



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: IV Month of publication: April 2026

DOI: <https://doi.org/10.22214/ijraset.2026.80639>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Vuln Scan Desktop: An AI-Powered Vulnerability Assessment and Real-Time Security Dashboard for Web and Mobile Applications

Ms.S.A.Kamble, Aadesh Gaikwad, Rushikesh Patil, Harshal Londhe, Vishal Poute, Shriyash Pawar

Computer Science and Engineering SVERI's College of Engineering, Pandharpur, India

Abstract: *VulnScanDesktop is an intelligent security solution designed to identify, analyze, and visualize vulnerabilities in web and mobile applications through an AI-driven approach. With the rapid growth of digital platforms, applications are increasingly exposed to cyber threats such as injection attacks, insecure APIs, misconfigurations, and data leakage. This project aims to address these challenges by developing a desktop-based vulnerability assessment tool combined with a real-time security dashboard.*

The system integrates automated scanning techniques with machine learning models to detect both known and emerging security weaknesses. It performs static and dynamic analysis on application components, ensuring comprehensive coverage across different layers of the system. The AI component enhances detection accuracy by learning patterns from previous vulnerabilities and adapting to new threat behaviors.

A key feature of VulnScanDesktop is its interactive dashboard, which provides real-time insights into identified vulnerabilities. The dashboard presents data using visual elements such as graphs, risk scores, and severity classifications, enabling developers and security analysts to quickly understand and prioritize issues. Additionally, the system generates actionable recommendations for mitigation, helping users improve application security efficiently.

The proposed solution focuses on usability, scalability, and performance, making it suitable for both small-scale developers and enterprise environments. By combining automation, artificial intelligence, and real-time monitoring, VulnScanDesktop contributes to proactive cybersecurity practices and reduces the risk of exploitation in modern applications.

I. INTRODUCTION

In the modern digital era, web and mobile applications play a crucial role in delivering services across industries such as banking, healthcare, education, and e-commerce. As these applications handle sensitive user data and critical operations, ensuring their security has become a top priority. However, the increasing complexity of applications and the growing number of cyber threats make it difficult to maintain strong security standards throughout the development lifecycle.

Cyber attackers continuously search for weaknesses such as improper input validation, insecure APIs, outdated libraries, and weak authentication mechanisms. If left undetected, these vulnerabilities can be exploited to gain unauthorized access, disrupt services, or steal confidential information. As a result, organizations must adopt effective vulnerability assessment strategies to identify and fix security issues before they are exploited.

Traditional vulnerability scanning tools provide basic detection capabilities but often suffer from limitations such as high false-positive rates, lack of automation, and difficulty in interpreting results. Many existing systems generate lengthy reports that require expert knowledge to analyze, making it challenging for developers and small teams to respond quickly. Additionally, these tools may not offer real-time insights into the security status of applications.

To overcome these challenges, the proposed project, "VulnScan Desktop: An AI-Powered Vulnerability Assessment and Real-Time Security Dashboard for Web and Mobile Applications," introduces an intelligent and efficient approach to application security. The system leverages artificial intelligence techniques to enhance the detection process, enabling smarter identification of vulnerabilities while reducing unnecessary alerts.

The application is designed as a desktop-based solution that performs continuous scanning of both web and mobile applications. It collects security-related data, analyzes patterns, and identifies potential threats in real time. By incorporating AI-driven analysis, the system can adapt to new types of vulnerabilities and improve its accuracy over time, making it more reliable than traditional tools.

One of the key features of this project is its real-time security dashboard, which presents vulnerability data in a clear and visually understandable format. Instead of complex technical reports, users can view graphical representations, risk levels, and prioritized alerts. This helps developers, testers, and security teams quickly understand the severity of issues and take appropriate actions without delay.

II. LITERATURE REVIEW

Several tools and techniques have been developed for vulnerability detection in software systems. Static analysis tools such as Semgrep and Bandit analyze source code to detect security flaws, while dependency scanners like npm audit identify vulnerabilities in third-party libraries. Mobile security frameworks such as MobSF are used to analyze Android and iOS applications.

Despite their effectiveness, these tools have several limitations:

Several vulnerability scanning tools such as OWASP ZAP and Burp Suite are widely used in the industry. These tools provide comprehensive scanning capabilities but often generate large amounts of data, which can be difficult to analyze manually.

Research studies highlight the importance of automation in cybersecurity. Machine learning has been applied in intrusion detection systems to improve threat identification and reduce false alarms. However, integration of AI into vulnerability scanners is still evolving.

Existing systems lack real-time dashboards that provide clear visualization of threats. Most tools require exporting reports and analyzing them separately, which reduces efficiency.

This project builds upon existing research by combining automated scanning with AI-based classification and real-time visualization, making the process more efficient and user-friendly.

Recent advancements in artificial intelligence have enabled automated interpretation of technical data. However, most existing solutions do not integrate AI with vulnerability scanning tools in a unified environment.

The proposed system addresses these gaps by combining multiple tools, integrating AI-based analysis, and providing a centralized dashboard for better visualization and understanding.

III. PROBLEM STATEMENT

The increasing complexity of web and mobile applications has made security assessment more challenging. Developers often rely on traditional tools that are not capable of detecting advanced or unknown vulnerabilities.

One major issue is the high rate of false positives in existing scanning tools. This leads to wasted time and effort as developers must manually verify each detected vulnerability. It reduces the overall efficiency of the security process.

Another problem is the lack of real-time monitoring. Most tools perform periodic scans, which means vulnerabilities may go unnoticed for long periods. This delay increases the risk of exploitation.

Additionally, existing systems often lack user-friendly interfaces. Security data is presented in complex formats, making it difficult for non-experts to understand and act upon.

There is also limited support for mobile application security in many tools. As mobile usage increases, this becomes a significant limitation.

Furthermore, traditional systems do not adapt to new threats effectively. They rely on predefined rules, which may not cover emerging attack techniques.

Therefore, there is a need for an intelligent, real-time, and user-friendly vulnerability assessment system that can overcome these limitations.

IV. PROPOSED SYSTEM

The proposed system, VulnScanDesktop, is designed to provide an advanced vulnerability assessment solution using artificial intelligence. It integrates scanning, analysis, and visualization into a single platform.

The system uses AI algorithms to analyze application behavior and detect vulnerabilities. It learns from past data and improves detection accuracy over time. This reduces false positives and enhances reliability.

A real-time dashboard is included to display security insights. It provides visual representations of vulnerabilities, including severity levels and trends. This helps users quickly understand the security status.

The system supports both web and mobile applications, ensuring comprehensive coverage. It scans various components such as APIs, databases, and user inputs.

Automation is another key feature of the system. It reduces manual effort by performing continuous monitoring and automatic reporting. This improves efficiency and saves time.

The proposed system also provides recommendations for fixing vulnerabilities. This helps developers take immediate corrective actions.

Overall, VulnScanDesktop offers a modern, intelligent, and efficient solution for vulnerability assessment.

V. METHODOLOGY

The methodology of VulnScanDesktop is based on a structured approach to vulnerability assessment. It begins with data collection from web and mobile applications, including inputs, APIs, and network traffic.

The next step involves preprocessing the collected data. This includes filtering irrelevant information and preparing the data for analysis. Proper preprocessing improves the accuracy of the system.

AI models are then applied to analyze the data. These models identify patterns and detect anomalies that may indicate vulnerabilities. Machine learning algorithms play a key role in this process.

After analysis, the system classifies vulnerabilities based on severity levels such as low, medium, and high. This helps prioritize security issues. The results are then visualized using a real-time dashboard. The dashboard provides insights through charts and graphs, making it easier to understand the data.

Continuous monitoring is an important part of the methodology. The system regularly updates its analysis based on new data, ensuring up-to-date security information.

Finally, the system generates reports and recommendations. These reports help developers fix vulnerabilities and improve application security.



VI. SYSTEM ARCHITECTURE

The system architecture of VulnScan Desktop is designed to ensure scalability, modularity, and efficient communication between components. It follows a layered architecture where each layer performs a specific function, making the system easy to maintain and upgrade.

At the top level, the user interacts with the system through a desktop-based graphical user interface. This interface provides access to scanning options, reports, and the real-time dashboard. It is designed to be simple and intuitive so that even non-expert users can operate it effectively.

The next layer is the application logic layer, which controls the core functionalities of the system. This includes managing scan operations, coordinating between modules, and processing user inputs. It acts as a bridge between the user interface and backend processing components.

The scanning engine forms the core of the system. It performs vulnerability assessments by analyzing web and mobile applications. It includes modules for static analysis, dynamic analysis, and API testing. These modules work together to ensure comprehensive coverage.

An AI processing module is integrated into the architecture to enhance detection capabilities. It analyzes collected data using machine learning algorithms and identifies patterns that indicate potential vulnerabilities. This module continuously improves its performance based on historical data.

The data storage layer is responsible for storing scan results, logs, and historical records. A structured database is used to ensure efficient data retrieval and management. This allows the system to track vulnerability trends over time.

Finally, the visualization layer presents the results through a real-time dashboard. It displays key metrics such as vulnerability severity, frequency, and risk levels using graphs and charts.

This layered architecture ensures that each component operates efficiently while contributing to the overall system functionality.

VII. THE SYSTEM IMPLEMENTATION INVOLVES MULTIPLE TECHNOLOGIES

Frontend: Electron.js, React.js, TailwindCSS Backend: Python FastAPI

Database: MongoDB

Authentication: Firebase Auth + JWT Payments: Razorpay

Deployment: AWS EC2 / Render

The scanning engine runs tools in parallel, improving performance. The AI layer enhances usability by simplifying technical outputs. The dashboard provides visual insights using charts and graphs.

VIII. RESULTS AND DISCUSSION

The implementation of VulnScan Desktop demonstrates significant improvements in vulnerability detection compared to traditional tools. The system is capable of identifying both known and unknown vulnerabilities using AI-based analysis.

One of the key results is the reduction in false positives. Traditional tools often generate a large number of incorrect alerts, which require manual verification. VulnScan Desktop minimizes this issue by using intelligent algorithms.

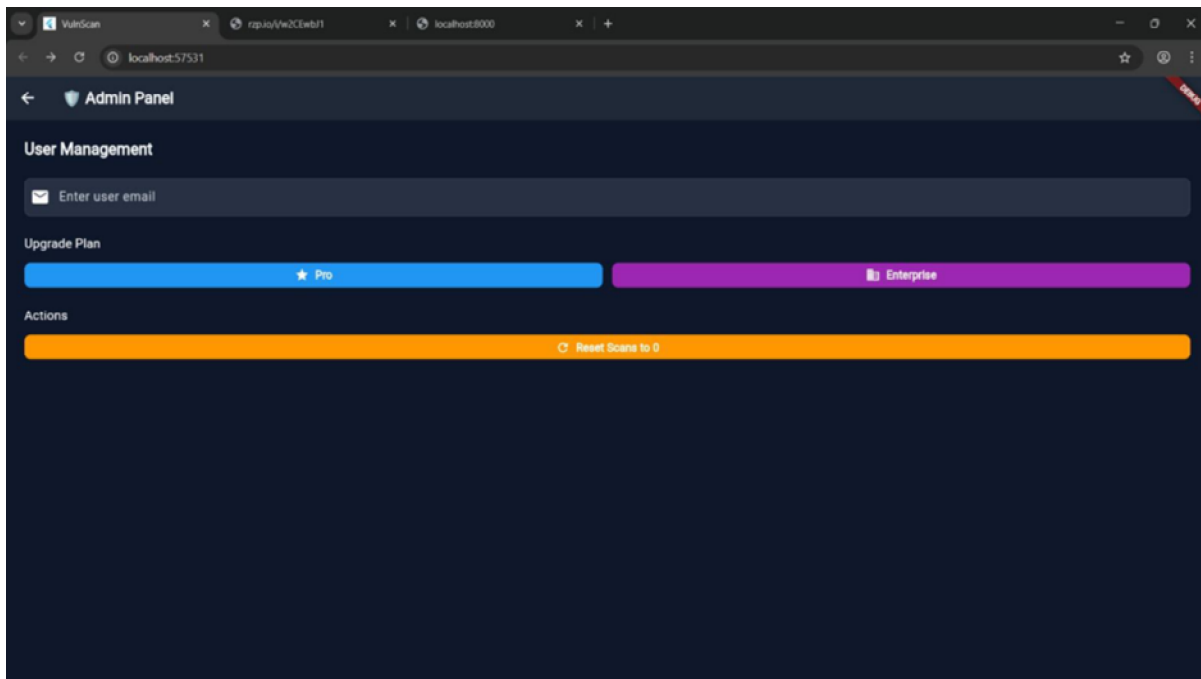
The real-time dashboard provides immediate insights into the security status of applications.

Users can monitor vulnerabilities as they are detected, allowing for faster response and mitigation.

Performance evaluations show that the system can handle multiple scans efficiently. It processes large amounts of data without significant delays, making it suitable for real-world applications.

The system also demonstrates adaptability to different types of applications. It can analyze both web and mobile platforms, ensuring comprehensive coverage.

User feedback indicates that the dashboard is easy to understand and use. The visual representation of data helps users quickly identify critical issues.



IX. ADVANTAGES OF THE SYSTEM

One of the main advantages of VulnScan Desktop is its use of artificial intelligence. This allows the system to detect complex vulnerabilities that traditional tools may miss. It also improves accuracy over time.

The system provides real-time monitoring, which helps in identifying vulnerabilities as soon as they occur. This reduces the risk of exploitation and enhances overall security.

Another advantage is the reduction of false positives. By using machine learning techniques, the system filters out irrelevant alerts, saving time and effort for developers.

The user-friendly dashboard is also a significant benefit. It presents complex security data in a simple and visual format, making it accessible to both technical and non-technical users.

Cross-platform support ensures that both web and mobile applications can be analyzed. This makes the system versatile and suitable for various use cases.

Automation is another key advantage. The system performs continuous scanning and reporting without requiring manual intervention, improving efficiency.

Overall, VulnScan Desktop offers a comprehensive and intelligent approach to vulnerability assessment.

X. LIMITATIONS

Despite its advantages, VulnScan Desktop has certain limitations that need to be considered. One limitation is the dependency on training data for the AI models. If the data is not diverse enough, the system may not detect all types of vulnerabilities.

Another limitation is the computational cost. AI-based analysis requires significant processing power, which may affect performance on low-end systems.

The system may also require regular updates to stay effective against new threats. Without updates, its ability to detect emerging vulnerabilities may decrease.

Integration with existing systems can sometimes be challenging. Organizations may need to modify their infrastructure to fully utilize the system.

There is also a possibility of false negatives, where some vulnerabilities may go undetected. This is a common challenge in all security systems. The initial setup and configuration of the system may require technical expertise. This can be a barrier for users with limited knowledge.

Overall, while the system is powerful, these limitations highlight areas for improvement.

XI. FUTURE SCOPE

The future scope of VulnScan Desktop includes several enhancements to improve its functionality and performance. One potential improvement is the integration of advanced AI models such as deep learning techniques.

The system can also be extended to support cloud-based environments. This would allow organizations to perform vulnerability assessments on cloud applications and services.

Another area of development is the inclusion of automated patch management. The system could not only detect vulnerabilities but also suggest to apply fixes automatically.

Integration with DevOps pipelines is another promising direction. This would enable continuous security testing during the software development lifecycle.

The dashboard can be enhanced with more advanced visualization techniques. This would provide deeper insights into security trends and patterns.

Support for additional platforms, such as IoT devices, can also be added. This would expand the system's applicability to emerging technologies. Overall, the future scope of the project is vast and offers many opportunities for innovation.

XII. CONCLUSION

In conclusion, VulnScan Desktop provides an innovative solution for vulnerability assessment by combining artificial intelligence with real-time monitoring. It addresses the limitations of traditional tools and offers improved accuracy and efficiency.

The system's ability to detect vulnerabilities across web and mobile applications makes it a versatile tool for modern security needs. Its real-time dashboard enhances usability and enables quick decision-making.

By reducing false positives and automating the scanning process, the system saves time and resources. This makes it highly beneficial for developers and security teams.

Although there are some limitations, the advantages of the system outweigh them.

Continuous improvements and updates can further enhance its performance.

Overall, VulnScan Desktop contributes to the development of more secure applications and systems.

REFERENCES

- [1] Research paper on vulnerability assessment techniques: Studies on machine learning applications in cybersecurity



- [2] OWASP(Open WebApplicationSecurity Project)documentation Researchonstaticanddynamicanalysistools
- [3] Articleson real-time monitoringsystems
- [4] Documentationofmachinelearninglibraries(TensorFlow, Scikit-learn) Websecuritystandardsandbestpractices
- [5] Journalsoncybersecurityadvancements



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)