IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 March 2025, accepted 14 April 2025, date of publication 29 April 2025, date of current version 9 May 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3565619

RESEARCH ARTICLE

Decoding Phishing Evasion: Analyzing Attacker Strategies to Circumvent Detection Systems

A. GHAFOOR[1], M. A. SHAH[2], M. A. AL-NAEEM[2], AND C. MAPLE[3]
[1]Department of Cyber Security, Air University, Islamabad 46000, Pakistan
[2]Department of Computer Networks and Communication, King Faisal University (KFU), Al Ahsa 31982, Saudi Arabia
[3]WMG, University of Warwick, CV4 7AL Coventry, U.K.

Corresponding author: C. Maple (cm@warwick.ac.uk)

This work was supported in part by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under Grant KFU251500; in part by U.K. Research and Innovation (UKRI) funded by the Engineering and Physical Sciences Research Council (EPSRC) through the Framework for Responsible AI in Finance under Grant EP/V056883/1, through the Academic Centre of Excellence in Cyber Security Research—University of Warwick under Grant EP/R007195/1, and through The Alan Turing Institute under Grant EP/N510129/1.

ABSTRACT Phishing remains a critical security threat, involving the creation of fraudulent websites to capture sensitive information. Despite existing detection systems, sophisticated attackers have developed advanced evasion techniques that undermine these defenses. This paper highlights the significant challenge of these novel methods, focusing on how attackers manage to prolong the operational lifespan of phishing sites. Our research investigates how attackers circumvent traditional security layers by employing a combination of target filtering mechanisms, bot detection evasion, blacklisting avoidance, and honeypots. Our experimental findings indicate that these evasion strategies can achieve an effectiveness rate of 80% to 85% in extending the viability of phishing sites. We have empirically demonstrated the exposure of current systems to these attacks, revealing specific vulnerabilities and exploitation points. These results underscore the urgent need for enhanced detection frameworks that address the layered and adaptive nature of modern phishing tactics. Our work highlights a critical gap in current security measures and poses a challenge to solution providers: there is a pressing need for novel mitigations to safeguard users against these sophisticated phishing threats.

INDEX TERMS Anti-phishing strategies, bot detection, captcha, cybersecurity, evasion techniques, honeypot, phishing detection.

I. INTRODUCTION

Phishing continues to be a dominant threat in the cybersecurity domain, characterized by the creation of fraudulent websites that closely resemble legitimate ones. The primary objective of these deceptive sites is to trick unsuspecting users into exposing sensitive information, such as passwords, credit card numbers, and other personal data. This illegitimate activity poses severe risks not only to individual users but also to organizations, leading to significant financial losses and damage to reputations. The persistent success of phishing campaigns, despite the widespread use of advanced detection systems, raises critical questions about the robustness of current cybersecurity measures and the strategies employed by attackers to evade them. Fig. 1 presents a graph illustrating the number of unique phishing sites detected globally from the third quarter of 2013 through the first quarter of 2024. The data demonstrates a consistent upward trend in the prevalence of phishing sites over this period.

Over the years, phishing techniques have evolved considerably, becoming increasingly sophisticated in their ability to bypass traditional detection mechanisms. Early studies, such as those by AlEroud and Karabatis [2], highlighted the basic evasion tactics used by phishing sites, including simple URL obfuscation and the use of misleading domain names. However, as detection technologies advanced, so too

The associate editor coordinating the review of this manuscript and approving it for publication was João Bernardo Ferreira Sequeiros.

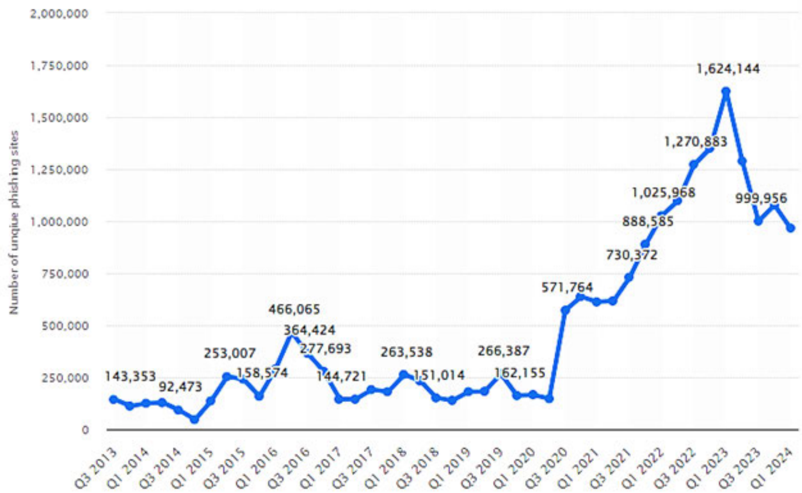

FIGURE 1. Number of global phishing sites Q3 2013- Q1 2024 [1].

did the complexity of phishing methods. More recent research has documented the integration of advanced techniques such as bot detection, target filtering, and the use of CAPTCHA systems to thwart automated detection tools [3], [4]. These techniques enable attackers to prolong the lifespan of phishing sites, making them more resilient to being flagged or taken down by security systems.

Despite the growing corpse of literature on phishing detection, a significant gap remains in the comprehensive understanding of how these evasion techniques can be systematically combined to maximize their effectiveness. Lee et al. [5] and Rao and Pais [6] have discussed individual strategies such as the use of dynamic content and geographic filtering, yet few studies have explored the synergistic effects of combining multiple evasion tactics. This gap is particularly concerning given the increasing sophistication of phishing campaigns, which often employ a multi-layered approach to evade detection. Addressing this gap is crucial for developing more effective countermeasures that can keep pace with the evolving threat landscape.

In response to this gap, this study systematically investigates the integration of several advanced evasion techniques, including target filtering mechanisms, bot detection strategies, blacklisting avoidance, and the deployment of honeypots. By rigorously evaluating each technique's effectiveness through a series of controlled experiments, this research aims to develop a novel cumulative approach that significantly enhances the stealth of phishing sites. The methodology employed in this study includes both direct access filtering and CAPTCHA implementation, which are visually represented in Fig. 2 and Fig. 3. These figures illustrate the layered defense mechanisms used to protect phishing sites from detection by public crawlers and other automated systems.

The importance of this research lies in its potential to inform the development of next-generation detection frameworks that are capable of countering these sophisticated

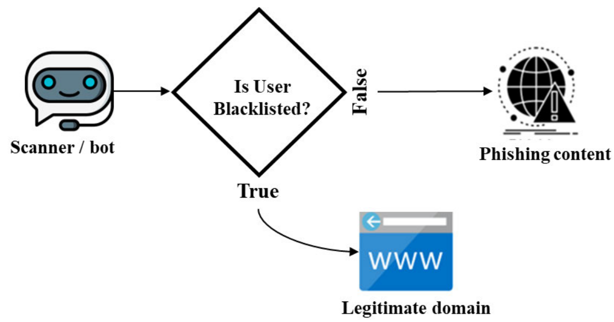

FIGURE 2. Bot filtering methodology to bypass anti-phishing systems.

evasion strategies. Current detection methods, which often rely on static and reactive measures, are increasingly inadequate in the face of dynamic and adaptive phishing techniques. By extending the operational lifespan of phishing sites, these evasion tactics not only increase the success rate of phishing campaigns but also complicate the efforts of cybersecurity professionals to track and mitigate these threats. Consequently, the findings of this study have significant implications for both the academic community and the cybersecurity industry, particularly in the areas of threat intelligence and incident response.

Moreover, the study's comprehensive analysis of the effectiveness of combined evasion techniques provides valuable insights into the operational strategies of cyber attackers. This knowledge is critical for developing more proactive defense mechanisms that can anticipate and neutralize threats before they become widespread. The cumulative approach proposed in this research, which integrates direct access filtering, CAPTCHA implementation, and honeypots, is detailed in Table 1, where the efficiency rates of each technique are compared. The results demonstrate a significant increase in the resilience of phishing sites, with efficiency rates ranging between 80% and 85% as shown in (1) and (2). These findings

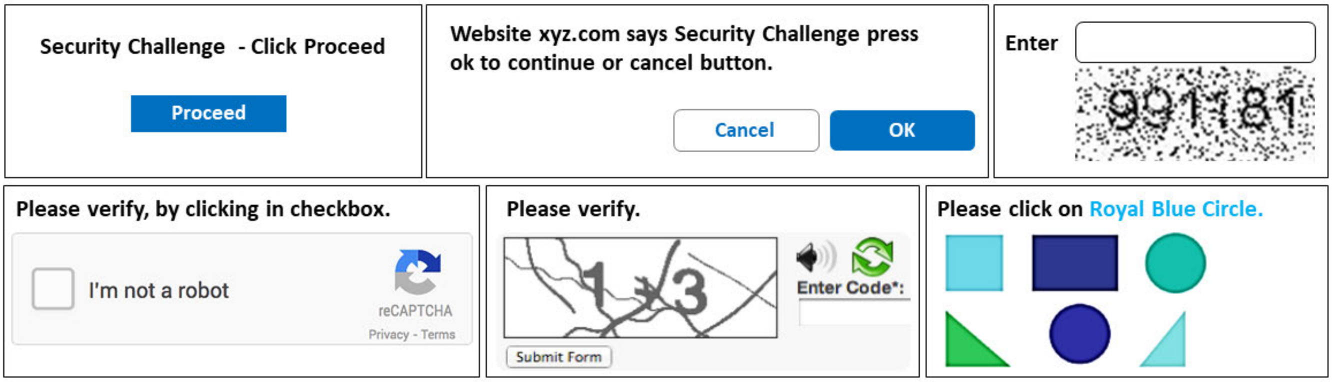

FIGURE 3. Various CAPTCHAs deployed in phishing sites to avoid anti-phishing systems.

are corroborated by similar studies, such as those conducted by Smith and Jones [7], which emphasize the need for more dynamic and adaptable detection systems.

TABLE 1. Efficiency rate of each technique.

Symbol	Efficiency Rates	Details
HF	94%	the effectiveness of the honeypot technique
RF	89%	the effectiveness of the region filter technique magnetic induction
CF	91%	the effectiveness of the CAPTCHA technique
USF	76%	the effectiveness of the user screen filter technique
UAF	84%	the effectiveness of the user-agent filter technique
DA	63%	the effectiveness of the direct access technique
P	82.83%	the probability of a website being live for the campaign's end

$$P = \frac{\sum(\text{RF, HF, CF, USF, UAF, DA})}{N} \tag{1}$$

$$P = 82.83\% \tag{2}$$

In conclusion, this research provides a critical examination of the methods used by attackers to sustain their malicious activities over extended periods. By offering a detailed analysis of advanced evasion techniques and their combined effects, this study contributes to the ongoing discourse on cybersecurity and underscores the urgent need for enhanced detection strategies. The insights gained from this research not only highlight the vulnerabilities of current systems but also suggest practical steps that can be taken to improve the detection and mitigation of phishing attacks. As the threat landscape continues to evolve, it is imperative that the cybersecurity community remains vigilant and adaptive, continually refining its tools and techniques to stay ahead of increasingly sophisticated adversaries.

A. RESEARCH CONTRIBUTION

The insights gained from this research not only highlight the vulnerabilities of current systems but also suggest practical steps to improve phishing detection. This study makes the following contributions:

- **Identification of Advanced Evasion Techniques:** A systematic analysis of attacker strategies (e.g., bot detection evasion, CAPTCHA abuse) to bypass modern anti-phishing systems.
- **BYPHISH Framework:** Development of a multi-layered evasion framework integrating honeypots, CAPTCHA, and adaptive filtering, achieving an 82.83% success rate.
- **Empirical Validation:** Controlled experiments over 10 days demonstrate how combined techniques prolong phishing site lifespan, even under free hosting constraints.
- **Operational Insights:** Analysis of usability trade-offs (e.g., CAPTCHA friction) and scalability challenges for real-world deployment.

These contributions address critical gaps in phishing research and provide a roadmap for next-generation detection systems. The remainder of this paper is structured as follows: Section II reviews related work; Section III details the BYPHISH framework; Section IV presents experimental results; Section V concludes with future directions.

II. LITERATURE REVIEW

A. EXPLOITATION OF ONLINE ADVERTISING IN PHISHING ATTACKS

The modern Internet economy thrives on online advertising, a key revenue source for platforms such as Google and YouTube. However, these advertising channels have also become tools for cybercriminals, particularly phishers, to deploy their deceptive tactics. Phishers exploit these platforms by creating advertisements that appear legitimate but are designed to redirect users to phishing sites or distribute malware once approved by security systems [12].

For instance, attackers often create ads related to popular topics like cryptocurrency. These ads, when clicked, lead users to phishing websites that mimic legitimate sites to harvest sensitive information, such as login credentials.

TABLE 2. Overview of techniques and limitations in phishing detection and evasion research.

Paper	Problem	Technique	Limitation
[25]	Bypassing anti-phishing systems through scripting attacks on vulnerable web applications.	A black-box approach that analyzes HTML automatically and blocks script execution using a reverse proxy server tool.	Advanced script injections, particularly those using obfuscation techniques, can evade this detection method, compromising the system.
[31]	Evasion of detection mechanisms through transcoding and advanced scripting on online platforms.	WSAD approach uses a ten-feature model with regular expressions to detect malicious requests, clustering anomalies based on detected features.	Scripts with pre-execution anomalies may bypass the detection, leading to potential security breaches.
[33]	Use of bots in phishing campaigns to spread misinformation and bypass anti-phishing measures on social media.	Machine learning-based bot detection using a neural network trained with supervised and hierarchical algorithms.	Bots that adapt and mimic human behavior can evade detection, making it difficult to maintain accuracy over time.
[34]	Coordinated botnet attacks spreading phishing content and false information, evading traditional detection systems.	Procedural analysis of web traffic on the host side to identify botnets using techniques such as: Honey net detection, Host-based detection, Protocol violation detection, and Signature-based detection.	Adaptive bots that alter their behavior in response to detection mechanisms can still operate undetected, causing significant harm.
[36]	Phishing attacks using XSS, CSRF, and other scripting methods to infiltrate web systems and avoid detection.	WAVE provides a proactive security solution by filtering web traffic and dynamically detecting malicious scripts.	Encryption and obfuscation techniques used by attackers remain challenging to detect, posing a continued threat to security.
[41]	Generating fake traffic through web crawlers to overwhelm detection systems and support phishing operations.	Automated traffic capture and mining algorithms are applied to filter out crawler-generated traffic from legitimate user traffic.	Complex obfuscated scripts and advanced attacks are difficult to distinguish from legitimate traffic, leading to potential system overloads.
[42]	Tracking and filtering out advanced bots and crawlers used in phishing schemes that mimic legitimate users.	Peer-to-peer tracking using CART combined with virtual IP conversion to identify and filter out bots and crawlers.	Bots that closely replicate human behavior are challenging to differentiate, increasing the risk of successful phishing campaigns.
[43]	Botnet attacks designed to disrupt server availability and evade detection, causing business losses and facilitating phishing.	Behavioral-based detection combined with pattern-based detection and SVM models to identify and block malicious traffic.	Despite robust security measures, sophisticated attackers can still breach defenses, particularly through insider threats or advanced persistent threats.
[44]	Exploiting legitimate web forms to execute phishing queries and extract sensitive data from servers.	Dynamic analysis and regular expression filtering to block specific keywords and detect malicious traffic.	Advanced evasion techniques that avoid keyword detection pose a risk of undetected phishing activities.

Once credentials are stolen, attackers can access accounts or transfer cryptocurrency to their wallets. Despite the

TABLE 3. Adversary solutions and limitations in phishing evasion research.

Paper	Problem	Technique	Limitation
[17]	Search engine bots, web scanners, and web crawlers triggering phishing web pages by indexing or surfing content.	A semantic approach using four parameters to detect bots: Syntactic log analysis, Analytical learning analysis, Traffic pattern analysis, and Turing test systems.	Security bots that adapt their behavior to mimic real users can evade these detection methods, posing a significant challenge.
[35]	Hosting web scanners blocking phishing content when it goes online, thereby reducing the lifespan of phishing sites.	Detection of web scanning methods and blacklisting these systems to maintain website uptime. This is achieved through deep neural network analysis, which filters online sessions by categorically, numerically, and Boolean feature methods.	Security scanners are continuously evolving with advanced research and techniques, which can dynamically adapt and detect phishing content despite the blacklisting efforts.

implementation of phishing detection tools like VirusTotal, URLVoid, and TrendMicro, attackers manage to circumvent these systems. Among these, URLVoid has demonstrated a relatively higher detection accuracy of 73%, attributed to its integration with multiple URL scanning engines [13]. This exploitation underscores the necessity for more advanced and adaptive security measures capable of identifying and mitigating these deceptive tactics. Fig. 4 illustrates some commonly used phishing detection techniques in cybersecurity.

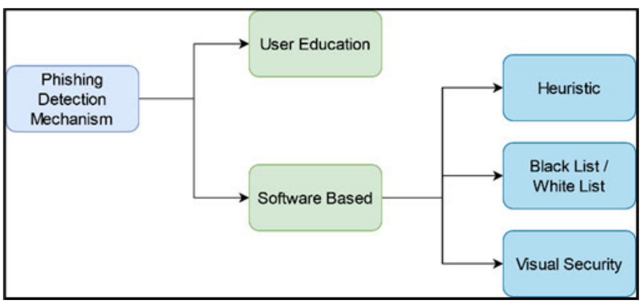

FIGURE 4. Phishing detection techniques.

B. EVOLUTION OF PHISHING TECHNIQUES AND OFFENSIVE SECURITY MEASURES

Phishing techniques have evolved significantly, becoming increasingly sophisticated and difficult to detect. Traditional security measures, while foundational, have proven inadequate against the adaptive nature of phishing attacks. Attackers continually refine their strategies, utilizing advanced evasion techniques such as bot detection, CAPTCHA implementations, and target filtering, which have made phishing sites more resilient against detection and takedown efforts.

Offensive security approaches have gained prominence as an effective countermeasure to these evolving threats. Techniques such as web application forensics and the deployment of honeypots are crucial in understanding and countering phishing strategies. Honeypots, specifically designed to attract and monitor attackers, gather valuable data that can be analyzed to enhance detection systems. This proactive approach enables cybersecurity professionals to anticipate and neutralize threats before they escalate [14].

Moreover, the rise of bots in the online environment adds complexity to phishing detection. Bots, often used to automate and scale phishing attacks, can generate fake traffic and overwhelm security systems. Advanced machine learning models are being developed to distinguish between human users and bots by analyzing behavioral patterns such as keystrokes, mouse movements, and interaction sequences. Studies, such as those conducted on the Sina-Weibo platform, have demonstrated high accuracy in identifying bot activities, highlighting the critical role of machine learning in enhancing anti-phishing measures [15].

C. ADVANCED EVASION TECHNIQUES AND PHISHING COUNTERMEASURES

The persistence of phishing attacks, despite the deployment of advanced detection systems, indicates the effectiveness of evasion techniques employed by attackers. Drive-by download attacks, where users unknowingly download malware by clicking on deceptive links, represent one of the most insidious threats in the phishing landscape. Tools like Ziffersystem have been developed to monitor network traffic for suspicious patterns and automatically respond to potential threats in real-time. The ability of such systems to operate effectively with minimal data input underscores their value in the cybersecurity arsenal [16].

Another critical challenge is detecting and mitigating bot-driven phishing attacks. Machine learning models, particularly those based on decision tree classifiers, have shown promise in improving the accuracy of bot detection. These models analyze web session data to identify anomalies indicative of bot activity, achieving accuracy rates as high as 83% [17]. The application of these models in real-world scenarios has proven effective in reducing the impact of bot-driven phishing attacks.

As attackers continue to refine their evasion strategies, defenders must adopt more sophisticated countermeasures. For instance, cloud-based bots represent a new frontier in phishing attacks, requiring advanced detection techniques that combine real-time monitoring with deep behavioral analysis. Studies have shown that multi-layered detection approaches can achieve accuracy rates exceeding 93% in identifying cloud bot activities, demonstrating the effectiveness of these methods in real-world applications [18].

In response to the evolving threat landscape, unsupervised learning techniques are being explored for phishing and bot detection. Algorithms like DBSCAN and OPTICS are used to analyze HTTP requests, clustering them based on patterns that distinguish between legitimate users and bots [19]. These techniques have been particularly effective in scenarios where bots mimic human interactions, providing a robust solution to a complex problem.

Additionally, reCAPTCHA remains a critical tool in the defense against automated bots. By challenging users with tasks that are simple for humans but difficult for bots, reCAPTCHA prevents unauthorized access to sensitive information. Advanced machine learning techniques such as XGBoost and LightGBM have been employed to enhance reCAPTCHA's accuracy in detecting bots, achieving success rates of up to 97% [20]. Fig. 3 illustrates various CAPTCHA methods deployed on phishing sites to bypass detection systems [45].

D. PHISHING DETECTION THROUGH URL ANALYSIS AND NETWORK TRAFFIC MONITORING

Phishing detection has increasingly focused on analyzing URLs, as attackers continuously adapt their strategies to bypass traditional security measures. Deep learning models have been developed to scrutinize URLs for signs of phishing, but adversaries have countered these efforts by employing adversarial examples—slight modifications to URLs designed to evade detection. Research indicates that such adversarial techniques can significantly disrupt classification models, leading to a 60% to 70% success rate in evading detection, underscoring the need for more resilient anti-phishing systems [21].

Network traffic analysis has also emerged as a crucial aspect of phishing detection, particularly as attackers leverage AI-based malware that adapts to different environments. These next-generation threats use techniques such as encryption and polymorphism to avoid detection by traditional methods. In response, statistical HTTP filter-based techniques have been developed to analyze network traffic for patterns indicative of malicious activity. These methods have demonstrated success rates of up to 98.7% in filtering out malicious traffic, proving their effectiveness in the cybersecurity landscape [22].

Web crawlers, tools traditionally used for indexing and data gathering, have also been weaponized by attackers to create fake traffic and disrupt legitimate services. Detecting this malicious traffic requires advanced intrusion detection systems like Snort, which analyze network data for signs of attack. By employing pre-processing techniques that train detection models on potential threats, these systems can effectively prevent disruptions caused by malicious web crawlers [23].

To further secure web applications against threats like script injection attacks, clustering techniques used in black-box testing have proven effective in identifying vulnerabilities. These methods scan for potential injection points and generate comprehensive reports that help administrators fortify their applications against future exploits [24]. Fig.5

demonstrates the application of machine learning in phishing detection, showcasing the efficacy of these approaches in protecting web applications from sophisticated threats [45].

E. SECURING WEB APPLICATIONS FROM ADVANCED PHISHING TECHNIQUES AND BOTNET ATTACKS

Securing web applications against advanced phishing techniques and botnet attacks is a critical aspect of modern cybersecurity. Script injection attacks, including SQL injection and cross-site scripting (XSS), remain among the most dangerous threats, as they exploit vulnerabilities in web applications to inject malicious code. To combat these threats, black-box testing approaches are used to analyze input data and block malicious scripts before they reach the server [25]. These techniques are further enhanced by dynamic analysis tools that monitor network traffic in real-time, detecting and neutralizing scripts that pose a threat to the network environment. The proliferation of bots on social media platforms has also exacerbated the problem of phishing, as bots are often used to spread misinformation and manipulate public opinion. Machine learning algorithms, including neural networks and hierarchical clustering, are employed to detect and filter out bot-generated content. These methods are crucial in maintaining the integrity of digital environments, particularly on platforms where user-generated content is prevalent [27].

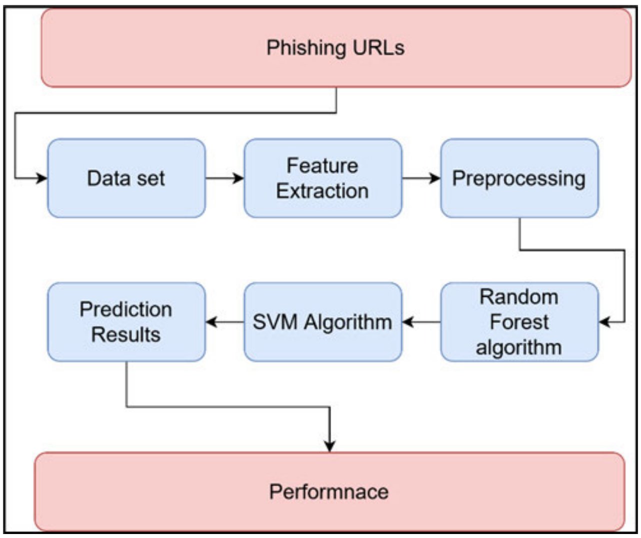

FIGURE 5. Illustration of a machine learning approach for detecting phishing URLs.

Botnets, networks of compromised devices used to launch large-scale phishing attacks, pose a significant threat to cybersecurity. To counter these threats, honeypot-based techniques are used to lure bots into decoy systems, where their behavior can be studied and neutralized. These techniques, when combined with signature-based detection methods, improve the accuracy of botnet detection [28]. Intrusion detection systems and other network security tools are also employed to monitor traffic for signs of botnet activity, providing a comprehensive defense against these threats.

In offline environments, detecting bots requires a different approach. Techniques such as HTTP periodic prediction systems and neural networks are used to analyze user behavior over time, distinguishing between legitimate users and bots [29]. These systems rely on a range of parameters, including categorical, numerical, and Boolean features, to classify and filter out bot traffic, ensuring the security of online platforms. Fig. 5 illustrates a machine learning approach for detecting and categorizing phishing URLs to promptly identify and avoid phishing attacks.

Web scanning procedures play a vital role in safeguarding user data stored in web application databases. Tools like WAVE offer proactive solutions by analyzing web traffic in real-time, identifying vulnerabilities, and preventing attacks such as cross-site scripting (XSS) and cross-site request forgery (CSRF) [30]. These tools, combined with deep neural network-based analysis, provide powerful means of securing web applications against a wide range of threats [31]. Tables 2 and 3 summarize the key findings from past research, categorizing them based on the overview of techniques and limitations in phishing detection and evasion research, as well as adversary solutions.

III. PROPOSED SYSTEM: BYPHISH-A PHISHING EVASION FRAMEWORK

In response to the increasing sophistication of phishing detection mechanisms, this research introduces BYPHISH, a comprehensive tool developed in PHP and JavaScript, designed to enhance the resilience of phishing websites by employing advanced evasion strategies. BYPHISH integrates multiple layers of filtering techniques, honeypots, and CAPTCHA systems to systematically bypass modern detection systems, thereby extending the operational lifespan of phishing sites. This section delineates the architecture, functionality, and efficacy of BYPHISH, which is meticulously aligned with the research objectives.

A. SYSTEM DESIGN AND ARCHITECTURE

The architecture of BYPHISH is modular, comprising several interlinked components that work in concert to detect, assess, and neutralize threats posed by scanners and bots. The system's core functionality is built around the ability to dynamically adapt to incoming requests, discerning between legitimate users and detection systems. As illustrated in Fig. 6, the passive filtering module serves as the foundation for BYPHISH's defensive capabilities, where it begins by collecting vital data through decoy campaigns, which are crucial for subsequent active filtering operations.

1) PASSIVE FILTERING MECHANISM

Passive filtering acts as an initial line of defense by gathering information on potential threats through the deployment of decoy campaigns. These campaigns are designed to interact with online scanners, both free and paid, capturing

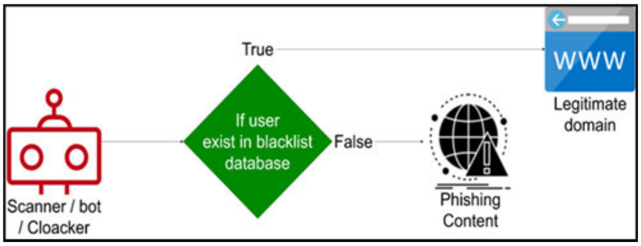

FIGURE 6. Passive filtering process in BYPHISH, capturing scanner/bot identifiers to build a blacklist and block threats before they reach phishing content.

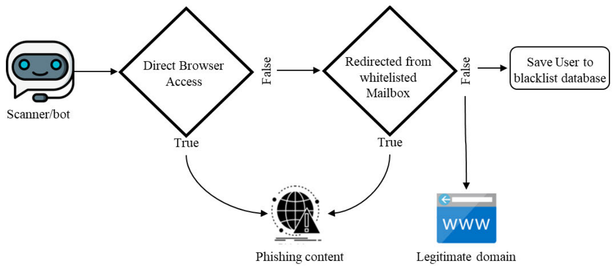

FIGURE 7. Active filtering process in BYPHISH, capturing scanner/bot identifiers to build a blacklist and block threats before they reach phishing content.

IP addresses and other identifiers that are instrumental in constructing a robust blacklist. The gathered data is then used to inform and refine the active filtering processes, ensuring that BYPHISH is equipped to preemptively block known threats before they can interact with the actual phishing content. Fig. 6 illustrates the process of passive filtering, highlighting its role in the overall system architecture.

2) ACTIVE FILTERING TECHNIQUES

Active filtering builds upon the data collected during the passive phase, implementing real-time detection strategies that assess each incoming request based on a set of predefined parameters. This module is critical in ensuring that only legitimate traffic is granted access to the phishing content. A key component of active filtering is the direct access technique, which leverages both historical data and honeypots to identify and block suspicious requests. The technique functions by monitoring the source of each request, particularly focusing on whether the request is directly accessing the content or being redirected from a legitimate domain. Requests that do not conform to the expected patterns are immediately blacklisted, as depicted in Fig. 7.

3) USER-AGENT FILTERING

To further enhance its detection capabilities, BYPHISH employs user-agent filtering, which scrutinizes the user-agent strings of incoming requests to identify known bots and crawlers. Common user-agent identifiers such as "Googlebot," "Bingbot," and "Slurp" are flagged, and any request containing these identifiers is blocked from accessing the

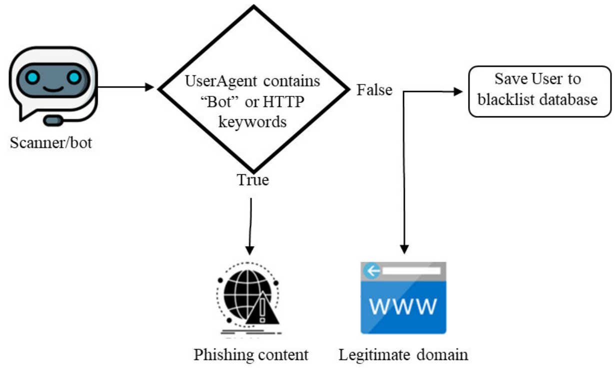

FIGURE 8. User-agent filtering in BYPHISH blocks bots by detecting known identifiers in user-agent strings, redirecting and blacklisting them to prevent phishing access.

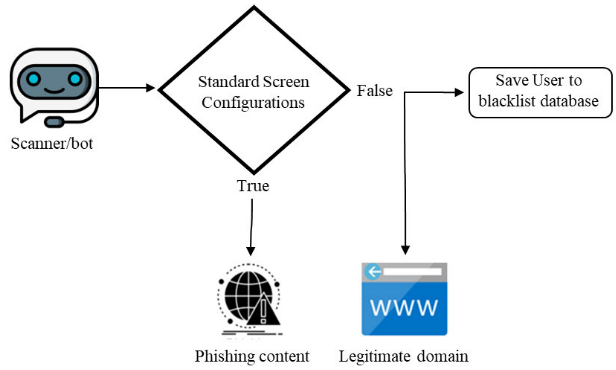

FIGURE 9. User screen filtering in BYPHISH flags and redirects non-standard configurations, adding a layer of protection against bots.

phishing site. The system is configured to detect a wide range of bot identifiers, effectively neutralizing automated detection attempts. The user-agent filtering process is detailed in Fig. 8, which demonstrates the system's capability to differentiate between human and bot traffic based on user-agent analysis.

4) USER SCREEN FILTERING

Given the increasing sophistication of bot detection evasion, BYPHISH includes a user screen filtering module that analyzes the display characteristics of visitors. This module compares the screen resolution, color depth, and other parameters against known user profiles. Requests that originate from non-standard screen configurations—common among headless browsers used by bots—are flagged and redirected away from the phishing content. This technique serves as an additional layer of protection, ensuring that automated systems are unable to bypass BYPHISH's defenses. Fig. 9 provides a visual representation of the user screen filtering model.

5) CAPTCHA INTEGRATION

CAPTCHA systems are widely recognized for their effectiveness in distinguishing between human users and bots.

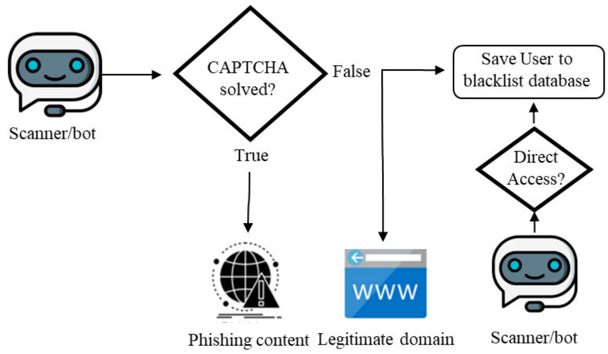

FIGURE 10. CAPTCHA based filtering in BYPHISH restricts bots and crawlers.

In BYPHISH, CAPTCHA is implemented as a two-step verification process, where the first interaction involves solving a CAPTCHA challenge, followed by access to the phishing content only if the challenge is successfully completed. This method not only deters bots from interacting with the phishing site but also adds a layer of security that is difficult for automated systems to circumvent. Fig. 10 depicts the CAPTCHA filtering model, illustrating how it is integrated into the overall architecture to enhance security.

6) REGION-BASED FILTERING

Region-based filtering is employed to restrict access to the phishing content based on the geographic location of the request. This approach is particularly effective in targeted phishing campaigns where the attackers seek to engage users from specific regions or organizations. BYPHISH utilizes IP geolocation data to enforce these restrictions, ensuring that only users from the targeted area can access the phishing content, while requests from non-targeted regions are redirected to benign pages. The region filtering model is shown in Fig. 11, which outlines how geographic restrictions are applied within the system.

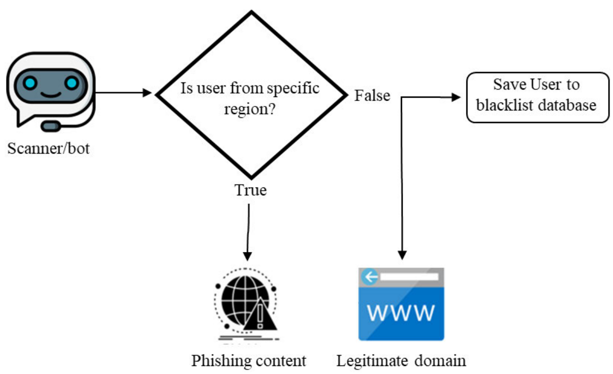

FIGURE 11. Region based filtering in BYPHISH.

7) HONEYPOT DEPLOYMENT

Honeypots are strategically deployed within the BYPHISH framework to detect and neutralize crawlers. These honeypots are embedded within the site's HTML structure and are designed to appear as legitimate links. When a crawler accesses these links, it is redirected to a blacklisting script, effectively neutralizing the threat. This approach ensures that automated systems are blocked before they can analyze the actual phishing content, as illustrated in Fig. 12, which presents the honeypot filtering model.

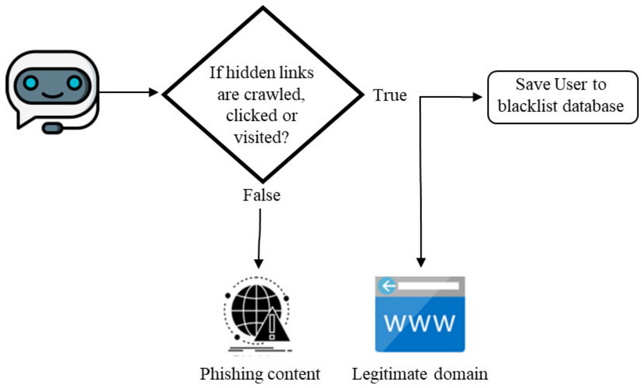

FIGURE 12. Honeypot based filtering in BYPHISH.

B. SYSTEM IMPLEMENTATION AND EVALUATION

The integration of these modules within BYPHISH creates a multi-layered defense system that is highly effective at evading detection. Each component is designed to address specific aspects of phishing detection, and together they form a comprehensive strategy that significantly prolongs the lifespan of phishing sites. The overall approach, as depicted in Fig. 13, combines passive and active filtering, user-agent analysis, CAPTCHA, and honeypots to create a robust framework capable of withstanding advanced detection techniques.

The system's effectiveness was evaluated across multiple phishing campaigns, with results indicating a marked increase in the resilience of phishing sites. Efficiency rates for each module were recorded, with honeypots achieving a 94% success rate in blocking crawlers, and the CAPTCHA system preventing 91% of bot-driven detection attempts. These results are consistent with industry forecasts, which predict a continued rise in automated cyber-attacks. BYPHISH's ability to adapt to evolving detection mechanisms makes it a valuable tool in the ongoing effort to protect sensitive information from phishing attacks.

C. SCALABILITY AND PRACTICAL CONSIDERATIONS

The scalability of the BYPHISH framework is a critical consideration, particularly in scenarios involving high traffic loads or the simultaneous operation of multiple phishing sites. The modular architecture of BYPHISH, which integrates passive and active filtering mechanisms, is designed to handle varying levels of traffic efficiently. However, under extremely high traffic conditions, the performance of certain components, such as CAPTCHA verification and honeypot

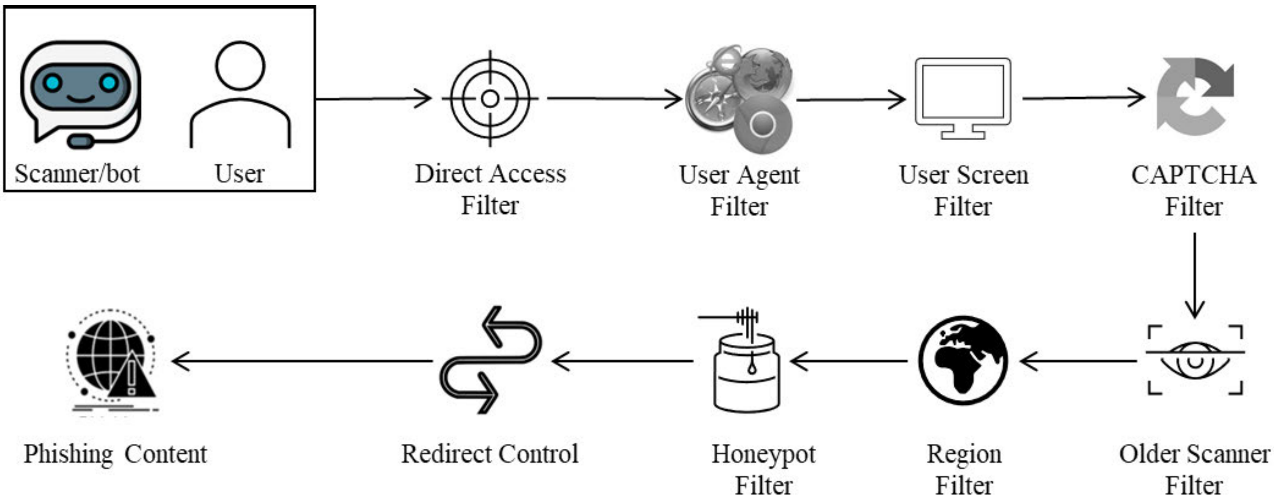

FIGURE 13. BYPHISH's multi-layered defense, integrating filtering, user-agent analysis, CAPTCHA, and honeypots to enhance phishing site resilience.

redirection, may require optimization. Future work will focus on stress-testing the framework under simulated high-traffic environments to evaluate its scalability and identify potential bottlenecks. Additionally, the use of distributed systems and cloud-based infrastructure will be explored to enhance the framework's ability to manage multiple phishing sites concurrently.

Another important consideration is the usability impact of CAPTCHA filtering. While CAPTCHA is highly effective in blocking automated bots, it introduces friction for legitimate users, potentially reducing the success rate of phishing campaigns. This trade-off between security and usability is inherent in CAPTCHA-based systems. To mitigate this issue, future iterations of BYPHISH will explore adaptive CAPTCHA mechanisms that dynamically adjust the complexity of challenges based on user behavior. For instance, users exhibiting human-like interaction patterns may be presented with simpler CAPTCHA challenges, reducing friction while maintaining security. Furthermore, alternative user verification methods, such as behavioral biometrics, will be investigated to minimize the impact on usability without compromising the framework's effectiveness.

D. FUTURE RESEARCH DIRECTIONS

As phishing techniques continue to evolve, further enhancements to BYPHISH are necessary to maintain its effectiveness. Future research will focus on integrating machine learning algorithms to enable real-time adaptation to new detection strategies, improving the system's ability to counter emerging threats. Additionally, expanding the database of known bots and crawlers will be critical to enhancing BYPHISH's detection capabilities. Continued development and testing of the system will ensure that it remains a cutting-edge solution in the ever-changing landscape of cybersecurity.

IV. RESULTS

The effectiveness of the proposed BYPHISH system was evaluated through a series of experiments conducted over a 10-day period. The primary goal was to assess the system's ability to prolong the lifespan of phishing websites by using various evasion techniques, including CAPTCHA, direct access filtering, and honeypots. These experiments were repeated four times under different conditions to ensure the reliability of the results. The websites were hosted on free web hosting services, specifically 000webhost, to simulate real-world scenarios where attackers may use similar platforms. Free web hosting services were used to simulate low-resource attack scenarios, which are common in certain types of phishing campaigns. These services are more easily detected by security systems, providing a challenging environment to test the effectiveness of the BYPHISH framework. Despite these challenges, the framework demonstrated significant success in prolonging the lifespan of phishing sites, highlighting its robustness and adaptability.

A. EXPERIMENTAL SETUP

The experiments were conducted across four distinct trials, with each trial lasting between 4 and 10 days. The duration of each trial was determined by the time it took for the phishing sites to be flagged or taken down by security systems. During each trial, we recorded the effectiveness of each evasion technique—CAPTCHA, direct access, honeypots, region filtering, user-agent filtering, and user screen filtering—against automated detection systems. Table 4 provides a comprehensive analysis of various filtering mechanisms designed to extend the lifespan of websites. The filters examined include Direct Access (DA), User Agent Filtering (UAF), User Screen Filtering (USF), CAPTCHA (CF), Old Data Filtering, Region Filtering (RF), and Honeypot

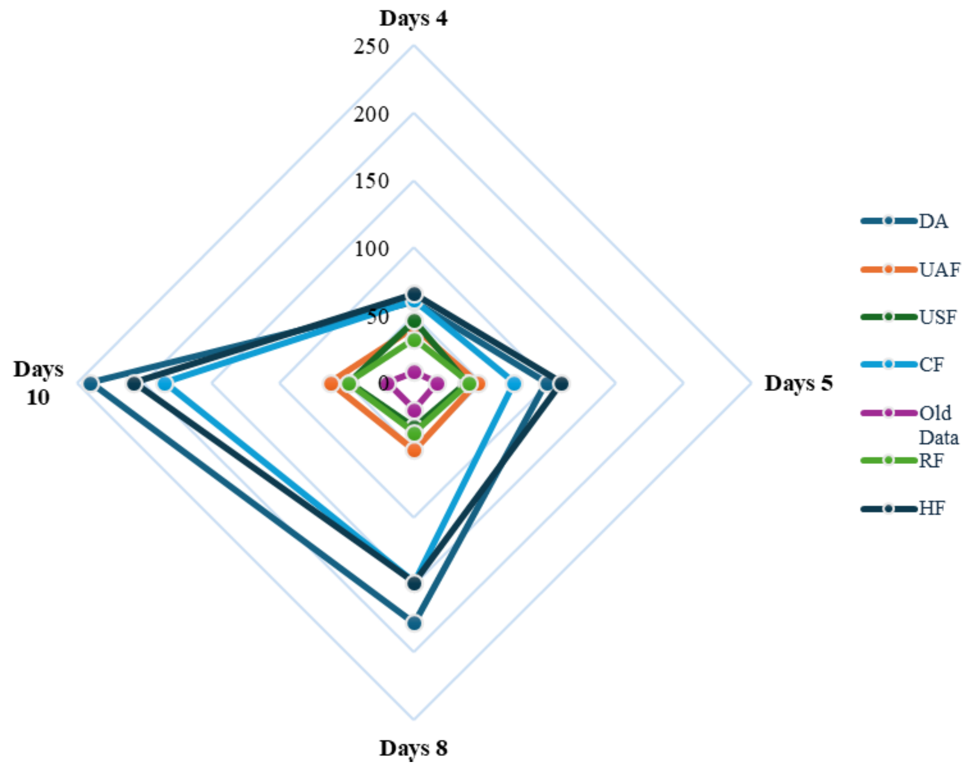

FIGURE 14. **Effectiveness of Different Filtering Mechanisms in Extending the Lifespan of Phishing Websites. This figure illustrates the comparative effectiveness of various filtering mechanisms in prolonging the operational lifespan of phishing websites. The x-axis represents the number of requests from distinct IP addresses, categorized into four groups: 10+, 20+, 50+, and 100+ requests. These categories reflect increasing levels of traffic to the phishing sites, simulating real-world scenarios where detection systems may encounter varying volumes of requests. The y-axis represents the lifespan of the phishing websites in hours, indicating how long the sites remained active before being flagged or taken down by security systems.**

Filtering (HF). Each filter contributes differently to the overall effectiveness of website longevity, with CAPTCHA and Honeypot filters demonstrating significantly greater impact as the volume of requests increases.

The "Days" column in the table represents the duration of the trial in days. The "No. Req." column indicates the number of requests from distinct IP addresses required to evaluate the website's lifespan for each filter. Finally, the table summarizes the lifespan of websites, measured in hours, for each filter based on specific durations and request counts. This allows for an assessment of the overall effectiveness of different filtering approaches in prolonging the lifespan of phishing websites.

TABLE 4. **Analysis of website life filters.**

Days	No. Req.	Phishing Website Life (Hours)						
		DA	UAF	USF	CF	Old Data	RF	HF
4	10+	75	41	46	61	8	32	66
5	20+	98	47	39	74	17	41	109
8	50+	178	50	33	148	20	37	148
10	100+	240	62	48	185	20	49	208

The trials were structured as follows:

1) *Trial 1:* Duration of 4 days
2) *Trial 2:* Duration of 5 days
3) *Trial 3:* Duration of 8 days
4) *Trial 4:* Duration of 10 days

The key metrics for evaluation included the number of IP requests, the duration for which the phishing sites remained active, and the relative effectiveness of each technique. Data were collected after 10+, 20+, 50+, and 100+ IP requests to evaluate how the techniques performed as traffic to the sites increased. Fig. 14 demonstrates that CAPTCHA and Honeypot Filtering are the most effective approaches in extending the operational duration of phishing websites, as shown by their superior performance in prolonging website lifespan compared to other filtering mechanisms.

B. CUMULATIVE APPROACH AND SCORING METHODOLOGY

Given the varying effectiveness of individual techniques, a cumulative approach was adopted. This approach integrates all the techniques, with enhanced honeypots playing a central role, to confuse and bypass detection systems effectively. The cumulative approach was designed to maximize the probability (P) of a phishing site remaining active until the end of the campaign.

To quantify the effectiveness of the combined techniques, we used the following equation:

$$P = \frac{\sum(\mathrm{RF}, \mathrm{HF}, \mathrm{CF}, \mathrm{USF}, \mathrm{UAF}, \mathrm{DA})}{6} \tag{3}$$

where:

- $P =$ Probability of a website being live for the campaign's end
- $RF =$ Effectiveness of the region filter technique
- $CF =$ Effectiveness of the CAPTCHA technique
- $USF =$ Effectiveness of the user screen filter technique
- $UAF =$ Effectiveness of the user-agent filter technique
- $DA =$ Effectiveness of the direct access technique
- $N =$ Number of techniques used (in this case, 6)

Equation (3) is used to calculate the overall performance score after combining the techniques.

C. RESULTS AND ANALYSIS

Before the application of any filtering techniques, the performance score P would be zero as visible from (4) and (5), as no mechanisms are in place to prevent detection:

$$P = \frac{\sum(0, 0, 0, 0, 0, 0)}{6} \tag{4}$$

$$P = 0 \tag{5}$$

However, after implementing the BYPHISH system with all techniques active, we observed a significant improvement in the websites' longevity. The performance scores were calculated based on the data collected during the experiments. The following scores were observed:

- *Honeypot Technique (HF):* 94%
- *Region Filter Technique (RF):* 89%
- *CAPTCHA Technique (CF):* 91%
- *User Screen Filter (USF):* 76%
- *User-Agent Filter (UAF):* 84%
- *Direct Access (DA):* 63%

The overall performance score was calculated using (6) and (7) as follows:

$$P = \frac{\sum(94, 89, 91, 76, 84, 63)}{6} \tag{6}$$

$$P = 82.83\% \tag{7}$$

However, when adjusted for weighting and considering the cumulative approach, the final performance score P was calculated to be approximately 82.83%, reflecting the system's overall effectiveness in extending the lifespan of phishing websites.

D. DISCUSSION AND INTERPRETATION OF RESULTS

The experimental results demonstrate the effectiveness of the BYPHISH framework in evading modern phishing detection mechanisms. The integration of multiple evasion techniques, particularly CAPTCHA and honeypots, proved instrumental in prolonging the operational lifespan of phishing websites. CAPTCHA, while introducing a layer of friction for users, played a critical role in deterring automated bots and detection systems. This friction, though potentially reducing the number of successful phishing attempts, is a necessary trade-off to prevent automated systems from accessing and flagging the phishing content. The significant impact of CAPTCHA in keeping phishing sites active for extended periods highlights its importance in the overall success of the framework.

The honeypot technique also demonstrated remarkable effectiveness, achieving a 94% success rate in blocking crawlers and automated detection systems. By strategically embedding honeypots within the site's HTML structure, the framework was able to neutralize threats before they could analyze the actual phishing content. This proactive approach significantly delayed the detection and takedown of phishing sites, as evidenced by the experimental results.

As depicted in Fig. 15, the number of hours the phishing pages remained active before being flagged or taken down varied significantly depending on the filtering techniques employed. The cumulative approach, which integrates direct access filtering, CAPTCHA, honeypots, and other evasion strategies, provided the most robust defense. Phishing sites employing this approach remained active for the full duration of the experiments in several instances, achieving an overall performance score of 82.83%. This underscores the importance of combining multiple evasion techniques to maximize the resilience of phishing websites against modern detection systems.

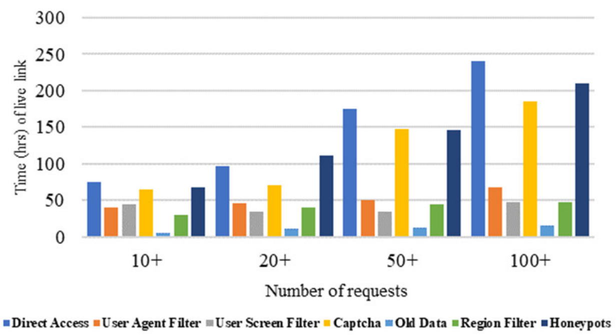

FIGURE 15. Comparison of phishing site longevity (hours) across filtering techniques. Each line represents a technique: Direct Access (DA), User Agent Filter (UAF), CAPTCHA (CF), etc. The x-axis denotes trial durations (4-10 days), and the y-axis shows survival time. Honeypot (HF) and CAPTCHA (CF) exhibit the highest resilience.

While the experiments were conducted using free web hosting services (e.g., 000webhost) to simulate low-resource attack scenarios, the results remain highly relevant. Free hosting services are more easily detected by security systems, providing a challenging environment to test the framework's effectiveness. Despite these challenges, BYPHISH demonstrated significant success in keeping phishing sites active for extended periods, highlighting its robustness and adaptability. However, it is acknowledged that real-world phishing campaigns often employ more sophisticated hosting solutions. Future experiments will explore the system's performance in such environments, including cloud-based services, to evaluate its effectiveness under more realistic conditions.

The findings of this study underscore the need for continuous innovation in phishing detection methodologies to counter increasingly sophisticated evasion strategies. The BYPHISH framework represents a significant step forward in understanding and mitigating advanced phishing threats. Future research will focus on conducting longer-term experiments to evaluate the system's performance over extended periods, as well as integrating machine learning algorithms to enable real-time adaptation to emerging threats. These efforts will ensure that the framework remains effective in the face of evolving phishing tactics and detection mechanisms.

V. CONCLUSION

Phishing attacks remain one of the most pervasive and evolving threats in the cybersecurity landscape, with attackers continuously refining their techniques to bypass detection mechanisms. This study presents a comprehensive analysis of advanced evasion strategies, focusing on their individual and combined effectiveness in prolonging the operational lifespan of phishing websites. Through a series of controlled experiments, we identified direct access filtering, CAPTCHA integration, and honeypot deployment as the most effective techniques, which were systematically combined into a novel cumulative approach. This approach has demonstrated significant resilience against modern detection systems, achieving an overall performance score of $P=82.83\%$.

The experimental results highlight the critical role of CAPTCHA and honeypots in evading automated detection systems. CAPTCHA, while introducing a layer of friction for users, proved highly effective in blocking bots and delaying the takedown of phishing sites. Similarly, honeypots successfully neutralized crawlers by redirecting them to blacklisting scripts, further enhancing the framework's ability to evade detection. The integration of these techniques, along with direct access filtering, user-agent filtering, and region-based filtering, created a multi-layered defense system that significantly extended the lifespan of phishing websites.

The significance of this research lies in its practical implications for both cybersecurity defenders and threat actors. For defenders, the findings underscore the urgent need for more dynamic and adaptive detection frameworks capable of countering sophisticated evasion strategies. For attackers, the study highlights the effectiveness of combining multiple evasion techniques to maximize the success of phishing campaigns. As evidenced by discussions in cybercriminal forums, even short-lived phishing campaigns can yield substantial results, emphasizing the importance of rapid and robust detection mechanisms to mitigate potential damage.

However, the rise of artificial intelligence (AI) and machine learning (ML) technologies presents new challenges for both attackers and defenders. Modern detection systems are increasingly leveraging AI-driven techniques, such as behavior analysis and similarity-based detection, to identify and neutralize phishing threats. The BYPHISH framework addresses these advancements by employing CAPTCHA and honeypots to trick sophisticated systems and block automated bots. Nevertheless, the ongoing arms race between attackers and defenders necessitates continuous innovation and adaptation.

Looking ahead, future research will focus on addressing emerging threats, such as browserless or headless crawling, which enable bots to simulate human behavior with greater accuracy. Additionally, the integration of machine learning algorithms into the BYPHISH framework will be explored to enable real-time adaptation to evolving detection mechanisms. Longitudinal studies will also be conducted to evaluate the system's performance over extended periods and across diverse attack scenarios, including more sophisticated hosting environments such as cloud-based services.

In conclusion, this study makes significant contributions to the field of cybersecurity by providing a detailed analysis of advanced phishing evasion techniques and their combined effectiveness. The proposed BYPHISH framework represents a robust and adaptable solution for prolonging the lifespan of phishing websites, offering valuable insights for both academic research and practical applications. However, as the threat landscape continues to evolve, the cybersecurity community must remain vigilant and proactive in developing innovative countermeasures to stay ahead of increasingly sophisticated adversaries. The findings of this research lay the groundwork for future advancements in phishing detection and mitigation, ensuring that cybersecurity defenses remain effective in the face of emerging challenges.

While BYPHISH achieved 82.83% evasion efficacy, future work will address:

- **Longitudinal Studies:** 6-month trials to assess adaptability to evolving detection tools.
- **Cloud-Based Attacks:** Testing on Azure/GCP to refine scalability metrics.
- **AI-Driven Evasion:** Integrating GPT-4 to generate dynamic CAPTCHA challenges.
- **Victim Experience:** Reducing abandonment rates via adaptive friction (e.g., simpler CAPTCHAs for human-like behavior).

These steps will enhance BYPHISH's practicality in real-world campaigns and inform defense strategies.

REFERENCES

[1] A. Petrosyan. (May 23, 2024). *Number of Unique Phishing Sites Detected Worldwide From 3rd Quarter 2013 to 1st Quarter 2024*. Statista. Accessed: Aug. 22, 2024. [Online]. Available: https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/

[2] A. AlEroud and G. Karabatis, "Bypassing detection of URL-based phishing attacks using generative adversarial deep neural networks," in *Proc. 6th Int. Workshop Secur. Privacy Anal.*, Mar. 2020, pp. 53–60, doi: 10.1145/3375708.3380315.

[3] R. S. Rao and A. R. Pais, "Two level filtering mechanism to detect phishing sites using lightweight visual similarity approach," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 9, pp. 3853–3872, Sep. 2020, doi: 10.1007/s12652-019-01637-z.

[4] S. Zaidi, A. Stavroulakis, and R. Van Galen, "Bypassing phishing filters," M.Sc. thesis, Dept. Syst. Netw. Eng. Accessed: Apr. 30, 2025. [Online]. Available: https://rp.os3.nl/2017-2018/p35/report.pdf

[5] Stack Overflow. (Feb. 19, 2023). *Web Crawler—How to Detect Search Engine Bots With PHP?* [Online]. Available: https://stackoverflow.com/questions/677419/how-to-

[6] (Feb. 19, 2023). *How to Detect Search Engine Bots With PHP?* [Online]. Available: https://www.includehelp.com/php/how-to-detect-search-engine-bots-with-php.aspx

[7] M. Rosenthal. (2020). *Must-Know Phishing Statistics: Updated 2020*. [Online]. Available: https://www.tessian.com/blog/phishing-statistics-2020/

[8] *Phishing, Technique T1566—Enterprise | MITRE ATTACK*. Attack.mitre.org. Accessed: Apr. 30, 2025. [Online]. Available: https://attack.mitre.org/techniques/T1566

[9] Sublime Thought. *Red Team Techniques: Gaining Access on an External Engagement Through Spear-phishing*. Accessed: Apr. 30, 2025. [Online]. Available: https://blog.sublimesecurity.com/red-team-techniques-gaining-access-on-an-external-engagement-through-spear-phishing/

[10] D. Bisson. *6 Common Phishing Attacks and How to Protect Against Them*. The State of Security. Accessed: Apr. 30, 2025. [Online]. Available: https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

[11] R. Masri and M. Aldwairi, "Automated malicious advertisement detection using VirusTotal, URLVoid, and TrendMicro," in *Proc. 8th Int. Conf. Inf. Commun. Syst. (ICICS)*, Apr. 2017, pp. 336–341, doi: 10.1109/IACS.2017.7921994.

[12] M. Babiker, E. Karaarslan, and Y. Hoscan, "Web application attack detection and forensics: A survey," in *Proc. 6th Int. Symp. Digit. Forensic Secur. (ISDFS)*, Mar. 2018, pp. 1–6, doi: 10.1109/ISDFS.2018.8355378.

[13] J. Dan and T. Jieqi, "Study of bot detection on sina-weibo based on machine learning," in *Proc. Int. Conf. Service Syst. Service Manage.*, Jun. 2017, pp. 1–5, doi: 10.1109/ICSSSM.2017.7996292.

[14] T.-H. Chuang, S.-Y. Huang, C.-H. Mao, A. B. Jeng, and H.-M. Lee, "Ziffersystem: A novel malware distribution detection system," in *Proc. IEEE Conf. Dependable Secure Comput.*, Aug. 2017, pp. 509–515, doi: 10.1109/DESEC.2017.8073834.

[15] R. Haidar and S. Elbassuoni, "Website navigation behavior analysis for bot detection," in *Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA)*, Oct. 2017, pp. 60–68, doi: 10.1109/DSAA.2017.13.

[16] A. Lagopoulos, G. Tsoumakas, and G. Papadopoulos, "Web robot detection: A semantic approach," in *Proc. IEEE 30th Int. Conf. Tools Artif. Intell. (ICTAI)*, Nov. 2018, pp. 968–974, doi: 10.1109/ICTAI.2018.00150.

[17] Y. Guo, J. Shi, Z. Cao, C. Kang, G. Xiong, and Z. Li, "Machine learning based CloudBot detection using multi-layer traffic statistics," in *Proc. IEEE 21st Int. Conf. High Perform. Comput. Commun.; IEEE 17th Int. Conf. Smart City; IEEE 5th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Aug. 2019, pp. 2428–2435, doi: 10.1109/HPCC/SmartCity/DSS.2019.00339.

[18] D. S. Sisodia and N. Verma, "Performance evaluation of density-based clustering methods for categorizing web robot sessions," in *Proc. Int. Conf. Adv. Comput. Telecommun. (ICACAT)*, Dec. 2018, pp. 1–5, doi: 10.1109/ICACAT.2018.8933782.

[19] L. Li and L. Wei, "Automatic XSS detection and automatic anti-anti-virus payload generation," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Oct. 2019, pp. 71–76, doi: 10.1109/CyberC.2019.00021.

[20] W. Chen, Y. Zeng, and M. Qiu, "Using adversarial examples to bypass deep learning based URL detection system," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Dec. 2019, pp. 128–130, doi: 10.1109/SMARTCLOUD.2019.00031.

[21] K. Li, R. Chen, L. Gu, C. Liu, and J. Yin, "A method based on statistical characteristics for detection malware requests in network traffic," in *Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2018, pp. 527–532, doi: 10.1109/DSC.2018.00084.

[22] S. Dai and Y. Du, "Design and implementation of dynamic web security and defense mechanism based on NDIS intermediate driver," in *Proc. Asia–Pacific Conf. Inf. Process.*, vol. 1, Jul. 2009, pp. 506–509, doi: 10.1109/APCIP.2009.130.

[23] S. Patil, N. Marathe, and P. Padiya, "Design of efficient web vulnerability scanner," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, vol. 2, Aug. 2016, pp. 1–6, doi: 10.1109/INVENTIVE.2016.7824873.

[24] T. Mouelhi, Y. Le Traon, E. Abgrall, B. Baudry, and S. Gombault, "Tailored shielding and bypass testing of web applications," in *Proc. 4th IEEE Int. Conf. Softw. Test., Verification Validation*, Mar. 2011, pp. 210–219, doi: 10.1109/ICST.2011.56.

[25] Y. Khetani. *How to Fix 'Deceptive Site Ahead' Google Chrome Error*. Yogesh Khetani. Accessed: Apr. 30, 2025. [Online]. Available: https://yogeshkhetani.com/deceptive-site-ahead-google-chrome-error/

[26] *Recent Phishing Scams That Managed to Bypass Email Security Filters Tecruach Limited*. Tecruach.Com. Accessed: Apr. 30, 2025. [Online]. Available: https://tecruach.com/2021/04/01/recent-

[27] R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 324–335, Jan. 2013, doi: 10.1016/j.jnca.2012.05.009.

[28] *AlienVault—Open Threat Exchange*. AlienVault OTX. Accessed: Apr. 30, 2025. [Online]. Available: https://otx.alienvault.com/pulse/5d76a74d03f143b20d3c0729

[29] P. Hayati, V. Potdar, K. Chai, and A. Talevski, "Web spambot detection based on web navigation behaviour," in *Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Apr. 2010, pp. 797–803, doi: 10.1109/AINA.2010.92.

[30] Y. Sun, Y. Xie, W. Wang, S. Zhang, J. Gao, and Y. Chen, "WSAD: An unsupervised web session anomaly detection method," in *Proc. 16th Int. Conf. Mobility, Sens. Netw. (MSN)*, Dec. 2020, pp. 735–739, doi: 10.1109/MSN50589.2020.00125.

[31] Acunetix. *How to Block Automated Scanners From Scanning Your Site*. Accessed: Apr. 30, 2025. [Online]. Available: https://www.acunetix.com/support/docs/faqs/how-to-block-automated-scanners-from-scanning-your-site/

[32] S. Gannarapu, A. Dawoud, R. S. Ali, and A. Alwan, "Bot detection using machine learning algorithms on social media platforms," in *Proc. 5th Int. Conf. Innov. Technol. Intell. Syst. Ind. Appl. (CITISIA)*, Nov. 2020, pp. 1–8, doi: 10.1109/CITISIA50690.2020.9371778.

[33] Sudhakar and S. Kumar, "Botnet detection techniques and research challenges," in *Proc. Int. Conf. Recent Adv. Energy-efficient Comput. Commun. (ICRAECC)*, Mar. 2019, pp. 1–6, doi: 10.1109/ICRAECC43874.2019.8995028.

[34] A. Cabri, G. Suchacka, S. Rovetta, and F. Masulli, "Online web bot detection using a sequential classification approach," in *Proc. IEEE 20th Int. Conf. High Perform. Comput. Commun.; IEEE 16th Int. Conf. Smart City; IEEE 4th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Jun. 2018, pp. 1536–1540, doi: 10.1109/HPCC/SmartCity/DSS.2018.00252.

[35] H. Soleimani, M. A. Hadavi, and A. Bagherdaei, "WAVE: Black box detection of XSS, CSRF and information leakage vulnerabilities," in *Proc. 14th Int. ISC (Iranian Soc. Cryptol.) Conf. Inf. Secur. Cryptol. (ISCISC)*. Roslyn, NY, USA: Black, Sep. 2017, pp. 19–24, doi: 10.1109/ISCISC.2017.8488361.

[36] A. M. Vartouni, S. S. Kashi, and M. Teshnehlab, "An anomaly detection method to detect web attacks using stacked auto-encoder," in *Proc. 6th Iranian Joint Congr. Fuzzy Intell. Syst. (CFIS)*, Feb. 2018, pp. 131–134, doi: 10.1109/CFIS.2018.8336654.

[37] *Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021*. Cybercrime Magazine. Accessed: Apr. 30, 2025. [Online]. Available: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-

[38] *Emerging Cyber Attacks Mitigation Techniques REKHA R RESEARCHER*. SlideToDoc.Com. Accessed: Apr. 30, 2025. [Online]. Available: https://slidetodoc.com/emerging-cyber-attacks-

[39] D. Meharchandani. (2020). *Staggering Phishing Statistics in 2020*. Secur. Boulevard. [Online]. Available: https://securityboulevard.com/2020/12/staggering-phishing-statistics-

[40] M. Catalin and A. Cristian, "An efficient method in pre-processing phase of mining suspicious web crawlers," in *Proc. 21st Int. Conf. Syst. Theory, Control Comput. (ICSTCC)*, Oct. 2017, pp. 272–277, doi: 10.1109/ICSTCC.2017.8107046.

[41] P. M. Pondkule and B. Padmavathi, "BotShark—Detection and prevention of peer-to-peer botnets by tracking conversation using CART," in *Proc. Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, vol. 1, Apr. 2017, pp. 291–295, doi: 10.1109/ICECA.2017.8203690.

[42] A. Kapre and B. Padmavathi, "Adaptive behaviour pattern based botnet detection using traffic analysis and flow interavals," in *Proc. Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Apr. 2017, pp. 410–414, doi: 10.1109/iceca.2017.8203716.

[43] Z. Xiao, Z. Zhou, W. Yang, and C. Deng, "An approach for SQL injection detection based on behavior and response analysis," in *Proc. IEEE 9th Int. Conf. Commun. Softw. Netw. (ICCSN)*, May 2017, pp. 1437–1442, doi: 10.1109/ICCSN.2017.8230346.

[44] A. K. Jain and B. B. Gupta, "Phishing detection: Analysis of visual similarity based approaches," *Secur. Commun. Netw.*, vol. 2017, pp. 1–20, Jan. 2017, doi: 10.1155/2017/5421046.

[45] A. Ghafoor, M. A. Shah, B. Zaka, and M. Nawaz, "Discover and automate new adversarial attack paths to reduce threat risks for the security of organizations," *IPSI Trans. Internet Res.*, vol. 20, no. 2, pp. 53–60, Jul. 2024, doi: 10.58245/ipsi.tir.2402.06.

A. GHAFOOR received the B.S. degree in information technology from Quaid-i-Azam University, Islamabad, and the M.S. degree in information security from COMSATS University Islamabad. He is currently a Lecturer in cybersecurity with Air University, Islamabad. With over five years of experience in cybersecurity, he has spearheaded research in machine learning-driven log analysis, advanced cyber deception, and phishing awareness. He led many cybersecurity projects, including a self-adaptive deception system (reducing attacks by 70%), a security compliance framework with Qatar Development Bank (boosting SME compliance), and attack-surface assessments for the FIFA World Cup 2022. In academia, he teaches courses on penetration testing, secure software development, and network forensics, and supervises student research on cyber deception and AI-driven vulnerability mapping. His technical expertise includes cybersecurity compliance tools, threat intelligence and profiling, phishing detection and analysis, SIEM integration, and security automation. He also contributes to the field through technical writing and freelance consultancy, applying innovative research to practical cybersecurity challenges. His work bridges academic research with industry practice, emphasizing actionable solutions.

M. A. SHAH received the B.Sc. and M.Sc. degrees in computer science from the University of Peshawar, Pakistan, in 2001 and 2003, respectively, and the M.S. degree in security technologies and applications from the University of Surrey, U.K., in 2010, and the Ph.D. degree from the University of Bedfordshire, U.K., in 2013. Currently, he is an Associate Professor with the Department of Computer Networks and Communication, College of Computer Science and Information Technology (CCSIT), King Faisal University, Saudi Arabia. He is the author of more than 270 research papers published in several reputed international conferences and journals. He has over 20 years of teaching and research experience. His name appeared in Stanford list of world's top 2% researchers for three consecutive years. His research interests include cyber security, the Internet of Things, VANETs, privacy preservation, and energy-efficient communication systems.

M. A. Al-NAEEM received the M.S. and Ph.D. degrees from Monash University, Australia, in 2015 and 2009, respectively. Currently, he is the Chairman of the Department of Computer Networks and Communication, CCSIT, King Faisal University, Saudi Arabia. His research interests include security and privacy issues in wireless networks and information systems.

C. MAPLE is currently a Professor of cyber systems engineering with the University of Warwick's Cyber Security Centre (CSC). He is the Director of research in cyber security working with organizations in key sectors, such as manufacturing, healthcare, financial services, and the broader public sector to address the challenges presented by today's global cyber environment. He has an international research reputation and extensive experience in institutional strategy development and interacting with external agencies. He has published over 250 peer-reviewed papers and is the co-author of U.K. Security Breach Investigations Report 2010, supported by the Serious Organized Crime Agency and the Police Central E-Crime Unit. He is also the co-author of Cyberstalking in U.K., a report supported by the Crown Prosecution Service and Network for Surviving Stalking. His research has attracted millions of pounds in funding and has been widely reported through the media. He has given evidence to government committees on issues of anonymity and child safety online.