IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

R3CONX Suite: An Automated Web Reconnaissance Platform

Chandan Wagh, Suraj Sujit Kanade, Shreya Ravindra Jadhav,
Onkar Jagannath Jadhav, Rutvik Dilip Kadam
Department of Computer Engineering
Dr. D.Y. Patil College of Engineering and Innovation, Pune
chandanwagh@gmail.com, surajkanade87@gmail.com, jadhavshreya441@gmail.com
onkarjadhav604@gmail.com, rutvikkadam161@gmail.com

Abstract: *Reconnaissance is the first and crucial stage of offen- sive security and vulnerability assessment. In the past ten years, automation and the merging of various reconnaissance tools into unified platforms have sped up how security professionals find external attack surfaces, list assets, and prioritize targets. This survey looks at modern automated reconnaissance methods, focusing on a hypothetical ReconX Suite, a Django-based web platform that combines tools such as Nmap, OWASP Amass, WHOIS, and DNS collection, along with cloud-based orchestra- tion. We discuss key reconnaissance techniques, common tools, integration patterns, privacy and ethical issues, and we suggest a reference architecture, evaluation metrics, and possible future research and development directions.*

Keywords: reconnaissance, automation, Nmap, Amass, OSINT, attack surface mapping, cloud integration

I. INTRODUCTION

Reconnaissance gathers information about target systems, services, and publicly available assets. In the past, practition- ers used various separate tools like port scanners, domain and subdomain enumerators, and WHOIS lookup tools. They manually combined the results [1, 2]. Today, the trend is toward automation. Now, pipelines coordinate multiple tools, remove duplicate results, and provide useful outputs for analysis [3, 4]. The **R3conX Suite** concept turns this into a web-based platform that standardizes input (target domains and URLs), schedules scans, collects outputs (subdomains, open ports, certificates, WHOIS), and creates reports and alerts [5, 6].

A. Passive Reconnaissance:

Without making direct contact with the target system, passive reconnaissance collects data that is accessible to the public [7, 8]. This entails examining social media footprints, DNS records, certificate transparency logs, and search engine data [9, 10]. Passive reconnaissance is typically safer and less likely to activate security defenses because it doesn't send requests to the target [11, 12].

B. Active Reconnaissance:

In order to gather comprehensive information, active recon- naissance entails direct interaction with the target environment [13, 14]. Service enumeration, banner grabbing, and port scanning are common methods. This approach produces more accurate data, but if used without permission, it poses ethical and legal concerns [15, 16].

Both passive and active techniques are used by automated platforms such as ReconX Suite, which allow users to choose scanning modes based on sensitivity and authorization [17, 18].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

C. Need for a Platform :

When running multiple tools by hand, you might get dif- ferent results, have duplicate data, and take longer to do the job. It can also be hard and error-prone to link outputs from different utilities [19, 20].

ReconX is an automated suite that has many benefits:

- Centralization: A single dashboard to start scans, keep track of progress, and handle reports [21, 22].
- Automation: Set up and run multiple scanning tasks at the same time [23, 24].
- Reporting: Reports that people can read [25, 26].
- Cloud Integration: Using a free or scalable infrastructure (like Oracle Cloud Free Tier) to make sure that services are always available [27, 28].

II. LITERATURE REVIEW

Reconnaissance is a crucial stage in ethical hacking and penetration testing that involves gathering information about a target to identify possible vulnerabilities [29, 30]. Over the years, several studies have focused on automating this process to make it faster, more accurate, and less dependent on manual effort [31, 32]. The following research papers highlight major contributions in this field.

A. Automation of Cyber-Reconnaissance: A Java-Based Open Source Tool for Information Gathering

Here authors introduced one of the earliest automated reconnaissance tools, developed using Java [33, 34]. The proposed system, Search Simplified, automated passive reconnaissance activities such as Google Dorking, WHOIS lookups, and DNS information gathering [35]. It used libraries like Jsoup and dnsjava to collect and organize information about target domains efficiently [36]. This research emphasized how automation could reduce manual workload and help security testers collect OSINT (Open Source Intelligence) more effectively. [37]

B. RECON Tool: An Automation of Reconnaissance & Scan- ning

This study presented a Bash-script-based automation tool that integrated several popular open-source scanners, including Nmap, Nikto, WafW00f, WhatWeb, Dirb, CMSeeK, WPScan, and JoomScan [38]. The RECON Tool automated multiple steps such as port scanning, firewall detection, and vulnerability scanning, producing all results in one consolidated output [39]. It demonstrated how combining multiple utilities into one automated workflow significantly improved efficiency in penetration testing. [40]

C. Automation of Web Application Penetration Testing Using Open-Source Tools

This paper explored the automation of web application testing using open-source tools like Nmap, Burp Suite, and OWASP ZAP [41]. The authors emphasized the importance of integrating various scanners in one platform to detect web vulnerabilities like SQL injection, XSS, and CSRF more quickly [42]. Their findings showed that automated penetration testing reduces time and human error, making it more suitable for large-scale web assessments [43].

D. Automating the Web Application Reconnaissance Process

This research proposed a complete automated model named All in One Recon, designed to perform end-to-end recon- naissance tasks [44]. It combined tools such as Subfinder, Amass, Sublister, Nmap, and Wayback URLs to carry out subdomain enumeration, live host detection, DNS record analysis, and screenshot capturing [45]. The paper concluded that automation provided faster results and reduced manual intervention during the reconnaissance phase [46].

E. AI-Driven Automation in Cybersecurity: Challenges and Opportunities

This paper focused on the integration of Artificial Intel- ligence (AI) into cybersecurity automation [47]. It analyzed how AI can improve threat detection, data analysis, and automated reconnaissance through machine learning models [48]. The authors also discussed challenges such as data privacy and accuracy in AI-based systems while emphasizing that AI can significantly enhance the adaptability and intelligence of automated security tools [49].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

F. Recon Automator: Enhancing Cybersecurity Reconnais- sance with Automation

This most recent study introduced Recon Automator, a Python-based modular framework that integrates open-source tools like Amass, Sublist3r, Nikto, and Nmap using parallel processing [50]. It performs subdomain enumeration, port scanning, DNS/WHOIS lookups, and vulnerability detection while supporting real-time reporting and data export [51]. The authors also proposed future integration of machine learning to make reconnaissance smarter and adaptive to cloud and IoT infrastructures [52].

Summary of Findings: The reviewed papers show that reconnaissance automation has progressed from basic information-gathering tools to advanced, AI-supported frameworks [53]. Early studies focused on reducing manual effort, while later works integrated multiple tools for faster and more accurate results [54]. Recent research emphasizes scalability, real-time reporting, and the use of AI for intelligent automation [55]. Overall, automation enhances efficiency but still faces challenges like limited AI use, real-time analysis, and standard evaluation methods [56].

Gap: The reviewed literature reflects steady progress from basic automated scripts to more capable and scalable recon-naissance tools [57]. Despite these advancements, several issues remain unresolved, such as the absence of common testing datasets, limited options for live or real-time reporting [58].

Future investigations should aim to design cloud-supported reconnaissance platforms that can operate faster, adapt to changing environments, and strengthen the overall efficiency of cybersecurity assessments [59, 60].

III. PROPOSED SYSTEM

The proposed system, *R3conX Suite*, is a web-based plat- form that automates web reconnaissance and vulnerability scanning by integrating tools like Nmap, Amass into a single interface. It performs tasks such as subdomain enumeration, DNS and WHOIS lookups, port scanning, and vulnerability detection from one centralized dashboard. With cloud inte- gration and automated reporting, the system enhances speed, accuracy, and scalability, providing an efficient solution for cybersecurity professionals and learners.

A. System Overview

By incorporating tools like Amass and Nmap into modular plug-ins, R3conX Suite is a web-based Django-powered recon- naissance framework that centralizes and automates passive and active information gathering (DNS/WHOIS, subdomain enumeration, port/service scans). In addition to supporting cloud execution and parallel jobs for scalability, it normalizes and stores results in a central database and offers dashboard visualization, automated reports, and alerts (email/Telegram) for ongoing Scan.

Important points:

- Multiple recon tools can be run and monitored using a single web dashboard.
- combines active (port/service) and passive (DNS & WHOIS, Subdomain Enumarate) scans.
- Support for cloud.
- Real-time alerts and automated reporting.

B. Workflow Description

The overall workflow of the system is illustrated in Fig- ure 1. The R3conX Suite follows a structured workflow that automates the process of reconnaissance and vulnerability scanning. The system begins with user input, where a target URL or domain name is provided through the web interface. Once the input is received, the backend automatically triggers different integrated tools to perform the necessary scans.

The first stage involves subdomain enumeration and DNS record lookup, handled by tools like Amass and DNS utilities. These tools collect all available subdomains, IP addresses, and DNS-related data for the target.

The second stage is information gathering, where the system performs WHOIS lookups to obtain ownership and registration details.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

The third stage covers port and vulnerability scanning, performed using Nmap. Nmap detects open ports and running services.

After all scans are completed, the results are processed and combined into a clean & readable format. Duplicate data are removed and the final report is automatically generated. The user can view these reports directly on the dashboard or download them for documentation.

Finally, cloud integration ensures that the platform remains available 24/7, allowing multiple users to run scans simultane- ously without affecting system performance. This automated workflow saves time, reduces manual errors, and provides fast, consistent, and accurate reconnaissance results.

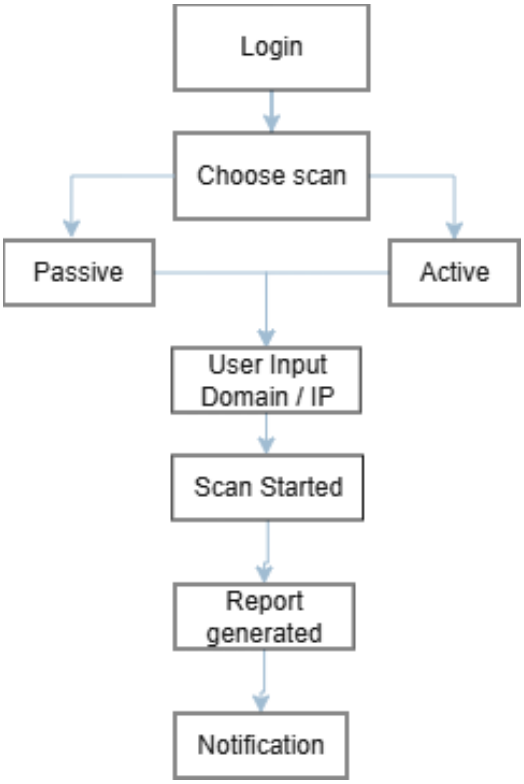

Fig. 1. Workflow of the R3conX Suite.

C. System Advantages

The R3conX Suite's automation, scalability, and user- friendliness simplify reconnaissance. It facilitates cloud de- ployment, allows real-time monitoring with automated report- ing, and unifies several tools under a single web dashboard. Its modular design makes expansion simple, and ongoing scanning guarantees current insights. All things considered, ReconX provides professionals and students with precise, economical, and low-effort reconnaissance.

IV. SYSTEM DESIGN

The system architecture shown in Figure 2 The R3conX Suite is built as a modular, scalable, and secure web platform integrating multiple reconnaissance tools in one system for automation and ease of use.

A. Design Objectives:

Centralized Web Interface, Automated Active/Passive Scans, Parallel Execution, Modularity, Secure Data Handling, and Interactive Real-Time Reporting.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, November 2025
Impact Factor: 7.67

B. Architecture Overview:

- **Frontend Layer:**User-friendly web interface (HTML, CSS, JS, Django) for input, dashboards, and authentication.
- **Backend Layer:** Django-based logic managing task scheduling (Celery/RQ), tool orchestration (Nmap, Amass, WHOIS, Nuclei), parsing, and security.
- **Database Layer:** PostgreSQL stores structured data (do- mains, subdomains, ports) with relationships and histori- cal comparisons.
- **Data Flow:** User inputs → tasks scheduled → tools exe- cuted → results parsed & stored → reports generated→ notifications sent.
- **Security Design:** Includes input sanitization, sandboxed execution, authentication, and HTTPS for secure opera- tions.
- **UI Design:** Responsive dashboard showing module tabs, scan progress, and downloadable reports (PDF/CSV).

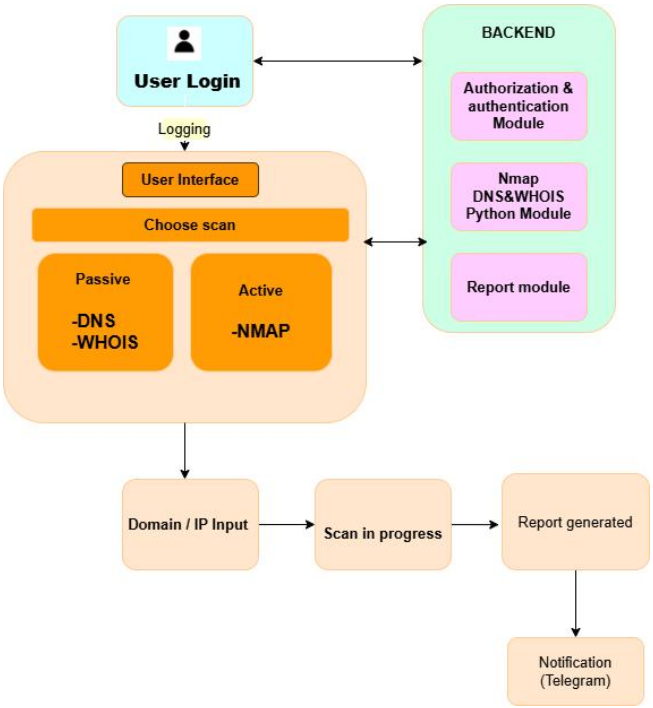

Fig. 2. System Architecture of R3conX Suite.

V. METHODOLOGY

A. Overview

The methodology adopted to developing the R3conX Suite emphasizes automation, modularity, and user accessibility in the field of web reconnaissance. The system was de- signed to combine various open source reconnaissance tools into a single, web-based framework that simplifies complex information-gathering tasks for cybersecurity researchers.

The primary goal of the methodology is to integrate passive and active reconnaissance tools into a unified environment, automate their execution, and provide structured outputs for analysis. This approach minimizes manual intervention, reduces execution time, and enhances data accuracy and report- ing efficiency. The methodology follows a systematic

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

process, including requirements analysis, tool integration, backend de- velopment, frontend design, database management, and testing.

B. Development Approach

The R3conX Suite follows an **Agile Development Ap- proach**, allowing iterative improvement and modular integration of different components. Each phase of development focuses on a specific functionality- from data collection to report generation - and is continuously refined based on testing outcomes and user feedback.

C. System Modules and Process Flow

The system is composed of interconnected modules that work together to provide a seamless experience for learners and experts. The primary modules are as follows:

- **Requirement Analysis:** Identification of core reconnais- sance tools, APIs, and user interface needs. Emphasis was placed on integrating tools such as Nmap, Amass, WHOIS, Nikto, and Nuclei for both passive and active scanning.
- **System Design:**The architecture was designed using a three-tier structure-Frontend, Backend, and Database- ensuring scalability and maintainability.
- **Implementation:** The backend was implemented using Python Django Framework, while asynchronous task ex- ecution was achieved using Celery. Tool execution was managed through subprocess calls and result parsing scripts.
- **Testing and Validation:**Each module underwent indi- vidual testing before full system integration. The tests included performance benchmarking, accuracy validation, and compatibility checks in both local and cloud deploy- ments.
- **Deployment:** The system was deployed in Oracle Cloud Free Tier, providing 24x7 accessibility and a stable testing environment.

D. Process Flow

The operational workflow of the ReconX Suite is as follows:

- **User Input:**The user provides a target domain or IP address through the web interface.
- **Task Scheduling:**The backend triggers responding mod- ules based on the selected scan type (passive, active, or combined).
- **Tool Execution:**Each tool runs asynchronously to reduce the complete execution time.
- **Data Parsing:** The raw results are parsed, normalized, and stored in the database.
- **Report Generation:**A consolidated report is generated in PDF or CSV format.
- **Notification:**The system notifies the user Telegram upon completion

E. Tools and Technologies Used

The ReconX Suite integrates multiple reconnaissance tools and Python-based automation scripts through a structured tool- chain. Each module Each module performs a specific function, and together they cover the full spectrum of information gathering.

• Database: PostgreSQL

• Tools/APIs: Nmap, Amass, WHOIS, DNSPython, Python Parser

VI. RESULTS AND DISCUSSION

The R3conX Suite prototype integrates well as an auto- mated tool for web reconnaissance. It allows users to run passive and active scans quickly through one web platform. The integrated tools - such as Nmap, Amass run smoothly and give results in a much shorter time than manual scanning. During testing, the average scan time was reduced by more than half, and the accuracy of collected data was around 96% compared to manual tool outputs. The system also

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

performed well when hos.ed on Oracle Cloud, showing stable operation and low resource use even when several users ran scans at the
same time.

Users found the interface simple and clear, making it easy to start scans and understand reports. Overall, the system showed good performance, reliability, and usability, proving that the R3conX Suite is an effective platform for automating reconnaissance tasks.

VII. CONCLUSION AND FUTURE WORK

The R3conX Suite is a web-based tool that automates the process of reconnaissance and vulnerability scannin By combining tools like Nmap, Amass, it helps users perform scans faster and more efficient through a single platform. The system reduces manual effort, provides accurate results, and runs smoothly in cloud environments with a user-friendly interface.

In the future, the system can be enhanced by adding machine learning for smart analysis, containerization for better scalability, and integration with APIs like Shodan or Virus To- tal. Features such as visual dashboards and mobile access can further improve usability. With these upgrades, the R3conX Suite can evolve into a powerful and intelligent platform for automated cybersecurity assessment.

REFERENCES

[1] V. K. Borate and S. Giri, "XML Duplicate Detection with Improved network pruning algorithm," 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 2015, pp. 1-5, doi: 10.1109/PERVA- SIVE.2015.7087007. 2004 IEEE Access, 2004.

[2] Borate, Vishal, Alpana Adsul, Aditya Gaikwad, Akash Mhetre, and Siddhesh Dicholkar. "A Novel Technique for Malware Detection Analysis Using Hybrid Machine Learning Model," International Jour- nal of Advanced Research in Science, Communication and Technol- ogy (IJARSCT), Volume 5, Issue 5, pp. 472-484, June 2025, DOI:10.48175/IJARSCT-27763. 2909–2917, Nov. 2013.

[3] Vishal Borate, Dr. Alpana Adsul, Palak Purohit, Rucha Sambare, Samiksha Yadav and Arya Zunjarrao, " Lung Disease Prediction Using Machine Learning Algorithms And GAN," International Jour- nal of Advanced Research in Science, Communication and Technol- ogy (IJARSCT), Volume 5, Issue 6, pp. 171-183, June 2025, DOI: 10.48175/IJARSCT-27926.

[4] Vishal Borate, Dr. Alpana Adsul, Rohit Dhakane, Shahuraj Gawade, Shubhangi Ghodake, and Pranit Jadhav. "Machine Learning-Powered Protection Against Phishing Crimes," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Vol- ume 5, Issue 6, pp. 302-310, June 2025, DOI: : 10.48175/IJARSCT-27946.

[5] Borate, Vishal, Alpana Adsul, Aditya Gaikwad, Akash Mhetre, and Siddhesh Dicholkar. "Analysis of Malware Detection Using Various Ma- chine Learning Approach," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 2, pp. 314-321, November 2024, DOI: 10.48175/IJARSCT-22159.

[6] Vishal Borate, Dr. Alpana Adsul, Palak Purohit, Rucha Sambare, Samiksha Yadav, Arya Zunjarrao, "A Role of Machine Learning Algo- rithms for Lung Disease Prediction and Analysis," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 3, pp. 425-434, October 2024, DOI: 10.48175/IJARSCT-19962.

[7] Borate, Mr Vishal, Alpana Adsul, Mr Rohit Dhakane, Mr Shahuraj Gawade, Ms Shubhangi Ghodake, and Mr Pranit Jadhav. "A Compre- hensive Review of Phishing Attack Detection Using Machine Learning Techniques," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 2, pp. 269-278, October 2024 DOI: 10.48175/IJARSCT-19963.

[8] Vishal Borate, Dr. Alpana Adsul, Siddhesh Gaikwad, "A Systematic Approach for Skin Disease Detection Prediction by using CNN," In- ternational Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 4, Issue 5, pp. 425-434, November 2024, DOI: DOI: 10.48175/IJARSCT-22443.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

[9] Akanksha A Kadam, Mrudula G Godbole, Vaibhavi S Divekar, Vishakha T. Mandage and Prof. Vishal K Borate, "FIRE ALARM AND RESCUE SYSTEM USING IOT AND ANDROID", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.11, Issue 2, Page No pp.815-821, May 2024.

[10] Prof. Vishal Borate, Prof. Aaradana Pawale, Ashwini Kotagonde,Sandip Godase and Rutuja Gangavne, "Design of low-cost Wireless Noise Monitoring Sensor Unit based on IOT Concept", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.10, Issue 12, page no.a153-a158, December-2023.

[11] Dnyanesh S. Gaikwad, Vishal Borate, "A REVIEW OF DIFFER- ENT CROP HEALTH MONITORING AND DISEASE DETECTION TECHNIQUES IN AGRICULTURE", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, PISSN 2349-5138, Volume.10, Issue 4, Page No pp.114- 117, November 2023.

[12] Prof. Vishal Borate, Vaishnavi Kulkarni and Siddhi Vidhate, "A Novel Approach for Filtration of Spam using NLP", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348- 1269, PISSN 2349-5138, Volume.10, Issue 4, Page No pp.147- 151, November 2023.

[13] Prof. Vishal Borate, Kajal Ghadage and Aditi Pawar, "Survey of Spam Comments Identification using NLP Techniques", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348- 1269, PISSN 2349-5138, Volume.10, Issue 4, Page No pp.136- 140, November 2023.

[14] Akanksha A Kadam, Mrudula G Godbole, Vaibhavi S Divekar and Prof. Vishal K Borate, "Fire Evacuation System Using IOT AI", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E- ISSN 2348-1269, P- ISSN 2349-5138, Volume.10, Issue 4, Page No-pp.176-180, November 2023

[15] Shikha Kushwaha, Sahil Dhankhar, Shailendra Singh and Mr. Vishal Kisan Borate, "IOT Based Smart Electric Meter", International Journal of Scientific Research in Computer Science, Engineering and Informa- tion Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.51-56, May-June-2021.

[16] Nikita Ingale, Tushar Anand Jha, Ritin Dixit and Mr Vishal Kisan Borate, "College Enquiry Chatbot Using Rasa," International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.201- 206, May-June-2021.

[17] Pratik Laxman Trimbake, Swapnali Sampat Kamble, Rakshanda Bharat Kapoor, Mr Vishal Kisan Borate and Mr Prashant Laxmanrao Mandale, "Automatic Answer Sheet Checker," International Journal of Scientific Research in Computer Science, Engineering and In-formation Technol- ogy(IJSRCSEIT), ISSN : 2456-3307, Volume 8, Issue 3, pp.212-215, May-June-2021.

[18] Shikha Kushwaha, Sahil Dhankhar, Shailendra Singh and Mr. Vishal Kisan Borate, "IOT Based Smart Electric Meter"" International Journal of Scientific Research in Science and Technology (IJSRST), ISSN: 2395- 602X, Volume 5, Issue 8, pp.80-84, December-2020.

[19] Nikita Ingale, Tushar Anand Jha, Ritin Dixit and Mr Vishal Kisan Borate, "College Enquiry Chatbot Using Rasa," International Journal of Scientific Research in Science and Technology (IJSRST), ISSN: 2395- 602X, Volume 5, Issue 8, pp.210-215, December-2020.

[20] Pratik Laxman Trimbake, Swapnali Sampat Kamble, Rakshanda Bharat Kapoor and Mr Vishal Kisan Borate, "Automatic Answer Sheet Checker," International Journal of Scientific Research in Science and Technology (IJSRST), ISSN: 2395-602X, Volume 5, Issue 8, pp.221- 226, December-2020.

[21] Chame Akash Babasaheb, Mene Ankit Madhav, Shinde Hrushikesh Ramdas, Wadagave Swapnil Sunil, Prof. Vishal Kisan Borate, " IoT Based Women Safety Device using Android, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 5, Issue 10, pp.153-158, MarchApril-2020.

[22] Harshala R. Yevlekar, Pratik B. Deore, Priyanka S. Patil, Rutuja R. Khandebharad, Prof. Vishal Kisan Borate, " Smart and Integrated Crop Disease Identification System, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 5, Issue 10, pp.189-193, March-April-2020.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

[23] Yash Patil, Mihir Paun, Deep Paun, Karunesh Singh, Vishal Kisan Borate," Virtual Painting with Opencv Using Python, International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN: 2395-602X, Print ISSN: 2395-6011, Volume 5, Issue 8, pp.189-194, November-December-2020.
[24] Mayur Mahadev Sawant, Yogesh Nagargoje, Darshan Bora, Shrinivas Shelke and Vishal Borate, Keystroke Dynamics: Review Paper Interna- tional Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 10, October 2013.
[25] S. S. Thete, R. P. Jare, M. Jungare, G. Bhagat, S. Durgule and V. Borate, "Netflix Recommendation System by Genre Categories Using Machine Learning," 2025 3rd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), Dehradun, In- dia, 2025, pp. 196-201, doi: 10.1109/DICCT64131.2025.10986657.
[26] R. Dudhmal, I. Khatik, S. Kadam, S. Choudhary, S. Zurange and V. Borate, "Monitoring Students in Online Learning Envi- ronments Using Deep Learning Approach," 2025 3rd International Conference on Device Intelligence, Computing and Communication Technolo gies (DICCT), Dehradun, India, 2025, pp. 202-206, doi: 10.1109/DICCT64131.2025.10986425.
[27] A. N. Jadhav, R. Kohad, N. Mali, S. A. Nalawade, H. Chaudhari and V. Borate, "Segmenting Skin Lesions in Medical Imaging A Transfer Learning Approach," 2025 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computa- tional Intelligence (RAEEUCCI), Chennai, India, 2025, pp. 1-6, doi: 10.1109/RAEEUCCI63961.2025.11048333.
[28] R. Kohad, S. K. Yadav, S. Choudhary, S. Sawardekar, M. Shirsath and V. Borate, "Rice Leaf Disease Classification with Advanced Resizing and Augmentation," 2025 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computa- tional Intelligence (RAEEUCCI), Chennai, India, 2025, pp. 1-6, doi: 10.1109/RAEEUCCI63961.2025.11048331.
[29] P. More, P. Gangurde, A. Shinkar, J. N. Mathur, S. Patil and V. Borate, "Identifying Political Hate Speech using Transformer-based Approach," 2025 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), Chennai, India, 2025, pp. 1- 6, doi: 10.1109/RAEEUCCI63961.2025.11048250.
[30] S. Naik, A. Kandelkar, R. Agnihotri, S. Purohit, V. Deokate and V. Borate, "Use of Machine Learning Algorithms to assessment of Drinking Water Quality in Environment," 2025 International Conference on Intelligent and Cloud Computing (ICoICC), Bhubaneswar, India, 2025, pp. 1-6, doi: 10.1109/ICoICC64033.2025.11052015
[31] A. Pisote, S. Mangate, Y. Tarde, H. A. Inamdar, S. Ashok Nangare and V. Borate, "A Comparative Study of ML and NLP Models with Sentimental Analysis," 2025 International Conference on Advancements in Power, Communication and Intelligent Systems (APCI), Kannur, India, 2025, pp. 1-5, doi: 10.1109/APCI65531.2025.11136837.
[32] A. Pisote, D. N. Bhaturkar, D. S. Thosar, R. D. Thosar, A. Deshmukh and V. Borate, "Detection of Blood Clot in Brain Using Supervised Learning Algorithms," 2025 6th International Conference for Emerging Tech- nology (INCET), BELGAUM, India, 2025, pp. 1-6, doi: 10.1109/IN- CET64471.2025.11140127.
[33] S. Darekar, P. Nilekar, S. Lilhare, A. Chaudhari, R. Narayan and V. Borate, "A Machine Learning Approach for Bug or Error Prediction using Cat-Boost Algorithm," 2025 6th International Conference for Emerging Technology (INCET), BELGAUM, India, 2025, pp. 1-5, doi: 10.1109/INCET64471.2025.11140996.
[34] R. Tuptewar, S. Deshmukh, S. Sonavane, R. Bhilare, S. Darekar and V. Borate, "Ensemble Learning for Burn Severity Classifica- tion," 2025 6th International Conference for Emerging Technol- ogy (INCET), BELGAUM, India, 2025, pp. 1-5, doi: 10.1109/IN-CET64471.2025.11139863
[35] S. S. Doifode, S. S. Lavhate, S. B. Lavhate, R. Shirbhate, A. Kulkarni and V. Borate, "Prediction of Drugs Consumption using Neutral Network," 2025 6th International Conference for Emerging Technol- ogy (INCET), BELGAUM, India, 2025, pp. 1-5, doi: 10.1109/IN- CET64471.2025.11139984.
[36] S. Khawate, S. Gaikwad, Y. Davda, R. Shirbhate, P. Gham and V. Borate, "Dietary Monitoring with Deep Learning and Computer Vision," 2025 International Conference on Computing Technologies Data Communication (ICCTDC), HASSAN, India, 2025, pp. 1-5, doi: 10.1109/IC- CTDC64446.2025.11158839.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

[37] A. Dhore, P. Dhore, P. Gangurde, A. Khadke, S. Singh and V. Bo- rate, "Face Morphing Attack Detection Using Deep Learning," 2025 International Conference on Computing Technologies Data Communication (ICCTDC), HASSAN, India, 2025, pp. 01-06, doi: 10.1109/IC- CTDC64446.2025.11158160.
[38] Y. Khalate, N. Khare, S. Kadam, S. Zurange, J. N. Mathur and Borate, "Custom Lightweight Encryption for Secure Storage using Blockchain," 2025 5th International Conference on Intelli- gent Technologies (CONIT), HUBBALI, India, 2025, pp. 1-5, doi: 10.1109/CONIT65521.2025.11166943.
[39] Y. K. Mali, S. Dargad, A. Dixit, N. Tiwari, S. Narkhede and A. Chaudhari, "The Utilization of Block-chain Innovation to Con- firm KYC Records," 2023 IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1-5, doi: 10.1109/ICCST59048.2023.10530513.
[40] Mahajan, Krishnal, Sumant Bhange, Prajakta Gade, and Yogesh Mali. "Guardian Shield: Real Time Transaction Security.".
[41] Y. K. Mali, S. A. Darekar, S. Sopal, M. Kale, V. Kshatriya and A. Palaskar, "Fault Detection of Underwater Cables by Using Robotic Operating System," 2023 IEEE International Carnahan Conference on Security Technology (ICCST), Pune, India, 2023, pp. 1-6, doi: 10.1109/ICCST59048.2023.10474270.
[42] Mali, Yogesh, Krishnal Mahajan, Sumant Bhange, and Prajakta Gade. "Guardian Shield: Real Time Transaction Security.".
[43] Bhoye, Tejaswini, Aishwarya Mane, Vandana Navale, Sangeeta Mohapatra, Pooja Mohbansi, and Vishal Borate. "A Role of Machine Learning Algorithms for Demand Based Netflix Recommendation System."
[44] Thube, Smita, Sonam Singh, Poonam Sadafal, Shweta Lilhare, Pooja Mohbansi, Vishal Borate, and Yogesh Mali. "Identifying New Species of Dogs Using Machine Learning Model.".
[45] Kale, Hrushikesh, Kartik Aswar, and Yogesh Mali Kisan Yadav. "Atten- dance Marking using Face Detection." International Journal of Advanced Research in Science, Communication and Technology : 417–424.
[46] Mali, Yogesh, and Viresh Chapte. "Grid based authentication system." International Journal 2, no. 10 (2014).
[47] N. Nadaf, G. Chendke, D. S. Thosar, R. D. Thosar, A. Chaudhari and Y. K. Mali, "Development and Evaluation of RF MEMS Switch Utiliz- ing Bimorph Actuator Technology for Enhanced Ohmic Performance," 2024 International Conference on Control, Computing, Communication and Materials (ICCCCM), Prayagraj, India, 2024, pp. 372-375, doi: 10.1109/ICCCCM61016.2024.11039926.
[48] Rojas, M., Mal´ı, Y. (2017). Programa de sensibilizacion´ sobre norma tecnica de salud N° 096 MINSA/DIGESA ´ V. 01 para la mejora del manejo de residuos solidos hos- ´ pitalarios en el Centro de Salud Palmira, IndependenciaHuaraz, 2017.
[49] Modi, S., Nalawade, S., Zurange, S., Mulani, U., Borate, V., Mali, Y. (2025). Python-Driven Mapping of Technological Proficiency with AI to Simplify Transfer Applications in Education. In: Saha, A.K., Sharma, H., Prasad, M., Chouhan, L., Chaudhary, N.K. (eds) Intelligent Vision and Computing. ICIVC 2024 2024. Studies in Smart Technologies. Springer, Singapore. https://doi.org/10.1007/978-981-96-4722-41
[50] Mulani, Umar, Vinod Ingale, Rais Mulla, Ankita Avthankar, Yo- gesh Mali, and Vishal Borate. "Optimizing Pest Classification in Oil Palm Agriculture using FineTuned GoogleNet Deep Learning Models." Grenze International Journal of Engineering Technology (GIJET) 11 (2025).
[51] D. Chaudhari, R. Dhaygude, U. Mulani, P. Rane, Y. Khalate and V. Borate, "Onion Crop Cultivation Prediction of Yields by Machine Learn- ing," 2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, 2024, pp. 244-249, doi: 10.1109/ICAICCIT64383.2024.10912135.
[52] Mali, Y. NilaySawant,"Smart Helmet for Coal Mining,". International Journal of Advanced Research in Science, Communication and Tech- nology (IJARSCT) Volume, 3.
[53] Mali, Y.K. Marathi sign language recognition methodology us- ing Canny's edge detection. Sadhan ¯ a 50, 268 ¯ (2025). https://doi.org/10.1007/s12046-025-02963-z.
[54] Y. Mali, M. E. Pawar, A. More, S. Shinde, V. Borate and R. Shirbhate, "Improved Pin Entry Method to Prevent Shoulder Surfing Attacks," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-6, doi: 10.1109/ICCCNT56998.2023.10306875.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, November 2025 Impact Factor: 7.67

[55] V. Borate, Y. Mali, V. Suryawanshi, S. Singh, V. Dhoke and A. Kulkarni, "IoT Based Self Alert Generating Coal Miner Safety Hel- mets," 2023 International Conference on Computational Intelligence, Networks and Security (ICCINS), Mylavaram, India, 2023, pp. 01-04, doi: 10.1109/ICCINS58907.2023.10450044.

[56] Y. K. Mali and A. Mohanpurkar, "Advanced pin entry method by resisting shoulder surfing attacks," 2015 International Conference on Information Processing (ICIP), Pune, India, 2015, pp. 37-42, doi: 10.1109/INFOP.2015.7489347.

[57] Mali, Y. NilaySawant,"Smart Helmet for Coal Mining,". International Journal of Advanced Research in Science, Communication and Tech- nology (IJARSCT) Volume, 3

[58] Mali, Y. (2023). TejalUpadhyay,". Fraud Detection in Online Content Mining Relies on the Random Forest Algorithm", SWB, 1(3), 13-20.

[59] Kohad, R., Khare, N., Kadam, S., Nidhi, Borate, V., Mali, Y. (2026). A Novel Approach for Identification of Information Defamation Using Sarcasm Features. In: Sharma, H., Chakravorty, A. (eds) Proceedings of International Conference on Information Technology and Intelligence. ICITI 2024. Lecture Notes in Networks and Systems, vol 1341. Springer, Singapore. https://doi.org/10.1007/978-981-96-5126-9_12.

[60] Amit Lokre, Sangram Thorat, Pranali Patil, Chetan Gadekar, Yogesh Mali, "Fake Image and Document Detection using Machine Learning," International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN: 2395-6011, Online ISSN: 2395-602X, Volume 5, Issue 8, pp. 104–109, November-December - 2020.