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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

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

Ms.S.A.Kamble, Aadesh Gaikwad, Rushikesh Patil, Harshal Londhe, Vishal Poute, Shriyash Pawar
ComputerScience and Engineering SVERI'sCollegeofEngineering, Pandharpur,India

Abstract: ***VulnScanDesktopisanintelligentsecuritysolutiondesignedto identify, analyze, andvisualize vulnerabilitiesin webandmobile applicationsthroughan AI-driven approach.With the rapid growthofdigitalplatforms, applicationsare increasinglyexposedtocyberthreatssuchas injectionattacks,insecureAPIs,misconfigurations,anddataleakage.Thisprojectaimsto addressthese challengesbydevelopinga desktop-basedvulnerabilityassessmenttool combinedwitha real-timesecuritydashboard. Thesystemintegratesautomatedscanningtechniqueswithmachinelearningmodelstodetectbothknownandemergingsecurityweaknesse s.Itperformsstaticanddynamicanalysisonapplicationcomponents,ensuringcomprehensivecoverageacrossdifferentlayersofthesystem. TheAIcomponentenhancesdetectionaccuracybylearningpatternsfromprevious vulnerabilitiesandadaptingtonewthreatbehaviors. AkeyfeatureofVulnScanDesktopisitsinteractivedashboard,whichprovidesrealtimeinsightsintoidentifiedvulnerabilities.Thedashboar dpresentsdatausingvisualelementssuch asgraphs,riskscores,andseverityclassifications,enablingdevelopersandsecurityanalysts toquicklyunderstandandprioritizeissues.Additionally,thesystemgeneratesactionablerecommendationsformitigation,helpingusersim proveapplicationsecurityefficiently.***

Theproposedsolutionfocusesonusability,scalability,andperformance,makingitsuitable forbothsmall-scaledevelopers andenterprise environments. Bycombiningautomation, artificialintelligence,andreal-timemonitoring,VulnScanDesktopcontributestoproactive cybersecuritypracticesandreducestheriskofexploitationinmodernapplications

I. INTRODUCTION

Inthemoderndigitalera,webandmobileapplicationsplaya crucial role indeliveringservices acrossindustriessuchas banking,healthcare, education,ande-commerce.Asthese applicationshandlesensitiveuserdataandcriticaloperations,ensuringtheirsecurityhas becomea toppriority.However,theincreasingcomplexityofapplicationsandthegrowing numberofcyberthreatsmakeitdifficultto maintainstrong securitystandardsthroughoutthe developmentlifecycle.

Cyberattackerscontinuouslysearchforweaknessessuchasimproperinputvalidation,insecureAPIs,outdatedlibraries,andweakauthenticatio nmechanisms.Ifleftundetected, thesevulnerabilitiescanbeexploitedtogainunauthorizedaccess,disruptservices,orsteal confidential information. Asa result,organizationsmustadopteffectivevulnerability assessmentstrategiesto identifyandfixsecurity issues beforetheyareexploited.

Traditionalvulnerabilityscanningtoolsprovidebasicdetectioncapabilitiesbutoftensuffer fromlimitationssuchashighfalse-positiverates, lackofautomation,anddifficultyin interpretingresults.Manyexistingsystemsgeneratelengthyreportsthatrequireexpert knowledge toanalyze, makingitchallengingfordevelopersandsmallteamstorespond quickly.Additionally,thesetoolsmaynotofferreal-timeinsightsin tothesecuritystatusof applications.

Toovercomethesechallenges,theproposedproject,"VulnScanDesktop:AnAI-Powered VulnerabilityAssessmentandReal-TimeSecurity DashboardforWebandMobile Applications,"introducesanintelligentandefficientapproachtoapplicationsecurity.The systemleverages artificial intelligence techniques toenhance the detectionprocess, enabling smarteridentification ofvulnerabilities whilereducingunnecessaryalerts.

Theapplicationisdesignedas a desktop-basedsolutionthatperformscontinuousscanningof bothwebandmobileapplications. Itcollectssecurity-relateddata,analyzespatterns,and identifiespotentialthreatsinrealtime.ByincorporatingAI-drivenanalysis, thesystemcanad apttonewtypesofvulnerabilitiesandimproveitsaccuracyovertime,makingitmore reliablethantraditionaltools.

Oneofthekeyfeaturesofthisprojectisitsreal-timesecuritydashboard,whichpresents vulnerabilitydataina clearandvisually understandable format. Insteadof complextechnical reports,users canview graphical representations, risk levels, and prioritizedalerts. This helps developers,testers,andsecurityteamstoquicklyunderstandtheseverityofissuesandtake appropriateactionswithoutdelay.

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, VulnScan Desktop, 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, VulnScan Desktop offers a modern, intelligent, and efficient solution for vulnerability assessment.

V. METHODOLOGY

The methodology of VulnScan Desktop 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.

Thenextstepinvolvespreprocessingthecollecteddata.Thisincludesfilteringirrelevantinformationandpreparingthedataforanalysis.Properpreprocessingimprovestheaccuracyofthesystem.

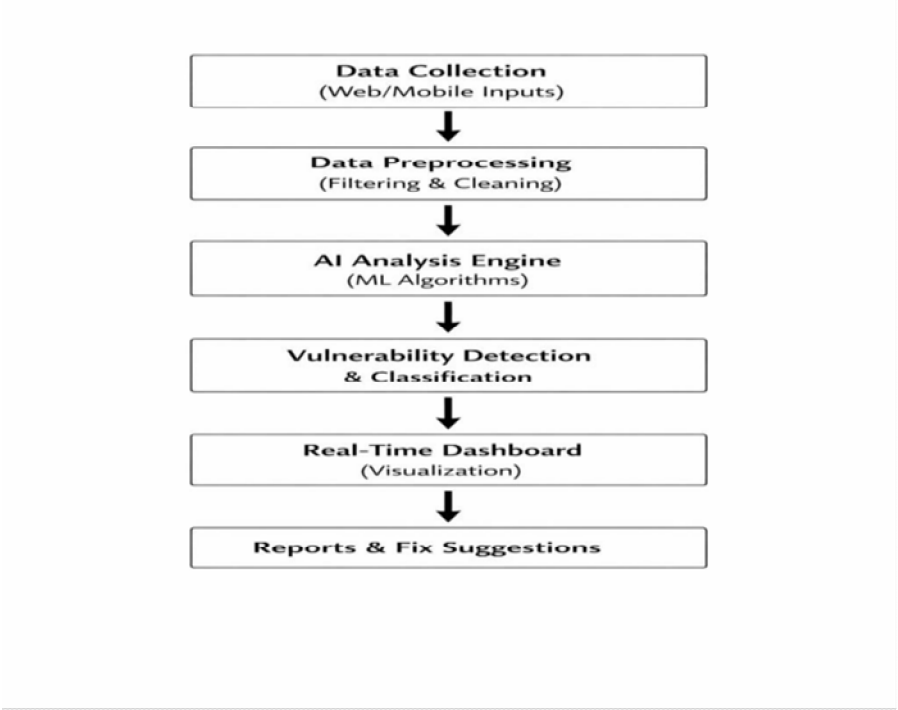
AImodelsarethenappliedtoanalyzethedata.Thesemodelsidentifypatternsanddetectanomaliesthatmayindicatevulnerabilities.Machinelearningalgorithmsplay a key roleinthis process.

Afteranalysis,thesystemclassifiesvulnerabilitiesbasedonseveritylevelssuchaslow, medium,andhigh.Thishelpsprioritizesecurityissues.

Theresultsarethenvisualizedusing a real-timedashboard.Thedashboardprovidesinsights throughchartsandgraphs,makingit easiertounder standthedata.

Continuousmonitoringisanimportantpartofthemethodology.Thesystemregularlyupdates itsanalysisbasedonnewdata,ensuringup-to-datesecurityinformation.

Finally,thesystemgeneratesreportsandrecommendations.Thesereportshelpdevelopersfixvulnerabilitiesandimproveapplicationsecurity.



VI. SYSTEM ARCHITECTURE

The system architectureofVulnScanDesktopisdesignedtoensurescalability,modularity,and efficientcommunication betweencomponents. Itfollows a layeredarchitecturewhereeach layerperformsa specificfunction, makingthesystemeasiertomaintainandupgrade.

Atthetoplevel,theuserinteractswiththesystemthrough a desktop-basedgraphicaluser interface. Thisinterfaceprovides accesstoscanningoptions,reports,andthereal-time dashboard.Itisdesignedto besimpleandintuitiveso thatevennon-expertuserscanoperate iteffectively.

Thenextlayeristheapplicationlogiclayer,whichcontrolsthecorefunctionalitiesofthesystem.Thisincludesmanagingscanoperations,coordinatingbetweenmodules,and processing user inputs. Itacts as a bridgebetween the user interface andbackendprocessing components.

Thescanningengineformsthecoreofthesystem.Itperformsvulnerabilityassessmentsbyanalyzingwebandmobileapplications.Itincludesmodulesforstaticanalysis,dynamic analysis,andAPItesting.Thesemodulesworktogethertoensurecomprehensivecoverage.

An AIprocessing moduleis integratedinto thearchitecture to enhancedetectioncapabilities. Itanalyzescollecteddata usingmachinelearningalgorithmsandidentifiespatternsthatindicatepotentialvulnerabilities.Thismodulecontinuouslyimprovesitsperformancebased onhistoricaldata.

Thedatastoragelayerisresponsibleforstoringscanresults,logs,andhistoricalrecords.Astructureddatabaseisusedtoensureefficientdataretrievalandmanagement.Thisallows thesystemtotrackvulnerabilitytrendsovertime.

Finally,thevisualizationlayerpresentstheresultsthrougha real-timedashboard.Itdisplays keymetricssuchasvulnerability severity, frequency,andrisklevelsusinggraphsandcharts.

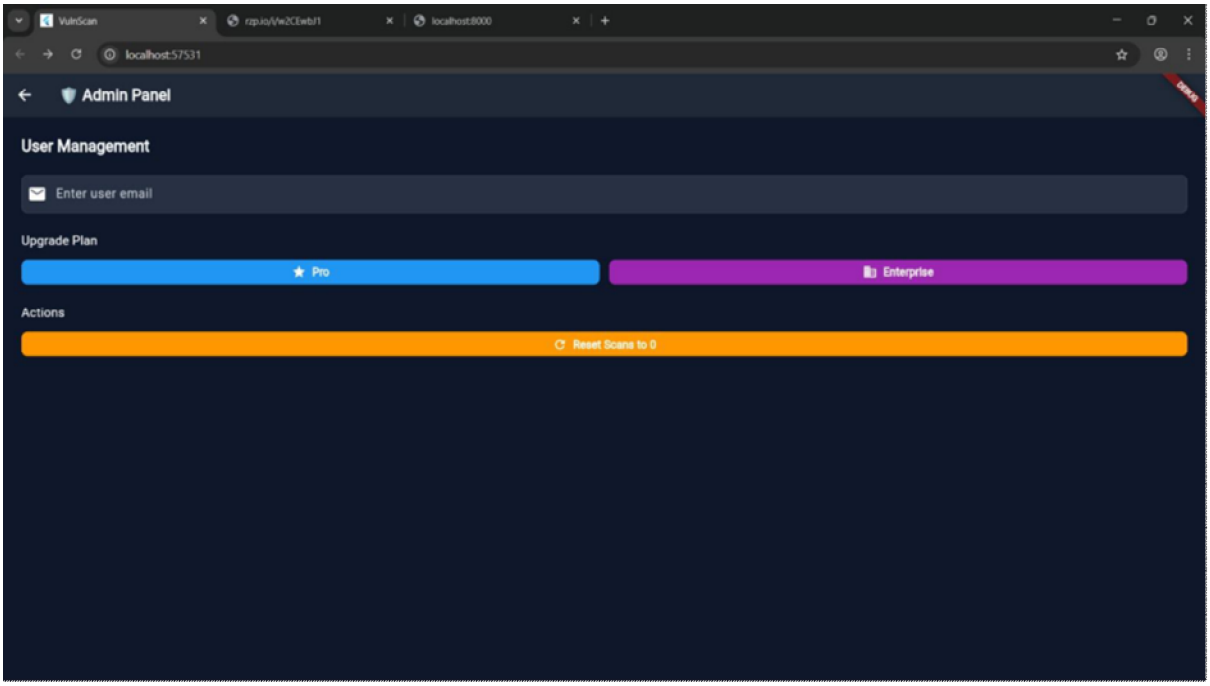
Thislayeredarchitectureensuresthateachcomponentoperatesefficientlywhilecontributing totheoverallsystemfunctionality.

VII. THESYSTEM IMPLEMENTATION INVOLVES MULTIPLE TECHNOLOGIES

Frontend: Electron.js, React.js,TailwindCSS Backend:PythonFastAPI
Database: MongoDB
Authentication: FirebaseAuth+ JWT Payments:Razorpay
Deployment: AWSEC2 / Render
Thescanningenginerunstoolsinparallel,improvingperformance.TheAIlayerenhances usability bysimplifying technical outputs.Thedashboard provides visual insightsusingcharts andgraphs.

VIII. RESULTS AND DISCUSSION

TheimplementationofVulnScanDesktopdemonstratessignificantimprovementsinvulnerabilitydetectioncomparedtotraditionaltools.Thesystemiscapableofidentifyingboth knownandunknownvulnerabilitiesusingAI-basedanalysis.
Oneofthekeyresultsisthereductioninfalsepositives.Traditionaltoolsoftengeneratealargenumberofincorrectalerts,whichrequiremanualverification.VulnScanDesktop minimizesthisissuebyusingintelligentalgorithms.
Thereal-timedashboardprovidesimmediateinsightsintothesecuritystatusofapplications.
Userscanmonitorvulnerabilitiesastheyaredetected,allowingforfasterresponseand mitigation.
Performanceevaluationshowsthatthesystemcanhandlemultiplescansefficiently.Itprocesseslargeamountsofdatawithoutsignificantdelays, makingitsuitableforreal-world applications.
Thesystemalsodemonstratesadaptabilitytodifferenttypesofapplications.Itcananalyze bothwebandmobileplatforms,ensuringcomprehensivecoverage.
Userfeedbackindicatesthatthedashboardiseasytounderstandanduse.Thevisual representationofdatahelpsusersquicklyidentifycriticalissues.



IX. ADVANTAGESOF THE SYSTEM

One ofthemainadvantages ofVulnScanDesktopis itsuse of artificialintelligence.This allows the system to detectcomplexvulnerabilitiesthattraditionaltoolsmaymiss.Italsoimproves accuracyovertime.
Thesystemprovidesrealtimemonitoring,whichhelpsinidentifyingvulnerabilitiesassoonastheyoccur.Thisreducestheriskofexploitationandenhancesoverallsecurity.

Anotheradvantageisthereductionoffalsepositives.Byusingmachinelearningtechniques,thesystemfiltersoutirrelevantalerts,savingtimeandeffortfordevelopers.
Theuser-friendlydashboardisalso a significantbenefit.Itpresents complexsecuritydata ina simpleandvisualformat,makingit accessibletobothtechnicalandnon-technicalusers.
Cross-platformsupportensuresthatbothwebandmobileapplicationscan be analyzed.This makesthesystem versatile andsuitableforvarioususecases.
Automationisanotherkeyadvantage.Thesystemperformscontinuousscanningandreportingwithoutrequiringmanualintervention,improvingefficiency.
Overall,VulnScanDesktopoffersa comprehensiveandintelligentapproachtovulnerability assessment.

X. LIMITATIONS

Despiteitsadvantages,VulnScanDesktophascertainlimitationsthat need to be considered. Onelimitation is thedependency ontraining datafor the AImodels.If thedatais not diverse enough,thesystemmaynotdetectalltypesofvulnerabilities.
Another limitation isthecomputational cost.AI-basedanalysisrequiressignificantprocessing power,whichmayaffectperformanceonlow-endsystems.
Thesystemmayalsorequireregularupdatestostayeffectiveagainstnewthreats.Withoutupdates,itsabilitytodetectemergingvulnerabilities maydecrease.
Integrationwithexistingsystemscansometimesbechallenging.Organizationsmayneedtomodifytheirinfrastructuretofullyutilizethesystem.
Thereisalsoa possibilityoffalsenegatives,wheresomevulnerabilitiesmaygoundetected. Thisisa commonchallengeinallsecuritysystems.
The initialsetupandconfigurationof thesystemmayrequiretechnicalexpertise. This can be a barrierforuserswithlimitedknowledge.
Overall,whilethesystemispowerful,these limitationshighlight areasforimprovement.

XI. FUTURE SCOPE

ThefuturescopeofVulnScanDesktopincludesseveralenhancementstoimproveitsfunctionalityandperformance.Onepotentialimprovement istheintegrationofadvancedAI modelssuchasdeeplearningtechniques.
The system can also be extended to support cloud-based environments. This would allow organizations to performvulnerabilityassessmentsoncloud applicationsandservices.
Anotherareaofdevelopmentistheinclusionofautomatedpatchmanagement.Thesystemcouldnotonlydetectvulnerabilitiesbutalsosuggestorapplyfixesautomatically.
IntegrationwithDevOpspipelinesisanotherpromisingdirection.Thiswouldenablecontinuoussecuritytestingduringthesoftwaredevelopmentlifecycle.
Thedashboardcanbeenhancedwithmoreadvancedvisualizationtechniques.Thiswouldprovidedeeperinsightsintosecuritytrendsandpatterns.
Supportforadditionalplatforms,suchasIoTdevices,canalsobeadded.Thiswouldexpandthesystem'sapplicabilitytoemergingtechnologies.
Overall,the futurescopeof the project isvast and offersmanyopportunitiesforinnovation.

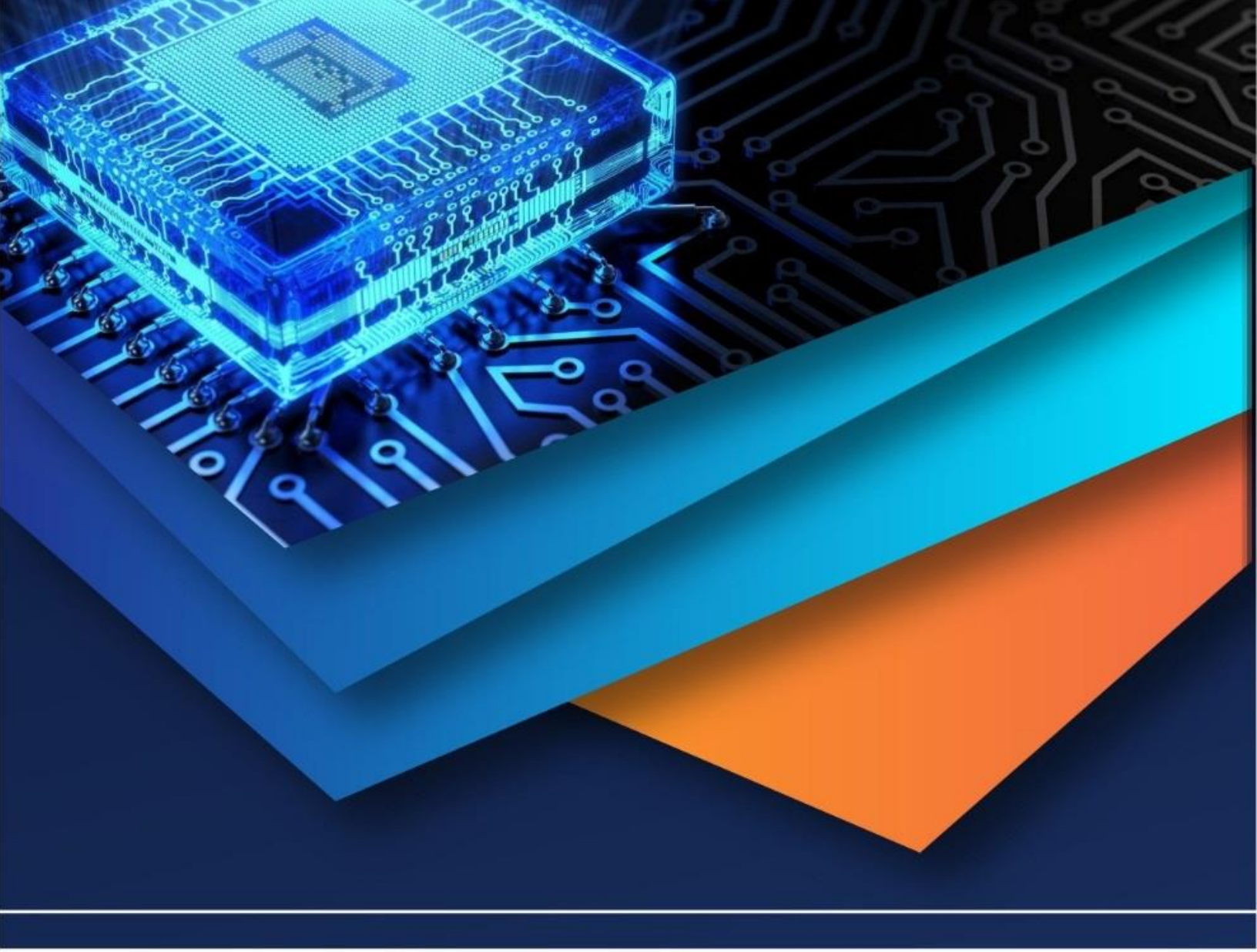
XII. CONCLUSION

Inconclusion,VulnScanDesktopprovidesan innovativesolutionforvulnerabilityassessment bycombiningartificialintelligencewithreal-timemonitoring.Itaddressesthelimitationsof traditionaltoolsandoffersimprovedaccuracyandefficiency.
Thesystem'sabilitytodetectvulnerabilitiesacrosswebandmobileapplicationsmakesita versatiletoolformodernsecurityneeds.Itsreal-timedashboardenhancesusabilityand enablesquickdecision-making.
Byreducingfalsepositivesandautomatingthescanningprocess,thesystemsavestimeandresources.Thismakesithighlybeneficialfordevelopersandsecurityteams.
Althoughtherearesomelimitations,theadvantagesofthesystemoutweighthem.
Continuousimprovementsandupdatescanfurtherenhanceitsperformance.
Overall,VulnScanDesktopcontributestothedevelopmentofmoresecureapplicationsand systems

REFERENCES

[1] Researchpapersonvulnerabilityassessmenttechniques Studies on machinelearningapplicationsincybersecurity

[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