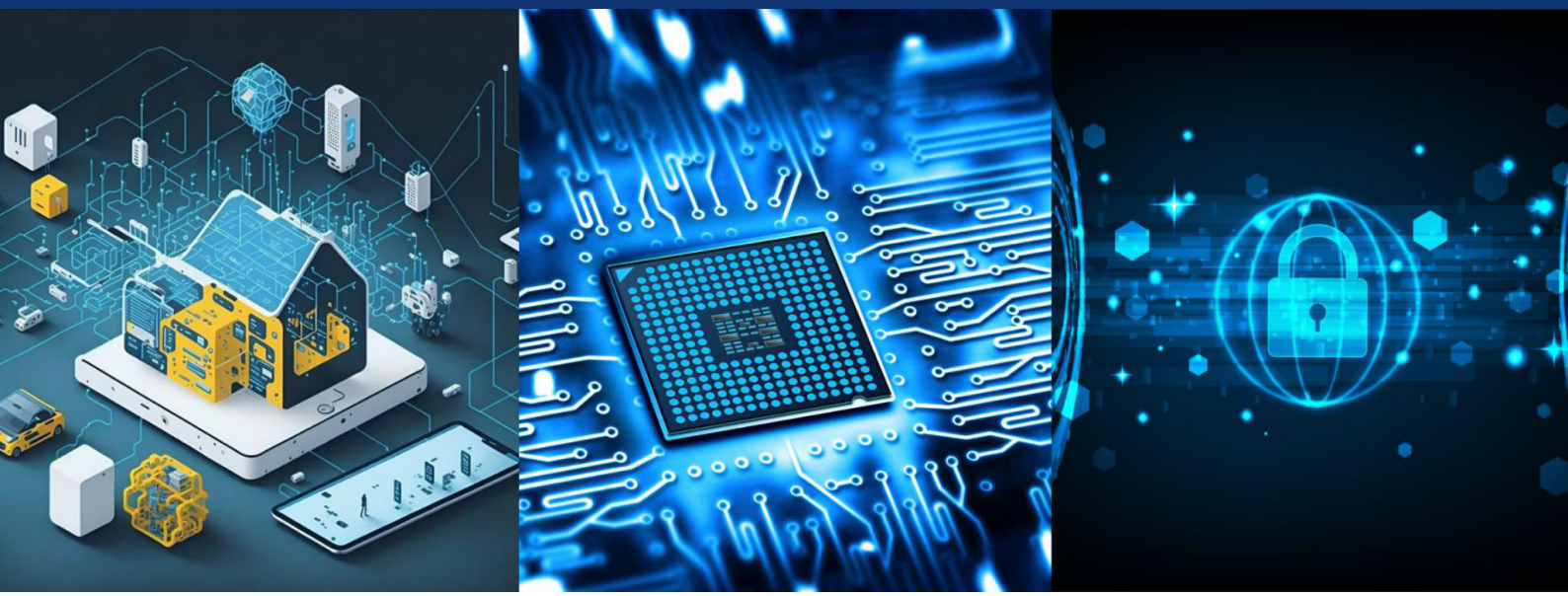
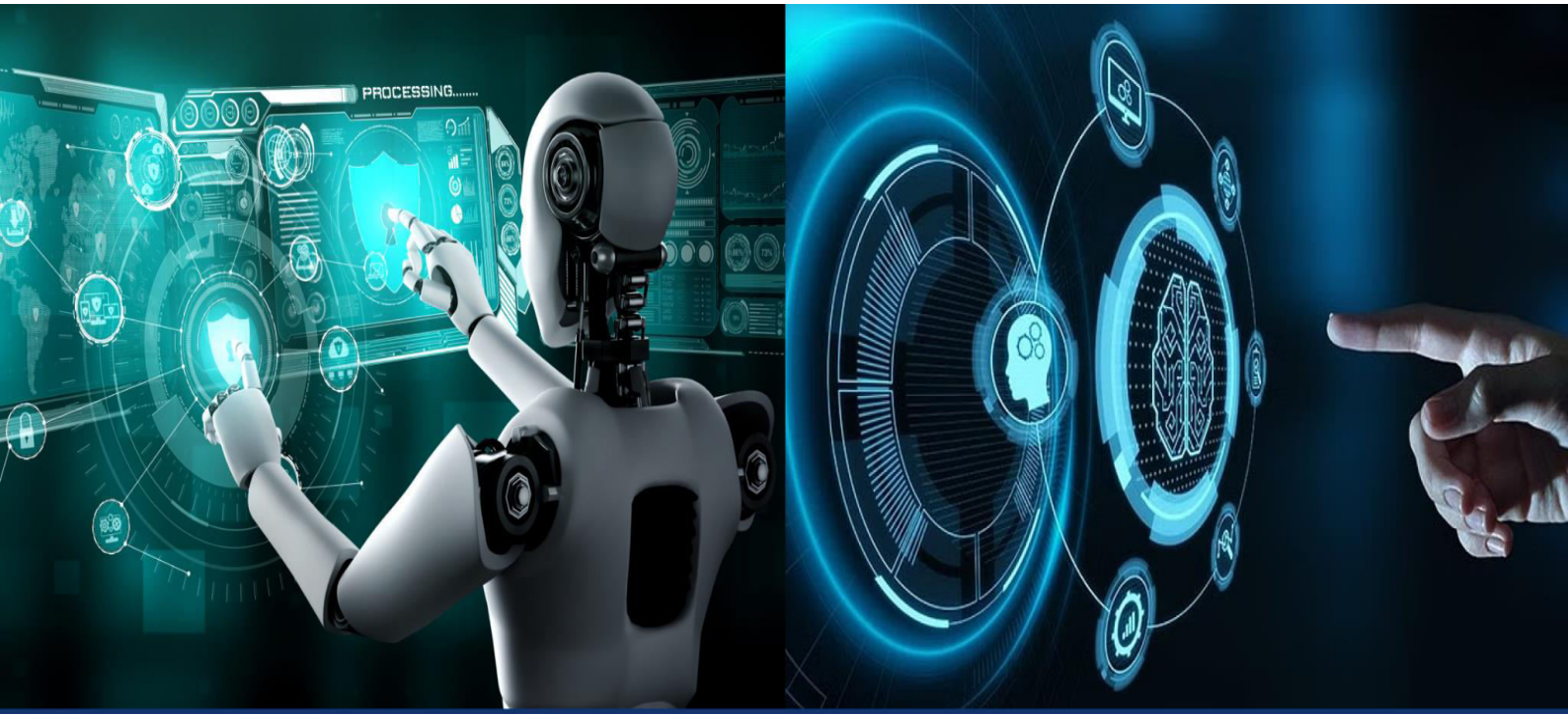
ISSN(O): 2320-9801
ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927 **Volume 14, Issue 11, November 2026**

© 2026 IJIRCCE | Volume 14, Issue 11, November 2026 DOI: 10.15680/IJIRCCE.2026.1411013

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

CyberShield.AI: A Web-Based Multi-Category Cyber Threat Detection and Vulnerability Assessment Framework

Vishal V P[1], Pooja N Annigere[1], Keerthi Manjunath Geddappanavar[1], Prof. Chaithra B M[2]

UG Students, Dept. of CSE, Jain Institute of Technology, Davangere, Karnataka, India[1]

Assistant Professor, Dept. of CSE, Jain Institute of Technology, Davangere, Karnataka, India[2]

ABSTRACT: The rapid growth of digital communication and internet-based services has increased the risk of cyber threats such as phishing attacks, malicious URLs, fraudulent emails, suspicious APK files, insecure APIs, fake links, and deceptive SMS messages. These threats can compromise sensitive information, affect system security, and expose users to financial and privacy-related risks. Traditional security approaches may require users to rely on multiple tools to examine different types of potential threats, making the detection process difficult and time-consuming. To address these challenges, **CyberShield.AI** is proposed as a web-based cybersecurity threat scanning and analysis system that provides a centralized platform for identifying and assessing potentially harmful digital content. The system supports the scanning of six major categories of digital threats, including URLs, emails, APK files, APIs, fake links, and SMS messages. It analyses the submitted inputs and presents a vulnerability percentage along with a security assessment to help users understand the potential risks associated with the scanned content. The proposed system incorporates separate user and administrator interfaces to support secure access and centralized monitoring of scanning activities. Users can examine scan results, maintain their scanning history, search previous records, and download individual scan reports in PDF format for documentation and future reference. When potentially harmful content is identified, users can report the suspicious scan to the administrators for further review, whereas inputs assessed as safe are presented without raising unnecessary threat alerts. The administrator dashboard enables authorized administrators to monitor reported threats and manage relevant scanning activities. By integrating multiple scanning categories, report generation, scan history management, and threat reporting within a single platform, CyberShield.AI aims to improve the accessibility and organization of basic cybersecurity assessment. The system provides a practical approach to helping users recognize potential digital threats and make more informed decisions before interacting with suspicious online content.

KEYWORDS: Cybersecurity, Cyber Threat Detection, Phishing Detection, Malicious URL Analysis, Vulnerability Assessment, Email Security, APK Scanning, Web-Based Security System.

I. INTRODUCTION

1.1 Background and Problem Significance

The rapid growth of internet technologies and digital communication has made online platforms an essential part of everyday life. People increasingly rely on websites, emails, mobile applications, APIs, and messaging services for communication, financial transactions, and information sharing. However, this growing dependence on digital platforms has also increased the risk of cyber threats such as phishing attacks, malicious URLs, fraudulent emails, fake links, suspicious APK files, insecure APIs, and scam SMS messages. These threats can lead to data theft, financial loss, unauthorized access, and privacy violations. Many users find it difficult to distinguish between genuine and malicious digital content, while using separate security tools for different types of threats can make the detection process complicated and time-consuming. To address these challenges, CyberShield.AI is developed as a web-based cybersecurity threat scanning and analysis platform that supports six categories of scanning, namely URLs, emails, APK files, APIs, fake links, and SMS messages. The system provides a vulnerability percentage and security assessment for submitted inputs, along with features such as scan history, PDF report generation, suspicious-content reporting, and separate user and administrator dashboards. By bringing these functionalities together in a single platform, the proposed system aims to simplify preliminary cyber threat assessment and help users make more informed decisions while interacting with digital content.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1.2 Limitations of Existing Approaches

Existing cybersecurity solutions often focus on detecting specific categories of threats, such as malicious URLs, phishing emails, suspicious files, or network vulnerabilities, requiring users to depend on multiple tools for different security assessments. This makes the process less convenient and increases the time required to examine potential threats. Some existing tools provide limited information about detected risks, making it difficult for ordinary users to understand the severity of a threat and take appropriate action. Additionally, the availability of centralized scan history, downloadable reports, and user-based threat reporting may vary across platforms. Many solutions also lack an integrated interface that allows users and administrators to manage scanning activities and reported threats in an organized manner. These limitations highlight the need for a centralized system that supports multiple categories of cyber threat scanning, provides understandable security assessments, maintains scan records, and enables users to report suspicious content for further administrative review.

1.3 Our Contribution

CyberShield.AI addresses the limitations of existing cybersecurity approaches through an integrated platform that provides scanning and analysis of six categories of digital threats, including URLs, emails, APK files, APIs, fake links, and SMS messages. First, the system provides a centralized scanning interface that enables users to examine different types of digital content and receive a vulnerability percentage along with a corresponding security assessment. Second, it incorporates scan history management and individual PDF report generation, allowing users to review previous scanning activities, search stored records, and maintain reports for future reference. Third, the platform introduces a suspicious-content reporting facility through which users can report potentially harmful results to administrators for further review. Separate user and administrator dashboards support organized access and management of scanning activities. These contributions combine threat assessment, report management, and user-based threat reporting within a single web-based cybersecurity platform, making the scanning process more accessible and convenient.

II. KEY CONCEPTS AND DEFINITIONS

Cybersecurity refers to the practice of protecting computers, networks, applications, and digital information from unauthorized access, malicious activities, and cyberattacks. It involves identifying potential security risks, analysing suspicious activities, and implementing appropriate measures to prevent data breaches and other digital threats. In CyberShield.AI, cybersecurity forms the foundation of the system, enabling the assessment of different types of digital content that may expose users to security risks.

Threat detection is the process of identifying potentially harmful digital content or activities that may compromise the security of a system or user. It involves examining submitted information and identifying suspicious patterns or characteristics associated with cyber threats. In the proposed system, threat detection is applied to six categories: URLs, emails, APK files, APIs, fake links, and SMS messages. The scanning results are presented along with a vulnerability percentage and a corresponding security assessment to help users understand the possible risks.

Phishing is a cyberattack technique in which attackers create fraudulent websites, emails, messages, or links that appear legitimate to deceive users into sharing confidential information. Such attacks commonly target login credentials, banking details, and personal information. Phishing detection involves examining suspicious content to identify characteristics that may indicate fraudulent activity. CyberShield.AI includes scanning facilities for emails, URLs, fake links, and SMS messages to support the identification of potentially harmful content.

An Application Programming Interface (API) is a mechanism that allows different software applications to communicate and exchange information. APIs are widely used in web applications, mobile applications, and cloud-based services. However, improperly secured APIs may expose sensitive information or create opportunities for unauthorized access. API security assessment involves examining API-related inputs and identifying potential security weaknesses or suspicious characteristics that may require further investigation.

An Android Application Package (APK) is the file format used to distribute and install applications on Android devices. APK files contain application components and resources required for installation and execution. Although they are commonly used for distributing legitimate applications, modified or malicious APK files may contain harmful components. APK scanning involves examining submitted application packages for potentially suspicious characteristics to help users assess associated security risks.

© 2026 IJIRCCE | Volume 14, Issue 11, November 2026 DOI: 10.15680/IJIRCCE.2026.1411013

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Vulnerability assessment is the process of identifying and evaluating possible weaknesses or security risks within digital content or systems. It helps users understand the potential severity of identified security issues. In CyberShield.AI, the scanning results include a vulnerability percentage and a security status indicating whether the submitted content is assessed as safe or potentially harmful.

III. SYSTEM ARCHITECTURE AND METHODOLOGY

3.1 Overall Design Philosophy

CyberShield.AI is designed as a centralized web-based cybersecurity threat scanning and analysis platform consisting of interconnected modules that perform different security-related operations. The system supports six categories of scanning, namely URLs, emails, APK files, APIs, fake links, and SMS messages. Its architecture separates the scanning process, result analysis, user management, administrator operations, report generation, and scan history management into distinct functional components. This modular organization makes the system easier to maintain and allows individual functionalities to be modified or extended without affecting the entire application. The platform provides separate interfaces for users and administrators, ensuring that scanning activities and administrative operations are handled through appropriate access points. The overall design focuses on providing an accessible interface, organized threat assessment, and convenient management of scanning records.

3.2 Multi-Category Threat Scanning Module

When a patient selects an oral cavity photograph and submits the screening form, the Flask backend first validates that the file format is acceptable — JPEG and PNG are supported — and that the file size falls within the twenty-megabyte limit. The accepted file is saved to a timestamped path within the static uploads directory to prevent filename collisions between concurrent submissions. The preprocessing stage then converts the image to RGB color space, discarding any alpha transparency channel and normalizing grayscale inputs to three-channel format. The image is subsequently resized to 224 by 224 pixels using bicubic interpolation, which preserves edge continuity more reliably than cruder nearest-neighbor alternatives. Finally, each pixel's intensity value is divided by 255 to map all three-color channels from their original integer range into floating-point values between zero and one, a normalization step that promotes stable numerical behavior during model inference.

3.3 Vulnerability Assessment and Result Analysis

After the scanning process is completed, the system presents the analysis results through a structured result interface. A vulnerability percentage is displayed to represent the assessed level of potential security risk associated with the submitted input. The result is accompanied by a corresponding security status, helping users understand whether the scanned content is considered safe or suspicious. When the submitted content is assessed as safe, the system displays the appropriate result without generating an unnecessary threat alert. If potentially harmful characteristics are identified, the result indicates the associated security concern so that the user can take suitable precautions. The generated assessment is also associated with the respective scanning record, allowing the result to be accessed later through the scan history. This module helps simplify the interpretation of scanning results for users who may not have advanced cybersecurity knowledge.

3.4 User and Administrator Management Framework

The platform incorporates separate login facilities for users and administrators to organize access to different system functionalities. After successful authentication, users are directed to their dashboard, where they can access the available scanning categories, examine scanning results, view previous records, and download individual PDF reports. The user interface also provides an option to report suspicious scanning results to the administrators for further examination. The administrator dashboard provides a centralized interface for monitoring reported security concerns and managing relevant administrative activities. The project supports three administrator accounts for handling these operations. This separation of responsibilities helps maintain an organized workflow between users who perform scans and administrators who review reported threats.

3.5 PDF Report Generation

CyberShield.AI includes a report generation facility that enables users to obtain a PDF document for an individual scanning activity. The generated report presents the relevant scan information, including the submitted content or its associated details, scanning category, assessment result, and vulnerability percentage, based on the information available in the scanning record. This allows users to retain a copy of their security assessment for documentation and

© 2026 IJIRCCE | Volume 14, Issue 11, November 2026 DOI: 10.15680/IJIRCCE.2026.1411013

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

future reference. In addition, the scan history module maintains records of previously performed scanning activities. Users can access their historical records, search for particular scans, and delete unwanted entries through the provided interface. By combining report generation with history management, the system provides a convenient method for reviewing and maintaining previous security assessments.

3.6 Threat Reporting and Administrative Monitoring

The threat reporting module establishes communication between users and administrators when potentially harmful digital content is identified. If a scan indicates suspicious or unsafe content, the user can submit a report to notify the administrators about the identified concern. The submitted report becomes available through the administrator dashboard, where authorized administrators can review the reported information and monitor the associated scanning activity. This functionality provides an additional level of review beyond the initial scanning process and allows suspicious findings to be brought to administrative attention. The integration of threat reporting with separate user and administrator dashboards creates an organized process for handling reported security concerns. Overall, this module complements the scanning functionality by supporting user participation and centralized monitoring within the CyberShield.AI platform.

IV. UNIQUE CONTRIBUTIONS AND NOVEL ANGLE

CyberShield.AI incorporates four major design contributions that distinguish it from conventional approaches to cybersecurity threat assessment. First, the system integrates six categories of digital threat scanning, including URLs, emails, APK files, APIs, fake links, and SMS messages, within a single web-based platform. This approach reduces the need for users to depend on multiple independent tools for examining different types of suspicious digital content and provides a common interface for preliminary security assessment.

Second, the platform combines vulnerability percentage assessment with understandable security results. Instead of presenting only a scanning outcome, the system provides an associated vulnerability percentage and security status, helping users interpret the potential risks of submitted content. This feature makes the assessment process more accessible to users who may not have specialized cybersecurity knowledge.

Third, CyberShield.AI incorporates persistent scan history and individual PDF report generation. Users can retrieve previous scanning records, search for specific scans, delete unwanted history entries, and download reports containing the relevant assessment details. This functionality allows users to maintain documentation of their scanning activities and refer to earlier results whenever required.

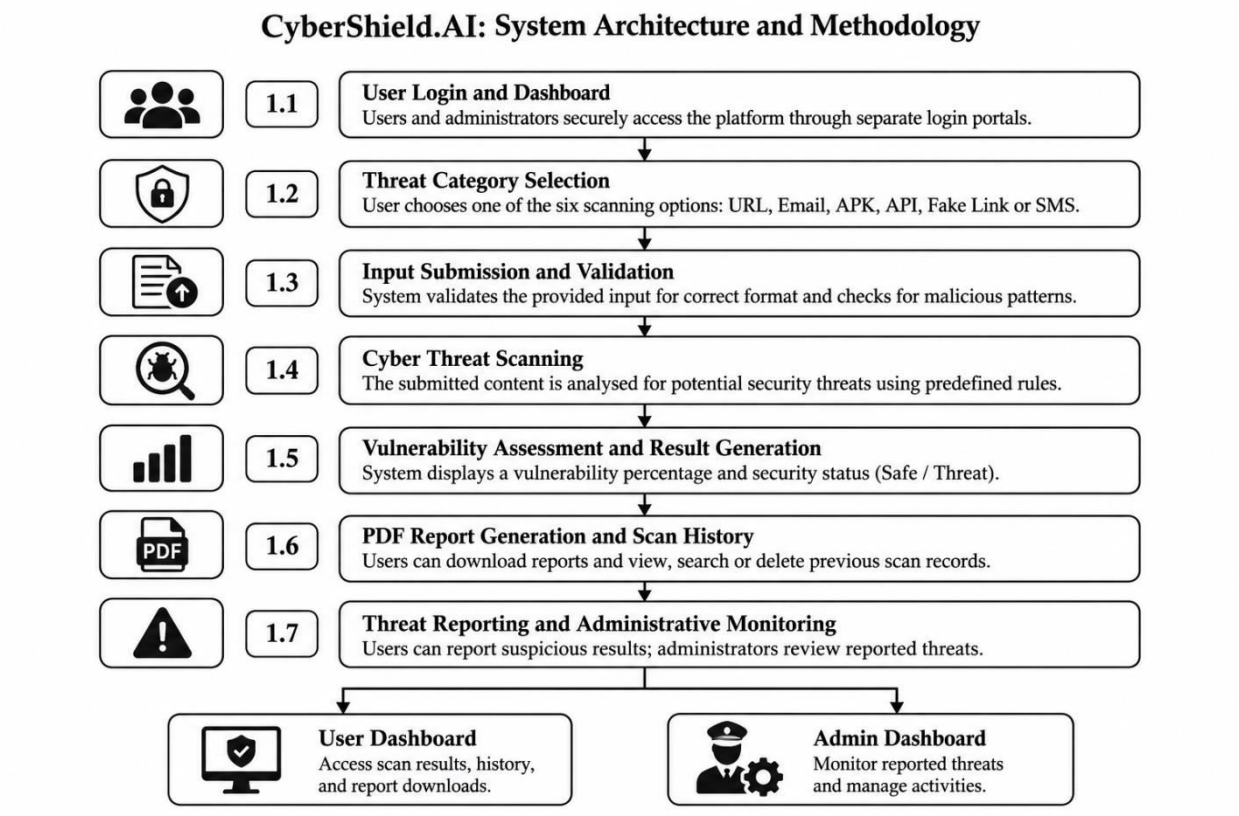
Fourth, the system introduces a user-based threat reporting mechanism supported by separate user and administrator dashboards. Users can report suspicious scanning results to administrators, who can review the submitted reports through their dedicated interface. The platform supports three administrator accounts to facilitate the monitoring and management of reported security concerns. The integration of multiple scanning categories, assessment results, report management, and administrative monitoring within one application represents the primary contribution of CyberShield.AI.

© 2026 IJIRCCE | Volume 14, Issue 11, November 2026 DOI: 10.15680/IJIRCCE.2026.1411013

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



V. IMPLEMENTATION RESULTS AND SYSTEM DEMONSTRATION

The CyberShield.AI platform was implemented as a web-based cybersecurity threat scanning and analysis system with separate interfaces for users and administrators. The developed application integrates six scanning categories, including URLs, emails, APK files, APIs, fake links, and SMS messages. The implementation focuses on providing a centralized interface through which users can submit digital content, examine scanning results, and manage their previous security assessment records.

The authentication module provides separate login options for users and administrators. After successful authentication, users are directed to their respective dashboards, where they can access the available scanning categories and other platform functionalities. Administrators are provided with a dedicated dashboard for monitoring reported threats and managing administrative activities. This role-based interface helps maintain a clear separation between user operations and administrative responsibilities.

The scanning interface allows users to select the required threat category and submit the corresponding input for analysis. Based on the selected category, the system processes the submitted information using the implemented scanning mechanism and generates an assessment result. The result interface displays the vulnerability percentage along with the corresponding security status. When the submitted content is assessed as safe, the system displays the safe result without raising unnecessary threat alerts. If suspicious or potentially harmful content is identified, the system presents the corresponding threat indication to the user.

The PDF report generation module enables users to download reports for individual scanning activities. Each report contains the relevant scanning information, including the selected category, assessment result, vulnerability percentage, and other available scan details. The scan history module maintains previously performed scanning records and provides options to view, search, and delete individual records. These functionalities allow users to review earlier assessments and maintain documentation of their scanning activities.

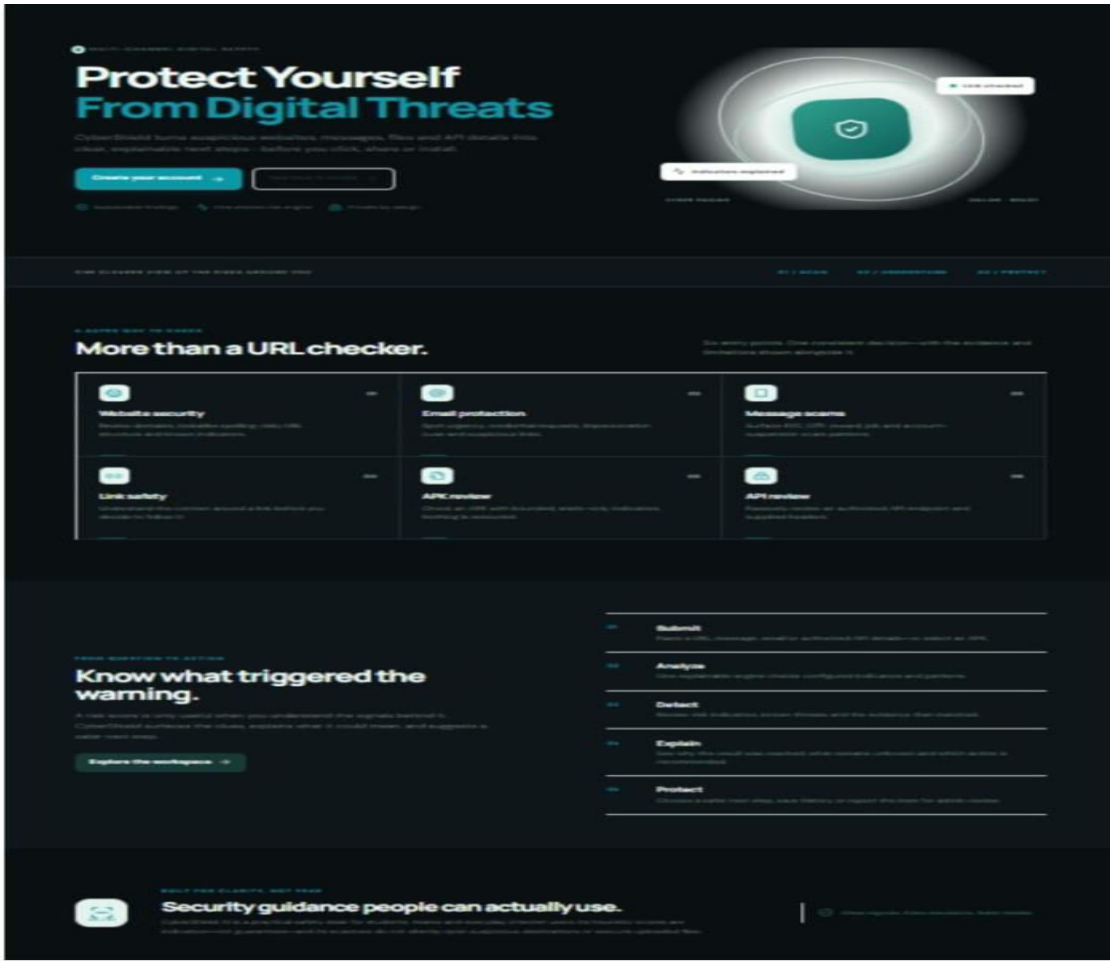
© 2026 IJIRCCE | Volume 14, Issue 11, November 2026 DOI: 10.15680/IJIRCCE.2026.1411013

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The threat reporting functionality allows users to submit suspicious scanning results to administrators for further review. Reported concerns are made available through the administrator dashboard, where authorized administrators can monitor the submitted reports and manage relevant activities. The platform supports three administrator accounts for handling administrative operations. Through the integration of multi-category scanning, vulnerability assessment, PDF report generation, scan history management, and threat reporting, CyberShield.AI demonstrates a unified approach to preliminary cybersecurity assessment and organized threat management.

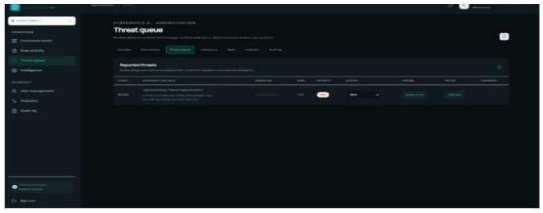


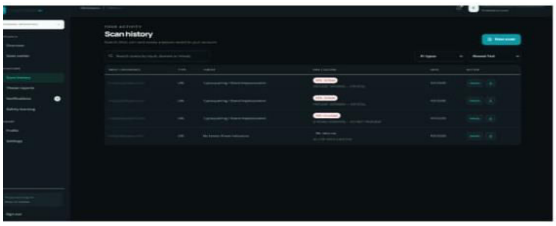
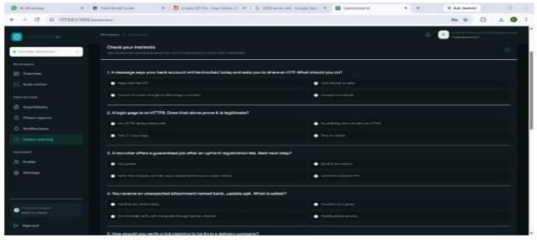
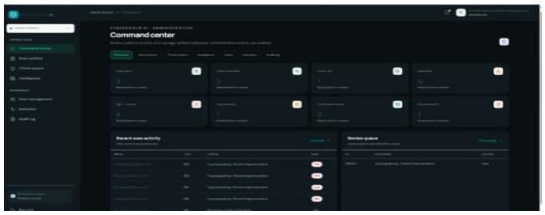
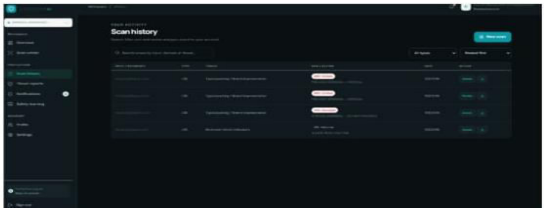
© 2026 IJIRCCE | Volume 14, Issue 11, November 2026 DOI: 10.15680/IJIRCCE.2026.1411013

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



VI. CHALLENGES AND LIMITATIONS

Several limitations affect the current implementation of CyberShield.AI and its ability to provide comprehensive cybersecurity protection. One of the primary challenges is the difference in structure and characteristics among the six supported scanning categories, namely URLs, emails, APK files, APIs, fake links, and SMS messages. Each category requires different validation and analysis techniques to identify potentially harmful content. Malicious inputs may also be designed to resemble legitimate websites, applications, or communications, making accurate identification difficult. Furthermore, newly developed phishing techniques, modified malicious links, and emerging cyber threats may not always be recognized by the currently implemented scanning mechanisms. As a result, the system's ability to identify threats depends on the detection techniques and security checks available within the current implementation.

Another limitation concerns the interpretation of vulnerability percentages and scanning results. The displayed vulnerability percentage represents the assessment generated by the implemented scanning mechanism and should not be considered an absolute measurement of security risk. A result classified as safe does not guarantee that the submitted content is completely free from threats, particularly when previously unknown attack patterns are involved. Similarly, suspicious content may require additional investigation before its actual security impact can be confirmed. The system is therefore intended to provide preliminary threat assessment and user awareness rather than replace professional cybersecurity analysis, penetration testing, or advanced enterprise security solutions.

The current platform also depends on the quality and format of the information submitted by users. Incorrect URLs, incomplete email content, unsupported APK files, or improperly formatted API inputs may affect the scanning process and the reliability of the resulting assessment. Additionally, the system provides PDF report generation and scan history management, but the usefulness of these features depends on the availability and accuracy of stored scanning records. The administrator dashboard allows reported threats to be reviewed, but the verification and handling of suspicious submissions may require manual examination. As the number of users and reported threats increases, maintaining efficient administrative monitoring may become more challenging.

© 2026 IJIRCCE | Volume 14, Issue 11, November 2026 DOI: 10.15680/IJIRCCE.2026.1411013

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VII. FUTURE SCOPE AND RESEARCH DIRECTIONS

The future development of CyberShield.AI can focus on improving threat detection accuracy by integrating updated threat intelligence databases and advanced analysis techniques. Expanding the scanning capabilities to identify newly emerging cyber threats, malicious applications, and sophisticated phishing attacks would improve the system's effectiveness. Further improvements can include strengthening vulnerability assessment, introducing automated threat notifications, and enhancing security checks for all six scanning categories.

The platform can also be enhanced by implementing stronger authentication, encrypted data storage, and real-time threat monitoring to improve data protection. Integrating automated reporting and alert mechanisms would help administrators respond to suspicious activities more efficiently. Future research may also explore machine learning-based threat classification, improved detection techniques, and integration with external cybersecurity services. These developments could make CyberShield.AI more reliable, scalable, and effective in addressing evolving cybersecurity threats.

VIII. CONCLUSION

CyberShield.AI demonstrates the development of a centralized web-based platform for identifying and assessing potential cybersecurity threats across six categories: URLs, emails, APK files, APIs, fake links, and SMS messages. By integrating multiple scanning functionalities into a single application, the system simplifies the process of preliminary threat assessment and reduces the need for users to depend on separate security tools. Its modular structure supports scanning, vulnerability assessment, report generation, scan history management, and administrative monitoring, making the platform organized and convenient to use.

The system also provides separate user and administrator dashboards, individual PDF report generation, searchable scan records, and a facility for reporting suspicious content. These features improve accessibility, record management, and administrative monitoring of potential threats. Although further improvements in detection techniques, threat intelligence integration, data protection, and automated notifications are required, CyberShield.AI establishes a practical foundation for centralized cybersecurity assessment.

REFERENCES

[1] M. Khonji, Y. Iraqi, and A. Jones, “Phishing Detection: A Literature Survey,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091–2121, 2013.
[2] A. Aleroud and L. Zhou, “Phishing Environments, Techniques, and Countermeasures: A Survey,” Computers & Security, vol. 68, pp. 160–196, 2017.
[3] S. Marchal, J. François, R. State, and T. Engel, “PhishStorm: Detecting Phishing With Streaming Analytics,” IEEE Transactions on Network and Service Management, vol. 11, no. 4, pp. 458–471, 2014.
[4] OWASP Foundation, “OWASP API Security Top 10,” 2023.
[5] C. Pascoe, S. Quinn, and K. Scarfone, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST Cybersecurity White Paper, CSWP 29, 2024.
[6] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” RFC 8446, 2018.
[7] OWASP Foundation, “OWASP Top 10: The Ten Most Critical Web Application Security Risks,” 2021.
[8] R. M. Mohammad, F. Thabtah, and L. McCluskey, “Predicting Phishing Websites Based on Self-Structuring Neural Network,” Neural Computing and Applications, vol. 25, pp. 443–458, 2014.



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details