	May suffer from interpretability issues
– Phishing image/text datasets				
Hybrid approaches	Ensemble methods (combining multiple algorithms)	Improved detection accuracy	Complex to implement and interpret	Requires careful model selection and tuning
– Combined labeled and image/text datasets				
Content-based analysis techniques	NLP techniques (sentiment analysis, named entity recognition), image analysis (logo detection, layout inconsistencies)	Identifies phishing attempts based on content	Requires current training data reflecting trends	Susceptible to obfuscation techniques
– Text and image datasets				
Behavioral analysis techniques	User activity monitoring, anomaly detection	Real-time detection based on user behavior patterns (e.g., rapid clicks)	Distinguishing between normal and malicious behavior	Privacy and ethical considerations
– User interaction datasets				

## REFERENCES




- [1] D. Ranganayakulu and C. Chellappan, "Detecting malicious URLs in e-mail – an implementation," *AASRI Procedia*, vol. 4, pp. 125–131, 2013, doi: 10.1016/j.aasri.2013.10.020.
- [2] G. Vrbančič, I. Fister, and V. Podgorelec, "Datasets for phishing websites detection," *Data in Brief*, vol. 33, 2020, doi: 10.1016/j.dib.2020.106438.
- [3] N. Beu *et al.*, "Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation," *Computers and Security*, vol. 131, 2023, doi: 10.1016/j.cose.2023.103313.
- [4] R. Hoheisel, G. V. Capelleveen, D. K. Sarmah, and M. Junger, "The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains," *Computers and Security*, vol. 128, 2023, doi: 10.1016/j.cose.2023.103158.
- [5] A. Wu, Z. Feng, X. Li, and J. Xiao, "ZTWeb: Cross site scripting detection based on zero trust," *Computers and Security*, vol. 134, 2023, doi: 10.1016/j.cose.2023.103434.

- [6] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Computers and Security*, vol. 132, 2023, doi: 10.1016/j.cose.2023.103387.
- [7] L. Sawe, J. Gikandi, J. Kamau, and D. Njuguna, "Sentence level analysis model for phishing detection using KNN," *Journal of Cyber Security*, vol. 6, pp. 25–39, 2024, doi: 10.32604/jcs.2023.045859.
- [8] E. J. Williams and A. N. Joinson, "Developing a measure of information seeking about phishing," *Journal of Cybersecurity*, vol. 6, no. 1, pp. 1–16, 2020, doi: 10.1093/cybsec/tyaa001.
- [9] N. A. Azeez and E. Anochirionye, "Detecting malicious and compromised URLs in e-mails using association detecting malicious and compromised URLs in e-mails using association rule," *Covenant Journal of Informatics & Communication Technology*, vol. 5, no. 2, 2017.
- [10] A. A. Orunsolu, A. S. Sodiya, and A. T. Akinwale, "A predictive model for phishing detection," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 2, pp. 232–247, 2022, doi: 10.1016/j.jksuci.2019.12.005.
- [11] G. Palaniappan, S. Sangeetha, B. Rajendran, Sanjay, S. Goyal, and B. S. Bindhumadhava, "Malicious domain detection using machine learning on domain name features, host-based features and web-based features," *Procedia Computer Science*, vol. 171, pp. 654–661, 2020, doi: 10.1016/j.procs.2020.04.071.
- [12] S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "A systematic literature review on phishing email detection using natural language processing techniques," *IEEE Access*, vol. 10, pp. 65703–65727, 2022, doi: 10.1109/ACCESS.2022.3183083.
- [13] C. Opara, Y. Chen, and B. Wei, "Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics," *Expert Systems with Applications*, vol. 236, 2024, doi: 10.1016/j.eswa.2023.121183.
- [14] S. D. Gupta, K. T. Shahriar, H. Alqahtani, D. Alsalmán, and I. H. Sarker, "Modeling hybrid feature-based phishing websites detection using machine learning techniques," *Annals of Data Science*, vol. 11, no. 1, pp. 217–242, 2024, doi: 10.1007/s40745-022-00379-8.
- [15] S. K. Punia, M. Kumar, T. Stephan, G. G. Deverajan, and R. Patan, "Performance analysis of machine learning algorithms for big data classification: ML and AI-based algorithms for big data analysis," *International Journal of E-Health and Medical Communications*, vol. 12, no. 4, pp. 60–75, 2021, doi: 10.4018/IJEHMC.20210701.oa4.
- [16] L. Liu, O. D. Vel, Q. L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: a survey," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 2, pp. 1397–1418, 2018, doi: 10.1109/COMST.2018.2800740.
- [17] S. Paliath, M. A. Qbeitah, and M. Aldwairi, "Phishout: Effective phishing detection using selected features," in *2020 27th International Conference on Telecommunications (ICT)*, 2020, pp. 1–5, doi: 10.1109/ICT49546.2020.9239589.
- [18] B. B. Gupta, K. Yadav, I. Razzak, K. Psannis, A. Castiglione, and X. Chang, "A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment," *Computer Communications*, vol. 175, pp. 47–57, 2021, doi: 10.1016/j.comcom.2021.04.023.
- [19] M. S. -Paniagua, E. F. Fernandez, E. Alegre, W. Al-Nabki, and V. G.-Castro, "Phishing URL detection: A real-case scenario through login URLs," *IEEE Access*, vol. 10, pp. 42949–42960, 2022, doi: 10.1109/ACCESS.2022.3168681.
- [20] S. Gerke, T. Minssen, and G. Cohen, "Ethical and legal challenges of artificial intelligence-driven healthcare," *Artificial Intelligence in Healthcare*, pp. 295–336, 2020, doi: 10.1016/B978-0-12-818438-7.00012-5.
- [21] A. Safi and S. Singh, "A systematic literature review on phishing website detection techniques," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 2, pp. 590–611, 2023, doi: 10.1016/j.jksuci.2023.01.004.
- [22] D. J. Liu, G. G. Geng, X. B. Jin, and W. Wang, "An efficient multistage phishing website detection model based on the CASE feature framework: Aiming at the real web environment," *Computers and Security*, vol. 110, 2021, doi: 10.1016/j.cose.2021.102421.
- [23] G. J. W. Kathrine, P. M. Praise, A. A. Rose, and E. C. Kalaivani, "Variants of phishing attacks and their detection techniques," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019, pp. 255–259, doi: 10.1109/ICOEI.2019.8862697.
- [24] F. V. Farahani, K. Fiok, B. Lahijanian, W. Karwowski, and P. K. Douglas, "Explainable AI: A review of applications to neuroimaging data," *Frontiers in Neuroscience*, vol. 16, 2022, doi: 10.3389/fnins.2022.906290.
- [25] B. Mahbooba, M. Timilsina, R. Sahal, and M. Serrano, "Explainable artificial intelligence (XAI) to enhance trust management in intrusion detection systems using decision tree model," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/6634811.
- [26] E. Tjoa and C. Guan, "A survey on explainable artificial intelligence (XAI): toward medical XAI," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 11, pp. 4793–4813, 2021, doi: 10.1109/TNNLS.2020.3027314.
- [27] M. Vorokhob, R. Kyrychok, V. Yaskevych, Y. Dobryshyn, and S. Sydorenko, "Modern perspectives of applying the concept of zero trust in building a corporate information security policy," *Cybersecurity: Education, Science, Technique*, vol. 1, no. 21, pp. 223–233, 2023, doi: 10.28925/2663-4023.2023.21.223233.
- [28] S. Ghasemshirazi, G. Shirvani, and M. A. Alipour, "Zero trust: applications, challenges, and opportunities," *arXiv-Computer Science*, pp. 1–23, 2023.
- [29] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and application of zero trust security: a brief survey," *Entropy*, vol. 25, no. 12, 2023, doi: 10.3390/e25121595.
- [30] S. R. Oh, Y. D. Seo, E. Lee, and Y. G. Kim, "A comprehensive survey on security and privacy for electronic health data," *International Journal of Environmental Research and Public Health*, vol. 18, no. 18, 2021, doi: 10.3390/ijerph18189668.
- [31] S. Li, M. Iqbal, and N. Saxena, "Future industry internet of things with zero-trust security," *Information Systems Frontiers*, 2022, doi: 10.1007/s10796-021-10199-5.
- [32] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of zero trust networks in cloud computing: a comparative review," *Sustainability*, vol. 14, no. 18, 2022, doi: 10.3390/su141811213.
- [33] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, 2019, doi: 10.3390/FI11040089.
- [34] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: Threats, mitigation and approaches," *BMJ Health and Care Informatics*, vol. 26, no. 1, 2019, doi: 10.1136/bmjhci-2019-100031.
- [35] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity threats and their mitigation approaches using machine learning—a review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 527–555, 2022, doi: 10.3390/jcp2030027.
- [36] E. M. Maseno, "Vishing attack detection model for mobile users," *M.Sc. Thesis*, Faculty of Computing and Information Management, KCA University, Nairobi, Kenya, 2017.
- [37] T. Chin, K. Xiong, and C. Hu, "Phishlimiter: A phishing detection and mitigation approach using software-defined networking," *IEEE Access*, vol. 6, pp. 42513–42531, 2018, doi: 10.1109/ACCESS.2018.2837889.
- [38] S. Ashfaq, S. A. Patil, S. Borde, P. Chandre, P. M. Shafi, and A. Jadhav, "Zero trust security paradigm: a comprehensive survey and research analysis," *Journal of Electrical Systems*, vol. 19, no. 2, pp. 28–37, 2023, doi: 10.52783/jes.688.




- [39] P. M. Bhujbal, A. Jadhav, J. N. Nandimath, P. S. Kadam, P. R. Chandre, and P. N. Mahalle, "Zero trust paradigm: advancements, challenges, and future directions in cybersecurity," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 19s, pp. 613–623, 2024.
- [40] S. Ashfaq, P. Chandre, S. Pathan, U. Mande, M. Nimbalkar, and P. Mahalle, "Defending against vishing attacks: a comprehensive review for prevention and mitigation techniques," in *Cyber Security and Digital Forensics*, 2024, pp. 411–422, doi: 10.1007/978-981-99-9811-1\_33.
- [41] M. S. -Paniagua, E. Fidalgo, E. Alegre, and R. A. -Rodríguez, "Phishing websites detection using a novel multipurpose dataset and web technologies features," *Expert Systems with Applications*, vol. 207, 2022, doi: 10.1016/j.eswa.2022.118010.
- [42] R. J. V. Geest, G. Cascavilla, J. Hulstijn, and N. Zannone, "The applicability of a hybrid framework for automated phishing detection," *Computers and Security*, vol. 139, 2024, doi: 10.1016/j.cose.2024.103736.
- [43] L. Ribeiro, I. S. Guedes, and C. S. Cardoso, "Which factors predict susceptibility to phishing? An empirical study," *Computers and Security*, vol. 136, 2024, doi: 10.1016/j.cose.2023.103558.

## BIOGRAPHIES OF AUTHORS



**Prof. Ashvini Jadhav**    is a research scholar and a professional in the field of Computer Science and Engineering, specializing in computer networks. She obtained her Master's degree in Computer Science and Engineering (Computer Network) from G H Raisoni College of Engineering and Management, Wagholi, in 2013. Currently, she serves as a dedicated Assistant Professor in department of information technology at the MIT School of Computing in Loni, Pune, where she shares her extensive knowledge and expertise with aspiring computer engineers. With more than 14 years of hands-on experience in Computer Engineering, Ashvini has honed her skills across various domains within the discipline, with a specific focus on computer networks, cyber security, and programming. Her dedication to advancing the field of computer science is underscored by her on-going pursuit of a Ph.D. at the MIT School of Computing, MIT ADT, Pune, India where she is actively involved in pioneering research endeavours. She can be contacted at email: ashvinigjadhav@gmail.com.



**Dr. Pankaj R. Chandre**    has obtained his B.E degree in Information Technology from Sant Gadge Baba Amravati University, Amravati, India, M.E. degree in Computer Engineering from from Mumbai University Maharashtra, India in the year 2011 and Ph.D. in Computer Engineering from Savitribai Phule Pune University, Pune, India in the year 2021. He is currently working as an Associate Professor in Department of Computer Science and Engineering, MIT School of Computing, MIT ADT, Pune, India. He has published 60 plus papers at international journals and conferences. He has guided more than 30 plus undergraduate students and 20 plus postgraduate students for projects. His research interests are network security and information security. He can be contacted at email: pankaj.chandre@mituniversity.edu.in.