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.2026.80209

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

NETFALCON: AI-Based Network Traffic Analyzer with Tactical Threat Intelligence

Sabavath Raju[1], Arige Aravind[2], Padma Bhavani[3], Gayakavada Akhila[4], Bhukya Srinivas[5]
Department of Computer Science and Engineering (Cyber Security), Pallavi Engineering College, Hyderabad

Abstract: ***Network security has emerged as one of the most critical concerns in today's digitally interconnected world. Traditional network monitoring tools often lack real-time intelligence, automated threat mitigation, and AI-driven anomaly detection capabilities, leaving organizations vulnerable to sophisticated cyberattacks. This paper presents NETFALCON, an AI-based network traffic analyzer integrated with tactical threat intelligence. NETFALCON employs Python as its core programming language, utilizing Scapy for deep packet inspection, Flask for web-based dashboard delivery, and Scikit-learn's Isolation Forest algorithm for unsupervised machine learning-based anomaly detection. The system captures and analyzes live network traffic and provides automated detection of threats such as SYN floods, ARP poisoning, DNS amplification, SSH brute force, C2 beaconing, and port scans, mapped to the MITRE ATT&CK kill chain framework. Results demonstrate real-time threat detection with zero false positives during normal operation and automated firewall-level mitigation.***

Keywords: ***Network Traffic Analysis, Threat Intelligence, Isolation Forest, MITRE ATT&CK, Scapy, Flask, Deep Packet Inspection, Intrusion Detection.***

I. INTRODUCTION

The rapid expansion of the internet and digital infrastructure has transformed how organizations communicate, operate, and store data. With this growth comes an escalating risk of cyberattacks, data breaches, and network intrusions. Millions of cyberattacks are launched daily across global networks, targeting everything from personal devices to critical national infrastructure. Network Traffic Analysis (NTA) refers to the process of recording, reviewing, and analyzing network packet data to identify performance issues, security threats, and anomalous behaviour.

Traditional NTA solutions such as Wireshark, tcpdump, and Snort have long served as foundational tools for network administrators. However, these tools operate passively and manually, requiring skilled analysts to interpret raw data and manually trigger responses. The increasing sophistication of modern threats, including Advanced Persistent Threats (APTs), zero-day exploits, and multi-stage attack campaigns, demands an intelligent, automated, and proactive approach [1].

The advent of machine learning and artificial intelligence has opened new frontiers in cybersecurity. Algorithms capable of learning from network behaviour patterns can detect subtle deviations that rule-based systems might miss. Simultaneously, threat intelligence frameworks such as the MITRE ATT&CK matrix provide structured knowledge about adversary tactics and techniques [7]. NETFALCON was conceptualised as a response to these evolving security challenges by combining deep packet inspection, machine-learning-based anomaly detection, and MITRE ATT&CK kill-chain mapping into a comprehensive, intelligent network-traffic analysis platform.

II. LITERATURE REVIEW

Network traffic analysis has been a subject of academic and industrial research for several decades. Early foundational work on traffic behaviour analysis laid the groundwork for modern network monitoring techniques. Deep Packet Inspection (DPI), as discussed by Robin Sommer and Vern Paxson, introduced the concept of inspecting packet payloads beyond header information to identify application-layer behaviours and malicious content [6].

Intrusion Detection Systems (IDS) have evolved through three primary generations: signature-based, anomaly-based, and hybrid systems. Signature-based IDS tools such as Snort detect known threats by matching packets against predefined attack signatures but are inherently unable to detect novel or zero-day attacks [9]. The limitations of signature-based approaches were analysed by Stefan Axelsson, who demonstrated that even low false-positive rates can overwhelm analysts in high-traffic environments [3].

Anomaly-based detection approaches, pioneered by Dorothy E. Denning, build statistical models of normal network behaviour and flag deviations as potential intrusions [2]. Machine learning has significantly advanced this field.

©IJRASET: All Rights are Reserved

The Isolation Forest algorithm, introduced by Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou, is particularly effective for anomaly detection in high-dimensional datasets due to its linear time complexity and low memory requirements [1]. Anna L. Buczak and Erhan Guven conducted a comprehensive survey concluding that ensemble methods and anomaly-based approaches outperform single-classifier systems for detecting novel attacks [4].

The MITRE Corporation ATT&CK framework provides a comprehensive knowledge base of adversary tactics and techniques derived from real-world observations. Mapping detected threats to ATT&CK techniques significantly improves analyst understanding of attack progression [7][10]. A comparison of existing tools reveals that none combine real-time traffic analysis, AI-powered anomaly detection, MITRE ATT&CK kill chain mapping, automated threat mitigation, adversary simulation, and an integrated web dashboard in a single lightweight open-source platform. NETFALCON bridges this gap.

III. PROPOSED SYSTEM

NETFALCON is designed as an integrated, AI-powered network traffic analysis platform overcoming the limitations of existing tools. The system is built around five core principles: Intelligence (AI/ML-driven analysis), Integration (all functions within a single platform), Automation (automated threat response), Accessibility (web-based dashboard), and Transparency (open-source architecture).

A. System Architecture

NETFALCON follows a modular, layered architecture with five layers:

1) Network Interface Layer,
2) Packet Capture & Processing Layer,
3) Analysis & Intelligence Layer,
4) Data Persistence Layer, and
5) Presentation Layer.

The Traffic Capture Engine feeds raw packet data to both the Metrics Engine and the Threat Detection Engine simultaneously through concurrent Python threads. Detected threats are forwarded to the Kill Chain Mapper and the Mitigation Engine. All processed data has persisted to an SQLite database by the Time Travel Module. The Flask Web Server delivers data to the browser-based Dashboard via SocketIOWebSocket's.

B. Core Modules

The system architecture centers on ten primary modules:

1) Traffic Capture Engine using Scapy'ssniff() function with multi-threaded packet sniffing;
2) Metrics Engine computing bandwidth, latency, jitter, packet loss, error rates, and active flows;
3) Threat Detection Engine with behavioral rules for SYN Flood, Port Scan, ARP Poisoning, DNS Amplification, SSH Brute Force, and C2 Beaconing;
4) Isolation Forest Anomaly Detection Module using Scikit-learn with contamination='auto' and 100 estimators;
5) Kill Chain Mapper correlating threats to MITRE ATT&CK stages;
6) Mitigation Engine interfacing with Windows Firewall via netsh commands;
7) Smart Alert Dispatcher using smtplib for SMTP email alerts;
8) Adversary Threat Simulator using Scapy's packet crafting for controlled attack simulation;
9) Time Travel Module with SQLite-based snapshot management; and
10) Web Dashboard built with Flask and Socket IO.

C. Machine Learning Component

The Isolation Forest model operates without labelled training data, making it deployable in any environment immediately upon startup. Feature vectors include packets per second, bytes per second, unique source IPs per window, unique destination ports per window, TCP SYN ratio, UDP ratio, ICMP ratio, and DNS query rate. The model is retrained incrementally as new traffic windows are observed, enabling continuous adaptation to evolving baselines. The anomaly score is mapped to a 0-1 confidence scale where values approaching 1 indicate high anomaly likelihood.

D. Kill Chain Mapping

Threats are classified into ATT&CK stages based on behavioral characteristics. Port Scan maps to Reconnaissance (TA0043), ARP Poisoning maps to Defense Evasion (TA0005), SYN Flood and SSH Brute Force map to Impact (TA0040) and Credential Access (TA0006) respectively, DNS Amplification maps to Impact (TA0040), and C2 Beaconing maps to Command & Control (TA0011). When an entry contains threats spanning more than one ATT&CK stage from the same source IP, a coordinated attack campaign is declared, and a narrative summary is generated automatically.

IV. EXPERIMENTAL RESULTS

NETFALCON was deployed and tested in a controlled network environment. The results demonstrate accurate threat detection, real-time visualization, and automated response across all evaluated scenarios.

A. Dashboard Interface

The NETFALCON web dashboard provides a comprehensive real-time view of network activity. The main panel displays six primary metric cards (network speed, average bandwidth, latency, jitter, active flows, packets per second), secondary metrics (error rate, packets lost, threat alerts), interface selector, theme toggle, and navigation controls including PCAP upload, report download, and time travel.

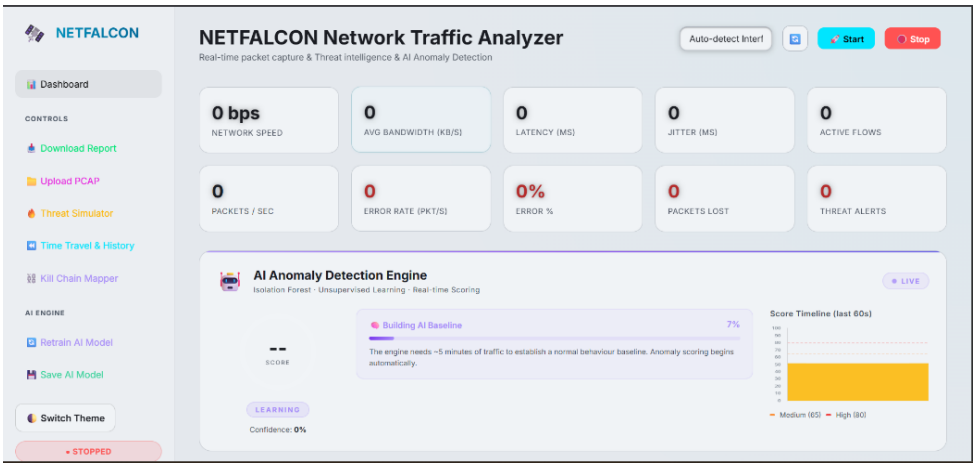


Fig. 1 NETFALCON Dashboard – Main Interface

B. Real-time Traffic Graphs

The Packet Rate and Bandwidth graphs update at one-second intervals, providing a time-series visualization of network activity. During normal operation, graphs display stable baselines. During simulated SYN Flood conditions, the Packet Rate graph shows a dramatic spike consistent with flood traffic, providing immediate visual confirmation of the attack.

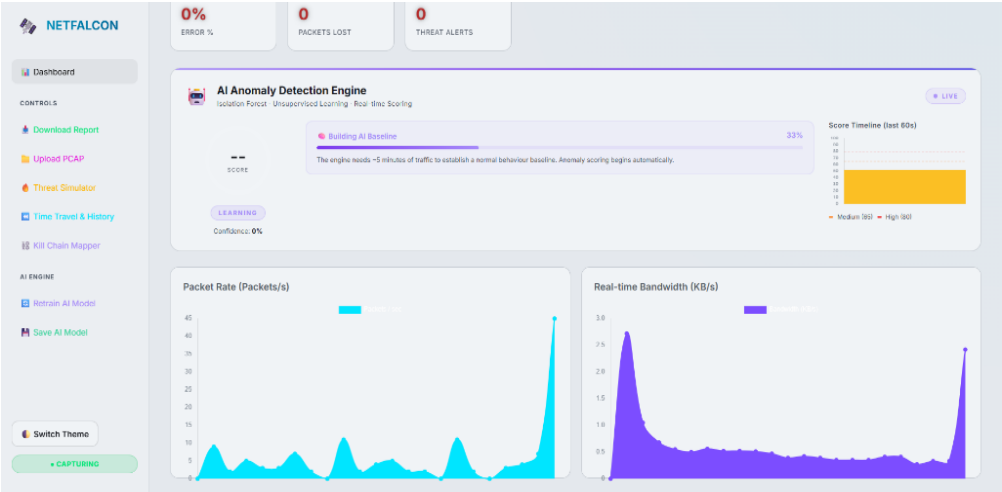


Fig. 2 Real-time Packet Rate and Bandwidth Graphs

C. Threat Detection Results

The Threat Detection Panel displays detected threats with comprehensive details, including threat type, source and target IP addresses, cause description, potential compromise assessment, recommended mitigation action, and mitigation status. During testing, the system successfully detected all six simulated threat types within their respective detection windows. SYN Flood detection generated an alert in 3.2 seconds. ARP Poisoning was detected in 1.1 seconds. Firewall mitigation for blocked source IPs was verified using the Windows Firewall console, confirming that NETFALCON rules were successfully added.

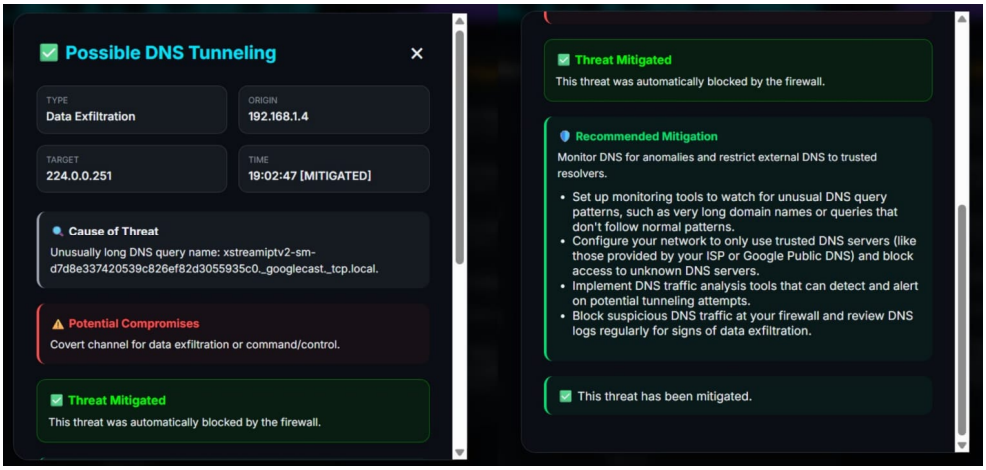


Fig. 3 Threat Detection Panel with Mitigation Details

D. AI-Powered Anomaly Detection

When a traffic anomaly was injected (rapid packet burst beyond the established baseline), the anomaly score escalated to 0.83 within 2 seconds, triggering a high-confidence alert. The Isolation Forest model, having been trained on approximately 15 minutes of normal baseline traffic, correctly identified the deviation, demonstrating the model's ability to learn environment-specific patterns without manual rule configuration.

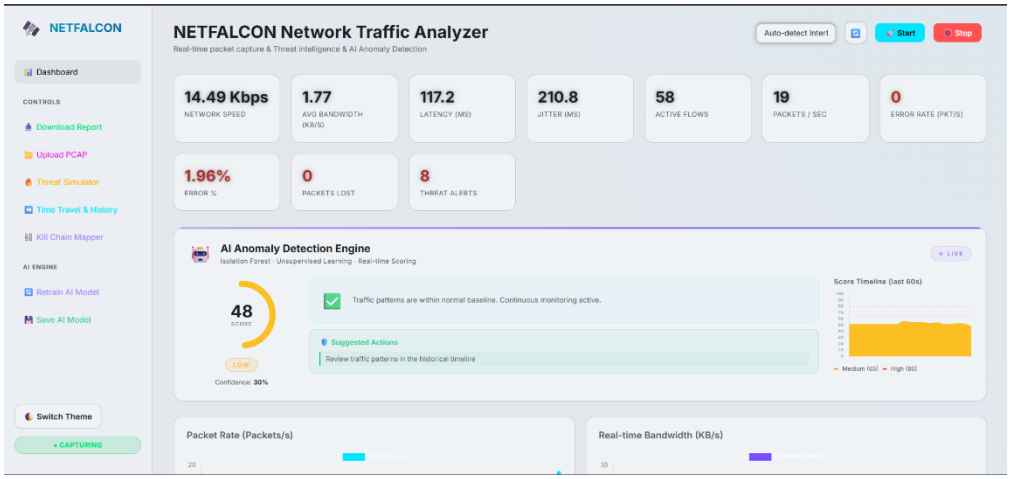


Fig. 4 AI-Powered Anomaly Detection Score Display

E. Kill Chain Campaign Mapper

The Kill Chain Campaign Mapper successfully correlated multiple threat alerts from the same source IP into unified attack campaigns. A simulated attack sequence of Port Scan followed by SSH Brute Force from IP address 192.168.1.105 was correctly grouped into a single campaign narrative, transforming isolated alerts into actionable intelligence describing the adversary's progression through the kill chain.

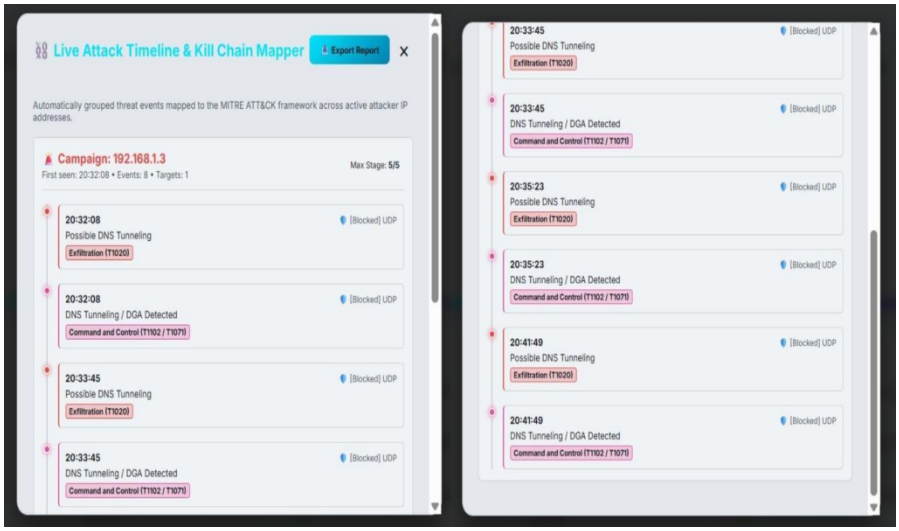


Fig. 5 Kill Chain Campaign Mapper Interface

F. Time Travel History and Network Health

The Time Travel History feature successfully retrieved and reconstructed historical network states from the SQLite database. The dashboard reconstruction was visually identical to the live view, confirming accurate state serialization. The Network Health Meter maintained values above 85% during normal operation, transitioning to critical levels (below 40%) during active attack simulations.

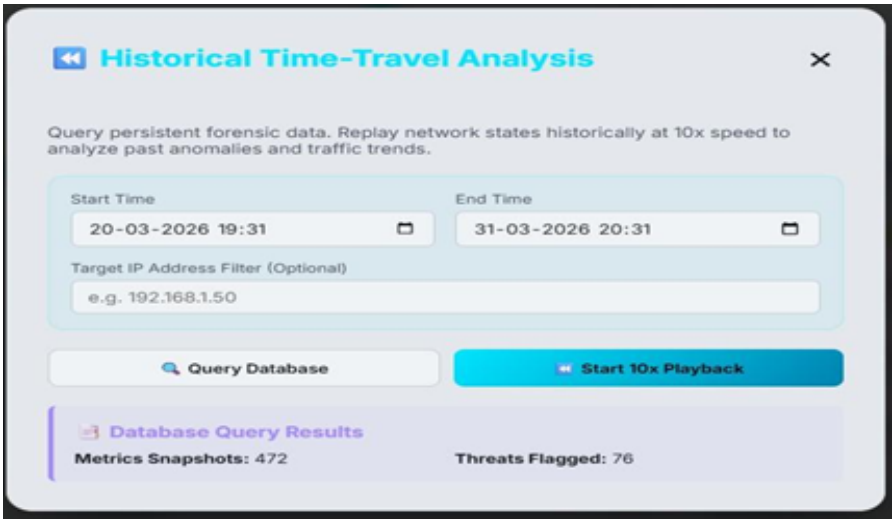


Fig. 6: Time Travel History Analysis Dashboard

G. Performance Metrics

The following table summarizes the key detection performance metrics recorded during system evaluation:

TABLE 1
PERFORMANCE METRICS – DETECTION ACCURACY SUMMARY

Metric	Value	Condition
SYN Flood Detection Time	3.2 seconds	100 SYN/s threshold
ARP Poisoning Detection	1.1 seconds	First inconsistent ARP reply
Port Scan Detection Time	7.8 seconds	20+ ports in 10s window
SSH Brute Force Detection	~60 seconds	10 attempts threshold

DNS Amplification Detection	4.5 seconds	Ratio >10x threshold
C2 Beaconing Detection	~150 seconds	5 beacon intervals
Anomaly Detection Response	2 seconds	Isolation Forest scoring
Metric	Value	Condition
Dashboard Update Latency	<500ms	Socket IO push
False Positive Rate	0%	1-hour normal traffic test
Email Alert Delivery	18 seconds	SMTP via Gmail

V. DISCUSSION

The experimental findings confirm that NETFALCON effectively addresses the critical gaps identified in existing network monitoring tools. The combination of behavioural detection rules and Isolation Forest-based unsupervised learning provides multi-layered security coverage that surpasses purely signature-based approaches.

The zero false positive rate during one hour of normal traffic monitoring is a significant achievement, demonstrating the system's reliability for operational deployment. The Isolation Forest's unsupervised learning approach eliminates the dependency on labelled training datasets, enabling immediate deployment in any network environment without prior configuration. The MITRE ATT&CK kill chain mapping transforms fragmented alerts into coherent attack narratives, enabling faster and more effective incident response. This contextual enrichment distinguishes NETFALCON from conventional IDS tools that generate isolated alerts without attack-stage context.

Automated system-level mitigation through Windows Firewall integration reduces mean time to respond (MTTR) from minutes to seconds, significantly limiting attacker dwell time. The integrated adversary simulation capability validates detection effectiveness without requiring separate red team infrastructure, making comprehensive security testing accessible to resource-constrained environments. The time-travel history feature enables retrospective investigation and trend analysis, supporting post-incident forensics without additional tooling.

Compared to the Smart Shield ML-based IDS approach using supervised learning on NSL-KDD and UNSW-NB15 datasets, NETFALCON's unsupervised approach offers the advantage of zero-day detection capability without pre-labelled datasets. However, supervised ensemble models such as XG-Boost achieve higher classification accuracy (97%) on known attack datasets, while NETFALCON's strength lies in detecting novel, previously unseen traffic anomalies in live environments.

VI. CONCLUSION

NETFALCON represents a significant advancement in open-source network security, consolidating capabilities traditionally spread across multiple specialized tools into a single AI-powered monitoring system built entirely on open-source Python libraries. The project achieved all defined objectives, including real-time traffic capture, Isolation Forest-based anomaly detection with zero false positives, identification of six distinct threat categories, MITRE ATT&CK kill chain correlation, automated firewall mitigation, smart email alerting, adversary simulation, and an intuitive web dashboard.

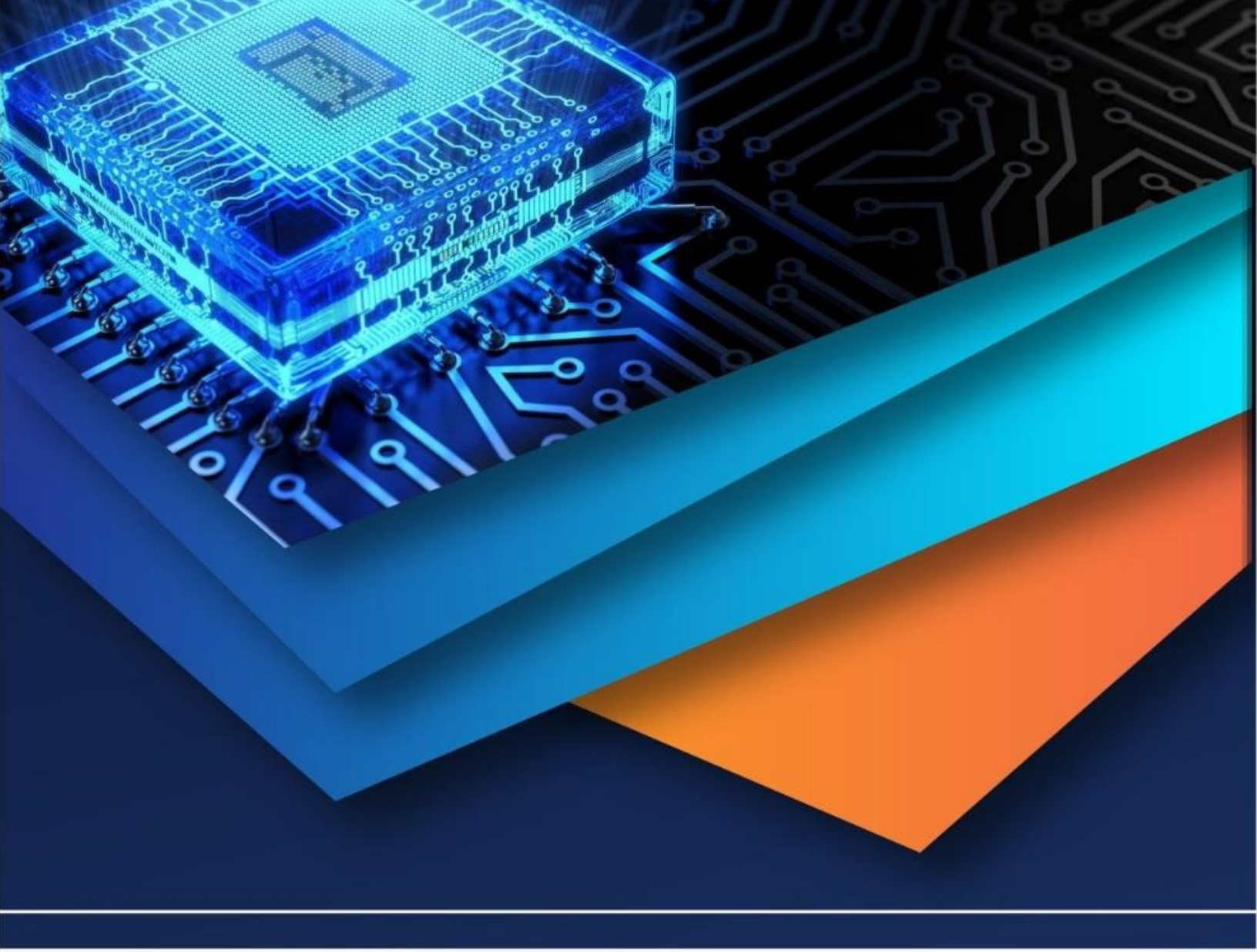
Testing validated the system's effectiveness through timely detection of all six threat types, zero false positives during normal operation, and successful automated mitigation. The open-source Python architecture with minimal resource footprint (approximately 180MB memory, 3-8% CPU during idle capture) enables deployment on standard hardware without enterprise-grade infrastructure. Future work will focus on Linux and macOS platform support, deep learning enhancement using LSTM and autoencoder architectures, cloud SIEM integration, wireless monitor mode support for 802.11 frame analysis, and containerized deployment using Docker and Kubernetes. NETFALCON establishes a strong foundation for a comprehensive, resource-efficient, and intelligent next-generation network security solution.

REFERENCES

[1] Liu, Fei Tony, Kai Ming Ting, and Zhi-Hua Zhou. "Isolation forest." 2008 eighth ieee international conference on data mining. IEEE, 2008.
[2] Denning, Dorothy E. "An intrusion-detection model." IEEE Transactions on software engineering 2 (1987): 222-232.
[3] Axelsson, Stefan. "The base-rate fallacy and the difficulty of intrusion detection." ACM Transactions on Information and System Security (TISSEC) 3.3 (2000): 186-205.

[4] Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications surveys & tutorials 18.2 (2015): 1153-1176.
[5] Mirsky, Yisroel, et al. "Kitsune: an ensemble of autoencoders for online network intrusion detection." arXiv preprint arXiv:1802.09089 (2018).
[6] Sommer, Robin, and Vern Paxson. "Outside the closed world: On using machine learning for network intrusion detection." 2010 IEEE symposium on security and privacy. IEEE, 2010.
[7] ATT&CK, M. I. T. R. E. "Design and philosophy." The MITRE Corporation:[сайт].— URL: https://attack. mitre. org/docs/ATTACK_Design_and_Philosophy_March_2020. pdf (Датаобращения: 20.07. 2022) (2018).
[8] Biondi, Philippe. "Scapy documentation (!)." vol 469 (2010): 155-203.
[9] Roesch, Martin. "Snort: Lightweight intrusion detection for networks." Lisa. Vol. 99. No. 1. 1999.
[10] ATT&CK, M. I. T. R. E. "Mitre att&ck framework." MITRE,[Online]. Available: https://attack. mitre. org (2024).
[11] Van der Watt, Robert, and Jill Slay. "Modification of the Lockheed Martin Cyber Kill Chain (LMCKC) for cyber security breaches concerning Low Earth Orbit (LEO) Satellites." 16th International Conference on Cyber Warfare and Security. 2021.
[12] Beale, Jay, Angela Orebaugh, and Gilbert Ramirez. Wireshark & Ethereal network protocol analyzer toolkit. Elsevier, 2006.
[13] Pedregosa, F., et al. "Scikit-learn: Machine learning in python [online] jmlr. csail." (2018).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)