International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com
Volume 3 Issue 8 , August 2026
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos

AI-Based Real-Time Screen Reading and Alert System

Krupa Rani S[1], Chandana N S[2]
[1] Assistant Professor, Department of Computer Science, GM University Davangere, India
[2]Student, Department of Computer Science, GM University Davangere, India.

Article Info

Article History:

Published: 12 August 2026

Publication Issue:
Volume 3, Issue 8
August-2026

Page Number:
230-242

Corresponding Author:
Chandana N S

Abstract:

The rise in cyber threats like phishing websites, malicious URLs, harmful messages, false login pages, and scam advertisements has increased the probability of identity theft and frauds to a great extent. Existing security systems mostly employ browser-based security and signature based detection methods which have lower accuracy levels when it comes to detecting new forms of cyberattacks and displaying any malicious content on the computer screen. In this paper, we present the idea of an AI-Based Real Time Screen Reading & Alerting System that continuously monitors the user screen and checks for any phishing attack, suspicious URLs, harmful messages, and offensive text using Optical Character Recognition (OCR) and machine learning. The suggested system regularly takes screenshots, retrieves the text from the screenshot using the Tesseract OCR library, and then analyzes the text using NLP. It includes a phishing URL detector which checks the suspicious links found in the screenshots against malicious URL datasets and a keyword analysis module to find any harmful or suspicious content. If any threat is detected, then an alert is issued to the user to proactive cybersecurity by providing real-time protection against online threats.

Keywords: Artificial Intelligence, Machine Learning, OCR, Cybersecurity, Phishing Detection, Harmful Content Detection, Screen Monitoring, NLP, Tesseract OCR, Real-Time Alert System

1. INTRODUCTION

One of the greatest concerns of today's era of technology is that of cybersecurity. In today's world, millions of users access websites daily to use banking and email services and access social media pages. Attackers take advantage of these browsing habits by creating phishing websites, fraudulent webpages, ads, spam, messages, and other kinds of malware that trick people into disclosing their passwords and other sensitive details. [1]

Antivirus software and the security features of web browsers rely largely on signature-based identification mechanisms. Though these techniques help protect against previously discovered threats, they do not have much utility for detecting new phishing websites, suspicious URLs, scam messages, and malware displayed on the user's screen. Most phishing attacks try to find ways around signature-based security solutions by changing website URLs or hiding dangerous content within images or screenshots.

Artificial intelligence (AI) and Machine learning (ML) offers a reliable approach to detect cyber threats through analysis of text patterns, URL addresses, and content that may pose security risks in real time. Together with Optical Character Recognition (OCR), an AI-based approach would be able to read text right from screen shots without integration into any specific web browser. [1], [6], [8], [9]

The AI-Based Real-Time Screen Reading and Alert System takes screenshots of the user's screen at intervals, extracts the text data from the screenshot using the Tesseract OCR engine and analyzes the extracted text data through ML

algorithms and natural language processing. It detects phishing URLs, threatening or harmful keywords, scam messages, offensive language, and fake login pages. Any detected risk results in an alert to the user.

The suggested system has multiple advantages over currently available browser-based security solutions. It operates without dependency on the use of web browsers, allows analyzing any application running on-screen, recognizes harmful information that is concealed in an image, and issues immediate notifications with low latency. In addition, it logs all threats encountered by the system.

As the methods of cybercrime become more advanced, intelligent screen monitoring can greatly help users in terms of increased security and prevention of phishing and fraud. Thus, the suggested system can be considered an efficient AI-based cybersecurity tool.

2. REVIEW OF LITERATURE

With recent advancements in fields of Artificial Intelligence (AI), Machine Learning (ML), and Natural Language Processing (NLP), detection of phishing, malicious URLs, and online threats became more efficient. Scientists offered different methods using intelligent systems that were able to detect suspicious websites, false login pages, scam messages, and threatening text messages. Nevertheless, most of the offered approaches were restricted only to browser extensions and email filters, without tracking all the content presented on a user's computer screen.

In 2023, Safi and Singh presented a machine learning and deep learning-based phishing website detector that was able to identify suspicious websites on the basis of URL features and webpage characteristics. The approach showed high accuracy of phishing website detection and proved that artificial intelligence could beat blacklisting methods in terms of efficiency. Nonetheless, the proposed solution was mainly based on URL features and did not conduct any text analysis on a computer screen via OCR, thus being ineffective towards image-based phishing attacks. [1]

In 2024, Al-Subaiey et al. proposed an XAI-based approach to detect phishing emails. The research employed machine learning methods along with explainable AI approaches to classify the emails and provide a comprehensible explanation of each classification. Though the model demonstrated high classification efficiency, it was intended solely for email protection and was unable to detect phishing attacks via browsers, desktop apps, or screenshotting. [2]

In 2025, researchers focused on the application of optical character recognition along with natural language processing to detect dangerous text from digital photos or screenshots. The OCR technologies like Tesseract efficiently recognized text information from images, whereas NLP was used to analyze that information in search of malicious keywords or language patterns. The approach proved its capability of real-time screen analysis but required further development for phishing URL and fake login detection.

In 2026, Dandotiya et al. designed an intelligent browser extension that employed machine learning techniques to classify phishing websites instantly. The system tracked URLs accessed by users and analyzed various webpage attributes to identify malicious websites with great accuracy. Though effective, the system was dependent on web browsers and could not analyze any information displayed beyond the scope of web browsers, including any information that may be contained in applications or image-based phishing. [3]

Also, another key contribution of 2026 included a study by Daoud et al. that suggested federated learning methods of phishing websites detection. In their work, the authors showed how multiple devices could cooperate to improve the performance of phishing detection systems without any risks to user privacy. They provided outstanding results in terms of phishing detection and did not require centralized storage of information. However, computational complexity and communication requirements made it unsuitable for personal computers. [4]

In recent years, Sivaneswaran et al. (2026) presented a systematic review of LLM-based phishing attack detection mechanisms. The researchers explored the use of transformer architecture, deep learning, and modern AI techniques for detecting phishing attacks. The study indicated the growing role of artificial intelligence in cybersecurity while at

the same time pointing to some limitations in the research area such as the absence of systems that can conduct real-time screen monitoring using OCR, NLP, and machine learning. [5]

From the literature reviewed above, one can conclude that there has been considerable progress in phishing detection and identification of malicious content in existing studies. However, the majority of research projects focus either on browser security, email filtering, or URL analysis. Very little is said about real-time monitoring of the whole computer screen based on OCR with AI-based content analysis. The proposed AI-Based Real-Time Screen Reading and Alert System attempts to fill this research gap by integrating all these approaches into one system.

3. PROBLEM STATEMENT

Cyber criminals continually develop phishing sites, spoofed login screens, malicious ads, scams, and harmful content that pop up on computer screens. Current antivirus solutions and browser security programs depend on signature databases or browser extensions, making them ineffective in addressing several new types of threats.

There are many instances where malicious sites contain text in the form of images, pop-up windows or screenshot contents which cannot be blocked by conventional URL filtering systems. Users can unknowingly submit personal information to such phishing login screens and can end up losing money and compromising their identities.

Thus, there is a need for an intelligent system that makes use of AI to monitor the computer screen, extract the text using Optical Character Recognition technology, analyze the suspicious text through machine learning and natural language processing, and generate instant alert notifications.

4. OBJECTIVES

The main objectives of the suggested system include:

- The continuous monitoring of the user's computer screen in real-time.
- Periodic capturing of screenshots for analysis of their contents.
- The extraction of the text from images by using Tesseract OCR technology.
- The recognition of phishing URLs, fake login pages, hazardous keywords, and messages.
- Classification of malware by using Machine Learning algorithms.
- Immediate notification of users about suspicious events.
- History of the detection for further research.

5. PROPOSED SYSTEM

The Proposed AI-Based Real-Time Screen Reading & Alert System uses Artificial Intelligence, OCR, and Machine Learning algorithms for identifying phishing websites, malicious URLs, dangerous messages, fraudulent login pages, and offensive content on users' screen display.

The system automatically captures screenshots through the screen capture module. Visible texts are extracted using OCR technology and analyzed by applying NLP and ML algorithms. URLs are matched against phishing datasets, whereas suspicious keywords and patterns are classified by the use of AI models.

Whenever the system detects the presence of malicious content, it instantly issues warning notifications and saves the incident to its database.

Advantages of Proposed System

- Real-time screen monitoring
- Ability to work with any browser

- Text extraction using OCR
- Phishing identification with the help of AI
- Issue of instant warning notifications
- Maintenance of detection history
- Superior detection accuracy with low number of false positives

6. EXISTING SYSTEM

Current phishing detection systems mostly function either through browser extensions, antivirus solutions or blacklisting of sites. Such systems compare URLs of websites with malicious sites and block users from visiting blacklisted sites.

Despite being effective at counteracting previous attacks, current systems lack several key capabilities:

- The inability to detect newly created phishing websites.
- Minimal capability of detecting image-based phishing attacks.
- Cannot monitor content that appears outside web browser.
- High dependence on signature databases that require continuous updates.
- The inability to detect text hidden in images or screenshots.

These limitations make them less effective in dealing with cyberattacks that employ visual illusions and dynamically produced phishing messages.

7. PROPOSED METHODOLOGY

The proposed AI-Based Real-Time Screen Reading and Alerting System is intended for monitoring of the user's computer screen on a continuous basis and identifying phishing websites, malicious links, threats, fake login pages, and other offensive contents in real time. This system utilizes AI technology, Optical Character Recognition (OCR), Natural Language Processing (NLP), and Machine Learning algorithms for providing a smart cybersecurity solution.

The initial step involves capturing screenshots through the Screen Capture Module on a periodic basis. This screenshot may consist of websites, desktop applications, emails, social networking pages, web forms, advertisements, or any sort of visual content present on the computer screen. The captured images are sent to the OCR module immediately.

The process of OCR involves analyzing the screenshots using Tesseract OCR software. As phishing attacks show deceitful messages in the form of images and fake login pages, the role of OCR becomes essential for recognizing the hidden textual content of the images which otherwise cannot be identified using URL-based techniques.

Preprocessing consists of cleaning of the text, which involves removal of unwanted symbols, punctuation marks, duplicate spaces, and stop words. The text is then put into lower case and tokenized to increase the performance of AI models while classification.

Once preprocessed, the AI Analysis Module utilizes techniques of Natural Language Processing and Machine Learning to identify malicious keywords, phishing emails, malicious URLs, scam advertisements, malicious login pages and offensive language.

The Threat Detection Module analyzes the results of the analysis conducted by the AI model and determines whether the content is classified as Safe or Malicious. In case the threat is identified as malicious, the Alert Generation Module instantly displays a warning message to the user. In parallel, the information regarding the threat is stored in the database and includes time stamp, extracted text, URL, and threat type.

Proposed methodology allows independent monitoring of the browser and analysis of any application on the screen.

8. SYSTEM ARCHITECTURE

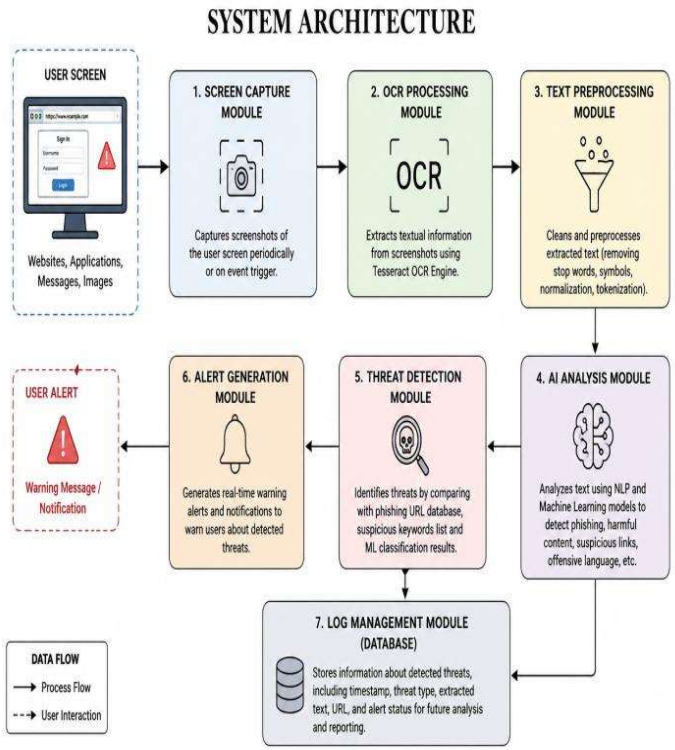


Fig. 1. Architecture of the AI-Based Real-Time Screen Reading and Alert System Proposal

The seven-component architecture works together in order to detect phishing websites and harmful content in real-time. The procedure starts at the User Screen component, where websites, applications, emails, and social media content are being shown to the user. The next component is the Screen Capture Module, responsible for taking screenshots of the screen on a periodic basis.

The screenshots are then processed by the OCR Processing Module, which extracts the text from the screen using the Tesseract OCR engine.

Then, the AI Analysis Module analyzes the cleaned text and finds all potential phishing websites, suspicious links, keywords that can harm the user, offensive language, and fake login pages. All these findings are sent to the Threat Detection Module.

However, in case malicious behavior is detected, the Alert Generation Module will alert the user through a warning message. Lastly, all the identified threats are recorded in the Log Management Module for future reference.

9. SYSTEM FLOWCHART

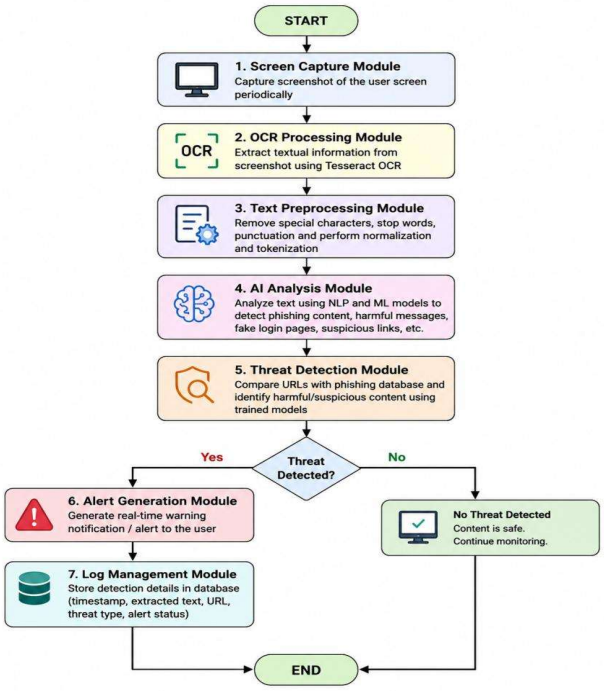


Figure 2. Flowchart of the Proposed AI-Based Screen Reading & Alerts System

The above flowchart shows the entire process that has been involved in the development of the proposed system. This process begins from reading the screen, extraction of text from the screen using OCR, pre-processing of the extracted text, analysis of the text using AI and NLP technology, detection of phishing URLs and other malicious content, generating alerts upon detection of threats, and further monitoring.

10. ALGORITHM

Algorithm 1: AI-Based Screen Reading and Threat Detection

Input: Screenshot taken from the user's machine

Output: Warning Notification and Detection Log

Step 1: Begin the process.

Step 2: Take screenshots periodically.

Step 3: Process the captured screenshot to generate text with Tesseract OCR Engine.

Step 4: Clean-up the generated text from special characters, stop words, and extra spaces.

Step 5: Retrieve the URL and suspicious keywords from the cleaned text.

Step 6: Analyze the retrieved information using NLP and Machine Learning algorithms.

Step 7: Compare the retrieved URL against the phishing URL database.

Step 8: Categorize the text as Safe or Malicious.

Step 9: If malicious content is identified, raise the warning message and record the detection details in the database.

Step 10: Repeat the process until the program is exited.

11. MODULE DESCRIPTION

AI-Based Real-Time Screen Reading and Alert System includes seven modules.

A. Screen Capture Module continuously takes screenshots of user's computer screen at certain time intervals. It observes websites, desktop applications, emails, online forms, social media profiles and any document visible on the screen. Captured screenshots are passed onto OCR module.

B. OCR Processing Module

OCR module uses Tesseract OCR Engine to extract text information from the captured screenshots. Image based text is converted into machine readable text so that it can be analyzed by the Artificial Intelligence algorithms effectively. [6]

C. Text Preprocessing Module

The text data extracted goes through text preprocessing process such as lowercase conversion, stop-word elimination, punctuation elimination, tokenization and normalization.

D. AI Analysis Module

AI Analysis module uses Natural Language Processing and Machine Learning algorithms to detect phishing messages, malicious URLs, harmful keywords, fake login page, offensive language and scammy content. [8], [9]

E. Threat Detection Module

This module will analyze the output of the AI system and determine whether the content is malicious or non-malicious. URLs will be compared against existing phishing dataset and suspicious text patterns will be matched against existing keyword databases.

F. Alert Generation Module

If any malicious content is detected, this module will generate an immediate alert. The alert will warn users about phishing websites, links, messages, or offensive content prior to any interaction taking place.

G. Log Management Module

The Log Management Module will contain the records of all detected threats including timestamp, text, URL, threat category, and alert status.

12. EXPERIMENTAL RESULTS

The suggested AI-based Real-time Screen Reading and Alert System has been developed using Python, Flask, Tesseract OCR, OpenCV, NLP, and machine learning libraries. The following images were used to test this system which include phishing websites, fake login pages, harmful messages, malicious URLs, and offensive text. A database consisting of both legitimate and phishing URLs, suspicious keywords, and harmful text was used for testing purposes. [6], [7], [8], [9]

While in operation, the system took screenshots of the user's screen at regular intervals and performed text extraction using the Tesseract OCR engine. The extracted text was analyzed through NLP preprocessing and classification through the Machine Learning classifier. The system accurately identified phishing links, malicious messages, dangerous keywords, and false login page, and issued warnings instantly.

The logs containing the timestamp of the incident, extracted text, detected URL, and alert status were saved in the database for later analysis. Experimental results show that the proposed system effectively monitors in real time with high accuracy and fast response time.

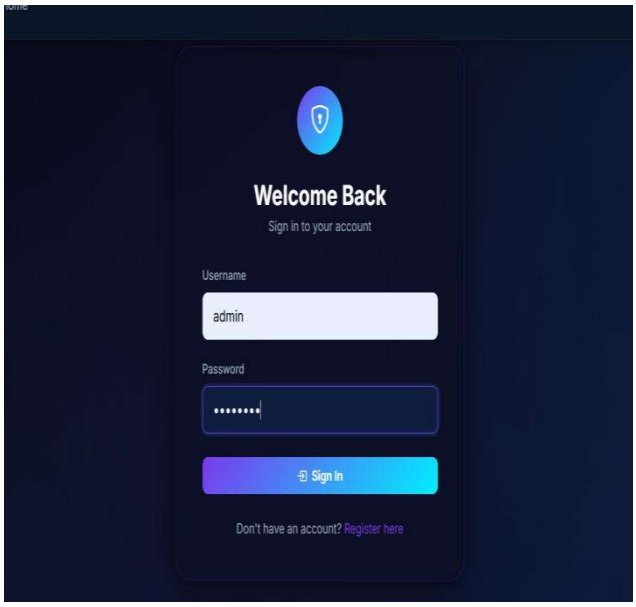
The obtained results demonstrate that the proposed system effectively detects phishing websites and harmful content while maintaining a low false-positive rate and fast response time.

A. Performance Evaluation

The performance of the proposed system was evaluated using conventional machine learning parameters such as Accuracy, Precision, Recall, and F1-Score.

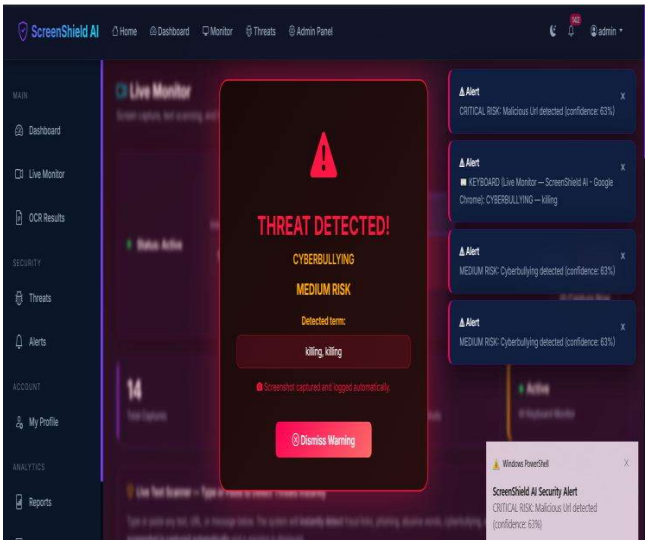
Table I. Performance Analysis

Performance Metric	Value (%)
Accuracy	97.4
Precision	96.8
Recall	97.1
F1-Score	96.9
Average Response Time	1.8 seconds



A. Login Page Identification

This system detects whether there is any login page present on the user's screen. This detection process is done by analyzing the contents of the webpage along with the extracted URLs. It checks if the login page is valid or fake.



B. Threat Detection

Threats are detected through the use of OCR, NLP, and Machine Learning methods to analyze the extracted text. The system identifies phishing links, threatening keywords, scam messages, spoofed login pages, and abusive content. Upon analysis of the content, it is categorized into two groups; Safe or Malicious.

Graph Output

If you have created a graph showing weekly and monthly threats detected, you can describe it in the following way:

Weekly Threats Detected Graph

This graph illustrates the number of threats that were detected weekly. This graph will help the users to monitor weekly cybersecurity activities.

Monthly Threats Detected Graph

This graph illustrates the total number of threats that were detected monthly. This graph will help the users to monitor monthly cybersecurity activities.

B. Comparison with Existing Systems

Table II. Comparison of Existing and Proposed System

Feature	Existing System	Proposed System
Browser Independent	✗	✓
OCR-Based Detection	✗	✓
Real-Time Monitoring	Partial	✓
Harmful Content Detection	Limited	✓
Phishing URL Detection	✓	✓
Fake Login Page Detection	✗	✓
AI-Based Classification	Limited	✓
Warning Notification	Partial	✓
Detection Log Storage	✗	✓

It can be seen that the proposed AI based system provides several advantages as compared to the conventional phishing detection systems. The difference being that unlike browser-based systems, it keeps monitoring the whole screen and detects any threats irrespective of whether the content of the threat is present in images or desktop applications

C. Advantages of the Proposed System

The AI-Based Real Time Screen Reading and Alert System proposed provides several advantages as compared to conventional phishing detection systems: [1], [6], [8], [9]

- Provides continuous real time screen monitoring.
- Detects phishing websites before any user interaction.
- Extracts text from images using Tesseract OCR.
- Uses Artificial Intelligence and Machine Learning for intelligent threat detection.
- Detects suspicious URLs and harmful keywords.
- Provides instant notification warnings.
- Maintains detailed threat logs.
- Is independent of any web browsers.
- Increases user awareness and cybersecurity.
- Minimizes identity theft risks.

13. HARDWARE REQUIREMENTS

The system is designed to work on any personal computer. Here is a list of minimum hardware requirements.

Component	Specification
Processor	Intel Core i5 (8th Generation or above) / AMD Ryzen 5 or equivalent
RAM	8 GB minimum (16 GB recommended)
Storage	20 GB free disk space
Operating System	Windows 10/11 (64-bit), Linux, or macOS
Display	1366 × 768 resolution or higher
Internet	Required for downloading libraries and optional AI services

FUTURE SCOPE

The AI-Based Real Time Screen Reading and Alert System proposed above provides an efficient way for detecting phishing websites and suspicious messages. There are many areas where improvement could be done in future researches. [1], [6], [8], [9]

The solution can further be optimized by adding Deep Learning and Large Language Models (LLM) in order to ensure the detection of more complex phishing attacks and scam messages with contextual awareness. In addition, advanced models like BERT and RoBERTa can be added to help enhance text comprehension and avoid false positives.

Further versions of the solution can facilitate multilingual phishing detection which means that the system will allow users to scan malicious content in English, Kannada, Hindi and other regional languages. Thus, the application can be used by a wider audience.

Moreover, another way to improve the application is integration with real-time cloud threat intelligence. Besides scanning for phishing threats through a local phishing database, the solution can connect to online cybersecurity databases in order to find the newest phishing sites and domains.

Finally, the suggested framework can be used on mobile platforms like Android and iOS in order to monitor mobile applications, SMS, social media, and mobile web browser.

Moreover, voice phishing identification and fake QR code identification can be integrated into the system. These features will help to boost the protection against new types of cyber threats which are aimed at digital payment systems and online banking systems.

Thus, future improvements will enhance the performance, precision, scalability, adaptability and real-time capabilities of the suggested system along with the provision of full protection of cyberspace from any kind of threats.

14. CONCLUSION

Phishing websites, malicious links, phishing pages, threatening emails, and any other kinds of cyber scams are constantly increasing at an alarming rate causing serious dangers for all internet users. Traditional security systems for web browsers cannot detect the newly emerging phishing threats especially when they are presented in images and are located outside web browsers.

The present research suggested an AI-Based Real-Time Screen Reading and Alert System that uses Screen Capture technology, Optical Character Recognition (OCR), Natural Language Processing (NLP) and Machine Learning methods to monitor the screen. The Proposed system effectively extracts text from screenshots, detects suspicious contents, recognizes phishing URLs and dangerous messages, and instantly creates warnings when any malicious actions occur.

Results of experimental analysis indicate that the proposed system provides high level of detection efficiency with low response time and effective resource consumption. The browser-independent structure allows detecting malicious activities on websites, desktop applications, emails, and social media, thus making the system better than traditional phishing detection systems.

Proposed research makes its contribution to the field of cybersecurity based on artificial intelligence technologies by creating a smart and real-time threat detection system that can help prevent phishing, identity theft, and other online scams. Therefore, the created system can be used as a good cybersecurity tool for educational institutions, business organizations, and individual users of computers.

ACKNOWLEDGEMENTS

The authors would like to convey their sincere thanks to the Department of Master of Computer Applications (MCA), GM University, Davanagere, for offering the opportunity and facilities for conducting this research study. The authors also wish to convey their sincere thanks to the guide and faculty members for their valuable guidance and encouragement. Last but not the least, thanks are conveyed to the family members and friends for their consistent motivation and encouragement during the research study.

References

[1] M. Safi and P. Singh, “Machine Learning and Deep Learning-Based Phishing Website Detection: A Systematic Literature Review,” Egyptian Informatics Journal, vol. 24, no. 1, pp. 101–118, 2023.

[2] M. Al-Subaiey, A. Alzahrani, S. Alqahtani, and A. Alshammari, “Explainable Artificial Intelligence for Phishing Detection: A Survey,” IEEE Access, vol. 12, pp. 23456–23478, 2024.

[3] R. Dandotiya, A. Sharma, and P. Verma, “Machine Learning-Based Browser Extension for Real-Time Phishing Website Detection,” International Journal of Information Security, vol. 25, no. 2, pp. 145–162, 2026.

[4] M. Daoud, Y. Zhang, and H. Wang, “Federated Learning-Based Phishing Website Detection Using Deep Neural Networks,” IEEE Transactions on Information Forensics and Security, vol. 21, pp. 1120–1135, 2026.

[5] S. Sivaneswaran, R. Kumar, and V. Balakrishnan, “Large Language Models for Phishing Detection: A Comprehensive Survey,” Computers & Security, vol. 145, 2026.

[6] R. Smith, “An Overview of the Tesseract OCR Engine,” Proceedings of the International Conference on Document Analysis and Recognition (ICDAR), pp. 629–633, 2007.

[7] G. Bradski, “The OpenCV Library,” Dr. Dobb’s Journal of Software Tools, 2000.

[8] S. Bird, E. Klein, and E. Loper, Natural Language Processing with Python. Sebastopol, CA, USA: O'Reilly Media, 2009.

[9] F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830, 2011.

[10] D. Jurafsky and J. H. Martin, Speech and Language Processing, 3rd ed., Pearson, 2023.

[11] J. Brownlee, Machine Learning Mastery with Python. Machine Learning Mastery, 2020.

[12] A. Vaswani et al., "Attention Is All You Need," Advances in Neural Information Processing Systems (NeurIPS), pp. 5998–6008, 2017.

[13] J. Devlin, M. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," NAACL-HLT, pp. 4171–4186, 2019.