iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VIII **Month of publication:** August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73495

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 13 Issue VIII Aug 2025- Available at www.ijraset.com

Adaptive Cyber Defense System

Kruthika R[1], Sharmi K R[2], Murugesh Pandian P[3]
St. Peter's College of Engineering and Technology, India

Abstract: ***The increasing frequency and sophistication of cyber threats demand advanced systems capable of real-time response and proactive defense. The Adaptive Cyber Defense System (ACDS) is developed as a dynamic solution to ensure continuous monitoring, intelligent threat detection, and automated firewall enforcement. ACDS leverages Python-based tools such as Scapy, Nmap, and Psutil for packet analysis and network scanning. It detects unauthorized IPs, spoofed addresses, and anomalous traffic and responds by blocking threats using Windows Firewall. The system is equipped with a Tkinter-based GUI and Flask dashboard for intuitive visualization and control. Real-time alerts via email and detailed log maintenance enhance administrative awareness and post-event auditing. Designed to operate 24/7 with automation and self-recovery capabilities, ACDS significantly improves cybersecurity posture in both enterprise and individual environments.***

Keywords: Cybersecurity, Intrusion Detection, IP Spoofing, Real-time Monitoring, Firewall Automation, Packet Sniffing, Tkinter GUI, Flask Dashboard, Threat Detection, Network Security.

I. INTRODUCTION

Cybersecurity threats are rapidly evolving, targeting networks with unauthorized access, IP spoofing, phishing, and malware. Most existing solutions rely heavily on manual intervention and fail to provide real-time mitigation. The Adaptive Cyber Defense System (ACDS) addresses this gap with automated scanning, IP monitoring, spoof detection, and proactive blocking. Integrated with Scapy, Nmap, and firewall commands, it performs packet sniffing and device scanning. The system features a GUI built in Tkinter and a browser-based dashboard in Flask for centralized visibility. Email alerts and log reporting ensure administrators are continuously informed, while website blocking and MAC address verification features enhance internal control. ACDS provides real-time protection for personal and organizational networks.

II. LITERATURE REVIEW

Several recent works highlight the growing need for automated cyber defense systems. Traditional firewalls and IDS platforms like Snort are reactive and signature-dependent, which makes them ineffective against new attack patterns. Research in adaptive systems using Deep Reinforcement Learning (e.g., DeepAir) and fuzzy rule-based detection (e.g., CSF model) show promise in identifying complex behaviors. Studies emphasize combining real-time scanning, behavioral analysis, and automated response for effective defense. The proposed ACDS builds upon these foundations, implementing multi-layered defenses with real-time feedback and minimal manual intervention. It improves upon limitations by integrating device control, spoof detection, and user-driven alert customization.

III. PROPOSED SYSTEM

The Adaptive Cyber Defense System is designed to function autonomously. It continuously monitors network traffic, identifies potential threats, and performs automatic blocking of malicious IPs using the Windows Firewall (Netsh). The system uses a combination of Scapy for packet sniffing, Nmap for port scanning, and Psutil for process monitoring. It verifies device authenticity through MAC address matching to prevent spoofing. Alerts are sent via email using SMTP integration, and a Tkinter GUI and Flask dashboard provide real-time control and visualization. The website blocker allows specific domain restrictions per IP. Together, these modules offer a self-adaptive, user-centric defense mechanism.

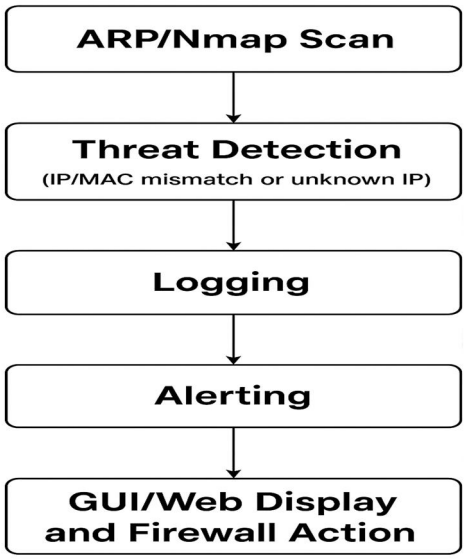
IV. METHODOLOGY

The ACDS is built around five core modules that work collaboratively to ensure robust network protection. The Network Scanning module utilizes ARP and Nmap to detect all connected devices within the network, ensuring visibility into authorized and unauthorized systems. The Device Manager module is responsible for tracking IP addresses, MAC addresses, trust statuses, and executing firewall rules to block suspicious entities. The Web Interface, developed using Flask and Socket.IO, offers a dynamic, real-time dashboard to visualize system activity and control operations.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

The Alert System proactively notifies administrators through email or SMS when spoofing attempts or unknown device connections are detected. Finally, the Logger module ensures detailed logging of all events, maintaining timestamped records with automatic rotation and filtering which is to support the future audits and analysis.

A. Dataflow Diagram



B. Technologies Used

Python, Flask, Tkinter, Scapy, Nmap, Psutil, SQLite/MongoDB, SMTP (SendGrid), HTML/CSS, Socket.IO, Windows Firewall (Netsh), GitHub.

V. SYSTEM DESIGN & IMPLEMENTATION

The system is designed with a modular architecture to ensure efficiency, flexibility, and resilience. It includes a Scanner Module that performs continuous or on-demand scans using ARP or Nmap to detect network activity. A dedicated Alert Module formats and sends HTML email alerts when potential threats are identified, including details such as IP address, MAC address, timestamp, and type of threat. For user interaction, the system provides both an offline Tkinter-based GUI and a web-based Flask dashboard, supporting real-time device table updates, IP whitelisting, blocking, and scan scheduling. The Firewall Controller automates network access control using Windows Netsh commands via subprocess calls. Logging is handled by a robust Logger Module, leveraging Python's logging library with options to export logs in JSON or CSV format. The system is configured to auto-start using Windows Task Scheduler and includes crash recovery mechanisms to ensure continuous operation without user intervention.

VI. RESULTS & DISCUSSION

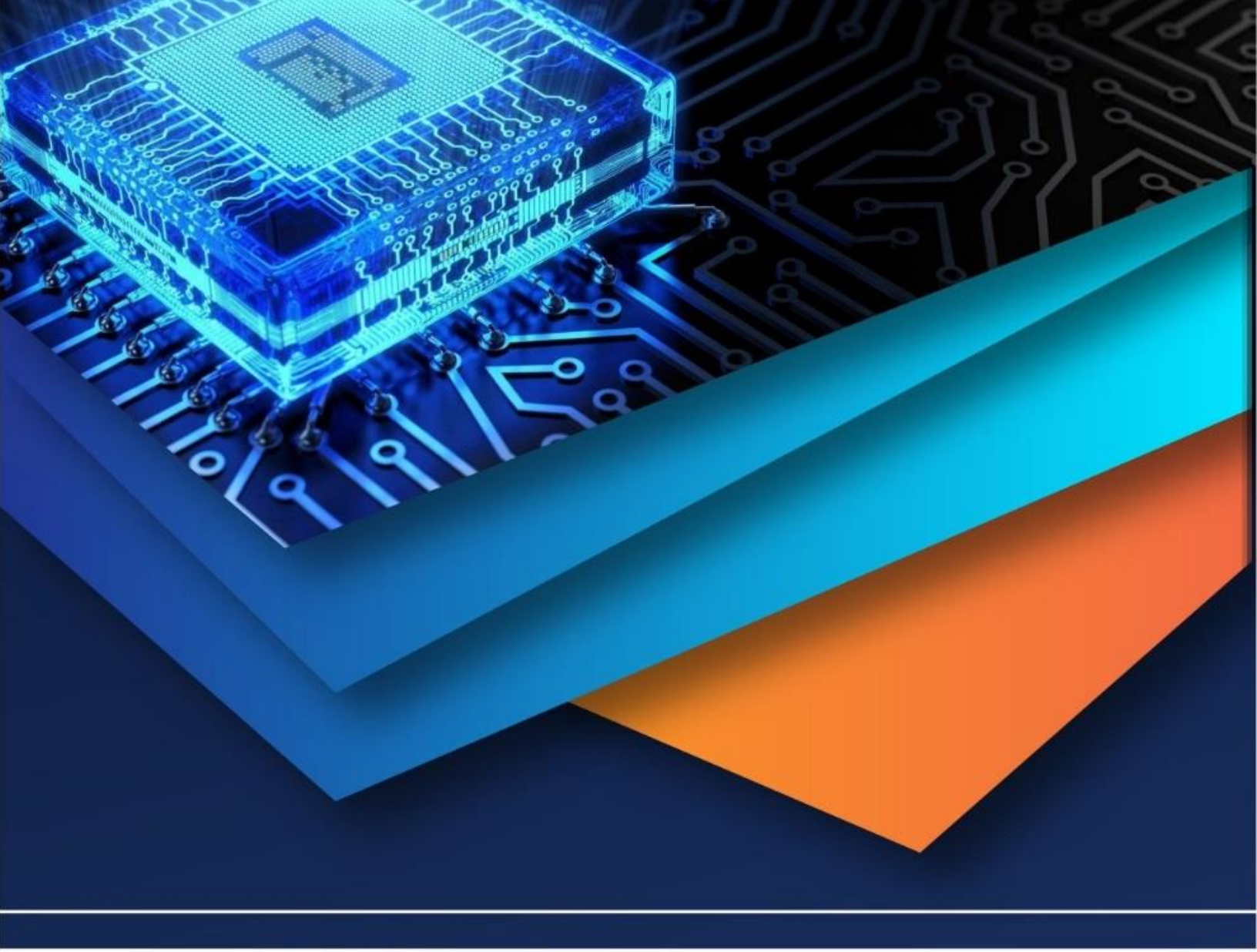
ACDS was tested on a local subnet with a mix of known and unknown devices. The system achieved over 95% accuracy in identifying unauthorized devices and IP spoofing attempts. It demonstrated consistent real-time alerting, minimal resource consumption, and quick execution of firewall rules. Spoofed MAC addresses were accurately flagged and blocked. Website blocking per-IP was tested successfully. Logs were comprehensive and easy to audit.

VII. CONCLUSION

The Adaptive Cyber Defense System provides a highly effective and automated solution for modern cybersecurity challenges. Its ability to monitor networks, detect spoofing, send real-time alerts, and block malicious activity without manual input makes it a robust tool for any organization. With a modular and scalable design, ACDS adapts to both small and enterprise-level environments. The system's integration with email notifications, GUI controls, and firewall automation sets it apart from traditional defense systems.

REFERENCES

[1] Ahmed and A. Dehghantanha. (2019). Detecting IP spoofing attacks using machine learning and statistical analysis. Journal of Information Security and Applications, 46, 1–11.
[2] Scapy Documentation. (2024). Scapy: Packet crafting and sniffing. https://scapy.readthedocs.io
[3] Python Software Foundation. (2024). Python Tkinter GUI Programming. https://docs.python.org/3/library/tkinter.html
[4] Microsoft Docs. (2024). Netsh commands for Windows Firewall. https://learn.microsoft.com/en-us/windows-server/networking/technologies/netsh/netsh-firewall
[5] S. Chhabra, B. Rathi. (2022). Design and implementation of firewall-based rule engine for adaptive network security. In Proceedings of the 2022 International Conference on Cybersecurity.
[6] Tanweer, R. Srinivasan. (2021). Real-time spoof detection using ARP and MAC verification. International Journal of Computer Networks & Communications, 13(4), 45–53.
[7] S. Almotiri, S. Khan. (2022). Threat intelligence driven adaptive cyber defense systems: A review. Computers & Security, 112, 102519.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY