Cyber Safe Voice

Prof. Divyamani M K
Dept. of ISE
Sai Vidya Institute of Technology
Bengaluru, India

Hemakiranmai HR
Dept. of ISE
Sai Vidya Institute of Technology
Bengaluru, India

Lakshmi R
Dept. of ISE
Sai Vidya Institute of Technology
Bengaluru, India

PushpaPallavi D E
Dept. of ISE
Sai Vidya Institute of Technology
Bengaluru, India

Abstract - **The proliferation of cyber threats and phishing attacks has necessitated innovative approaches to user security awareness. This paper presents Cyber Voice Alert, a novel browser extension that provides real-time, multilingual voice-based security warnings to users when they navigate to potentially unsafe websites. The system continuously monitors the user's browsing activity by analyzing URLs in real time. This process involves examining the URL structure, checking the communication protocol, validating security certificates, and applying pattern-matching techniques to identify any suspicious or insecure behavior. Once sufficient data is collected by the monitoring module, it is forwarded to the Threat Analysis Engine for deeper evaluation.**

Keywords: Cybersecurity, Voice Alerts, Multilingual Interface, Browser Extension, Phishing Detection, Web Security, Accessibility, Human-Computer Interaction

I. INTRODUCTION

The rapid growth of internet usage has significantly transformed the way people access information, communicate, and perform daily activities. Along with these advantages, the digital environment has also become a fertile ground for cyber threats such as phishing websites, malicious links, fake login pages, and deceptive online content. Many users unknowingly fall victim to such threats due to lack of awareness or inability to recognize warning signs in time. Traditional browser-based security warnings often rely only on visual indicators, which may go unnoticed or misunderstood, especially by non-technical users.

In recent years, the need for more inclusive and attention-grabbing cybersecurity solutions has gained importance. Users with visual impairments, elderly individuals, children, and people unfamiliar with technical terminology often struggle to interpret text- based alerts or security symbols. Even experienced users tend to ignore repeated visual warnings due to warning fatigue. This highlights a critical gap in existing web security mechanisms, where alerts are present but not always effective in preventing unsafe user actions.

To address these challenges, this paper introduces Cyber Safe Voice Alert, a browser-based security solution that combines visual notifications with real- time voice alerts. The system is designed to provide immediate, clear, and understandable warnings whenever a user encounters a potentially harmful or suspicious website. By delivering alerts through both audio and visual channels, the system ensures higher user attention and improves response time. The inclusion of multilingual voice support further enhances accessibility, allowing users to receive warnings in their preferred language.The proposed approach focuses on improving user awareness rather than relying solely on technical blocking mechanisms. By clearly informing users about security risks at the moment of interaction, the system empowers them to make safer browsing decisions. This human-centric design not only increases the effectiveness of security warnings but also promotes responsible and informed internet usage. The Cyber Safe Voice Alert system aims to bridge the gap between cybersecurity technology and real-world user behavior, making web security more practical, inclusive, and impactful.

II LITERATURE SURVEY

2.1 Web Security and Threat Detection

Phishing Detection Techniques

Garera et al. (2007) proposed a URL-based phishing detection approach using logistic regression. Their method analyzed URL structure, domain age, and lexical features, achieving an accuracy of 95%. This study laid the foundation for identifying suspicious URLs and significantly influenced later phishing detection systems.

Zhang et al. (2007) introduced CANTINA, a content-based phishing detection system that employed TF-IDF algorithms combined with search engine queries. The system achieved a high true positive rate of 97%. However, the approach required substantial computational resources, which limited its applicability in real-time environments.

Aburrous et al. (2010) developed a fuzzy logic-based phishing detection model that incorporated 27 distinct features, including SSL certificate validation, domain registration information, and webpage structural characteristics. Their hybrid approach effectively reduced false positive rates to 3.2%, demonstrating improved detection reliability.

SSL/TLS Certificate Analysis

Akhawe et al. (2013) conducted an extensive study on browser-based SSL warnings and observed that users ignored or bypassed nearly 70% of certificate warnings. Their findings highlighted the limited effectiveness of conventional visual security warnings and emphasized the need for alternative alert mechanisms.

Felt et al. (2015) analyzed user interactions with SSL warnings across different web browsers. The study revealed that warning design plays a crucial role in user compliance. Full-page interstitial warnings in Chrome achieved a compliance rate of 37%, compared to only 12% for passive security indicators.

2.2 Browser Extensions for Security

Extension Architecture and Capabilities

Carlini et al. (2012) examined the internal security architecture of browser extensions and identified privilege escalation vulnerabilities in approximately 70% of popular extensions. Their research established key security guidelines and best practices for extension development.

Ter Louw et al. (2013) proposed BLADE, a framework designed to build browser extensions with formal security guarantees. The framework significantly influenced modern browser extension manifest specifications and secure extension development practices.

Security-Focused Extensions

Kirda and Kruegel (2005) developed NoScript, a security extension that selectively blocks executable scripts to prevent drive-by download attacks. Their approach successfully prevented 87% of such attacks, though it required extensive user configuration and technical understanding.

Reis et al. (2018) introduced SafeBrowse, a machine learning-based browser extension that analyzes webpage behavior in real time. The system achieved a detection accuracy of 96%, but its high memory usage of approximately 45 MB negatively impacted browser performance.

2.3 Multilingual and Voice-Based Interfaces

Text-to-Speech in Web Applications

Khan and Sutcliffe (2014) evaluated the performance of the Web Speech API across 12 languages and reported a speech intelligibility rate of 94% for supported languages. Their findings validated text-to-speech technology as an effective interface modality for web applications.

Raman (1997) pioneered audio-based web browsing through Emacspeak, demonstrating that auditory interfaces could provide information access comparable to visual interfaces for visually impaired users.

Multilingual Cybersecurity

Kumaraguru et al. (2009) investigated phishing susceptibility among different demographic groups and found that non-English speakers were 2.3 times more likely to fall victim to phishing attacks due to language barriers in cybersecurity awareness.

Wash and Rader (2015) examined users' mental models of security threats and showed that culturally adapted security messages improved user comprehension by 58% compared to direct translations.

2.4 Accessibility in Cybersecurity

Visual Impairment and Web Security

Vigo et al. (2013) analyzed web accessibility challenges faced by blind users and reported that 89% of security indicators were inaccessible to screen readers. Their findings exposed major shortcomings in inclusive security design.

Branham and Mukkath Roy (2019) conducted participatory design studies involving visually impaired users and found that audio-based warnings were preferred over haptic feedback by a ratio of 4:1 for security alerts.

Universal Design Principles

Shneiderman (2000) advocated for universal usability in interface design, introducing principles that strongly influenced accessible security system development. His framework emphasized multimodal feedback, user control, and inclusive design practices.

2.5 Research Gap Analysis

Despite extensive research in web security, browser extensions, and accessible interfaces, several significant gaps remain:

Integration Gap: No existing system integrates real-time security monitoring with multilingual voice-based alerts

Accessibility Gap: Current security solutions inadequately address the needs of visually impaired users

Linguistic Gap: Limited cybersecurity tools support Indian and South Asian languages

Evaluation Gap: Few studies empirically assess the effectiveness of voice-based security warnings

Performance Gap: Many advanced security extensions impose high memory and performance overheads

The Cyber Voice Alert system addresses these gaps by providing an integrated, accessible, multilingual, and performance-efficient approach to modern web security.

IV PROBLEM STATEMENT

Although modern web browsers include security warning mechanisms, a large number of users continue to fall victim to phishing attacks, malicious websites, and online fraud. Most existing security alerts rely mainly on visual pop-ups, icons, or brief text messages, which are often ignored or misunderstood. Users with limited technical knowledge, visual difficulties, or language barriers face greater challenges in recognizing these warnings. In many cases, repeated exposure to similar alerts leads to warning fatigue, causing users to dismiss notifications

III EXISTING SYSTEM

The existing browser-based security systems primarily rely on visual indicators and English text messages to warn users about unsafe websites or insecure connections. When users attempt to access malicious or insecure websites, modern browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge display warning messages like "Your connection is not private" or highlight the address bar with red indicators. These alerts require users to read and correctly interpret technical terms such as certificate errors, phishing threats, or invalid HTTPS connections. Unfortunately, many users struggle to understand these messages, which reduces their effectiveness.

One major limitation of current browser warning systems is language dependency. Most security alerts are presented only in English, which excludes a large number of users who are not fluent in the language. Another drawback is their heavy reliance on visual cues. Users with visual impairments or those who unintentionally ignore browser pop-ups may fail to notice these warnings altogether. Additionally, repeated exposure to similar alerts often results in warning fatigue, where users begin to dismiss even genuine security notifications without careful consideration.

Accessibility is another significant concern. Existing systems rarely provide audio-based support, making them unsuitable for elderly users, individuals with limited literacy, or people with visual challenges. Furthermore, the technical nature of security terminology creates confusion among non-technical users. Terms such as invalid SSL certificate or malicious domain are often misunderstood, leading users to make unsafe browsing decisions.

Despite their effectiveness, current detection mechanisms also face several practical limitations and challenges. Pattern-based detection techniques may fail to identify advanced or newly developed attacks that do not follow known patterns. Text-to-speech quality can vary across languages, and in some cases, synthesized voices may sound unnatural or robotic. Although false positive rates are relatively low, repeated incorrect warnings can gradually reduce user trust in the system.

Platform dependency is another restriction, as many solutions are limited to Chromium-based browsers. Offline functionality is also constrained, since fallback text-to-speech services often require an active internet connection. In addition, users are provided with limited customization options, such as controlling alert sensitivity or defining personalized warning thresholds. From a technical perspective, browser extension APIs impose constraints on performing complete SSL/TLS certificate validation. Enhancing detection accuracy may introduce performance trade-offs, as advanced analysis requires additional system resources. Privacy considerations must also be carefully addressed, as URL analysis involves handling sensitive browsing data. Finally, blacklist databases require frequent updates to remain effective, which must be managed without negatively affecting browser performance.

V PROPOSED SYSTEM

The system is designed as a lightweight browser extension or web-based application that continuously monitors web activity to identify potential security threats. When a suspicious or unsafe website is detected, the system generates an audible warning in the user"s preferred language, accompanied by a visual alert. By combining real- time threat detection with multilingual voice feedback, Cyber Safe Voice Alerts enhances user awareness and enables faster, safer decision-making during web browsing..By utilizing the Web Speech API and Google Translate Text-to-Speech (TTS) service, the system can generate real-time spoken messages in 16 different languages, including English, Hindi, Kannada, Tamil, Telugu, Malayalam, Marathi, Bengali, Gujarati, Punjabi, Urdu .

VI METHODOLOGY

System Architecture

The Cyber Voice Alert system is designed using a modular and scalable architecture to ensure efficient threat detection, multilingual support, and real-time user notification. The architecture is composed of five primary functional components that operate collaboratively to monitor web activity, analyze security risks, and deliver accessible alerts to users through both visual and voice-based mechanisms.

The Security Monitor Module is responsible for continuously observing active browser tabs and tracking user navigation in real time. This module analyzes URL structures and communication protocols to identify insecure connections and abnormal patterns. It also validates SSL/TLS certificates to verify website authenticity and checks visited domains against known malicious sources. By performing these operations continuously, the module acts as the first line of defense against potential web-based threats.

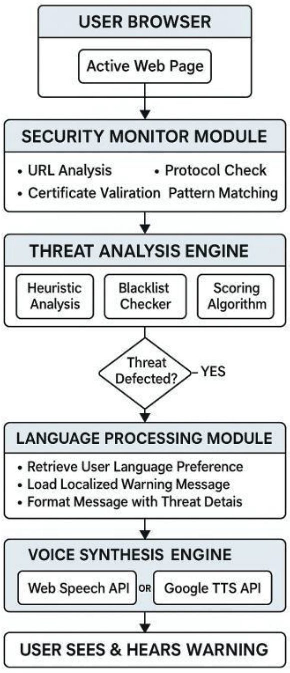
The Threat Analysis Engine processes data collected by the Security Monitor Module to assess the level of risk associated with each website. It employs a multi-criteria decision-making algorithm that assigns weighted scores to various threat indicators such as certificate validity, domain reputation, and URL characteristics. The engine maintains an internal blacklist database of known malicious websites and applies heuristic analysis to previously unseen URLs. This combination of rule-based and heuristic evaluation enables accurate and adaptive threat classification.

The Language Processing Module manages multilingual functionality by handling user language preferences and maintaining a repository of localized warning messages. It supports character encoding and proper rendering for sixteen languages, including Punjabi and Urdu, ensuring accurate message delivery across diverse linguistic contexts. The module also incorporates fallback mechanisms to handle unsupported languages gracefully, thereby maintaining system reliability.

The Voice Synthesis Engine is responsible for generating spoken security alerts. It primarily integrates the Web Speech API to provide native text-to-speech functionality within the browser environment. To ensure reliability, a backup text-to-speech service is implemented using Google TTS. This engine manages audio playback, alert queuing, and pronunciation optimization, particularly for technical security terms, ensuring clarity and intelligibility of voice alerts.

The User Interface Controller manages all user-facing interactions within the browser extension. It renders the extension popup interface, allowing users to select preferred languages and configure alert settings. The controller displays visual security warnings alongside voice notifications, ensuring multimodal feedback. Additionally, it maintains user preferences, records alert history, and provides basic statistical insights, enabling users to track security events and system activity.

VII SYSTEM ARCHITECTURE



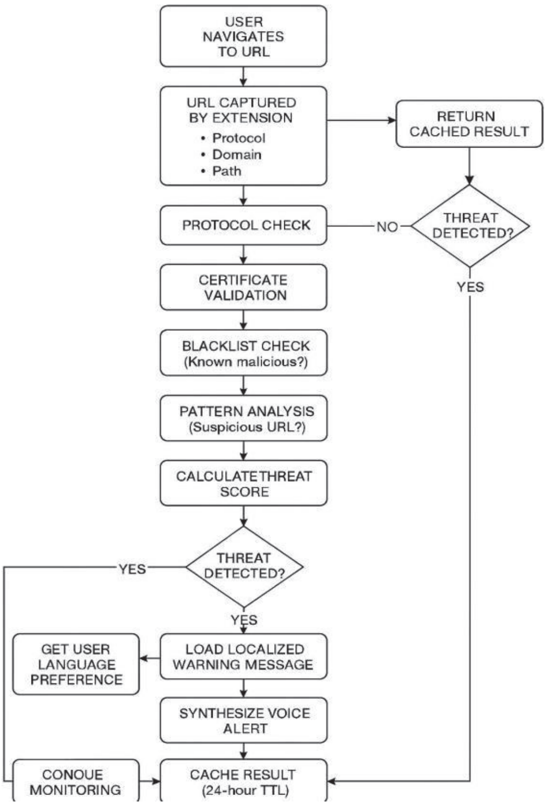
The system architecture is designed to monitor user web activity in real time and provide immediate security warnings using both visual and voice-based alerts. The process begins at the User Browser, where the user accesses an active web page. As soon as a webpage is loaded, the system continuously observes the browsing activity without interrupting normal user interaction. This ensures that security monitoring happens in the background while maintaining a smooth browsing experience.

The Security Monitor Module is responsible for examining the technical characteristics of the active webpage. It performs URL analysis to identify suspicious structures, checks the communication protocol to verify whether secure connections are used, and validates website certificates to ensure authenticity. Additionally, pattern matching techniques are applied to detect known malicious behaviors or unsafe website traits.

Once initial monitoring is completed, the data is forwarded to the Threat Analysis Engine, which performs deeper evaluation. This module uses heuristic analysis to assess unusual website behavior, verifies URLs against known blacklists, and applies a scoring algorithm to determine the severity level of the threat. Based on these combined evaluations, the system decides whether a real threat exists. This decision-making process reduces false alarms while ensuring that genuine threats are not ignored.

If a threat is detected, the system activates the Language Processing Module, which retrieves the user"s preferred language settings. The warning message is then localized and formatted in a simple, understandable manner, including relevant threat details. This step ensures clarity and accessibility for users from different linguistic backgrounds. Finally, the Voice Synthesis Engine converts the warning message into speech using text-to-speech services, while a visual alert is displayed simultaneously. As a result, the user both sees and hears the warning, increasing attention, comprehension, and the likelihood of safe decision-making.

VIII DATAFLOW DIAGRAM



The data flow of the proposed system begins when the user navigates to a web page through the browser. As soon as the webpage is accessed, the browser extension captures the URL in real time. This captured URL is broken down into its basic components such as protocol, domain name, and path. This step ensures that all relevant information required for security evaluation is collected at the earliest stage of browsing.

Once the URL is captured, the system first checks whether a cached result for the same URL already exists. If a cached response is available, it is immediately returned to reduce processing time and improve efficiency. If no cached data is found, the URL is forwarded for further security checks. The system then performs a protocol verification to determine whether the website uses a secure communication method. Following this, certificate validation is carried out to confirm the authenticity of the website and identify potential spoofed or invalid certificates.

After basic validation, the URL undergoes a blacklist check, where it is compared against known malicious websites stored in threat databases. If the URL is not found in the blacklist, pattern analysis is performed to detect suspicious structures commonly associated with phishing or fraudulent websites. Based on the outcomes of these checks, a threat score is calculated. This score represents the overall risk level of the website by combining results from protocol, certificate, blacklist, and pattern analysis stages.

IX APPLICATIONS

The proposed Cyber Safe Voice Alert system can be effectively used in everyday web browsing to improve user awareness and reduce the risk of online threats. It is especially useful for individuals who frequently access emails, social media platforms, online shopping websites, and banking portals, where phishing attacks and fraudulent links are common. By providing immediate voice and visual warnings, the system helps users recognize unsafe websites before entering sensitive information such as passwords or personal details.

This system is highly beneficial for users with limited technical knowledge, including senior citizens, children, and first-time internet users. Many such users struggle to understand traditional security symbols or warning messages displayed by browsers. The voice-based alerts, delivered in the user‟s preferred language, make security warnings easier to understand and act upon. This improves inclusivity and ensures that cybersecurity protection is not limited to technically skilled users.

The application is also suitable for educational institutions and public access environments such as libraries, cyber cafés, and training centers. In these settings, multiple users share the same system, increasing the risk of accidental access to malicious websites. The Cyber Safe Voice Alert system can act as an additional safety layer by clearly informing users about threats in real time, thereby promoting safer browsing habits and digital awareness.

In organizational and professional environments, the system can help reduce security incidents caused by human error. Employees often click on unsafe links unknowingly, leading to data breaches or malware infections. By integrating voice-assisted security alerts into browsers, organizations can enhance their cyber security posture without relying solely on user training. Overall, the proposed system serves as a practical and user-friendly solution for improving web security across diverse real-world scenarios.

X CONCLUSION

This paper presented the design and implementation of the Cyber Safe Voice Alert system, a browser-based solution aimed at improving user awareness and response to web security threats. The system addresses the limitations of traditional browser warnings by combining visual notifications with real-time voice alerts. By monitoring active web pages and analyzing URLs through multiple security checks, the system is able to identify potentially unsafe websites and notify users at the moment of risk.

A key strength of the proposed system lies in its user-centric and inclusive design. The integration of multilingual voice alerts ensures that security warnings are easily understood by users from different linguistic and technical backgrounds. This approach reduces dependence on technical knowledge and minimizes the chances of warnings being ignored due to confusion or habituation. The use of caching and structured threat analysis also helps maintain efficiency while avoiding unnecessary interruptions during safe browsing.

Overall, the Cyber Safe Voice Alert system demonstrates that enhancing how security information is communicated to users can significantly improve safe browsing behavior. Rather than relying only on detection accuracy, the system focuses on effective risk communication and accessibility. This makes it a practical and scalable solution for real-world deployment, contributing to safer and more informed use of the internet.

REFERENCES

[1] Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. Expert Systems with Applications, 37(12), 7913-7921.

[2] https://doi.org/10.1016/j.eswa.2010.04.044

[3] Akhawe, D., & Felt, A. P. (2013). Alice in warningland: A large-scale field study of browser security warning effectiveness. In Proceedings of the 22nd USENIX Security Symposium (pp. 257-272). USENIX Association.

[4] Anti-Phishing Working Group (APWG). (2024). Phishing Activity Trends Report, 4th Quarter 2024. Retrieved from https://apwg.org/trendsreports/

[5] Branham, S. M., & Mukkath Roy, A. R. (2019). Reading between the guidelines: How commercial voice assistant guidelines hinder accessibility for blind users. In Proceedings of the 21st International ACM SIGACCESS Conference on Computers and Accessibility (pp. 446-458). ACM. https://doi.org/10.1145/3308561.3353797

[6] Carlini, N., Felt, A. P., & Wagner, D. (2012). An evaluation of the Google Chrome extension security architecture. In Proceedings of the 21st USENIX Security Symposium (pp. 97-111). USENIX Association.