

AI-POWERED PHISHING DETECTION SYSTEM IN WHATSAPP WEB CLONE

R B Aarthinivasini¹, Sridevi S², Subashini M³, Roshini P⁴, Shanjana P⁵

¹Professor, Dept. of IT, Meenakshi College of Engineering, Tamilnadu, India

²UG Scholar, Dept. of IT, Meenakshi College of Engineering, Tamilnadu, India

³UG Scholar, Dept. of IT, Meenakshi College of Engineering, Tamilnadu, India

⁴UG Scholar, Dept. of IT, Meenakshi College of Engineering, Tamilnadu, India

⁵UG Scholar, Dept. of IT, Meenakshi College of Engineering, Tamilnadu, India

Abstract - Phishing is a significant cybersecurity issue, particularly on platforms like WhatsApp, where users often receive deceptive messages, harmful links, and media files. This project focuses on designing an AI-based phishing detection tool integrated into a WhatsApp Web Clone, which actively blocks phishing threats before user interaction. Advanced ML and DL models are used in the system to examine messages, links, and visual content for threats. Technologies like Next.js, Socket.io, and PostgreSQL support the frontend, real-time communication, and backend data storage for seamless operation. The core AI module, developed in Python, utilizes OpenCV, Tesseract OCR, BERT, CNN and Google's Safe Browsing API to identify phishing patterns in shared content. Zegocloud helps enable secure and verified voice and video calls by managing authentication and encrypted transmission. The application also features voice deepfake detection using advanced audio analysis to flag potential synthetic threats. Testing in various phishing scenarios showed reliable detection accuracy and effective mitigation of fraudulent transmissions. Future enhancements include integrating deepfake detection for video and voice calls, implementing behavioral analysis, deploying AI-powered CAPTCHA, and extending the system to mobile applications beyond the WhatsApp Web clone to further strengthen security.

Key Words: Artificial Intelligence, Phishing Detection, WhatsApp Web, Deepfake detection, Google safe browsing API, Zego Cloud, URL detection, Image detection

1. INTRODUCTION

Phishing has emerged as a serious cyber threat, especially on instant messaging platforms like WhatsApp. These platforms are frequently exploited by attackers to deceive users through fraudulent messages, disguised URLs, and misleading media content. Traditional phishing prevention strategies often fail to address real-time communication threats. This project introduces an AI-enhanced phishing detection system within a WhatsApp Web clone. The solution integrates advanced Natural Language Processing (NLP), Computer Vision (CV), and machine learning techniques to detect and block phishing attempts in real

time. Key components include BERT for text classification, OpenCV and CNN for image-based detection, and Wav2Vec for analyzing voice messages. The system ensures secure communication through AES-256 encryption and supports future enhancements for deepfake prevention and behavioural analysis.

1.1 Aim

The aim of this project is to develop an AI-powered phishing detection system integrated within a WhatsApp Web clone, capable of identifying and preventing phishing attacks in real time. By utilizing techniques from Natural Language Processing (NLP), Computer Vision (CV), this system will analyze messages, URLs, images, and deepfake voice message to detect potential phishing threats before user interaction. The goal is to enhance user security, prevent social engineering attacks, and create a safer messaging environment.

1.2 Objectives

The objective of this project is to develop an AI-powered phishing detection system within a WhatsApp Web clone that can identify and prevent phishing attacks in real time before users interact with harmful content. The system will use NLP (BERT) to analyze chat messages, Google Safe Browsing API for URL detection, and OpenCV with Tesseract OCR for phishing image analysis. Additionally, the system will provide real-time alerts to notify users of potential threats while ensuring secure messaging through end-to-end encryption (AES-256). The chat application will be built using Next.js, Prisma, PostgreSQL, and WebSockets to support fast and secure communication, with future enhancements planned for voice phishing detection and AI-driven fraud prevention.

1.3 Purpose

The primary purpose of this project is to safeguard users from phishing attacks within a messaging platform. Unlike traditional phishing detection systems that operate on emails and web browsers, this system actively prevents phishing inside real-time messaging applications. The AI-

powered system aims to reduce financial fraud, identity theft, and cyber scams by integrating advanced AI techniques directly into chat applications.

- Enhance security for WhatsApp-like messaging platforms by proactively detecting phishing content.
- Prevent cyber fraud through early phishing detection before users interact with malicious content.
- Improve digital trust by ensuring secure communication without privacy risks.
- Provide real-time AI-based protection that works across text messages, URLs, and multimedia content.

1.4 Scope

The scope of this project is to develop a fully functional WhatsApp Web clone with built-in AI-powered phishing detection. It focuses on real-time messaging security, ensuring that phishing attacks are identified before they can cause harm.

- Real-time Chat System - Built using Next.js, Prisma, PostgreSQL, and WebSockets.
- Phishing Detection in Messages & URLs - AI analyzes text messages and links in real time.
- Image-Based Phishing Detection - Uses Computer Vision (OCR + CNN) to analyze phishing images.
- Real-Time Alerts & Prevention - Users receive instant phishing warnings before clicking malicious content.
- Data Security & Encryption: Messages are end-to-end encrypted with AES-256 advanced encryption.
- Scalability for Future Enhancements: The system will allow future features like voice and video call phishing detection, behavioural analysis and AI-powered fraud alerts.

2. LITERATURE REVIEW

Extensive research has explored phishing detection, mainly focusing on email and website protection. Rule-based filtering and blacklists were early attempts but lacked adaptability to evolving attack methods. Recent approaches involve AI, combining NLP, ML, and CV techniques. Sharma et al. utilized ensemble models like Random Forest and XGBoost for URL classification. BERT, introduced by Devlin et al., improved phishing detection by capturing contextual semantics in text. Image-based phishing detection using CNNs and OpenCV has also shown promising results, particularly for detecting altered logos and scam screenshots. Real-time threat detection using WebSockets, and secure communication

via JWT or OAuth protocols, are critical to modern chat systems. Our system combines these state-of-the-art techniques to deliver a unified phishing prevention tool tailored to messaging platforms.

The growing prevalence of phishing attacks represents a critical challenge in the field of cybersecurity, targeting users through deceptive messages, fraudulent URLs, and malicious attachments. Traditional phishing detection techniques, such as rule-based filtering and blacklisting, have shown limitations in detecting zero-day phishing attacks, where attackers continuously modify their strategies to evade detection [1]. To overcome these limitations, various AI-based phishing detection systems have been proposed, integrating Machine Learning (ML), Natural Language Processing (NLP), and Computer Vision (CV) to enhance phishing identification accuracy [2].

One of the earliest approaches to phishing detection was rule-based filtering, which relied on analyzing message patterns, domain age, and textual features to classify phishing attempts. Sharma et al. (2021) introduced an ensemble learning model combining Random Forest and XGBoost for phishing detection in URLs, improving classification accuracy [3]. However, rule-based approaches struggle with detecting new phishing patterns, leading to the adoption of AI-driven models capable of learning from evolving attack strategies [4]. Liang et al. (2022) introduced a deep reinforcement learning model that dynamically adapts to new phishing strategies by learning from user interactions, significantly improving real-time phishing detection accuracy [5].

With the advancement of NLP techniques, deep learning models like Bidirectional Encoder Representations from Transformers (BERT) have become effective for text-based phishing detection. Research by Yang et al. (2021) demonstrated that transformer-based models outperform traditional ML classifiers in detecting phishing messages and emails by understanding context and semantic patterns [6]. Inspired by these findings, our project integrates BERT for chat message analysis in WhatsApp Web Clone, ensuring accurate phishing detection before user engagement.

In addition to text-based phishing detection, image-based phishing detection has gained attention due to attackers using fake QR codes, fraudulent logos, and phishing website snapshots to deceive users. Studies by Kumar et al. (2020) and Li et al. (2021) successfully implemented OpenCV and Convolutional Neural Networks (CNNs) to analyze phishing images, detecting scam logos and altered images in phishing attacks [7]. Our project adopts a similar approach by integrating OpenCV and Tesseract OCR for analyzing shared images in WhatsApp Web Clone, ensuring multi-modal phishing detection.

Another crucial aspect of our system is real-time phishing prevention. Research on Socket.io and WebSocket-based security architectures by Chang et al. (2020) highlights the benefits of low-latency, bidirectional data flow, making it ideal for instant messaging applications [8]. Our implementation of Socket.io enables real-time scanning and detection of phishing messages, providing immediate alerts before users interact with malicious content.

Authentication and security mechanisms are also essential for preventing phishing attacks. Researchers have emphasized the importance of OAuth and JWT-based authentication in securing messaging platforms, preventing unauthorized access and message tampering [9]. Our project integrates NextAuth.js for secure authentication to verify user identities before accessing the chat system. Additionally, Google Safe Browsing API, widely used in cybersecurity applications, enhances our phishing prevention capabilities by cross-checking URLs in real time [10].

Emerging threats such as voice and video phishing require advanced security measures. Studies have shown that attackers manipulate victims through voice calls and video messages, making detection more challenging [11]. To address this, our project integrates ZegoCloud's WebRTC API for encrypted voice and video calls, ensuring secure communication and reducing interception risks [12].

In summary, the literature highlights the need for a multi-modal phishing detection system in messaging applications, integrating NLP-based text analysis, image recognition, real-time messaging security, and authentication mechanisms. While existing studies have focused on individual aspects of phishing prevention, our project combines these techniques into a single AI-powered phishing detection system for WhatsApp Web Clone. By leveraging BERT for text phishing detection, OpenCV for image analysis, NextAuth.js for authentication, Google Safe Browsing API for URL security, and ZegoCloud for secure communication, our system offers a comprehensive and real-time phishing prevention solution. Future enhancements may include federated learning and adversarial AI techniques to further strengthen phishing detection against evolving cyber threats [13][14][15].

3. RELATED WORKS

3.1. Existing System

The current phishing detection systems primarily rely on outdated techniques such as static blacklists, rule-based spam filters, and predefined heuristics. These systems are only effective against previously identified threats and fail to detect newer or evolving phishing attacks. Real-time protection is significantly lacking, as most solutions do not analyze content dynamically or instantly. While some

systems can detect suspicious text messages, they often fail to analyze phishing attempts delivered via images, voice messages, or multimedia. Furthermore, traditional systems alert users only after a phishing link is clicked, which defeats the purpose of early detection. In addition, security and privacy remain major concerns, with many systems lacking end-to-end encryption and proper authentication mechanisms, leaving user data vulnerable to cyber threats.

- Detects only known phishing patterns; fails to handle zero-day attacks.
- No real-time scanning or instant alerts before user interaction.
- Lacks capability to analyze images, voice messages, or multimedia for phishing.
- Poor data privacy and no advanced encryption or secure communication mechanisms.

3.2 Proposed System

The proposed system introduces an AI-powered phishing detection system integrated into a WhatsApp Web Clone, offering real-time and multi-modal phishing detection capabilities. This system utilizes Natural Language Processing (NLP) for message analysis, Computer Vision (CV) and Convolutional Neural Networks (CNNs) for image phishing detection, and audio processing models like Wav2Vec for deepfake voice detection. The integration of Optical Character Recognition (OCR) enhances the ability to extract and analyze text embedded in images. Real-time alert mechanisms notify users immediately when suspicious content (text, URL, image, or voice) is detected, helping prevent interaction with phishing attempts. Additionally, AES-256 encryption is used to ensure secure message transmission, protecting user data from interception or tampering. The system is designed to be scalable and can be extended to other messaging platforms beyond WhatsApp, making it future-ready.

- AI-Based Real-Time Phishing Detection – Uses BERT NLP, OpenCV, and ML algorithms for phishing prevention.
- Google Safe Browsing API for URL Verification – Detects malicious URLs before user interaction.
- Image-Based Phishing Detection – Scans images, QR codes, and fake login screens to prevent scams.
- Real-Time Alerts and Notifications – Warns users before engaging with phishing messages.

4. ARCHITECTURAL DIAGRAM

The architecture is built using a modular and scalable approach to facilitate a wide range of functionalities such

as chat messaging, media sharing, voice and video calling and advanced security detections as shown in figure 4.1.

The frontend of the application is developed using the Next.js framework, which allows server-side rendering and static site generation, improving performance and user experience. The application follows a modular structure with key components, including the Login Page, Chatlist Module, Search and Messaging Module, Media Sharing Module, Voice and Video Call Module, and the Voice Notes Module. These modules collectively deliver a user interface that replicates the essential features of WhatsApp Web, offering users an intuitive and engaging environment.

The backend infrastructure is engineered to support real-time interaction, user authentication, data encryption, and AI-based analysis. The Prisma ORM acts as an interface between the application and the PostgreSQL database, ensuring efficient data querying with built-in validation and error handling. Firebase Authentication is utilized to handle user login and secure session management. Additionally, NextAuth.js is integrated for supporting third-party login providers and extending authentication mechanisms.

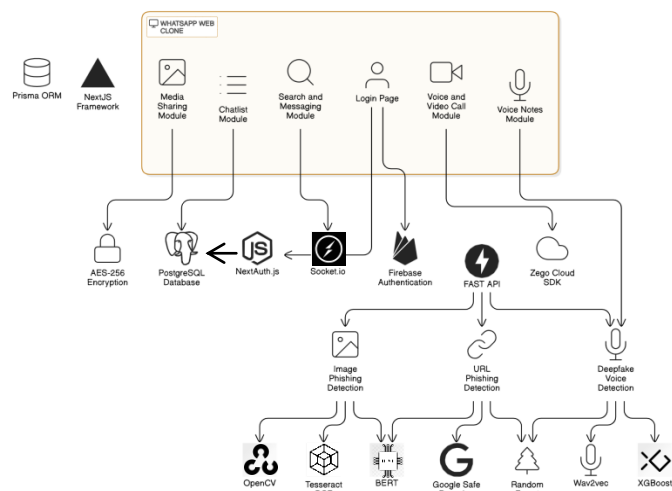


FIGURE 4.1. Architecture diagram

Socket.io plays a pivotal role in enabling real-time messaging by establishing bi-directional event-based communication between the server and the client. This is essential for implementing live chat and message delivery indicators such as seen ticks and typing status. Communication data including messages and media are encrypted using AES-256 encryption, which is a widely trusted encryption standard ensuring that all user data is protected from unauthorized access during transmission and storage.

To extend functionality and ensure system security, FAST API is used as a lightweight, high-performance web framework for building RESTful APIs that connect to various AI-based modules. One such module is the image phishing detection system, which combines OpenCV for image preprocessing, Tesseract OCR for text extraction and BERT for contextual analysis of the extracted text. This system is designed to identify and block images that contain embedded phishing content before they reach the user.

Similarly, the application incorporates a URL phishing detection system that leverages the Google Safe Browsing API. Whenever a user shares a link, the system cross-checks it against a constantly updated database of known phishing, malware, and deceptive websites. To combat deepfake threats, especially in voice messages and calls, the system includes a deepfake voice detection module. This component uses Wav2Vec for extracting speech features from voice recordings and XGBoost, a gradient boosting machine learning algorithm, to classify whether the voice is real or synthetically generated. By integrating this capability, the application not only supports voice communication but also ensures the integrity and authenticity of the audio content.

The real-time voice and video communication features are supported through the Zego Cloud SDK, which provides a reliable and scalable media streaming solution. This SDK enables high-quality audio and video calling functionality with low latency and efficient bandwidth management, mimicking the smooth experience users expect from platforms like WhatsApp.

In conclusion, the architecture combines the strengths of modern web development frameworks, real-time communication protocols, secure data handling mechanisms, and advanced AI-driven security modules.

5. SYSTEM DESCRIPTION

5.1. Login Module

The login module provides secure user authentication using email/password or third-party logins. It allows users to personalize their profile with a name, bio, and profile picture. Features include encrypted communication, secure password storage, session management (single sign-on), and informative error handling. Login attempts are logged for monitoring, and users can log out securely.

5.2. Voice Message Module

This module allows users to record, preview, delete, and send audio messages with playback controls. It supports hands-free recording with visual waveform feedback, adjustable playback speed, and timestamped audio. AES-

256 encryption ensures secure transmission and playback is restricted to intended recipients for privacy.

5.3. Voice and Video Call Module

Supports one-on-one and group calls using WebRTC and Zego Cloud SDK with adaptive bitrate streaming. Provides real-time call status, call history, and missed call alerts. Features include automatic fallback to audio in low bandwidth, participant display, and end-call confirmation. All communications are encrypted end-to-end for privacy and security.

5.4. Chatlist Call Module

Organizes ongoing and past chats with message previews, timestamps, and read/unread indicators. Shows contact names and profile pictures, supports real-time online status, chat sorting, and a responsive scrolling interface. Enhances accessibility to frequently contacted users.

5.5. Search and Messaging Module

Enables efficient message and contact search with real-time delivery and read statuses. Supports text, multimedia, emojis, and maintains a secure, complete chat history. Includes keyword, contextual, and contact-based search functions to simplify navigation and improve user interaction.

5.6. Media Sharing Module

Allows secure sharing of images, videos, documents, and audio using AES-256 encryption. Supports multiple formats and real-time phishing detection using OCR and AI models. Alerts users to threats before viewing/download, and applies content moderation using CNNs. Media is timestamped, preview-enabled, and optimized for cross-device compatibility.

6. SYSTEM IMPLEMENTATION

The primary aim of implementation is to deliver a fully functional product that matches the design specifications and satisfies user requirements. For our AI-Powered Phishing Detection System integrated with a WhatsApp Web Clone, this means ensuring that all modules phishing detection in text, images, and voice messages, real-time alerting system, secure login, and encrypted communication work seamlessly together within the messaging interface.

This stage also focuses on setting up the appropriate environment configurations, installing dependencies, connecting to real-time databases like Firebase, and deploying APIs built using frameworks like FastAPI. Testing plays a critical role during implementation. It involves running the system with sample data, validating

phishing detection responses, checking user interface responsiveness, and correcting bugs. Error handling, logging, and data validation mechanisms are also finalized to ensure system robustness.

In addition, security measures such as implementing AES-256 encryption for chats, secure OAuth-based login via Firebase, and phishing verification through Google Safe Browsing API are deployed during implementation. The system is then tested under real-time conditions using live data to ensure its accuracy, responsiveness, and reliability.

Another essential part of implementation is user configuration and training. Even if the system is technically sound, it must be easy to use. Therefore, the interface, user onboarding, and feedback mechanisms are fine-tuned during this stage. Deployment tools like Vercel are used to publish the frontend application, while backend services are hosted on platforms like Firebase and AWS for high availability and scalability.

- Code Integration: Combining different modules into a unified, functioning system.
- Environment Setup: Installing software, libraries, and dependencies across all development and deployment environments.
- API & Database Connection: Linking the backend logic to databases (PostgreSQL, Firebase) and integrating real-time APIs (FastAPI, Google Safe Browsing, ZegoCloud).
- Unit & Integration Testing: Testing individual components and their interactivity.
- Real-Time Data Testing: Feeding live inputs (URLs, images, audio files) to test detection response times and accuracy.
- Error Correction & Optimization: Identifying bottlenecks and refining algorithms for performance.
- Deployment: Hosting frontend and backend using tools like Vercel and Firebase.
- User Acceptance Testing (UAT): Evaluating the system with end users to ensure it meets expectations.
- Monitoring & Maintenance: Logging system activity, collecting analytics, and planning future updates.

Through successful implementation, the system transitions from a theoretical model to a real-world application capable of detecting phishing attacks across multiple communication formats URLs, images, and voice. It demonstrates how AI, when integrated with secure communication tools, can proactively protect users from phishing threats in real time. The system is now ready for

deployment, user testing, and further refinement based on feedback and evolving cyberattack patterns.

7. RESULTS AND DISCUSSION

The results obtained from the implementation of the AI-Powered Phishing Detection System demonstrate the practical effectiveness of integrating real-time threat detection into a messaging environment like WhatsApp Web. The system was tested across various phishing scenarios, including suspicious URLs, image-based scams (like QR codes and fake login screens), and voice messages potentially generated using deepfake technology. Upon interacting with potentially harmful content, the system successfully triggered alert popups, warning users before they could proceed. This proactive alert mechanism played a critical role in reducing user exposure to phishing content. The AI models specifically those using machine learning algorithms like Naïve Bayes and Random Forest for URL classification, and CNN-based models for image analysis consistently achieved high detection accuracy in controlled testing environments.

Furthermore, the deepfake voice detection module using LSTM and GAN architectures was able to distinguish between human and AI-generated audio samples, adding an extra layer of protection against voice phishing (vishing). The integration of Google Safe Browsing API for URL validation and AES-256 encryption for data protection enhanced the overall security and reliability of the system.

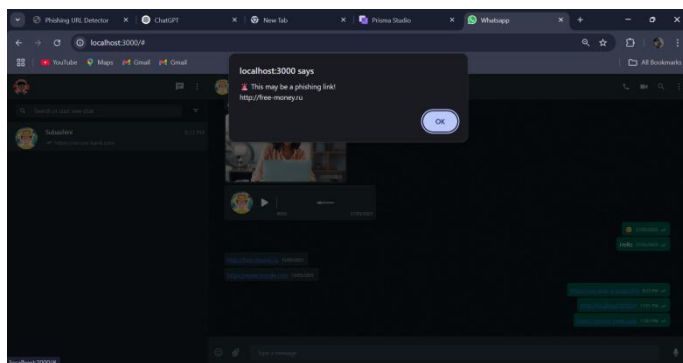


FIGURE 7.1. URL Phishing Detection

In Figure 7.1 shows that the system automatically detects malicious URLs in chats. A warning popup notifies the user of a potentially dangerous link. This helps users to avoid falling victim to malicious websites. Security features are deeply integrated into the messaging flows.

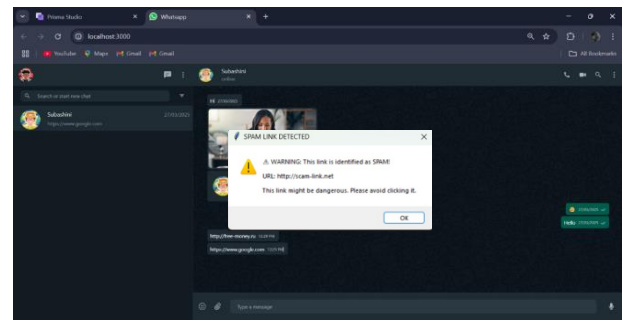


FIGURE 7.2. Image Phishing Detection

In Figure 7.2 shows that this screen shows a phishing alert for an image with a suspicious link. The system detects malicious image content and warns the user. It prevents users from falling for phishing tricks disguised as images. A warning popup highlights the detected threat.

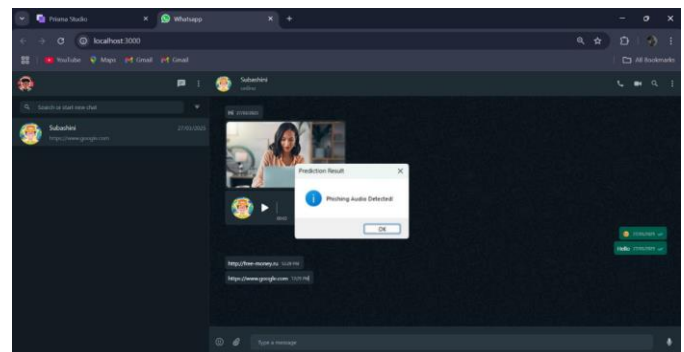


FIGURE 7.3. Deepfake Voice Phishing Detection

In Figure 7.3 shows that inside the chat, a phishing detection feature scans voice messages. An alert is shown when a phishing audio is detected. This improves security by preventing audio-based social engineering. The warning popup ensures users stay aware of threats.

8. CONCLUSION

The AI-powered phishing detection system for WhatsApp Web Clone represents a significant advancement in real-time cybersecurity for messaging applications. With the increasing sophistication of phishing attacks, traditional security measures such as blacklisting and rule-based filtering have proven inadequate in preventing evolving threats. This project successfully integrates machine learning, deep learning, and real-time monitoring to proactively identify phishing attempts in text messages, URLs, and multimedia content. By leveraging NLP models like BERT for text classification, OpenCV for image-based phishing detection. The incorporation of Google Safe Browsing API for real-time URL scanning and NextAuth.js for secure authentication adds an extra layer of protection to the platform. Furthermore, the system's real-time communication framework, built with Next.js, Prisma, and

WebSockets, ensures seamless user experience while maintaining security standards.

Unlike conventional phishing detection techniques, which operate in a reactive manner, this implementation provides a proactive approach to phishing prevention, significantly reducing user exposure to cyber threats. As phishing techniques continue to evolve, future improvements include integrating deepfake detection for video and voice calls, implementing behavioral analysis, deploying AI-powered CAPTCHA, and extending the system to mobile applications beyond the WhatsApp Web clone to further strengthen security. By integrating these advanced security mechanisms, this project lays a strong foundation for secure and intelligent real-time communication, contributing to the future of AI-driven cybersecurity solutions in digital messaging platforms.

9. FUTURE ENHANCEMENT

To strengthen further the AI-powered phishing detection system for WhatsApp Web Clone, several enhancements can be implemented in future:

- Behavioural Analysis – AI analyzes user interactions to detect suspicious behaviour and alerts the user instantly
- Deepfake Voice & Video Call Phishing Detection – Implement Generative Adversarial Networks (GANs) and deep learning models to detect AI-generated scam calls and manipulated videos.
- AI-Powered CAPTCHA for User Verification – Implement AI-based CAPTCHA in high-risk conversations to detect and block bot-driven phishing attempts.
- Mobile App Development (Android & iOS) – Extend the phishing detection system to mobile applications, ensuring users remain protected across all devices.

These enhancements will significantly improve security, scalability, and phishing detection accuracy, that ensures real-time messaging applications remain resilient against emerging cyber threats.

REFERENCES

- [1] Dalsaniya, Abhay. (2023). AI-Based Phishing Detection Systems: Real-Time Email and URL Classification.
- [2] Manurung, Ferdinand & Munawir, & Pradeka, Deden. (2025). Spam and Phishing Whatsapp Message Filtering Application Using TF - IDF and Machine Learning Methods. *Green Intelligent Systems and Applications*. 5. 1-13. 10.53623/gisa.v5i1.551.
- [3] Ansari, Meraj Farheen & Sharma, Pawankumar & Dash, Bibhu. (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. 3. 61-72. 10.47893/IJSSAN.2022.1221.
- [4] Mughaid A, AlZu'bi S, Hnaif A, Taamneh S, Alnajjar A, Elsoud EA. An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Comput.* 2022;25(6):3819-3828. doi: 10.1007/s10586-022-03604-4. Epub 2022 May 14. PMID: 35602317; PMCID: PMC9107003.
- [5] Aruna, Ms.M.G & V, Maheswari & M, Pranethaa. (2023). A web application for real-time phishing website detection. *International journal of scientific research in engineering and management*. 07. 1-11. 10.55041/IJSREM26477.
- [6] M. Sameen, K. Han and S. O. Hwang, (2020) "PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System," in *IEEE Access*, vol. 8, pp. 83425-83443, doi: 10.1109/ACCESS.2020.2991403.
- [7] Bauskar, Sanjay & Madhavaram, Chandrakanth & Galla, Eswar Prasad & Sunkara, Janardhana Rao & Gollangi, Hemanth Kumar. (2024). AI-Driven Phishing Email Detection: Leveraging Big Data Analytics for Enhanced Cybersecurity. *SSRN Electronic Journal*. 44. 7211-7224. 10.2139/ssrn.4980647.
- [8] S. Asiri, Y. Xiao, S. Alzahrani, S. Li and T. Li, (2023) "A Survey of Intelligent Detection Designs of HTML URL Phishing Attacks," in *IEEE Access*, vol. 11, pp. 6421-6443, doi: 10.1109/ACCESS.2023.3237798.
- [9] L. Tang and Q. H. Mahmoud, (2022) "A Deep Learning-Based Framework for Phishing Website Detection," in *IEEE Access*, vol. 10, pp. 1509-1521, doi: 10.1109/ACCESS.2021.3137636.
- [10] LAMINA, Oladimeji Azeez et al. (2024) Ai-Powered Phishing Detection And Prevention. *Path of Science*, [S.l.], v. 10, n. 12, p. 4001-4010. ISSN 2413-9009.
- [11] Y. A. Alsariera, M. H. Alanazi, Y. Said, and F. Allan, (2024) "An Investigation of AI-Based Ensemble Methods for the Detection of Phishing Attacks", *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 3, pp. 14266-14274.
- [12] Basit, A., Zafar, M., Liu, X. et al. (2021) A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommun Syst* 76, 139-154. <https://doi.org/10.1007/s11235-020-00733-2>
- [13] W. Li, S. Manickam, Y. -W. Chong, W. Leng and P. Nanda, (2024) "A State-of-the-Art Review on Phishing Website Detection Techniques," in *IEEE Access*, vol.

12, pp. 187976-188012, doi:
10.1109/ACCESS.2024.3514972.

- [14] Arun, Akshaya, and Nasr Abosata. (2024) "Next Generation of Phishing Attacks using AI powered Browsers." arXiv preprint arXiv:2406.12547.
- [15] Ravindra, Salvi & Sanjay, Shah & Gulzar, Shaikh & Pallavi, Khodke. (2021) "Phishing Website Detection Based on URL." International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 589-594. 10.32628/CSEIT2173124.



committed to contributing to the field of secure communication.

Shanjana P is a final-year UG scholar in Information Technology at Meenakshi College of Engineering. Her areas of interest include human-computer interaction and secure application development. She has collaborated on team-based AI research projects. She is dedicated to solving real-world problems through innovative technology.

BIOGRAPHIES



Mrs. R. B. Aarthinivasini is a Professor in the Department of Information Technology at Meenakshi College of Engineering, Tamil Nadu. She specializes in computer science. With academic experience, she is passionate about guiding UG scholars in cutting-edge research.



Sridevi S is a final-year UG scholar in the Department of Information Technology at Meenakshi College of Engineering. Her research interests include UI/UX designing and AI applications. She actively participates in academic projects. She aims to pursue a career in designing.



Subashini M is a final-year UG scholar in Information Technology at Meenakshi College of Engineering. She is focused on machine learning and data security research. Subashini has worked on academic projects involving AI-based threat detection. She aspires to become a technology innovator in digital security.



Roshini P is a final-year UG scholar in the Department of IT at Meenakshi College of Engineering. She has a keen interest in web technologies, AI-based systems, and information security. Her academic involvement includes developing user-friendly applications. She is