Designing Anti Hacking Software for Securing Social Media Platforms Like What'sApp

Prof.Sangeeta Mohapatra[1], Akshada Solas[2], Shraddha Solase[3], Atik Pathan[4]
[1,2,3,4]*Department Of Computer Engineering, Ajeenkya Dy Patil School of Engineering Pune, India*.

Abstract— **Phishing attacks have evolved into one of the most persistent and dangerous cybersecurity threats in today's digital landscape. Such attacks usually target users via deceptive emails, harmful URLs, counterfeit login pages, and manipulative communication tactics. As attack techniques evolve, cybercriminals are increasingly employing image-based phishing tactics like fake screenshots, malicious embedded visuals, and cloned interfaces, thereby making detection significantly more difficult. Conventional phishing detection systems, which depend mainly on rule-based filtering or text analysis, frequently struggle to effectively identify such sophisticated threats.**

This research proposes an intelligent phishing detection system based on artificial intelligence. The system combines text-based analysis with image-based classification powered by Convolutional Neural Networks (CNNs). The architecture comprises two primary modules. The initial module is dedicated to analyzing textual data, including URLs and message content, by extracting pertinent features. The second module employs deep learning techniques to analyze images and detect visual patterns indicative of phishing attacks.

Combining these two approaches allows the system to attain greater detection accuracy while substantially lowering false positive rates. The model is trained and evaluated on well-labeled datasets containing both phishing and legitimate samples. To ensure reliability, performance evaluation is conducted using metrics such as accuracy, precision, recall, and F1-score.

The findings demonstrate that the hybrid approach outperforms conventional single-method detection systems. The proposed system strengthens cybersecurity by offering an automated, intelligent, and real-time phishing detection solution that supports multiple data formats. This study underscores the efficacy of integrating deep learning and machine learning methods to counteract emerging cyber threats and enhance the security of online communication platforms.

I. INTRODUCTION

As digital technologies, online communication platforms, and internet-based services expand rapidly, the risk of cyber threats has risen dramatically. Among these threats, phishing attacks represent one of the most prevalent and damaging types of cybercrime. Phishing is a social engineering tactic in which attackers pose as trusted entities to deceive users into disclosing sensitive information like passwords, financial data, and personal details.

Phishing attacks are commonly executed via emails, counterfeit websites, malicious links, and altered images. These attacks are crafted to appear authentic and trustworthy, making it challenging for users to differentiate between legitimate and fraudulent content. As reliance on digital technologies expands, phishing attacks have grown increasingly sophisticated and pervasive, impacting individuals, businesses, and financial institutions worldwide.

Conventional phishing detection methods depend primarily on rule-based systems, blacklist databases, and the textual examination of URLs and email content. Although these methods are effective at detecting known phishing threats, they fail to counter newly generated attacks or visually deceptive content. Contemporary phishing tactics frequently employ image-based components like counterfeit login pages, replicated logos, and visually deceptive interfaces designed to evade text-based detection mechanisms.

Recent breakthroughs in artificial intelligence and deep learning have unlocked new avenues for enhancing cybersecurity systems. Convolutional Neural Networks (CNNs), in particular, have demonstrated exceptional performance in image recognition tasks. Integrating CNN-based image analysis with text-based feature extraction can lead to

the development of a more robust and intelligent phishing detection system.

This study introduces a hybrid AI-driven framework for phishing detection that combines both textual and visual analysis. The system is engineered to analyze URLs, message content, and webpage screenshots to more effectively identify phishing attempts. By integrating linguistic patterns with visual features, the proposed approach seeks to enhance detection accuracy, minimize false positives, and deliver real-time protection against phishing attacks.

This study advances the field of cybersecurity by showcasing the practical utility of deep learning techniques in identifying sophisticated phishing threats. The system can adapt to changing attack tactics and improve the security of digital communication environments.

II. LITERATURE REVIEW

Numerous research studies have been carried out in the field of phishing detection, examining various techniques and methodologies. This section outlines key contributions and their associated limitations.

1) Zhang et al. (2021) - "Large-Scale Analysis of Phishing Techniques"

- Performed a comprehensive analysis of phishing websites and client-side cloaking methods.
- Identified how attackers bypass traditional blacklist-based detection systems.
- Examined structural patterns within phishing domains and their associated webpage behaviors.
- Limitations: The study focused mainly on URL and domain behavior, omitting image-based phishing detection and deep learning models for visual analysis.

2) Alsharnouby et al. (2015) - "Why Phishing Still Works"

- Investigated user behavior and psychological factors that contribute to the success of phishing attacks.
- Identified usability weaknesses in traditional warning systems.
- Highlighted the importance of improving automated phishing detection.
- The study's limitations include a focus on user behavior instead of developing an intelligent detection model, as well as the absence of AI-based automated classification.

3) Bahnsen et al. (2017) - "Machine Learning-Based Phishing Detection"

- We applied machine learning algorithms, including Random Forest and Logistic Regression, to classify URL.
- We employed handcrafted URL-based features, such as domain length and the frequency of special characters.
- Achieved improved detection accuracy compared to rule-based systems.
- Limitations include reliance on manual feature engineering and the failure to account for visual phishing tactics like fake login page screenshots.

4) Huang et al. (2019) - "Deep Learning for Phishing Website Detection"

- Deep neural networks were implemented to automatically extract features from URLs
- Reduced dependency on handcrafted features.
- Demonstrated improved detection of newly generated phishing domains.
- Limitations: The study focused exclusively on textual and URL-based data, failing to address image-based spoofing or webpage layout imitation.

5) Abdelhamid et al. (2020) - "Visual Similarity-Based Phishing Detection Using CNN"

- Applied Convolutional Neural Networks (CNNs) to classify phishing webpage screenshots.
- Extracted visual layout patterns and logo similarities.
- Demonstrated strong performance in detecting cloned login interfaces.
- Limitations: Analyzed only visual features; lacked integration with textual indicators such as suspicious URLs or embedded links.

Gap Identified in Literature

- Most existing systems concentrate on either text-based URL analysis or image-based detection, seldom combining both within a unified framework.
- There is limited research on multi-modal phishing detection that combines linguistic and visual features.

- Many machine learning-based systems suffer from high false positive rates.
- The absence of real-time, scalable deployment models that are well-suited for mobile or web platforms.
- Inadequate adaptability to evolving phishing tactics that employ visual cloning and deceptive embedded images.

Proposed Contribution of This Project

- Develops a hybrid AI-driven phishing detection system that combines text-based URL analysis with image-based CNN classification.
- It enables real-time detection of phishing content in both message text and uploaded screenshots. •Reduces false positives through multi-modal feature evaluation.
- It offers a scalable and cost-effective framework ideal for both web and mobile environments.
- It strengthens cybersecurity by countering contemporary phishing tactics that exploit both text and visual deception.

III. METHODOLOGY

The proposed phishing detection system employs a combination of artificial intelligence techniques that analyze both textual and visual content. This improves the accuracy of phishing detection by simultaneously analyzing various types of data.

A) Data Collection

The performance of any machine learning model is heavily reliant on the quality and diversity of the data used for both training and testing. This system employs two distinct datasets.

Text Dataset:

This dataset comprises URLs and message content that are classified as either phishing or legitimate. It features examples exhibiting diverse traits, including atypical domain names, an overabundance of special characters, deceptive keywords, and irregular URL structures.

Image Dataset:

This dataset includes screenshots of both legitimate and phishing websites. These images feature deceptive designs such as fake login pages, duplicated interfaces, brand impersonation layouts, and other visually misleading elements commonly employed in phishing attacks.

The datasets are split into training and testing sets to assess the model's performance and generalization ability.

B) Data Preprocessing

Preprocessing is carried out before feeding the data into the model to enhance its accuracy and consistency.

Text Preprocessing:

The textual data undergoes multiple preprocessing stages, including the removal of extraneous symbols, URL normalization, tokenization, and feature extraction. Key features encompass URL length, the count of dots, the inclusion of special characters such as "@" or "-", the use of HTTPS, and domain-specific indicators.

Image Preprocessing:

The images are resized to a standard dimension appropriate for CNN input. Pixel values are normalized to maintain consistency throughout the dataset. Images are subsequently transformed into numerical arrays to facilitate processing by the neural network.

C) Feature Extraction and Model Development

1. Text-Based Detection Module

This module employs machine learning algorithms to categorize URLs and message content. The extracted features are employed to train the model to differentiate between phishing and legitimate inputs. The model identifies patterns including suspicious domain structures, atypical keywords, and irregular URL features.

2. Image-Based Detection Module (CNN)

The image classification module employs a Convolutional Neural Network (CNN) to analyze webpage screenshots. The CNN architecture comprises:

- Convolutional layers for feature extraction
- Activation functions (ReLU) to introduce non-linearity
- Pooling layers to reduce dimensionality
- Fully connected layers for classification
- Softmax layer for output probability

The CNN detects visual cues like layout patterns, logo positioning, input fields, and inconsistencies that signal phishing attempts.

D) System Integration

Both modules are integrated into a single unified system. Upon receiving user input like a URL or image, the system directs it to the appropriate module for processing. The result is then displayed through a user-friendly interface.

The architecture connects:

- Front-end interface
- Backend processing system
- AI models
- Database

This guarantees the system operates smoothly and efficiently.

E). Evaluation and Performance Metrics

The system is evaluated using standard classification metrics:

- Accuracy: Overall correctness of the model
- Precision: Correct identification of phishing cases
- Recall: Ability to detect all phishing instances
- F1-Score: Balance between precision and recall

A confusion matrix is also employed to evaluate false positives and false negatives. Cross-validation is employed to ensure the model performs consistently across different datasets.

F) Deployment and Continuous Learning

The final system is deployed as a web-based or mobile-compatible application. It offers real-time phishing detection and delivers immediate feedback to users.

Furthermore, the system employs continuous learning by regularly updating its dataset with newly discovered phishing samples. This enables the model to adjust to changing cyber threats and sustain high performance over time.

IV. APPLICATION

The proposed AI-based hybrid phishing detection system offers broad real-world applicability across various domains, thanks to its capacity to analyze both textual and visual data. As cyber threats continue to evolve, such a system becomes essential for ensuring digital security across various platforms.

1) Secure Messaging Platforms

One of the system's most significant applications lies in messaging platforms like WhatsApp, Telegram, and other instant messaging services. Phishing attacks are increasingly being delivered via messages that contain malicious links or deceptive content. The proposed system can be embedded into messaging apps to automatically scan incoming messages in real time.

It examines URLs, identifies suspicious patterns, and alerts users before they click on malicious links. Furthermore, it can analyze images shared in chats to detect fake login screenshots or fraudulent promotional material. This proactive strategy not only shields users from phishing attacks but also bolsters overall communication security.

2) Web Browser Security Enhancement

As the main entry point to the internet, web browsers are a crucial location for deploying security measures. The proposed system can be deployed as a browser extension or integrated into browser security frameworks.

Upon a user's visit to a website, the system concurrently evaluates the URL via a text-based module and analyzes the webpage layout using a CNN-based image module. This dual-layer verification validates both the structural and visual elements of a webpage before permitting user interaction.

This integration helps block access to phishing sites, lowers the risk of stolen credentials, and ensures a safer browsing experience.

3) Email Filtering Systems

Email continues to be one of the most prevalent channels for phishing attacks. Conventional spam filters, which depend mainly on keyword matching and blacklist databases, are inadequate for identifying advanced phishing attempts.

The proposed system improves email filtering by analyzing both the text and embedded images within emails. It is capable of identifying suspicious links, deceptive subject lines, and visually misleading attachments like counterfeit invoices or fake login pages.By enhancing detection accuracy and minimizing false negatives, the system bolsters email

security and shields users from sophisticated phishing attacks.

4) E-Commerce and Online Banking Security

Phishing attacks aimed at financial platforms pose a significant threat due to their potential to cause direct monetary losses. Attackers frequently craft deceptive login pages that mimic the appearance of authentic banking or e-commerce sites.

The hybrid detection system can be embedded into online banking and e-commerce platforms to track user interactions. It can detect suspicious login pages, identify cloned interfaces, and block unauthorized access attempts.

This application strengthens transaction security, safeguards sensitive financial data, and fosters user confidence in digital financial services.

5) Enterprise Cybersecurity Infrastructure

Organizations are frequently targeted by phishing attacks designed to steal confidential information or gain unauthorized access to internal systems. The proposed system can be integrated into enterprise networks as a component of the cybersecurity infrastructure.

It is capable of monitoring network traffic, scanning internal communications, and analyzing uploaded content for signs of phishing. By identifying threats early, the system helps avert data breaches and safeguard organizational security.

6) Educational Awareness Tools

Another significant application lies in educational institutions and cybersecurity awareness initiatives. This system serves as an educational tool to illustrate the mechanics of phishing attacks and methods for detecting them.

By offering real-time examples and detection results, it enables students and users to grasp the characteristics of phishing content. This fosters digital literacy and promotes safe online behavior.

7) Social Media Monitoring

Social media platforms are being increasingly exploited to disseminate phishing links and malicious content. The system can be integrated with social media monitoring tools to identify suspicious posts, messages, and shared links.

It is capable of analyzing both textual captions and images to detect fake advertisements, impersonation attempts, and scam campaigns. This ensures platform integrity and safeguards users against fraudulent activities.

V. RESULTS:

The proposed hybrid phishing detection gadget changed into evaluated using both textual and photograph datasets to evaluate its effectiveness and reliability. The assessment procedure concerned dividing the dataset into schooling and trying out subsets to make sure impartial overall performance dimension.

A. text-primarily based Detection effects

The text-based module established sturdy overall performance in identifying phishing URLs and suspicious message content material. via studying capabilities together with URL period, domain structure, presence of special characters, and keyword patterns, the version correctly categorized phishing and valid inputs.

The effects confirmed excessive accuracy and precision, indicating that the version was able to properly pick out phishing times with minimum fake positives. The consider cost turned into additionally excessive, making sure that most phishing attempts have been detected successfully.

The confusion matrix evaluation revealed a low charge of misclassification, demonstrating the robustness of the textual content-based version.

B. image-primarily based Detection consequences (CNN)

The CNN-primarily based photo type module turned into trained the usage of categorized screenshots of both valid and phishing webpages. The model was able to extract complicated visible functions along with format design, emblem placement, font fashion, and structural consistency.

The consequences indicated that the CNN completed excessive accuracy in distinguishing among actual and pretend webpages. The version efficiently detected cloned login pages and visually misleading interfaces. Precision and don't forget values had been sturdy, indicating reliable detection performance. The fake poor charge turned into considerably reduced, that is important in cybersecurity packages wherein lacking a phishing attack can have serious outcomes.

C. Hybrid version overall performance

the integration of textual content-based and photo-primarily based modules ended in stepped forward standard device overall performance. The hybrid version mixed the strengths of each procedure, leading to higher detection accuracy and reduced mistakes rates.

The gadget turned into able to handle diverse phishing situations, together with cases in which both textual or visible indicators alone had been inadequate. by reading a couple of statistics modalities, the version completed a greater comprehensive information of phishing styles. Cross-validation outcomes confirmed that the model maintained regular performance throughout one-of-a-kind dataset splits, demonstrating its generalization capability.

D. performance Metrics summary

the overall gadget performance may be summarized as follows:

•Excessive Accuracy in classifying phishing and valid samples

- Robust Precision indicating minimum false alarms
- High keep in mind ensuring powerful phishing identity
- Progressed F1-rating demonstrating balanced type performance

These findings validate that the proposed AI-pushed hybrid framework drastically enhances phishing detection capability in comparison to unmarried-method techniques.

VI. MOTIVATION

The fast development of digital technology has converted the way people and corporations have interaction, talk, and behavior business. With the good-sized use of online banking, e-trade systems, and social media packages inclusive of WhatsApp, customers are more and more depending on digital structures for normal activities. however, this extended dependency has additionally caused a great rise in cybersecurity threats, amongst which phishing attacks continue to be one of the most general and negative.

Phishing attacks are mainly risky due to the fact they take advantage of human psychology instead of purely technical vulnerabilities. Attackers design fantastically convincing messages, websites, and visual interfaces that seem legitimate, making it difficult for customers to distinguish between authentic and malicious content. those assaults frequently create a sense of urgency or agree with, prompting users to take immediately motion without verifying authenticity. As a end result, even nicely-informed users can fall sufferer to such assaults. Traditional phishing detection methods, consisting of blacklist-based totally filtering and rule-based totally structures, are now not sufficient to cope with modern threats. those approaches are reactive in nature, that means they could only discover phishing attempts which have already been identified and recorded. however, attackers constantly generate new phishing domain names, regulate URL structures, and use superior evasion strategies to pass those structures. moreover, traditional techniques consciousness mainly on textual analysis and fail to locate photograph-primarily based phishing attacks along with faux login screenshots, visually cloned web sites, and embedded malicious pics.

another foremost concern is the increasing scale and effect of phishing attacks on monetary institutions, corporations, and individuals. Phishing can result in severe results, inclusive of financial losses, identity theft, unauthorized get entry to to touchy records, and reputational harm. companies may additionally suffer sizable financial losses and loss of client agree with, while people may additionally face long-time period results which includes compromised non-public information and economic instability.

The emergence of artificial Intelligence and Deep mastering technology provides a promising strategy to these demanding situations. machine mastering fashions can analyze huge volumes of data and identify hidden styles which are difficult to discover using traditional techniques. Convolutional Neural Networks (CNNs), mainly, are notably effective in spotting visual styles and detecting anomalies in pics. through leveraging those technologies, it will become possible to develop a clever and adaptive phishing detection device.

The number one motivation at the back of this study is to deal with the constraints of current phishing detection systems by means of growing a hybrid method that combines each textual and visible analysis. via integrating those two methods, the gadget can provide a more complete information of phishing

attacks and improve detection accuracy. Moreover, there may be a need for actual-time detection structures which could offer immediate feedback to customers. behind schedule detection can result in users interacting with malicious content material, leading to serious effects. consequently, the proposed system targets to deliver immediate detection results, permitting customers to make knowledgeable choices and avoid capacity threats. Every other critical motivation is to create a scalable and deployable solution that can be incorporated into various systems, including messaging applications, internet browsers, electronic mail systems, and enterprise networks. This guarantees that the machine can be broadly followed and utilized in one-of-a-kind environments to enhance typical cybersecurity.in addition, the studies objectives to make a contribution to elevating focus about phishing attacks and selling more secure on-line behavior. by supplying customers with clear and accurate detection consequences, the gadget enables them understand the character of cyber threats and encourages them to undertake comfy practices. average, the inducement for these studies is driven by means of the urgent need to broaden a wise, adaptive, and reliable phishing detection machine that may efficiently combat contemporary cyber threats and make certain more secure virtual surroundings for customers.

VII. OUTCOMES:

The implementation of the proposed hybrid AI-based phishing detection system has resulted in several massive results that exhibit its effectiveness, reliability, and practical applicability in actual-world cybersecurity scenarios.one of the primary consequences of this study is a hit improvement of a device capable of correctly classifying phishing and legitimate content material. through integrating textual content-based analysis with picture-based totally type, the machine is able to detect complicated phishing patterns which can be frequently overlooked with the aid of conventional detection methods. The text module identifies suspicious URL systems and malicious textual indicators, while the CNN-based photo module detects visual anomalies inclusive of fake login pages, cloned interfaces, and misleading graphical elements. Another vital outcome is the machine's capability to hit upon formerly unseen phishing assaults. in contrast to traditional systems that rely on pre-defined regulations or blacklists, the proposed model uses machine learning and deep gaining knowledge of strategies to learn patterns from facts. This permits it to become aware of new and evolving phishing strategies, making it extra adaptable and future-evidence.

The discount in fake advantageous costs is another key fulfilment of the system. fake positives occur when valid websites are incorrectly categorised as phishing, that may cause person frustration and reduced believe within the gadget. with the aid of combining a couple of facts modalities, the hybrid version minimizes such errors and guarantees more correct category. This enhances person confidence and improves the general usability of the system.

The machine additionally demonstrates robust real-time detection competencies. it is able to examine URLs and pics immediately and offer instant feedback to users. that is particularly vital in stopping customers from interacting with malicious content, as timely detection can significantly reduce the threat of facts breaches and monetary losses.

Scalability is another important final result of the proposed gadget. The modular layout lets in it to be without problems deployed across exclusive systems, which includes net applications, cellular devices, and enterprise networks. The gadget can handle massive volumes of information correctly, making it suitable for real-international applications wherein excessive performance is needed.

The studies additionally executed a success integration of different additives, including statistics preprocessing, feature extraction, version training, and person interface layout. This end-to-quit system demonstrates the feasibility of enforcing a hybrid phishing detection framework in sensible environments. further to technical outcomes, the machine contributes to improving consumer protection and consciousness. via providing clean warnings and detection results, it allows users recognize ability threats and encourages them to undertake safer on-line practices. This instructional factor plays an important role in reducing the overall impact of phishing attacks. Moreover, the machine offers a strong basis for destiny upgrades. it can be extended with the aid of incorporating advanced deep getting to know architectures, increasing datasets, and integrating extra capabilities inclusive of behavioral analysis and anomaly detection. This guarantees that

the machine can preserve to conform and stay effective in opposition to rising cyber threats. Overall, the outcomes of these studies spotlight the effectiveness of the hybrid AI-primarily based method in enhancing phishing detection accuracy, lowering mistakes, and supplying a scalable and reliable answer for modern-day cybersecurity challenges.

VIII. CONCLUSION

The rapid evolution of phishing attacks presents a serious challenge to digital security systems worldwide. Traditional detection mechanisms, primarily based on blacklist filtering and rule-based URL analysis, are increasingly inadequate against modern phishing strategies that incorporate visual deception, domain obfuscation, and dynamically generated malicious links. This research addressed these limitations by proposing a hybrid AI-driven phishing detection framework that integrates text-based feature analysis with image-based classification using Convolutional Neural Networks (CNNs).

The proposed system successfully combines linguistic pattern recognition and deep visual feature extraction to improve

Furthermore, the modular architecture of the system allows scalability and real-time deployment across web platforms, messaging systems, email services, and enterprise security infrastructures. By leveraging artificial intelligence for automated threat detection, the proposed solution contributes to strengthening cybersecurity defenses and promoting safer digital communication environments.

In conclusion, this research demonstrates that integrating multi-modal analysis through AI and deep learning significantly enhances phishing detection capability. The proposed framework provides a robust, scalable, and adaptive solution capable of addressing the growing complexity of phishing attacks in modern digital ecosystems.

REFRENCES

[1] P. Zhang *et al.*, "CrawlPhish: Large-scale analysis of client-side cloaking techniques in phishing," in *Proc. IEEE Symp. Security Privacy (SP)*, 2021, pp. 1109–1124.

[2] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *Int. J. Hum. - Comput. Stud.*, vol. 82, pp. 69–82, 2015.

[3] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," *Neural Comput. Appl.*, vol. 25, no. 2, pp. 443–458, 2014.

[4] K. Jain and B. B. Gupta, "Phishing detection: Analysis of visual similarity-based approaches," *Secur. Commun. Netw.*, vol. 2017, Art. ID 5421046, 2017.

[5] S. Bahnsen, D. Aouada, and B. Ottersten, "Feature engineering for phishing detection: A comparative study," in *Proc. IEEE Int. Conf. Intell. Security Informatics*, 2017.

[6] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: Learning to detect malicious web sites from suspicious URLs," in *Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining*, 2009, pp. 1245–1254.

[7] Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection using convolutional neural networks," *Expert Syst. Appl.*, 2019.

[8] ENISA, "Cybersecurity threat landscape report," European Union Agency for Cybersecurity, 2021. [Online]. Available: https://www.enisa.europa.eu

[9] Anti-Phishing Working Group (APWG), "Phishing activity trends report," 2022. [Online]. Available: https://apwg.org

[10] Cisco, "Cybersecurity threat trends: Phishing and emerging threats report," 2021. [Online]. Available: https://umbrella.cisco.com

[11] S. Marchal, J. Francois, R. State, and T. Engel, "PhishStorm: Detecting phishing with streaming analytics," *IEEE Trans. Netw. Service Manag.*, vol. 11, no. 4, pp. 458–471, 2014.

[12] Le, A. Markopoulou, and M. Faloutsos, "PhishDef: URL names say it all," in *Proc. IEEE INFOCOM*, 2011, pp. 191–195.

[13] W. Han, J. Xue, and Y. Wang, "Phishing website detection based on deep learning," *Procedia Comput. Sci.*, vol. 129, pp. 165–171, 2018.

[14] H. Abutair and A. Belghith, "Using machine learning to detect phishing websites," *J. Inf. Security Appl.*, vol. 38, pp. 40–51, 2018.

[15] Y. Rao and A. Pais, "Detection of phishing websites using an efficient feature-based machine learning framework," *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3851–3873, 2019.

[16] Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet classification with deep convolutional neural networks," in *Adv. Neural Inf. Process. Syst. (NeurIPS)*, 2012, pp. 1097–1105.

[17] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *Int. Conf. Learn. Represent. (ICLR)*, 2015.