iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** X **Month of publication:** October 2025

DOI: https://doi.org/10.22214/ijraset.2025.74795

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 X Oct 2025- Available at www.ijraset.com

NetRaptor - Lawful Network Intelligence Tool

Dr. Radha Pimpale[1], Aryan Dekate[2], Aryan Wankhade[3], Shital Ghagre[4], SSpandan Chavan[5], Yash Atkari[6]
[1]*Associate Professor,* [2, 3, 4, 5, 6]*UG Students, Department of Information Technology Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India*

Abstract: ***"NetRaptor" is a lawful network intelligence tool designed to help law enforcement and cybersecurity teams combat scam and ransomware operations. The tool focuses on proactive threat detection by monitoring network activity and system behaviour to identify threats before significant damage occurs. NetRaptor stealthily collects digital evidence, such as keystrokes, files, and network data, while ensuring all actions are legally authorized and the evidence's integrity is preserved for court use. It securely transmits this data to a real-time dashboard for analysis, mapping the attacker's infrastructure to help dismantle their networks. The project's goal is to provide an effective, legally compliant solution for investigating and stopping cybercrime.***

I. INTRODUCTION

NetRaptor is a lawful network intelligence tool created to assist law enforcement and cybersecurity teams. Its main purpose is to detect, track, and investigate scam or ransomware operations. The tool works by collecting digital evidence such as files, screenshots, and network data. It is designed to operate while remaining hidden and ensures that all its actions are fully legal. Collected data is transmitted through secure channels and is accessible via a real-time analysis dashboard. NetRaptor also helps in mapping the attacker's network, including IPs, domains, and control servers, to help dismantle their operations effectively.

Key Features

1) Lawful and Stealth Operation: It operates only with proper authorization and a legal-first approach, ensuring all actions follow the law, and it features a kill-switch and audit logging.
2) Early Threat Detection: It includes Behavioural & Pre-Encryption Detection to track file and API calls, catching ransomware activity before encryption occurs.
3) Network Mapping and Monitoring: It monitors network traffic for suspicious IPs/domains and maps the attacker's full setup, including control servers.
4) Secure Evidence Collection: It collects critical evidence like files, keystrokes, and screenshots, preserving their integrity for use in court using hashing and secure chain-of-custody methods, and sends the data securely via encrypted channels.
5) Real-time Analysis Dashboard: It provides a secure, real-time dashboard for authorized analysts to view, filter, study, and manage alerts related to the collected data.

II. LITERATURE SURVEY

1) A literature survey on NetRaptor-Lawful Network Intelligence Tool is a research on scam and NetRaptor detection focuses on monitoring network traffic, file changes, and system behavior to spot malicious patterns early.
2) Studies highlight using threat intelligence, IP/domain tracking, and forensic analysis to map attacker infrastructure.
3) Legal and ethical guidelines stress collecting evidence without violating privacy or laws.
4) Tools like Zeek and Velociraptor offer examples of safe, lawful investigation systems.
5) Studies on lawful hacking underline that invasive monitoring (e.g., keylogging, mic activation) must have warrants, proportionality, and oversight.

Some Authors and there works are : Mr. P.V.S.N. Murthy, et al.(2025) – "Network Forensics and Incident Response Tool with AI-Assisted Threat Analysis" , Kenan Begović (2023) – Survey focusing on the Encryption phase of the attack"Cryptographic Ransomware Encryption Detection: Survey".

©IJRASET: All Rights are Reserved

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

III. PROPOSED METHODOLOGY

We studied the research article "Network Forensics and Incident Response Tool with AI-Assisted Threat Analysis" and found it focuses mainly on post-attack incident handling.Our NetRaptor improves it and catches threats early, follows legal rules, and keeps evidence safe for use in court.

The NetRaptor tool's operation is structured around a multi-faceted methodology to ensure effective, hidden, and legally compliant intelligence gathering:

1) Behavioural & Pre-Encryption Detection: Tracks file changes and API calls to identify and intercept ransomware activity *before* the critical encryption phase begins.
2) Network-Based Detection & Mapping: Monitors network traffic to detect suspicious IPs/domains and map the attacker's Command and Control (C2) servers.
3) Evidence Integrity & Forensic Readiness: Preserves digital evidence using hashing and secure chain-of-custody methods to ensure the data is legally admissible in court.
4) Stealth-Aware, Legal-First Operation: Operates only with authorization and features both a kill-switch and audit logging to ensure all actions are legal and traceable.
5) Secure Data Exfiltration: Collected information is sent back to the analysts securely through encrypted channels.
6) Real-Time Dashboard & Alerting: Provides a secure web interface for authorized analysts to review, filter, and manage alerts on the collected data in real time.
7) Improvement over Existing Tools: Unlike traditional network forensics that focus on post-attack analysis, NetRaptor's approach emphasizes early threat capture and maintaining legal compliance.
8) Attacker Network Dismantling: The gathered intelligence, including the mapping of attacker networks, is used to aid in the effective dismantling of scam or ransomware operations

IV. EXISTING SYSTEM

A. Current cyber defence and forensic systems fall into two major categories

1) Traditional Post-Attack Forensics & Incident Response (IR) Tools

These systems focus on analysis *after* a security incident has occurred, such as analysing packet capture (PCAP) files or system logs to determine the cause and scope of the damage.

- Pros: Thoroughly analyses the attack vector and root cause after the fact; essential for compliance and system hardening.
- Cons/Failure: Primarily post-attack; the damage (e.g., data encryption by ransomware) has already happened, making the response purely reactive. They often lack a legal-first methodology for evidence that holds up in court.

2) Modern Ransomware Detection Tools (ML/Behavioural)

These tools use machine learning (ML) or deep learning (DL) to proactively monitor for suspicious system activities like API calls and file changes.

- Pros: Capable of Pre-Encryption Detection, offering a chance to stop the attack before data is locked; effective against zero-day and polymorphic threats.
- Cons/Failure: Systems often fail to be lawful and stealth-aware. Their core function is detection, but they may lack the necessary legal framework (auditing, chain-of-custody, authorization) to use the gathered information to legally track and prosecute attackers.

B. NetRaptor-Lawful Network Intelligence Tool improves upon these existing systems by

1) Flipping the Focus to Lawful Intelligence: It changes the goal from *only* incident response to Lawful Network Intelligence.
2) Enabling Covert, Pre-Encryption Forensics: It implements Behavioural & Pre-Encryption Detection while operating in a stealth-aware mode.
3) Guaranteeing Legal Admissibility of Evidence: It enforces Evidence Integrity & Forensic Readiness using hashing and secure chain-of-custody, ensuring collected files, screenshots, and keystrokes can be safely used in court.
4) Mapping the Entire Criminal Infrastructure: It focuses on Network-Based Detection & Mapping to track attackers' IPs, domains, and control servers, aiding in dismantling their operations

©IJRASET: All Rights are Reserved

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

V. SYSTEM ARCHITECTURE OF THE NEW SYSTEM

The project's progress is represented on something like a Gantt chart. It connects with the customer and provides the project's anticipated completion date. It assists you in determining how long a project should take, determining the resources required, and planning the sequence in which tasks will be completed.

A. Data-Flow Diagram (DFD) for NetRaptor

The system begins with continuous Data Collection and Monitoring of all network and endpoint activities.
This data feeds into Behavioural and Pre-Encryption Detection, which uses a database to identify threats before they can encrypt files. Upon detection, Network-Based Intelligence and Mapping traces the threat's path and identifies all affected systems. Next, the system initiates Evidence Collection and Forensic Readiness to securely preserve digital proof for investigation. This collected evidence is then sent via Secure Data Transmission to a central analysis point. Finally, all findings are presented on the Authorized Analyst Dashboard. This secure interface allows security professionals to review the incident. From there, they can analyse the threat and orchestrate an effective response.

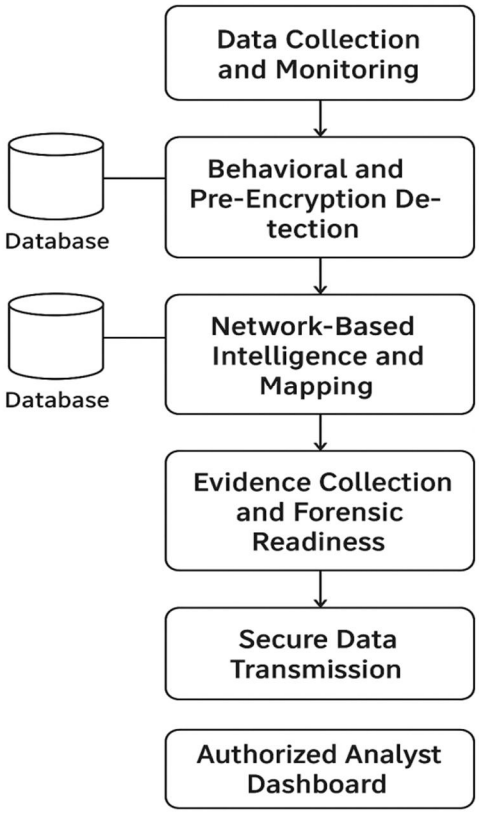


Figure-5.1: Data Flow Diagram (Dfd) For Netraptor

VI. MODULES AND FUNCTIONALITIES

The NetRaptor-Lawful Network Intelligence Tool is structured around distinct modules to manage the full lifecycle from covert deployment to legal analysis.

1) Client Module

- Functionality: Covert Data Acquisition and Encrypted Transmission.
- Key Activities:
  - Obtaining an executable file that is sent to the target machine.
  - Initiating a reverse and secure connection to the analyst's machine.
  - Watching and recording harmful network activity and system actions.

©IJRASET: All Rights are Reserved

2) *Server Module*
- Functionality: Secure Listening, Data Reception, and Command Processing.
- Key Activities:
  - Running the main listening component (e.g., python server.py).
  - Establishing a secure connection with the client using an RSA exchange and a Fernet session key.
  - Providing a live display of incoming victim keystrokes and messages.

3) *Detection & Mapping Module*
- Functionality: Early Threat Identification and Attacker Infrastructure Tracing.
- Key Activities:
  - Behavioral & Pre-Encryption Detection: Tracks file changes and API calls to catch ransomware activity *before* encryption.
  - Network-Based Detection & Mapping: Monitors network traffic to detect suspicious IPs/domains and map attacker control servers.

4) *Evidence & Integrity Module*
- Functionality: Forensic Readiness and Chain-of-Custody Assurance.
- Key Activities:
  - Collecting evidence like files, screenshots, keystrokes, and audio.
  - Preserving the legal evidence using hashing and secure chain-of-custody methods.
  - Storing collected messages (e.g., keystrokes) in a separate file for archival.

5) *Dashboard & Compliance Module*
- Functionality: Real-Time Analysis and Legal Governance.
- Key Activities:
  - Providing a secure dashboard for authorized teams to see, filter, and study the data in real time.
  - Enforcing Stealth-Aware, Legal-First Operation by requiring authorization and featuring kill-switch and audit logging functionalities.
  - Sending collected information securely through encrypted channels.

VII. RESULT

The Results of NetRaptor-Lawful Network Intelligence Tool are as follows:



FIGURE- 7.1
Established connection to scammers keyboard

The terminal output demonstrates the successful establishment of a secure, encrypted connection for data transfer, likely from the scammer's compromised system to a monitoring server. The line [*] Listening on 127.0.0.1:5000 indicates the server is ready to receive data, and the Connection established message confirms the two systems are communicating. A robust encryption handshake is performed using RSA to securely exchange a session key, followed by the establishment of a Fernet session key. This Fernet key is crucial, as it provides symmetric encryption for all subsequent keystroke data, ensuring that the captured information from the keylogger (as theorized previously) is transmitted securely and privately across the network.

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

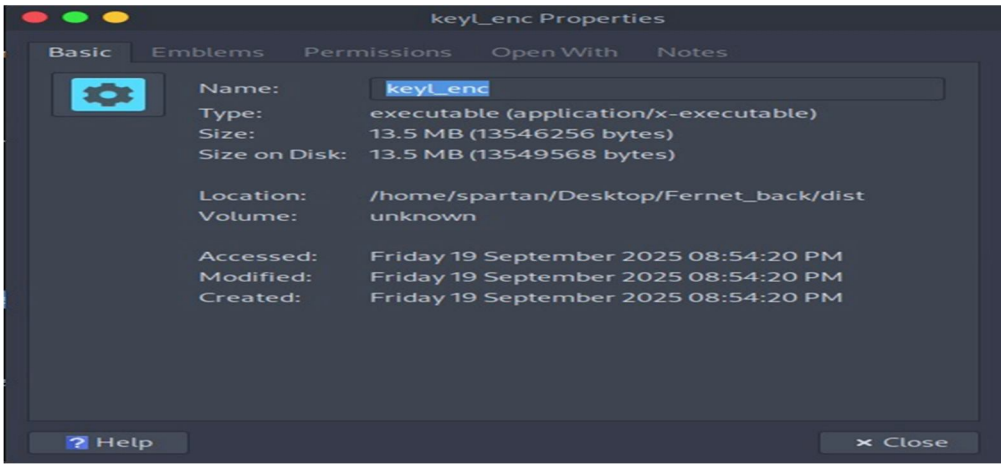


FIGURE- 7.2
Executed file after accessing keyboard

The executable file, named Kaylenc, is theorized to be a keylogger program designed for counter-surveillance against a scammer. As an executable (application/x-executable), its function is to covertly gain access to the target's keyboard input stream, a process known as keyboard hooking. Once running, it continuously captures all keystrokes, buffering the data internally. To maintain stealth and integrity, the collected typing data is then encrypted (suggested by the _enc suffix) before being periodically written to a separate, dynamically growing log file every 5 seconds. The primary role of the Kaylenc file itself is to execute the monitoring process, not to store the captured data, which is written to a designated, secure log file. This method ensures timely data exfiltration and protection of the gathered evidence from immediate detection.

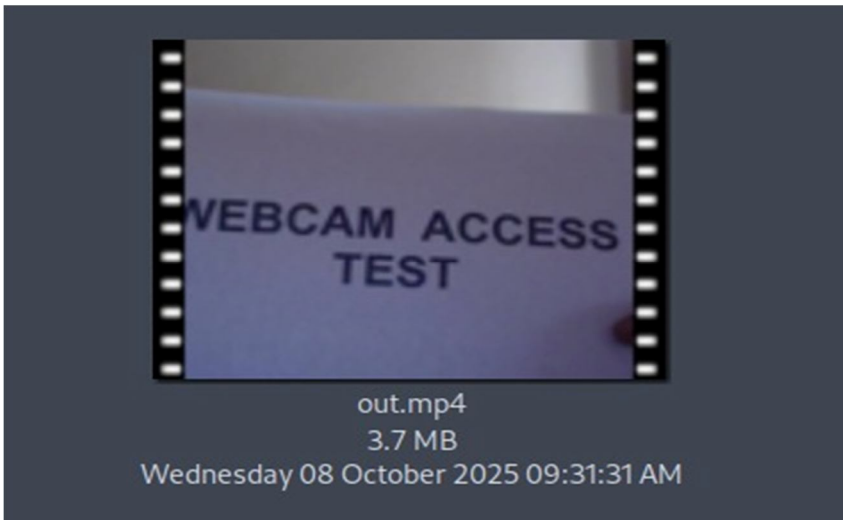


FIGURE- 7.3
Face cam access of scammers

The file out.mp4 is the resulting video log created by the NetRaptor monitoring tool, proving successful remote access to the scammer's webcam (face Cam). The mp4 extension confirms it is a standard video container format, and the small size (3.7 MB) suggests it is a brief clip, likely a test recording or a short segment of the intended continuous monitoring. The program responsible for this (a component of NetRaptor) would establish remote control over the webcam and periodically record video. Although the file *stores* video data, the program is designed to integrate the keylogging functionality (capturing typing data) from the previously discussed component. Therefore, the theory is that NetRaptor is simultaneously performing video surveillance (storing video in files like out.mp4) and keystroke logging (storing encrypted data in a separate log file) to provide a comprehensive record of the scammer's actions, with both data streams being captured and updated on a regular, possibly 5-second interval for near real-time intelligence gathering.

©IJRASET: All Rights are Reserved

VIII. CONCLUSION

The NetRaptor project successfully addresses critical shortcomings in existing cybersecurity and forensic methods. Its central achievement is creating a Lawful Network Intelligence Tool specifically designed to combat advanced scam and ransomware operations. By integrating Behavioural & Pre-Encryption Detection, NetRaptor significantly improves upon post-attack forensic tools by allowing threats to be intercepted before encryption and data loss occur. The implementation of the Client and Server Modules and secure RSA/Fernet key exchange demonstrates the foundation for covert and secure data acquisition. Crucially, the tool's emphasis on Evidence Integrity (using hashing) ensures that all collected proof, such as files, screenshots, and keystrokes, remains viable for use in court. Furthermore, its ability to map the full attacker network infrastructure (IPs, domains, C2 servers) provides invaluable intelligence for dismantling criminal operations effectively. Ultimately, NetRaptor provides authorized teams with a potent, legal-first solution to efficiently detect, investigate, and stop modern cyber threats while adhering to strict compliance rules.

IX. FUTURE ENHANCEMENTS

Future enhancements for the NetRaptor tool, based on the challenges and research gaps identified in the literature, should focus on improving scalability, adaptability, and integration:

1) Deep Learning (DL) Integration : Incorporate more advanced DL models to enhance the accuracy of Behavioural & Pre-Encryption Detection, specifically targeting new or sophisticated polymorphic ransomware variants.

2) High-Throughput Scalability : Optimize the server/client architecture for high-volume, dynamic network environments to ensure the tool remains effective under heavy traffic without compromising real-time performance.

3) Automated Incident Response (SOAR) : Develop automated response functionalities to perform immediate, isolated mitigation actions upon detection, rather than solely relying on manual analyst intervention.

4) Graphical User Interface (GUI) & SIEM Integration : Develop a richer, more user-friendly GUI for the dashboard and integrate with Security Information and Event Management (SIEM) systems for better usability and compatibility within existing cybersecurity infrastructures.

5) AI/ML Generalization: Refine the threat analysis algorithms to better generalize to attacks beyond the training data, reducing the likelihood of being bypassed by completely novel cyber threats

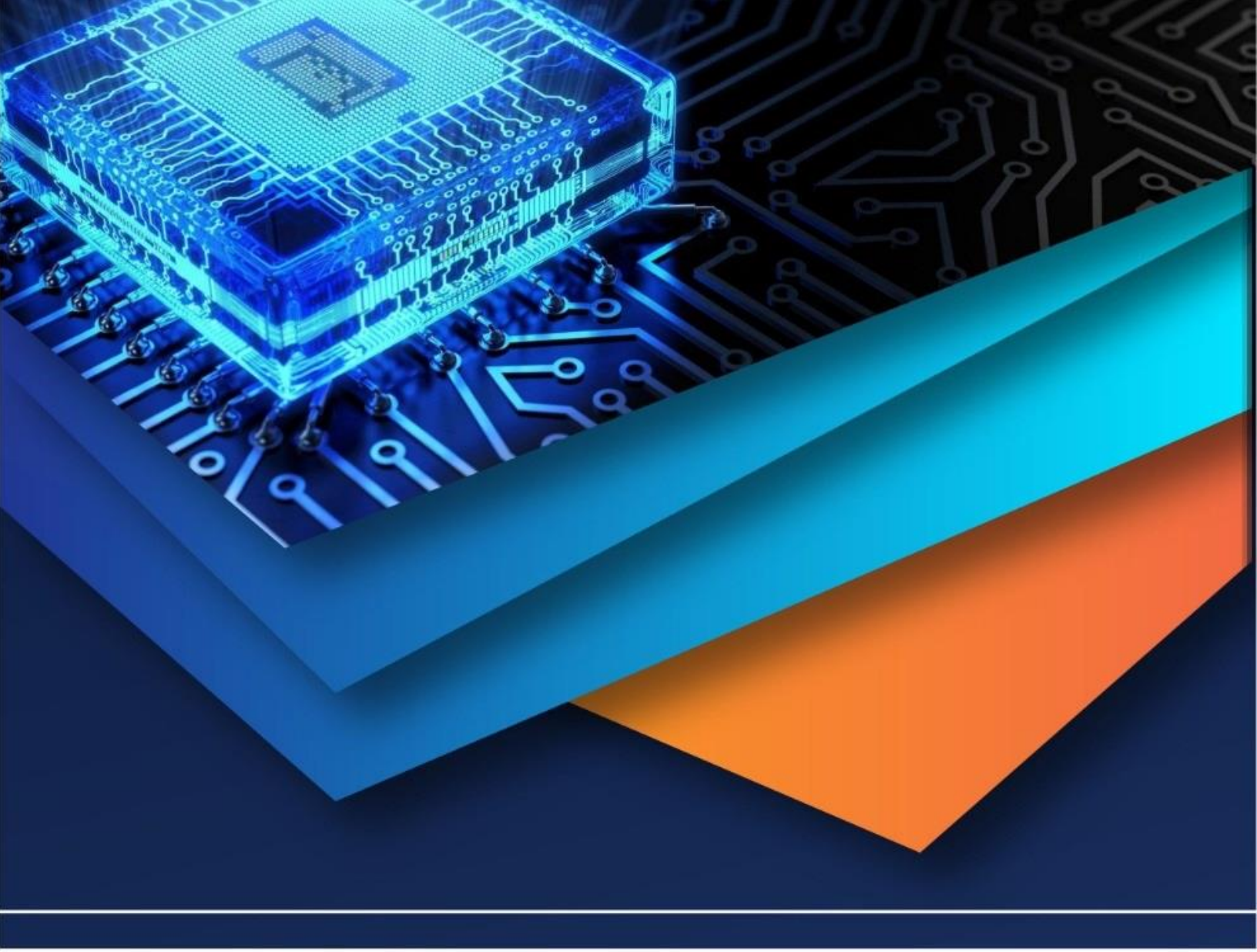
REFERENCES

[1] Mr. P.V.S.N. Murthy, Praneeth Kumar Neelamsetty, Pragya Gayatri Sreedharala, Madhu Babu Kondru, Likhith Kudara, “Network Forensics and Incident Response Tool with AI-Assisted Threat Analysis”, 13 March 2025, DOI – 10.22214/ijraset.2025.67471

[2] Sandoval et al., “Ransomware Detection with Machine Learning: Techniques, Challenges, and Future Directions”, February 2025, https://jisis.org/article/2025.I1.017/71744/

[3] Gurumallu et al., “Exploring Deep Learning Approaches for Ransomware Detection”, 2025, https://www.eurekaselect.com/article/140699

[4] Begović et al., “Cryptographic Ransomware Encryption Detection: Survey”, September 2023, https://www.sciencedirect.com/science/article/pii/S0167404823002596



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)