International Journal of Scientific Research and Engineering Development-– Volume X Issue X, Year

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Smart Phishing Detection System With Adaptive Threat Intelligence

Natha Priya R*, Padma Sundari E**

*(Student, Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli
Email:nathapriyar.ug22.cs@francisxavier.ac.in)

** (Assistant Professor, Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli
Email: padma@francisxavier.ac.in)

----------**********----------

Abstract:

One of the most significant cybersecurity concerns is phishing attacks. Phishing attacks are mostly carried out through malicious links, fake websites, and QR code scams. The conventional way of detecting these attacks is through static blacklisting. However, this is not an efficient way of detecting newly generated phishing sites. In this project, an AI-Powered Phishing Detection Web Application with an Accessibility Assistant is proposed. In this web application, the URL will be scanned in real time and classified as safe, suspicious, or phishing based on its characteristics such as its domain structure, presence of HTTPS, length of the URL, and presence of suspicious keywords. The web application also offers easy visualization of risks with the help of colors. In addition, an AI Robot Assistant with multiple languages and text-to-speech functionality is also offered to assist users in scanning the websites. In order to improve user awareness and usability, it also offers scan history and frequently visited sites. In this project, an efficient solution is proposed in the form of a lightweight web-based platform with an intuitive interface suitable for non-technical users, which can help in improving accuracy in detecting phishing sites.

Keywords — **Phishing Detection, Artificial Intelligence, URL Analysis, Cybersecurity, Web Application, Risk Visualization, Accessibility Assistant, Multilingual Support, Text-to-Speech, Scan History, Real-Time Detection, Machine Learning, User-Friendly Interface, QR Code Security, Domain Analysis**

----------**********----------

I. INTRODUCTION

Phishing attacks, which target people and organisations via phoney websites, malicious links, and bogus QR codes, have become one of the most common cybersecurity risks in recent years. Attackers utilise social engineering techniques to fool people into disclosing private information, including bank account information, login credentials, and personal information. Conventional security measures, such as browser alerts and blacklist-based detection systems, mostly rely on harmful URLs that have already been detected. Due to the continuous creation and modification of phishing websites, these traditional methods typically fail to identify newly developed threats, leaving consumers open to sophisticated attacks. Intelligent and proactive phishing detection systems are needed to get around these restrictions. Techniques for machine learning (ML) and artificial intelligence (AI) have demonstrated a great deal of promise in detecting questionable patterns in URLs and website structures. AI-driven systems are able to instantly categorise links as safe, suspicious, or phishing by examining attributes including domain characteristics, HTTPS usage, URL length, and suspicious phrases. Without depending exclusively on static databases, this method increases detection accuracy and makes it possible to identify unfamiliar phishing websites. Furthermore, giving users

 ©IJSRED: All Rights are Reserved

concise visual feedback and risk descriptions aids in their comprehension of the possible hazard level. In order to improve both security and usability, this study suggests an AI-Powered Phishing Detection Web Application with an Accessibility Assistant. Users can obtain immediate categorisation results with colour-coded risk indications by scanning URLs or QR codes. The program incorporates a multilingual AI robot assistant with text-to-speech capabilities and step-by-step instructions to enhance accessibility. This feature guarantees that the platform can be used efficiently by non-technical users, especially those with low literacy. In order to raise awareness and facilitate well-informed decision-making, the system also keeps track of scan history and frequently visited websites.

II. OBJECTIVE

This project's main goal is to create an AI-powered phishing detection web application that improves internet security by instantly identifying dangerous websites and links. In contrast to conventional methods that just rely on static blacklists, the suggested system seeks to give users with precise risk ratings by dynamically analysing URL properties. By assisting users in determining if a website is phishing, suspicious, or safe, the application lowers the likelihood of becoming a victim of online fraud.

Implementing sophisticated URL analysis using a variety of factors, including domain structure, HTTPS availability, URL length, and suspicious phrases, is another crucial goal. The algorithm can identify newly created phishing websites and classify links more efficiently by analysing these characteristics. Additionally, the initiative intends to make it easier for users to comprehend a link's security status by presenting the detection results using risk scores and clear visual indicators.

By including an AI-powered robot helper that offers detailed instructions, the system further concentrates on enhancing accessibility. This assistant's text-to-speech capabilities and multilingual instructions make it simple for non-technical users and those with low literacy to utilise the program. The system raises awareness of cybersecurity among a wider audience by providing voice-based interactivity and straightforward instructions.

In order to assist users in reviewing prior results and identifying often visited domains, the project also seeks to store scan history and frequently checked websites. This feature improves usability and enables users to leverage previous scans to make well-informed decisions. Additionally, the application may be simply accessible without complicated installations because to its lightweight web-based approach.

Lastly, the project aims to offer an effective and user-friendly phishing detection solution that incorporates real-time feedback, accessibility assistance, and AI-based analysis. The technology promotes safer browsing behaviour among users and helps to improve cybersecurity practices by combining intelligent detection with inclusive design.

By using domain-based analysis and real-time learning to lower false positives, the initiative also seeks to increase detection accuracy. The algorithm can improve its predictions and produce more dependable outcomes by examining regularly scanned webpages and identifying trusted domains. Future improvements like cloud-based data storage, QR code threat analysis, and integration with sophisticated machine learning models are also made possible by the application's modular architecture. This adaptability guarantees that the system can adjust to changing phishing tactics while preserving performance, scalability, and user-friendliness for a variety of users.

III. METHODOLOGY

In order to identify phishing websites in real time, the suggested system uses a systematic process that combines URL acquisition, feature extraction, intelligent analysis, and user-friendly result visualisation. The procedure starts with user input, in which the program receives a link to a website or a QR code. After that, the input is verified and

 ©IJSRED: All Rights are Reserved

preprocessed to extract important elements like the domain name and query parameters. To ascertain whether the link is safe, suspicious, or phishing, these characteristics are examined using rule-based and AI-assisted methods. By offering scan history monitoring, accessibility support, and visual feedback, the system further improves usability. By converting raw URL input into useful security data, our end-to-end pipeline empowers users to make defensible choices.

System Architecture: To improve usability for a variety of users, the system also includes an Accessibility Assistant module. This feature helps users engage with the program more efficiently by offering voice coaching and multilingual support. With text-to-speech capabilities, the assistant can help users navigate the scanning process, clarify findings, and provide security advice. This feature makes phishing detection accessible and simple to comprehend, which is especially helpful for non-technical users and those who need assistive technologies.Additionally, the program has a module called Scan History and Frequently Checked Websites that keeps track of previously examined URLs, their classification outcomes, and timestamps. Users may rapidly examine previous scans, find trustworthy websites, and analyse trends with the aid of this saved data. The technology also enables domain reputation analysis, which increases accuracy by identifying frequently visited trustworthy domains, by keeping a history database. As a result, there are fewer false positives and the detection results are more reliable.Additionally, real-time processing is supported by the design, which enables the system to analyse URLs instantaneously and without appreciable latency. Each component can function independently while also integrating seamlessly with other modules because to the modular architecture. Future improvements like machine learning-based classification, cloud-based threat intelligence, and QR code phishing detection are made possible by this method's increased scalability. Furthermore, logging and monitoring systems promote continual improvement by offering insights into system performance and detection accuracy. All things considered, the suggested architecture provides an adaptable, scalable, and user-friendly real-time phishing detection system with improved accessibility and intelligent risk analysis.

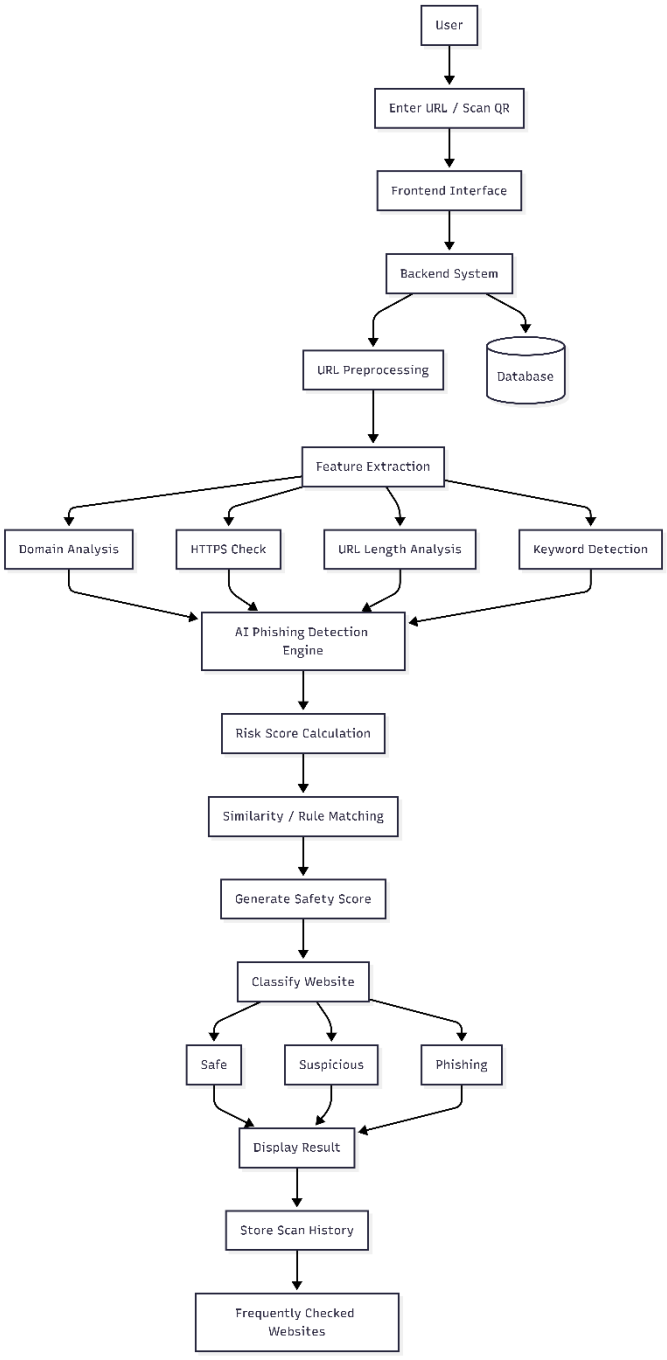

Fig. 1*. Block diagram of the proposed system*

A. ***URL Analysis Engine:*** To increase detection accuracy, the URL Analysis Engine also includes domain reputation assessment. The technique reduces false positives for valid websites by

 ©IJSRED: All Rights are Reserved

comparing frequently visited and well-known domains with stored history records. The reliability of the categorisation process is increased by this reputation-based evaluation, which aids in differentiating between newly formed suspicious links and trusted domains.

Additionally, the URL Analysis Engine uses pattern-based validation to identify obfuscation methods frequently employed in phishing scams. It looks for odd character combinations, overuse of special symbols, abbreviated URLs, and mismatched domain names that try to mimic real websites. The engine improves the detection of phishing links that are deceptively disguised by recognising these patterns. This extra layer of analysis improves the system's overall security while preserving quick processing, which makes it appropriate for real-time phishing detection in a web-based setting.

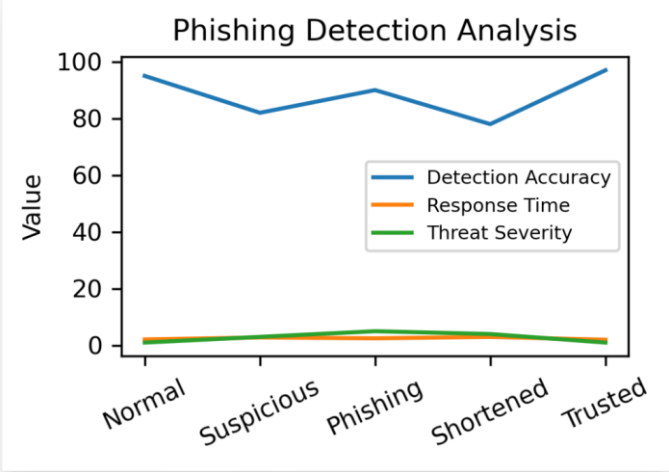

Fig 2: URL Threat Analysis in Phishing Detection Engine

B. ***Risk Scoring and Classification:*** The retrieved features are transformed into a numerical score that indicates the likelihood of phishing by the Risk Scoring Module. The algorithm divides the URL into three groups based on the computed value: phishing, suspicious, and safe. A high score points to possible phishing activity, whereas a low score denotes a trustworthy website. In order to minimise false positives for reliable websites, the classification logic additionally takes domain reputation into account. In order to help consumers comprehend the rationale behind the classification, the result is presented with visual cues and textual explanations. This strategy increases user confidence in the detection system and increases transparency.

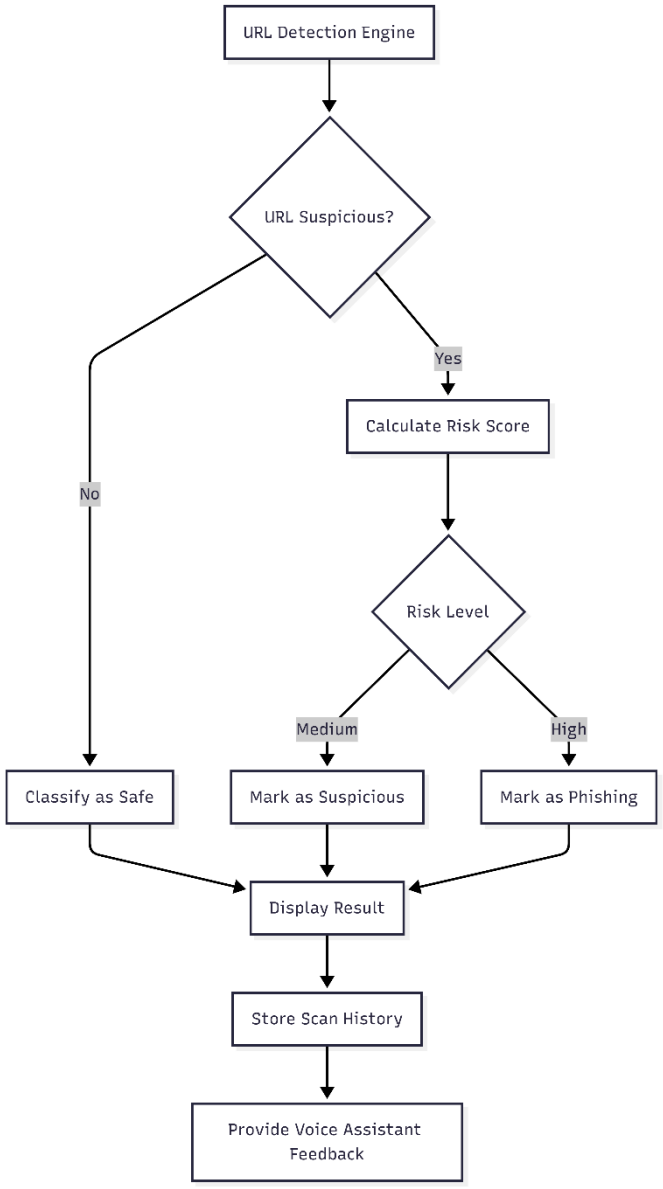

Fig.3. *Block diagram of the Deception Activation Layer*

C. ***Accessibility Assistant Module:*** The system incorporates an AI-based robot assistant that helps users navigate the scanning process in order to enhance usability. The assistant ensures accessibility for a variety of users by offering

 ©IJSRED: All Rights are Reserved

multilingual instructions in Tamil, Hindi, and English. Additionally, the assistant may aid visually impaired people by reading instructions aloud thanks to text-to-speech technology. The assistant provides step-by-step instructions in a scrollable popup and is visible as a fixed icon on the UI. This program raises non-technical users' understanding of cybersecurity and improves user engagement. Add two more lines.In order to help users promptly comprehend potential threats, the assistant also gives real-time feedback by notifying the safety status of scanned URLs. Additionally, it provides fundamental security advice and suggestions, urging users to steer clear of dubious connections and enhance secure browsing techniques.

D. ***History and Frequently Checked Websites Module:*** The risk scores and timestamps of previously scanned URLs are stored in the History Management Module. For convenience, this data is shown in a sidebar and kept locally. Additionally, the system recognises domains that are routinely examined, enabling users to swiftly examine frequently scanned websites. This feature enhances usability and aids users in identifying patterns that are trustworthy or questionable. The system offers a thorough and user-friendly phishing detection solution by fusing intelligent detection with history monitoring.award more points.The module also makes it possible for users to review previously scanned findings without reprocessing the same URLs, which speeds up response times and increases system effectiveness. Additionally, it helps improve domain reputation by learning from repeated scans, which over time enables the detection engine to produce classifications that are more accurate.

IV. RESULTS AND DISCUSSION

The efficiency of the suggested AI-powered phishing detection web application in spotting dangerous URLs and helping users make safe surfing choices was assessed. The assessment concentrated on accessibility features, detection accuracy, response time, and interface usability. The system's classification performance was evaluated using a mix of phishing, suspicious, and authentic URLs. To ascertain the overall usability and dependability of the system, the integration of the AI robot helper, scan history tracking, and visualisation components was also evaluated. The findings show that the suggested system effectively carries out real-time URL analysis while preserving an intuitive user interface appropriate for non-technical users.

1. Landing Page Interface

The main way that users can access the phishing detection system is through the landing page. It offers an easy-to-use interface for scanning QR codes and entering URLs. The system's features, such as real-time scanning, AI support, and history tracking, are prominently displayed in the layout. By enabling users to rapidly begin the scanning process without requiring technical understanding, this interface enhances usability.

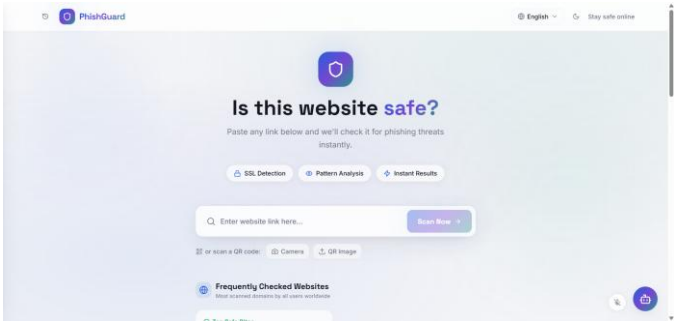

Fig.4. *Detection Engine – Threat Analysis Visualization*

2. URL Scanning and Detection Result

After correctly analysing input URLs, the system classifies them as Safe, Suspicious, or Phishing. Colour-coded markers are used to present the data, which enhances user comprehension of potential hazards. Based on features that have been retrieved, the detection engine generates a risk score and gives immediate feedback. This illustrates how well the feature-

 ©IJSRED: All Rights are Reserved

based analysis method works for spotting phishing websites.

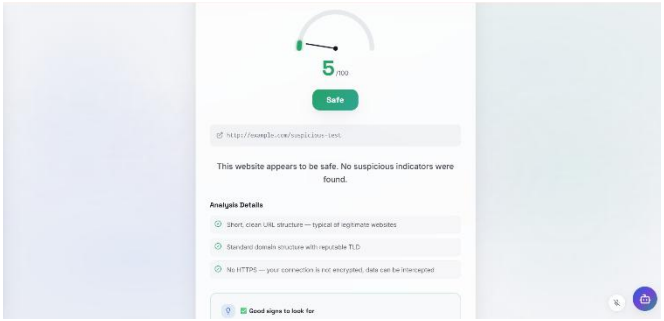

Fig. 5. *URL Scanning Result – Phishing Detection Output*

3. Risk Visualization Dashboard

Threat severity and detection accuracy are displayed graphically in the risk visualisation component. Users are better able to comprehend the relative risk levels connected to various URLs thanks to this graphical representation. The system's ability to offer both numerical and visual insights on phishing dangers is confirmed by the visualisation, which also improves decision-making.

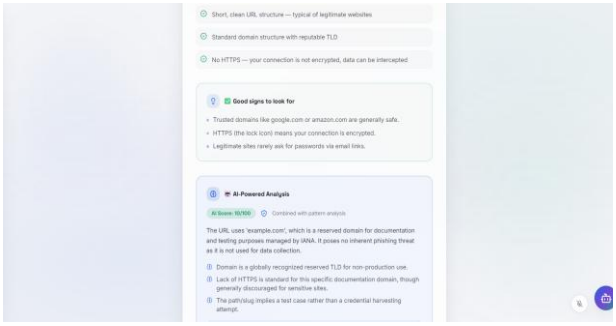

FIG. 6. *THREAT ANALYSIS – DETECTION ENGINE VISUALIZATION*

4. AI Robot Assistant Interface

The system successfully identifies malicious behavior and activates the deception protocol. The visual alert combined with automatic redirection ensures that attackers are isolated without affecting the host system. This confirms the effectiveness of the deception-based defense strategy.

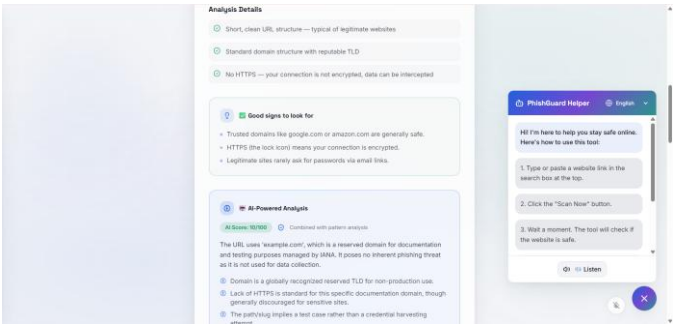

Fig. 7. *AI Robot Assistant – Accessibility Support Interface*

5. Scan History and Frequently Checked Websites

The scan history module keeps track of the risk levels of previously scanned URLs. Users can find frequently visited domains by looking over previous scans. This function enhances usability and aids in identifying reliable websites

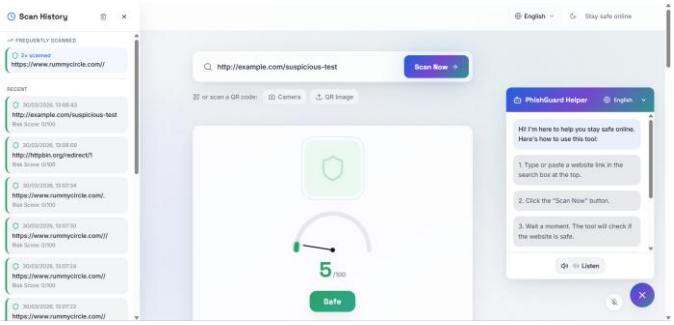

Fig. 8: *Scan History – Frequently Checked Websites Module*

V. REFERENCES

[1] N. ABDELHAMID, A. AYESH AND F. THABTAH, "PHISHING DETECTION BASED ASSOCIATIVE CLASSIFICATION DATA MINING," *EXPERT SYSTEMS WITH APPLICATIONS*, VOL. 41, NO. 13, PP. 5948–5959, 2014.

[2] M. A. ADEBOWALE, K. T. LWIN AND E. SANCHEZ, "INTELLIGENT WEB PHISHING DETECTION USING MACHINE LEARNING," *IEEE ACCESS*, VOL. 7, PP. 125020–125032, 2019..

[3] M. R. AHMED, M. M. ISLAM AND M. A. LAYEK, "PHISHING URL DETECTION USING COMPREHENSIVE FEATURE EXTRACTION AND MACHINE LEARNING TECHNIQUES," *IEEE ACCESS*, VOL. 12, PP. 45678–45690, 2024.

 ©IJSRED: All Rights are Reserved

[4] A. AL-QASMI, A. AL-ANAZI, L. AL-SHEHRI, S. AL-SHAMAN, W. AL-ATAWI AND O. ABBASS, "MACHINE LEARNING-BASED PHISHING DETECTION SYSTEM," IN *PROC. IEEE INT. CONF. ARTIFICIAL INTELLIGENCE AND CYBERSECURITY*, PP. 112–118, 2024.

[5] A. ALJOFEY, Q. JIANG AND A. RASOOL, "AN EFFECTIVE PHISHING DETECTION MODEL BASED ON MACHINE LEARNING," *IEEE ACCESS*, VOL. 9, PP. 135320–135333, 2021.

[6] R. BASNET, S. MUKKAMALA AND A. H. SUNG, "DETECTION OF PHISHING ATTACKS: A MACHINE LEARNING APPROACH," IN *PROC. IEEE INT. CONF. SOFT COMPUTING AND PATTERN RECOGNITION*, PP. 373–378, 2015.

[7] K. L. CHIEW, C. L. TAN, K. WONG, K. S. C. YONG AND W. K. TIONG, "A NEW HYBRID ENSEMBLE FEATURE SELECTION FRAMEWORK FOR MACHINE LEARNING-BASED PHISHING DETECTION," *IEEE ACCESS*, VOL. 6, PP. 71484–71497, 2018.

[8] A. S. BALAKRISHNAN AND M. S. ISLAM, "VM ISOLATION AND SANDBOXING TECHNIQUES FOR SECURE HOST ENVIRONMENTS," IEEE ACCESS, VOL. 9, PP. 24533-24546, 2021.

[9] Y. DING, N. LUKTARHAN, K. LI AND W. SLAMU, "A KEYWORD-BASED COMBINATION APPROACH FOR DETECTING PHISHING WEBPAGES," *IEEE ACCESS*, VOL. 7, PP. 23324–23335, 2019.

[10] A. EL AASSAL, S. BAKI, A. DAS AND R. M. VERMA, "AN IN-DEPTH BENCHMARKING AND EVALUATION OF PHISHING DETECTION RESEARCH FOR SECURITY NEEDS," IN *PROC. IEEE SECURITY AND PRIVACY WORKSHOPS*, PP. 1–8, 2020.

[11] I. FETTE, N. SADEH AND A. TOMASIC, "LEARNING TO DETECT PHISHING EMAILS," IN *PROC. IEEE INT. WORLD WIDE WEB CONF.*, PP. 649–656, 2007.

[12] S. GARERA, N. PROVOS, M. CHEW AND A. D. RUBIN, "A FRAMEWORK FOR DETECTION AND MEASUREMENT OF PHISHING ATTACKS," IN *PROC. ACM WORKSHOP ON RECURRING MALCODE*, PP. 1–8, 2007.

[13] A. K. JAIN, B. B. GUPTA AND S. JAIN, "A NOVEL APPROACH FOR PHISHING DETECTION USING MACHINE LEARNING," IN *PROC. IEEE INT. CONF. ADVANCES IN COMPUTING, COMMUNICATIONS AND INFORMATICS*, PP. 160–165, 2018.

[14] A. KUMAR, V. SINGH AND S. PATEL, "REAL-TIME PHISHING DETECTION USING DEEP LEARNING MODELS," *IEEE ACCESS*, VOL. 11, PP. 55234–55245, 2023.

[15] A. S. Ahuja and A. Reddy, "Artificial Intelligence-Based Assistance Systems: A Survey," *IEEE Access*, vol. 9, pp. 152643–152666, 2021.

 ©IJSRED: All Rights are Reserved