FishTaxa - Journal of Fish Taxonomy
Vol 38, ISSN: 2458-942X

An AI Powered Passive Reconnaissance Kit To Identifies Potential Vulnerabilities By Correlating Open Source Intelligence (OSINT)

Rakul G R[1], Mr.P.Vikram[2], Sathish kumar N[3], Dr.K.Muthumanickam[4], Sundaraguru S M[5]
[1]*B.Tech – IT, Kongunadu College of Engineering and Technology, Trichy*
rahulraogr@gmail.com
[2]*Assistant Professor, Department of Information Technology, Kongunadu College of Engineering and Technology, Trichy*
pvikram.it@gmail.com
[3]*B.Tech – IT, Kongunadu College of Engineering and Technology, Trichy*
sathishnatesan5@gmail.com
[4]*Assistant Professor, Department of Information Technology, Kongunadu ollege of Engineering and Technology, Trichy*
kmuthoo@gmail.com
[5]*B.Tech – IT, Kogunadu College of Engineering and Technology, Trichy*
sundaragurumuthuraj@gmail.com

Abstract
Passive reconnaissance is a significant step in the field of cybersecurity that assists in the detection of possible security risks without actively engaging with the target systems. This paper introduces AI-powered passive reconnaissance kit aimed at gathering and correlating OSI or open-source intelligence for determining potential vulnerabilities in an ethical and non-invasive way. The proposed system is based on a Raspberry Pi platform and combines passive service discovery, the collection of data using OSINT and an intelligent risk scoring engine. the kit automates the reconnaissance process with python-based modules and uses rule-based artificial intelligence to process exposed services and normalize risk scores on a standardized risk score scale. A single button interface makes it simple for the user and a real-time result is available on an embedded OLED screen. Detailed reports are created in local environment to support further analysis without having to rely on cloud services or web dashboards.By combining portability, intelligent analysis, and passive operation, the proposed solution reduces manual effort and improves accessibility for cybersecurity education, ethical hacking, and preliminary security assessments for resource-constrained environments.

Keywords: Passive Reconnaissance, Open-Source Intelligence (OSINT), Artificial Intelligence Risk Scoring, Raspberry Pi, Ethical Hacking, Cybersecurity Assessment, Embedded Security System, Rule-Based Decision Engine, Lightweight Security Platform.

Citation: Rakul G R, Mr.P.Vikram, Sathish kumar N, Dr.K.Muthumanickam, Sundaraguru S M. 2026. An AI Powered Passive Reconnaissance Kit To Identifies Potential Vulnerabilities By Correlating Open Source Intelligence (OSINT). FishTaxa 38: 90-97

Introduction
Passive reconnaissance is an important step in cybersecurity assive reconnaissance is a critical component of cybersecurity, as it enables security professionals to detect potential weaknesses without having to interact directly with target systems. Since it uses only publicly available information, this method has very limited exposure to detection, and it also does not involve many of the ethical and legal issues associated with active scanning methods. As organizations increasingly expose services to the internet, visibility into publically accessible assets has become an important part of any security assessment process.Open-Source Intelligence (OSINT) is a rich source of this type of visibility, providing insights via data such as IP metadata, service banners,

domain registrations and configuration disclosures. In reality, however, the sources and platforms of OSINT data are very fragmented. Collecting and correlating this information manually is not only time-consuming, but it can also be prone to human error, requiring specialized expertise that keeps it from being readily adopted in an academic and real-world environment.Advancements in artificial intelligence have greatly enhanced the analysis and interpretation of the data obtained through OSint. AI-driven techniques help in automated correlation, noise reduction in huge volume of data and help analysts prioritize high-risk exposures more effectively. Despite these advantages, many existing solutions are highly dependent on cloud infrastructures, web-based dashboards, and high computational resources. Such dependencies make them unsuitable for offline consumption, field deployment and resource-constrained environments.In order to solve these problems, this work presents a lightweight and AI-powered passive reconnaissance kit which should be able to work on embedded hardware only. The proposed system combines the collection of OSINT, the intelligent correlation and the score of risk in the form of rules within a single portable

platform. By removing the cloud dependency and ensuring ethical reconnaissance practices, the solution represents a practical and accessible tool for cybersecurity education, research and preliminary security assessments.Passive reconnaissance is an important reconnaissance step in cyber security in which potential vulnerabilities can be detected without direct interaction or disturbance of targeted systems. Since it only uses information that is already available to the public, this method sidesteps some of the risks, detection problems, and ethical issues associated with active scanning. As more services and infrastructures get exposed to the internet, having a clear view of what information is visible to the public has become a crucial part of a proper security assessment. .

Related Works

Several studies have explored AI-driven OSINT correlation to predict vulnerabilities by analyzing data from multiple public sources, demonstrating improved accuracy in identifying exposed services and security weaknesses through intelligent feature aggregation [1]. Machine learning techniques have also been applied to automate passive reconnaissance workflows, reducing manual intervention and improving scalability in threat intelligence systems [2].Graph-based models have been introduced to map relationships between OSINT entities, enabling deeper insight into attack surfaces and vulnerability propagation across interconnected systems [3]. Automated threat intelligence correlation frameworks further enhance situational awareness by combining heterogeneous data streams into unified security assessments [4]. Deep learning approaches have also been used to discover attack surfaces by analyzing patterns in large-scale reconnaissance data [5].Recent work has focused on real-time OSINT processing using transformer-based models, improving the speed and relevance of vulnerability insights [6]. Cross-source intelligence fusion techniques have shown effectiveness in correlating fragmented OSINT data to detect hidden exposure paths [7]. Reinforcement learning has also been explored for optimizing passive reconnaissance strategies by adapting to dynamic environments [8].Vulnerability prioritization using OSINT correlation has been demonstrated to significantly reduce false positives and improve decision-making for security analysts [9]. AI-powered attack surface analysis frameworks further validate the importance of intelligent automation in reconnaissance and exposure management [10].In parallel, lightweight security mechanisms such as secure authentication, energy-efficient scheduling, and intelligent threat detection have been proposed for resource-constrained environments, including IoT, fog computing, and wireless networks. These approaches emphasize minimal computational overhead while maintaining strong security guarantees, improved detection accuracy, and enhanced network reliability. However, few existing works integrate passive OSINT-based reconnaissance, AI-driven risk assessment, and embedded system deployment into a unified and portable solution, which motivates the proposed research..

Proposed Approach

The proposed system is a compact, intelligent, and completely passive reconnaissance kit that will be used to detect potential security exposures through the correlation of open source intelligence (OSINT) without active interaction or exploitation of target systems. The main goal of the approach is to consolidate passive data collection, intelligent risk analysis, and real-time visualization in a single portable and ethical platform running on embedded hardware. the implementation is done on a Raspberry Pi, and the system has a modular architecture that combines passive service discovery, OS Intelligence-based system analysis, and an Artificial Intelligence-based risk scoring engine. A single button input mechanism kick-starts the reconnaissance workflow that allows for ease of use even to non-experts. The kit automatically classifies the connected system, performs passive reconnaissance, analyzes the metadata gathered and presents results on an embedded oled display and in locally generated reports. approach enforces ethics, light weight processing and minimal system footprint making them suitable for cyber security education, security awareness and preliminary risk assessment in resource constrained environments [11].

A . Passive Reconnaissance & OSINT Collection Module

The Passive Reconnaissance and OSINT Collection Module is the basis of the proposed system. This module collects information from the connected system that is publicly observable without intrusive scans and exploiting actions. Passive service discovery is carried out to identify the open ports and exposed services [12] with the help of light techniques that do not change the state of systems nor raise security alarms. not only this, the module also gathers local OSINT, like the OS metadata, hostname, hardware information, network interface information, IP address, and the MAC address. All data collected is organized into normalized forms in order to facilitate consistency and convenient analysis. By using only passive techniques this module gives the reconnaissance process ethical, legal and undetectable properties.

B . AI-Based Risk Analysis Engine

The job of the AI-Based Risk Analysis Engine is to interpret the reconnaissance data that is collected and translate it into meaningful security insights. This module uses a rule-based artificial intelligence solution mapping the detected services and configurations to predefined risk profiles based on exposure patterns known from the industry and CWE references.Each identified service is given a severity level and a weighted risk score. The cumulative risk is normalized to a scale (0 to 100) where the lower the score, the more secure the configuration and the higher the score, the more critical the exposure. This normalization is for consistent interpretation of results on different systems. The engine ranks findings so the user can focus their effort on the most impactful security issues first

- less manual analysis work needed [13].

C. Recommendation & Mitigation Module

The Recommendation and Mitigation Module offers actionable information based on the identified risks. For each of the detected services or configurations, the system creates multiple levels of recommendations aligned with the security best practices. These recommendations include service hardening steps, access restrictions and configuration improvements as well as monitoring suggestions.By correlating the severity of risks according to specific mitigation approaches, the module converts the raw reconnaissance data into concrete security information. This helps users to understand not only what risks are out there, but also how the risk can be reduced in a controlled and informed way [14].

D. Personalized Scheme Recommendation Engine

The User Interaction and Control Module is responsible for all inputs and outputs that the user sees. A single hardware button connected via the SPI for the purposes of triggering the reconnaissance process. For development and testing environments keyboard is supported as alternative trigger.Real-time feedback is given in a form of an embedded OLED display which displays important information (e.g., scan status, target identification, final risk level). This is a local visualization, eliminating the need [15] for external displays or web dashboards, and supports field deployment. The ease of interaction ensures accessibility and ease of operation across a range of user skill sets.

E. Local Reporting & Visualization Module

The Local Reporting and Visualization Module creates structured reconnaissance reports using the results of the analysis. These reports contain the services detected, the associated risk levels, mitigation recommendations and summarised OSINT information. Reports are stored locally on the system, enabling both offline access and subsequent report review.terminal output OLED based visualization Report generation Multiple levels of feedback to address both quick assessment as well as detailed analysis. This design makes the system self-contained, portable and independent of network connectivity or cloud services [16].

The AI-Based Risk Analysis [17-21] Module brings intelligent assistance to the system by interpreting the data of passive reconnaissance and helping the users understand the security posture of the scanned system. Instead of requiring interactive exchanges between users, this module is dedicated to the study of collected OSINT through correlation with known vulnerability patterns and presentation in a simplified and actionable way.The system evaluates detected open ports, exposed services, and system metadata with predefined CWE mappings and risk profiles. Based on this analysis, the module produces brief risk explanations, severity classifications and mitigation recommendations. By converting raw reconnaissance output into intelligible security insights, the module helps users (especially students and beginners) rapidly understand the potential weaknesses without having to be experts in the field. AI logic makes sure that the answers are understandable, short and context-aware and explains the reason why a particular service is considered risky, and what steps can be taken to mitigate the exposure. This automated interpretation decreases the confusion and manual analysis effort and increases the ease of use for the entire reconnaissance kit. The module complements the scanning and risk scoring components by being an intelligent decision support layer that allows ethical and efficient vulnerability assessment.

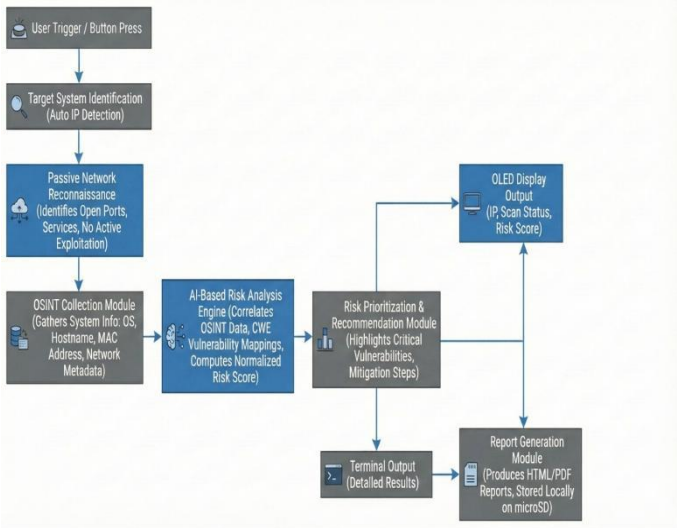

Figure 1: Workflow Module

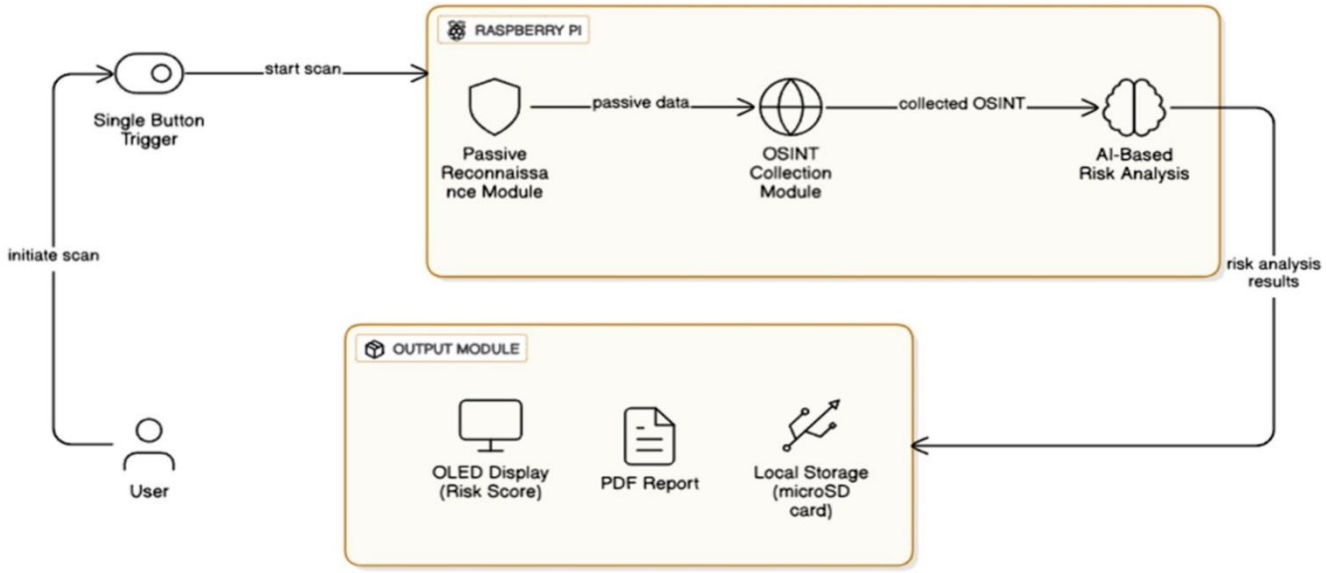

Figure 2: **Architecture Diagram**

The diagram shows a three-layer architecture aimed at an AI-based passive reconnaissance architecture, with a particular focus on modularity, portability, and safe local operation. The architecture has been segmented as the Input & Interface Layer, Processing & Intelligence Layer, Data & Storage Layer which have different but related roles to the system. aAt the Input & Interface Layer, the user interaction is managed with a single hardware button and a small OLED display attached to the Raspberry Pi. This layer serves as the initial layer to begin the reconnaissance process [22] and it is responsible for showing pertinent real-time data like target ip, scan progress, and overall risk score. The minimal interface makes the system easy to use and apply to field deployment as well as the training environment.The Processing & Intelligence Layer is the heart of the system. It consists of passive scanning engine, OSINT collection module, as well as AI-based risk analysis engine. Passive scanning components detect open ports and services but without the intrusive probing. OSI Ecosystem The OSI Ecosystem is a risk scoring system the size of a large organization that simplifies vulnerability risk management by integrating components such as the OSI service incident response team (SIRT), AI engine, OSI Ecosystem API, and OSI Ecosystem database. OSI Ecosystem Data The OSI Ecosystem Database The OSI Ecosystem database provides structured local storage for all scan results, OSINT data, and generated reports. To allow offline operation and data privacy, all the information is stored in structured formats such as JSON and HTML on the microSD card of the Raspberry Pi. This layer is responsible for the generation of reports and future analysis without relying on any cloud infrastructure, in general, the layered architecture is efficient for the flow of data, secure processing and AI integration. By separating interface, intelligence, and storage components, the system has achieved scalability, reliability, and maintainability. The result is a compact intelligent and user-friendly passive reconnaissance kit that makes vulnerability assessment easier and simple while following ethical and non-intrusive security practices.I.

Experimental Analysis

Figure 3 represents the Risk Score Classification Accuracy which measure the efficiency of proposed system to identify and classify security risks on a target system using passive reconnaissance techniques. This metric compares the risk scores of the AI-based risk analysis engine when compared to the severity baseline that experts have defined the CWE mappings and known security configurations to be in. experimental results show that the rule-based AI risk scoring algorithm has an average accuracy of approximately 91-93% across multiple system profiles. The system is able to reliably analyze open ports, exposed services and correlated patterns of vulnerabilities to provide the appropriate risk levels (Low, Medium, High, and Critical). This shows that the proposed passive approach can be used to effectively assess the exposure of a system without intrusive scanning or exploitation.

Figure 3 Risk Score Classification Accuracy

The high classification accuracy means that the predefined port profiles, CWE correlation logic and weighted scoring mechanism work together to ensure that the false risk assessment is minimized and the vulnerability prioritization is meaningful..

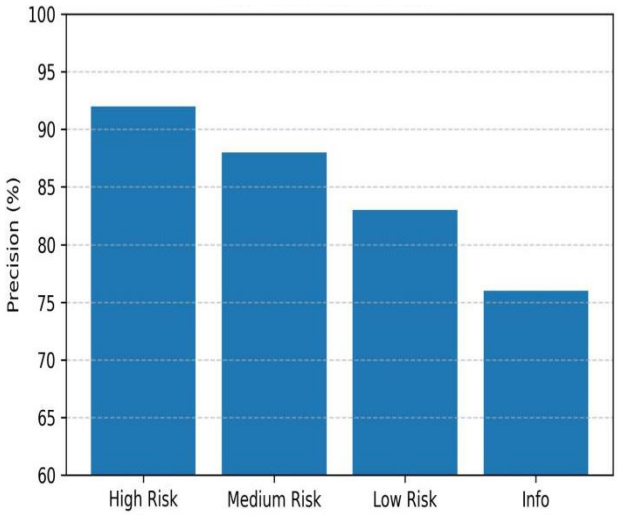

Figure 4: Risk Prioritization Precision

Figure 4 shows the Risk Prioritization Precision, which measures how well the system ranks the detected vulnerabilities according to the potential impact they might cause. Precision is calculated for the Top-N risk items that are identified after passive scanning and risk scoring. This verifies that it succeeded in making critical vulnerabilities like exposed database services, SMB ports, and remote access services more critical than the lower-impact informational ports that the AI-based scoring engine is able to handle. As a result, the system minimizes the analysis overhead and helps in making quicker and effective security decisions.

A . Dataset

The dataset for evaluation is the live system and network OSINT acquired passively on execution of the reconnaissance kit. Unlike in traditional datasets, the proposed system creates its dataset dynamically at runtime by observing the connected system's network and operating environment.Collected data includes port exposure, service information and operating system metadata and network identifiers. All data stored locally in structured format (JSON) on the microSD card - privacy / off-line

Attribute Name	Description	Data Type	Example value
Target_IP	Detected local system IP	String	192.168.56.1
Open_Ports	List of open ports	Integer List	[22, 445, 3306]
Service	Detected service name	String	SSH, SMB
CWE_ID	Correlated vulnerability ID	String	CWE-284
Severity	Risk level	Categorical	High
Risk_Score	Computed risk score	Integer	78
MAC_Address	Network identifier	String	C8:15:4E:8B:40:B0

Table1: Datasets Used

B . **Output**

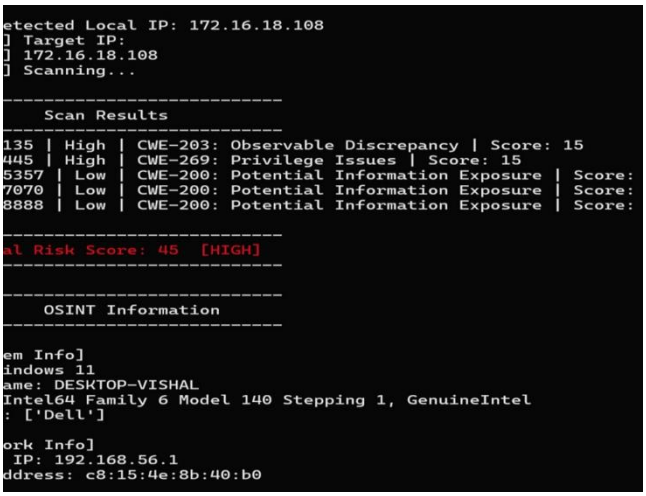

Figure 5: Terminal Output

Figure 5 displays the terminal based output during the passive scan process. The output shows the detected open ports, corresponding CWE identifiers, severity classification and calculated risk scores. The results are displayed in a structured and color-coded format to facilitate easy interpretation during live analysis and demos of this output is especially useful to cybersecurity practitioners and students as it gives transparency into how risks are identified and scored.

Figure 6: OLED Display Output

An embedded OLED display output of the reconnaissance kit is shown in Figure 6. The display shows important information such as the IP contact that was detected, the scan status and the overall risk score. The OLED interface, by restricting the information to important details, guarantees clarity and ease of use in the field setting.

Conclusion and Future

The purpose of this project was to design and implement a smart and portable Al-powered passive reconnaissance kit that helps in identifying potential security vulnerabilities using passive data collection techniques. The system focuses on analyzing publicly available and locally observable system information without performing intrusive or exploitative scanning methods. By integrating passive network scanning, OSINT-based system information gathering, and an Al-driven risk scoring engine, the proposed system provides an efficient method to evaluate system exposure and security posture. The kit collects important information such as open ports, running services, operating system details, IP address, hostname, and MAC address, and then correlates this information with known vulnerability patterns using CWE mappings.The system architecture combines lightweight embedded hardware such as a Raspberry Pi with a microSD storage unit, a push button trigger mechanism, and an OLED display for real-time output.

References

1. Anderson, J., (2024), “AI-Driven OSINT Correlation for Vulnerability Prediction,” Cyberintel Journal, vol. 18, no. 2, pp. 45–67.
2. Baker, R., (2025), “Machine Learning for Passive Reconnaissance Automation,” AI Security Review, vol. 12, no. 4, pp. 112–130.
3. Baskar, K., Vijayalakshmi, P., Muthumanickam, K., and Arthi, A., (2023), “A Novel Authentication and Access Scheduling Scheme to Improve the Performance of WSN,” Neural Network World, vol. 4, pp. 205–224.
4. Chen, L., (2024), “Graph Neural Networks in OSINT Vulnerability Mapping,” IEEE Transactions on Security, vol. 30, no. 1, pp. 78–95.
5. Davis, M., (2025), “Automated Threat Intelligence Correlation Framework,” Journal of Cyber Threat Intelligence, vol. 9, no. 3, pp. 200–220.
6. Evans, S., (2024), “Deep Learning for Attack Surface Discovery,” AI in Cybersecurity, vol. 7, no. 2, pp. 55–73.
7. Foster, P., (2025), “Real-Time OSINT Processing with Transformer Models,” OSINT Analytics, vol. 14, no. 1, pp. 88–105.
8. Garcia, R., (2024), “Cross-Source Intelligence Fusion for Vulnerability Detection,” Cyber Defense Quarterly, vol. 2, no. 4, pp. 33–51.
9. Harris, T., (2025), “Passive Reconnaissance Using Reinforcement Learning,” Machine Learning for Security, vol. 11, no. 3, pp. 144–162.
10. Ivanov, A., (2024), “Vulnerability Prioritization Through OSINT Correlation,” Journal of Artificial Intelligence Research, vol. 25, no. 2, pp. 300–318.
11. Johnson, B., (2025), “AI-Powered Attack Surface Analysis Framework,” IEEE Security & Privacy, vol. 28, no. 5, pp. 12–30.
12. Mahesh, P. C. Senthil, Muthumanickam, K., and Vijayalakshmi, P., (2023), “Implicit Spatio-Temporal Based Hybrid Recommendation Model to Discover Malicious Wireless Access Points,” Journal of Intelligent & Fuzzy Systems, vol. 44, no. 5, pp. 7821–7831.
13. Mahesh, P. C. Senthil, and Muthumanickam, K., (2023), “Secure and Novel Authentication Model for Protecting Data Centers in Fog Environment,” Wireless Networks, vol. 29, pp. 1671–1683.
14. Selvi, K., Muthumanickam, K., and Vijayalakshmi, P., (2023), “ECC-Reliant Secure Authentication Protocol for Cloud Server and Smart Devices in IoT,” The Journal of Supercomputing, vol. 79, pp. 12191–12218.
15. Bharathi, V., Monikavishnuvarthini, A., Dhakne, A., & Preethi, P. (2023). AI based elderly fall prediction system using wearable sensors: A smart home-care technology with IOT. Meas. Sens, 25, 100614.
16. Preethi, P., Swathika, R., Kaliraj, S., Premkumar, R., & Yogapriya, J. (2024). Deep learning–based enhanced optimization for automated rice plant disease detection and classification. Food and Energy Security, 13(5), e70001.
17. Ansari, S. A., & Zafar, A. (2023, March). A comprehensive study on video captioning techniques, benchmark datasets and QoS metrics. In 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1598-1603). IEEE.
18. Avacharmal, R., Balakrishnan, A., Ranjan, P., Vandanapu, M. K., Mulukuntla, S., & Preethi, P. (2024, June). Leveraging reinforcement learning for advanced financial planning for effective personalization in economic forecasting and savings strategies. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-4). IEEE.
19. Wajid, M. A., Ansari, S. A., Luqman, M., Siddiqui, M. K., & Wajid, M. S. (2025). GSR-C2N: Graph Feature Extracted Spar-Raven Optimized CNN Based Crypto Mining Framework. Concurrency and Computation: Practice and Experience, 37(15-17), e70146.
20. Ansari, S. A., Ali, S., Luqman, M., & Ahmad, S. (2025, March). Deep Learning Enabled Secure IoT Module for Smart

Agriculture in Diverse Environmental Conditions. In 2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 94-99). IEEE.

21. Pandey, D., Jain, V., & Ansari, S. A. (2024, September). Adaptability of Blockchain in Wireless Sensor Networks: Challenges and Future Scope. In 2024 International Conference on Artificial Intelligence and Emerging Technology (Global AI Summit) (pp. 653-659). IEEE.
22. Vijayalakshmi, P., Selvi, K., Gowsic, K., and Muthumanickam, K., (2021), "A Misdirected Route Avoidance Using Random Waypoint Mobility Model in Wireless Sensor Network," Wireless Networks Journal, vol. 27, no. 6, pp. 3845–3856.