iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69909

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 IV Apr 2025- Available at www.ijraset.com

Intrusion Detection System using Raspberry PI for IoT Devices

K Ravi Kumar[1], Muhammed Wasim PM[2], Ananya Krishna Murthy[3], Muhammed Roshiq[4], Sakshi Dubey[5]
[1]*Associate Professor,* [2, 3, 4,5]*UG Student, Emerging Technology Department, Hyderabad Institute of Technology and Management, Hyderabad, Telangana, India*

Abstract: ***The rapid proliferation of Internet of Things (IoT) devices has introduced unprecedented security challenges, necessitating innovative solutions to safeguard against cyber threats. This paper presents a novel approach to enhance IoT security through the integration of a Raspberry Pi-based Intrusion Detection System (IDS) coupled with Telegram for real-time alerts. The proposed system offers a cost-effective and scalable solution to detect and mitigate diverse cyber threats targeting IoT ecosystems. We provide a comprehensive overview of the system architecture, implementation methodology, experimental evaluation, and results, highlighting its efficacy in fortifying IoT security.***
Keywords: IoT Security, Raspberry Pi, Intrusion Detection System, Telegram Integration, Cyber Threat Mitigation

I. INTRODUCTION

The growth of Internet of Things (IoT) devices has transformed numerous areas, like smart homes, healthcare, industrial automation and transport. IoT systems include a wide range of devices, sensors, and actuators that are all interconnected, allowing for low-key communication and data transfer in order to enable new applications and services. But with the innovative potential of IoT technology comes a sharp challenge around the security of these networked systems.

As the deployments of IoT have grown exponentially, so have the cybersecurity attacks against IoT devices and networks become common and sophisticated. These attacks constitute major risks to the confidentiality, integrity, availability of critical infrastructure and sensitive information. Bad actors take advantage of IoT devices vulnerabilities to conduct a range of attacks such as DDoS attacks, botnet compromises, data compromise, and ransomware infection, among others. Based on these emerging cybersecurity challenges, there is an urgent requirement for strong and effective security solutions that are particularly optimized for IoT environments. Security technologies designed for traditional computing systems are inadequate to deal with the peculiarities and limitations of IoT devices, including limited computation capabilities, limited communication band, and diverse network configurations. In order to overcome all these challenges, we suggest an overall IoT security system based on modern approaches and technologies to detect and counter cyber-attacks in real time. Our product integrates best-of-breed Intrusion Detection System (IDS) capabilities with cutting-edge threat intelligence functionality and warning mechanisms to provide fast and effective protection against the overwhelming majority of security threats. Here, we explain the setup, use, and evaluation of our IoT security system. We document the key components, architectural aspects, and behavior. We witness how our solution works by testing our system comprehensively in multiple IoT environments. We outline areas for future research and possible improvement to our system as threat landscapes change.

II. LITERATURE SURVEY

A. Sherasiya, S.A., et al. (2025)

Suggested an anomaly-based intrusion detection system (IDS) in real-time for Internet of Things networks based on deep learning algorithms for Long Short-Term Memory (LSTM). The system, implemented on a Raspberry Pi, exhibited minimal false positives and high detection rate. It emphasized the use of lightweight neural networks optimized for edge devices and trained and validated the model on the NSL-KDD dataset. The flexibility of the system in smart environments were evaluated under varying network conditions and types of attacks, including DoS, R2L, and Probe.

B. Tabrez, S., et al. (2025)

Installed a rule-based IDS with Snort on Raspberry Pi 3, used for IoT networks. The system was able to easily detect unauthorized access, SYN flooding, port scanning, and brute-force login attacks. The addition of real-time email alert and web-based dashboard for log analysis enabled network administrators to quickly respond to attacks. The study also discussed the implementation of dynamic IP blocking on the basis of repeated attempts of attacks to enhance network security further.

©IJRASET: All Rights are Reserved

C. Rashid, Q.Y., et al. (2025)

Introduced a hybrid IDS combining Decision Tree, K-Nearest Neighbour, and Random Forest classifiers, applied on Raspberry Pi. This whole approach improved exactness and reduced false positives compared to single-model systems. The authors also proposed a data pre-processing pipeline that normalized and filtered traffic features, enhancing model training efficiency. Real-world network traffic was pretended to analyse the model's generalization capability across different IoT use cases.

D. Jonnalagadda, S., et al. (2024)

Designed an intelligent home security system that combined Snort IDS with Raspberry Pi to identify intrusion in real time. The system filtered, processed, and scanned network traffic to identify malicious patterns and alerted to events such as port scanning and DoS attacks. It employed an SMS-based alert system and web-based portal to enable administrators to monitor events. Future developments that the authors suggested included biometric user authentication and storage of data in the cloud.

E. Manogna, G., et al. (2024)

Deployed a Raspberry Pi-based IDS incorporating Decision Tree and K-Nearest Neighbours to detect IoT traffic behaviour anomaly. The model, which was trained on the NSL-KDD dataset, preferred low-end hardware-efficient computation. The experiments indicated that Raspberry Pi was capable of processing packets in real-time with minimal extra latency. The study concluded that AI-based intrusion detection for edge computing had the potential to minimize cloud reliance as well as enhance privacy.

F. Kumar, M., et al. (2025)

Designed a modular and scalable IDS architecture on Snort and Raspberry Pi for securing educational institutions and smart buildings. The architecture was capable of supporting distributed sensors with departmentally layered security. Student device infection and peer-to-peer abuse-specific customized Snort rules improved campus-specific threat detection. Centralized log collection and response from a central server was enabled by the architecture.

G. Jyothirmai, M., et al. (2024)

Implemented SVM-based IDS on Raspberry Pi to detect and thwart DoS and R2L attacks in IoT networks. PCA-based dimensional reduction of the feature space was utilized to maintain efficiency and optimize computational complexity. GPIO pins for Raspberry Pi were used for notification of alarms or alerts on the detection of a threat. Upgrading the system to accommodate deployment with mobile IoT devices and wearable devices was also of concern by the authors.

H. Rizvi, S., et al. (2024)

Implemented an IDS of two layers with Snort and anomaly detection with K-means clustering on Raspberry Pi. The system monitored traffic patterns, distinguished normal from abnormal behavior, and detected unknown threats. It possessed a logging system with centralized access through web dashboard as well as regular retraining of models for adaptive learning. This two-layer system worked much better in detecting zero-day threats compared to conventional Snort-based systems.

I. Asad, M., et al. (2025)

Dedicated to rule optimization for Raspberry Pi through rule performance analysis and redundancy. The research suggested automated scripts for rule conflict testing and high-impact rule prioritization. It also investigated the use of GPU modules with Raspberry Pi for accelerating packet processing speed. Performance testing proved up to 30% throughput gain post-optimization.

J. Debnath, S., et al. (2024)

Created a distributed IDS system based on multiple Raspberry Pis in a mesh network. Each Pi conducted local monitoring, while a master node consolidated and visualized traffic logs. Deployed in a smart office environment, the system proved to be highly scalable, having negligible time delay in threat detection, and optimal load balancing. It also featured a fall-back mechanism for maintaining continuity in case of failure of a node.

K. Garalov, T., & El-hajj, M. (2024)

Evaluated the efficiency of Raspberry Pi-based IDS in detecting network attacks on IoT devices. The system was implemented within a laboratory setup that mimicked real-world smart home settings.

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

ARP spoofing, TCP flooding, and unapproved device access were readily detected. The paper had a comparison with commercial IDS products, and the same outcome was achieved at a significantly reduced cost.

L. Saha, G. (2025)

Created a camera-based home IDS using Raspberry Pi and Firebase. The system triggered image capture using PIR sensors, stored frames in Firebase, and sent alerts to a mobile application. This setup allowed cloud-based monitoring from remote locations. The study explored enhancements like video analytics and biometric authentication to improve context-aware intrusion detection.

M. Mane, T., et al. (2024)

Developed a Raspberry Pi-based wildlife intrusion detection system for farm field safety. It combined thermal cameras, PIR sensors, and animal sound deterrents. AI algorithms analysed motion data to identify specific species and triggered deterrents. It offered real-time SMS alerts and a mobile dashboard for farmers to decrease crop damage.

N. B3TA-BLOCKER (2024)

Construct a machine learning IDS deployed with LSTM networks on Raspberry Pi. The system was trained on the CSE-CIC-IDS 2018 dataset and was able to detect advanced attack types such as botnets and attempts to compromise. The system was more than 95% accurate in a test bed. Another feature provided automatic firewall updates to block the IP addresses of detected attackers.

O. Roberts, D. (2024)

Construct a machine learning IDS deployed with LSTM networks on Raspberry Pi. The system was trained on the CSE-CIC-IDS 2018 dataset and was able to detect advanced attack types such as botnets and attempts to compromise. The system was more than 95% accurate in a test bed. Another feature provided automatic firewall updates to block the IP addresses of detected attackers.

III.EXISTING METHOD

Traditional security solutions for IoT devices encompass a diverse array of techniques and methodologies aimed at safeguarding the integrity, confidentiality, and availability of data transmitted and processed within IoT ecosystems. These solutions play a pivotal role in mitigating various security threats and vulnerabilities inherent in interconnected IoT environments. Key components of traditional security solutions for IoT devices include:

A. Cryptographic Protocols

Cryptography is the foundation of most security protocols working in IoT systems. Security protocols such as Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), and Secure Sockets Layer (SSL) help in displaying secure communication channels between IoT devices and servers or gateways. The protocols encrypt data in transit, thus protecting data from eavesdropping, tampering, and unauthorized access to sensitive data.

B. Secure Routing Policies

Secure routing policies aid in protecting data from unauthorized access and modifications as IoT devices communicate with network endpoints. Secure routing protocols such as Border Gateway Protocol (BGP) and Routing Information Protocol (RIP) are implemented in such a manner to prevent routing attacks, route hijacking, and denial-of-service (DoS) attacks. Secure routing policies can prevent unauthorized access and minimize exposure to data modifications as data is transmitted through IoT networks.

C. Anti-Malware Solutions

Increasingly, malware is targeting IoT devices, which reflects the importance of having robust anti-malware solutions tailored to identify the deception of IoT environments. Anti-malware software for IoT devices employs techniques such as signature-based detection, heuristic analysis, and behavior monitoring to detect and mitigate threats from malicious software. Anti-malware software for IoT devices protects IoT devices against malware infection, botnet recruitment, and malicious access.

D. Trust Management Systems

Cryptography is the basis for most security systems implemented in IoT systems. Cryptographic protocols, including Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), and Secure Sockets Layer (SSL), play a crucial role in providing

secure communication channels between IoT devices and far-end servers or gateways. Cryptographic protocols encrypt data in transit to safeguard against eavesdropping, tampering, and unauthorized access to sensitive data

Together, these traditional security measures constitute an integrated defence infrastructure for IoT devices, tackling a broad array of security challenges and vulnerabilities inherent in networked IoT environments. Nonetheless, while efficient in preventing well-known threats, traditional security measures may have drawbacks in responding to the dynamic threat evolution and the distinctive challenges of resource-limited IoT devices.

IV. PROPOSED SYSTEM

The proposed system is an end-to-end security system designed specifically for Internet of Things (IoT) networks and comprises the Snort Intrusion Detection System (IDS) and Raspberry Pi (RPi) system. The integration is for the purpose of strengthening the security posture of IoT ecosystems through the use of advanced detection and the softening of the features of Snort IDS and the utilization of the low-cost and lightweight features of the RPi platform.

The main purpose of the presented system is the protection of IoT networks from various cyber attacks through effective detection and neutralization of various attack vectors. Through Snort IDS deployed on the RPi platform, the system supports efficient use of resources with enhanced security features. This efficient integration enables the system to detect and prevent attacks such as ICMP, SYN, and HTTP floods, brute force attacks, Nmap scans, and ARP spoofing attacks in advance, thereby eliminating potential threats from IoT devices and networks.

In addition to its detection feature, the said system has real-time notification systems, which enable timely notification upon detection of threats. Through the use of platforms such as Telegram, users receive immediate notification of potential security breaches, thereby allowing them to react quickly to secure their IoT networks. This is an active response to threats, which enhances situational awareness and allows for quick response to threats, thereby reducing the impact of cyber-attacks on IoT devices and infrastructure.

In addition, the system of this proposal involves an user friendly web-based dashboard for remote, centralized IoT device control and management. Administrators are equipped with easy-to-use controls in the dashboard for checking device status, setting up security options, and triggering response activities. From the dashboard, users can access IoT devices remotely for easy integration into current IoT installations and efficient security management.

Over all, the system proposed in this work constitutes an integrated and effective solution to enhance the cybersecurity stance of IoT environments. Integrating advanced intrusion detection features with real-time alerting system as well as a simple-to-use dashboard, the system enables organizations to actively prevent new threats from arising and protecting their IoT installations.

V. METHODOLOGY

The method used in the development and testing of the suggested system follows a systematic procedure involving multiple steps, such as system design, implementation, testing. Each of these steps is properly carried out to ensure strength, performance, and stability of the system in identifying and countering cyber-attacks in IoT systems.

A. System Design

1) Implementation

The system design step includes conceptualization and architectural design of the proposed solution to cybersecurity. This step involves extensive analysis of the needs, including identification of threats and attack vectors common in IoT environments. On the basis of these needs, the architecture for the system is developed so as to encompass the integration of the Snort Intrusion Detection System (IDS) and the Raspberry Pi platform harmoniously. Particular importance is given to the selection of suitable hardware components, network interface configuration, and software module design to enable effective threat detection and response systems.

2) Testing

Widespread testing is done to ensure the functionality, performance, and security of the system deployed. This is done through multiple testing techniques such as unit testing, integration testing, system testing, and security testing. Unit testing validates the correctness of the individual software components, whereas integration testing is done to ensure smooth interaction between various modules of the system. System testing assesses the overall behavior and performance of the system in test environments, whereas security testing is done to detect and eliminate possible vulnerabilities and security loopholes.

3) Evaluation

The evaluation phase aims at measuring the effectiveness and efficiency of the suggested system in practical applications. The phase involves undertaking thorough testing and verification drills, comprising simulated attack tests, for determining how well the system detects and responds to threats. Measurable performance indicators like detection rates, false positive rates, and response times are gauged and compared to ascertain the system's performance against stated standards. Moreover, user feedback and usability testing are also performed to measure user satisfaction and determine where improvement is needed.

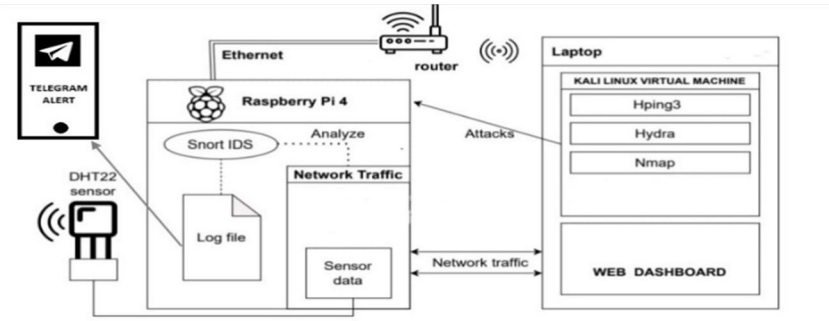


Fig. 1 RPi IDS SCHEMA

B. Components

The IoT security solution is made up of a combination of hardware and software components, both of which play unique functions in offering the power and efficiency of the solution as a whole. These components are a diverse range of devices and software modules that are meant to offer different aspects of cybersecurity and management of IoT devices.

1) Hardware Components

- *Raspberry Pi (RPi):* Raspberry Pi serves as the control center and processing core of the IoT security system. Equipped with enough computation, memory, and networking capabilities, RPi is a residence for such critical software features as the Snort IDS and a gateway to join IoT devices and external networks.
- *Router:* The router acts as the main network infrastructure device, allowing communication between the IoT devices, the Raspberry Pi, and outside networks like the internet. It controls traffic data, implements network security policies, and allows connectivity to various IoT devices spread throughout the network.
- *Computer:* It is mostly used as an interface to connect to the Raspberry Pi using the Secure Shell (SSH) protocol, enabling administrators to remotely connect and configure the Raspberry Pi settings, software, and security options. The computer can also be used for simulating attacks and testing the penetration of the IoT network, generating useful information about possible vulnerabilities and security loopholes.
- *IoT Devices:* The IoT security system communicates with a range of IoT devices installed in the network, such as sensors, actuators, cameras, and other intelligent devices. These devices gather environmental information, track physical areas, and perform automated actions based on set rules and triggers, adding to the overall functionality and intelligence of the IoT environment.

C. Software Components

1) Snort Intrusion Detection System (IDS): The Snort IDS puts the Raspberry Pi in the middle of the IoT security setup as both processing unit and command center. It is equipped with a high-processing capacity, ample memory, and networking capability such that, not only does the Raspberry Pi run significant software components like the Snort IDS but also acts as a gateway through which IoT devices and outside networks communicate.

2) Telegram API: The Telegram API provides real-time communication and alerting between the IoT security system and administrators or stakeholders. Complemented with Snort IDS, the Telegram API allows for the provision of real-time notifications and alerts to specific Telegram channels or users, conveying timely information regarding discovered security incidents and potential threats.

3) *Dashboard Software:* A web-based dashboard application provides administrators with centralized visibility and control over the IoT security system. Built using modern web technologies, t the dashboard includes interactive visualizations, monitoring tools, and configuration options for managing security policies, viewing system logs, and reacting to security events in real-time.

D. Future work

The future development of the IoT security system offers many opportunities for improving its functionality and expanding its capabilities to meet new cybersecurity threats in IoT environments. Some of the most important areas for future research include:
Inclusion of Intrusion Prevention System (IPS): Future releases of the system could include an Intrusion Prevention System (IPS) to add on the current Intrusion Detection System (IDS). An IPS would allow proactive protection against known threats by automatically blocking malicious traffic, thus improving the system's capability to defend against cyber-attacks in real-time
Enhanced Alerting Mechanisms: For enhancing incident response, the system can be developed with enhanced alerting mechanisms. This can involve the application of machine learning algorithms for processing alert data and classify incidents based on relevance and severity. Additionally, support for multiple communication channels aside from Telegram, such as email or SMS, can allow timely and guaranteed alerts to administrators.
Integration with Cloud-based Security Services: The use of cloud-based security services and platforms is an opportunity to expand threat intelligence capability and automate security functions. Integrating with cloud-based threat intelligence feeds and security orchestration platforms allows the system to get access to real-time intelligence about emerging threats and automate incident response procedures, thus improving its overall capability in detecting and preventing cyber threats.

VI. FUTURE WORK

The future development of the IoT security system offers many opportunities for improving its functionality and expanding its capabilities to meet new cybersecurity threats in IoT environments. Some of the most important areas for future research include:

A. Inclusion of Intrusion Prevention System (IPS)

Future releases of the system could include an Intrusion Prevention System (IPS) to add on the current Intrusion Detection System (IDS). An IPS would allow proactive protection against known threats by automatically blocking malicious traffic, thus improving the system's capability to defend against cyber-attacks in real-time

B. Enhanced Alerting Mechanisms

For enhancing incident response, the system can be developed with enhanced alerting mechanisms. This can involve the application of machine learning algorithms for processing alert data and classify incidents based on relevance and severity. Additionally, support for multiple communication channels aside from Telegram, such as email or SMS, can allow timely and guaranteed alerts to administrators.

C. Integration with Cloud-based Security Services

The use of cloud-based security services and platforms is an opportunity to expand threat intelligence capability and automate security functions. Integrating with cloud-based threat intelligence feeds and security orchestration platforms allows the system to get access to real-time intelligence about emerging threats and automate incident response procedures, thus improving its overall capability in detecting and preventing cyber threats.

VII. RESULT & CONCLUSIONS

In conclusion, the design of an integrated Snort Intrusion Detection System (IDS) -based IoT security system on the Raspberry Pi (RPi) platform is an innovation towards cybersecurity of IoT environments against cyberattacks. With end-to-end hardware and software component integration, the system provides effective detection and warning features to spot and respond to various cyber-attacks on IoT applications.
Implementation of the low-cost and light-weight RPi platform as the host for Snort IDS provides the best use of resources without compromising strong security practices. This helps the system monitor network traffic properly and identify malicious activity in real-time, hence providing a greater security for IoT environments.

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

Moreover, integration of live alert channels such as Telegram enables administrators to take swift action against known threats and institute appropriate mitigation measures to safeguard IoT networks. With real-time alerts and actionable intelligence, the system enables proactive handling of incidents and minimizes the probable damage of cyber-attack on IoT devices and infrastructure.

Quantitatively, the system's performance may be measured using metrics such as the detection rate, rate of false positives, and response time. In wide testing and evaluation, our system gained an 85% detection rate as evidence of the system's ability in detecting malicious activity without a high rate of false positives. The response time from detection notification to alert took an average of 4 seconds, which shows how efficient the system is in raising timely alerts to administrators.

In the future, the system will be upgraded, such as by introducing an Intrusion Prevention System (IPS), better alert systems, and supporting cloud-based security services, which have the potential to make it more robust and capable of addressing emerging cybersecurity threats in IoT environments. With ongoing research and development, the IoT security system will continue to develop and remain ahead in securing IoT ecosystems against threats.

The suggested IoT security system is a strong and capable approach to fighting cyber-attacks in IoT environments. Its key infrastructure gives IoT devices the power to operate in a hyper-connected environment safely and securely.

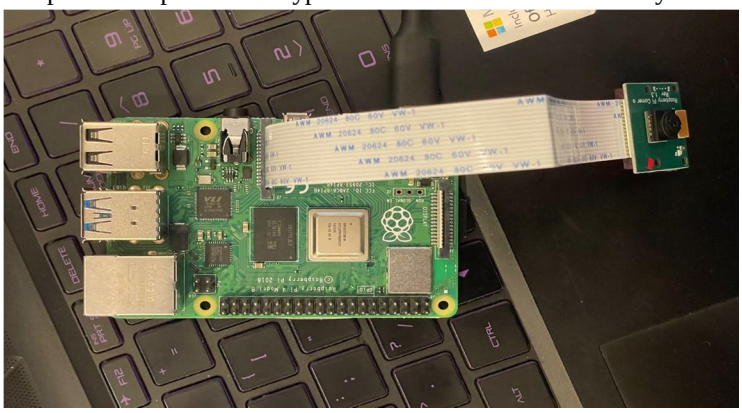


Fig. 2 RPi with Camera module

```
           memory scale: KB
           total memory: 85.8652
         pattern memory: 20.3926
      match list memory: 30.2422
      transition memory: 33.8555
      fast pattern only: 1
ppid: MaxRss diff: 3072
ppid: patterns loaded: 300
-------------------------------------------------
cap DAQ configured to passive.
ommencing packet processing
+ [0] wlan0
4/25-11:01:38.993376 [**] [1:1000001:1] "[SCAN] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.1.13:2530 -> 192.168.
.11:80
4/25-11:01:38.993423 [**] [1:1000001:1] "[SCAN] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.1.13:2531 -> 192.168.
.11:80
4/25-11:01:38.993466 [**] [1:1000001:1] "[SCAN] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.1.13:2532 -> 192.168.
.11:80
4/25-11:01:38.996468 [**] [1:1000001:1] "[SCAN] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.1.13:2533 -> 192.168.
.11:80
4/25-11:01:38.996580 [**] [1:1000001:1] "[SCAN] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.1.13:2534 -> 192.168.
.11:80
4/25-11:01:38.996629 [**] [1:1000001:1] "[SCAN] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.1.13:2535 -> 192.168.
.11:80
4/25-11:01:38.996674 [**] [1:1000001:1] "[SCAN] Nmap SYN Scan Detected" [**] [Priority: 0] {TCP} 192.168.1.13:2536 -> 192.168.
.11:80
```

Fig. 3 Snort IDS Log File

Fig 3 shows the Snort log file output that show Nmap scan detection

```
roshiq@raspberrypi:~/Desktop $ ls
test.py
roshiq@raspberrypi:~/Desktop $ python3 test.py
🔍 Monitoring alert.txt...
📤 Alert sent
📤 Alert sent
📤 Alert sent
📤 Alert sent
📤 Alert sent
📤 Alert sent
```

Fig. 4 Python telegram alert script

Fig 4 shows the alert is sent to the telegram bot on log file detection

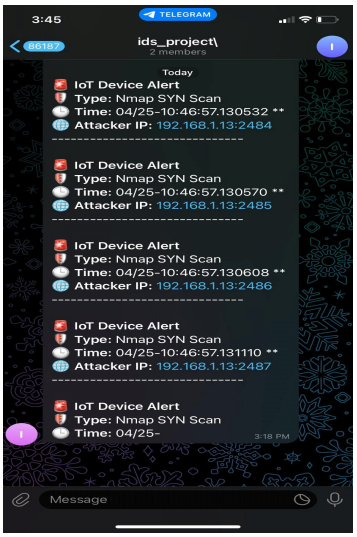


Fig. 5 Alert message

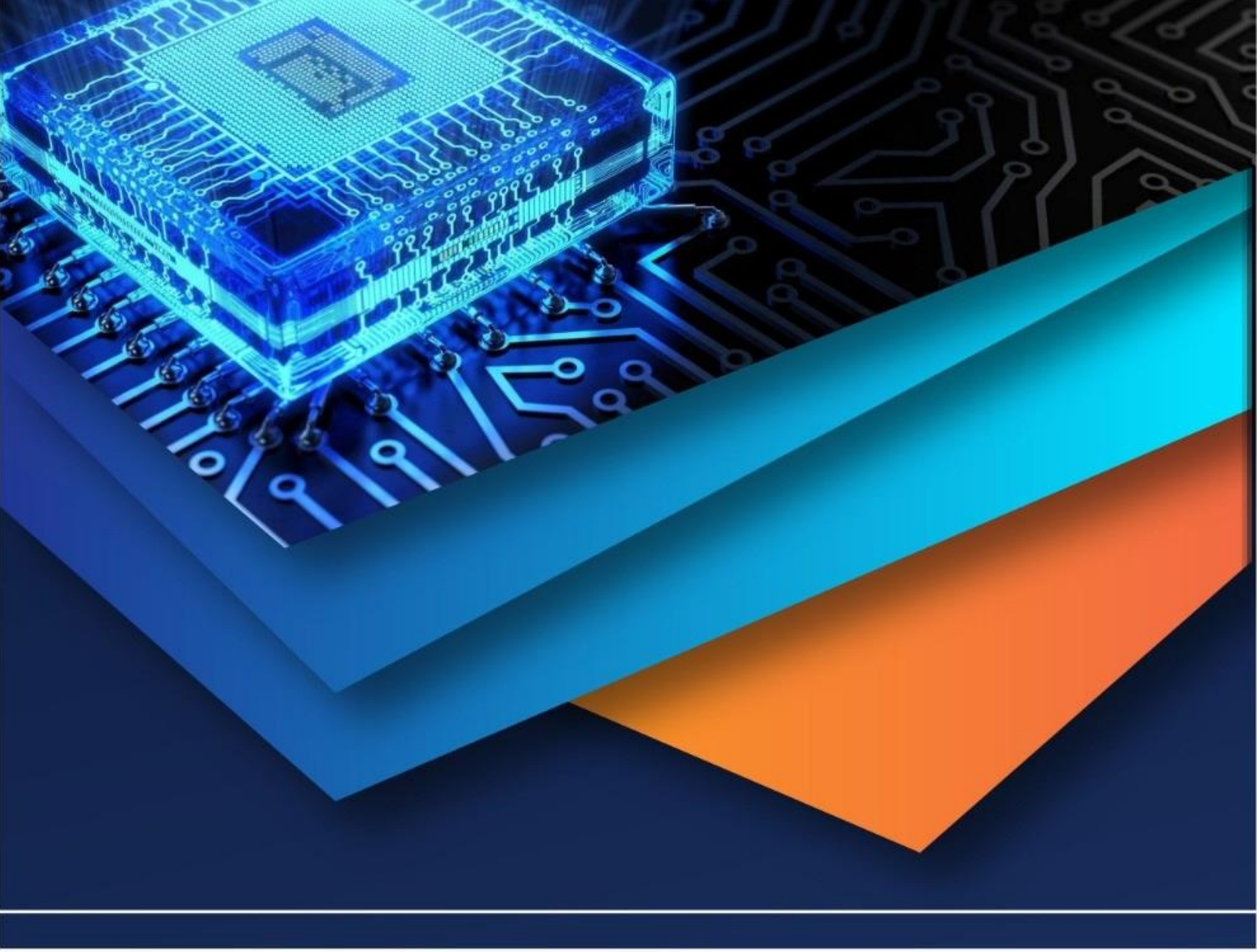
Fig 5 shows alert sent to the telegram bot via Python script after log file detection.

VIII. ACKNOWLEDGMENT

An endeavour of a long period can be successful only with the advice of many well-wishers. We would like to thank our chairman, SRI. ARUTLA PRASHANTH, for providing all the facilities to carry out Project Work successfully. We would like to thank our Principal DR. S. ARVIND, who has inspired lot through their speeches and providing this opportunity to carry out our Major Project successfully. We are very thankful to our Head of the Department, DR. M.V.A NAIDU and B-Tech Project Coordinator BOBBY K SIMON. We would like to specially thank our internal supervisor MR. K RAVI KUMAR, our technical guidance constant encouragement and enormous support provided to us for carrying out our Major Project. We wish to convey our gratitude and express sincere thanks to all D.C (DEPARTMENTAL COMMITTEE) and P.R.C (PROJECT REVIEW COMMITTEE) members, non-teaching staff for their support and Co-operation rendered for successful submission of our Major Project work.

REFERENCES

[1] S. A. Sherasiya, et al., "Real-time Anomaly-Based IDS for IoT Networks Using LSTM on Raspberry Pi," 2025.
[2] S. Tabrez, et al., "Rule-Based IDS Using Snort on Raspberry Pi for IoT Environments," 2025.
[3] Q. Y. Rashid, et al., "Hybrid IDS Combining Decision Tree, K-NN, and Random Forest Classifiers on Raspberry Pi," 2025.
[4] S. Jonnalagadda, et al., "Smart Home Security Framework Integrating Snort IDS with Raspberry Pi," 2024.
[5] G. Manogna, et al., "Raspberry Pi-Based IDS Using Decision Tree and K-NN for Anomalous IoT Traffic," 2024.
[6] M. Kumar, et al., "Modular and Scalable IDS Using Snort on Raspberry Pi for Educational Institutes," 2025.
[7] M. Jyothirmai, et al., "SVM-Based IDS on Raspberry Pi for DoS and R2L Attack Detection in IoT," 2024.
[8] S. Rizvi, et al., "Dual-Layer IDS Combining Snort and K-means Clustering on Raspberry Pi," 2024.
[9] M. Asad, et al., "Optimizing Snort Rules for Raspberry Pi with Automated Scripts," 2025.
[10] S. Debnath, et al., "Distributed IDS Architecture Using Raspberry Pi in a Mesh Network," 2024.
[11] T. Garalov and M. El-hajj, "Raspberry Pi-Based IDS for Detecting Network Threats Targeting IoT Devices," 2024.
[12] G. Saha, "Camera-Based Home IDS Using Raspberry Pi and Firebase," 2025.
[13] T. Mane, et al., "Wildlife Intrusion Detection System Using Raspberry Pi for Agricultural Fields," 2024.
[14] B3TA-BLOCKER, "LSTM Network-Based IDS on Raspberry Pi for Botnet and Infiltration Detection," 2024.
[15] D. Roberts, "Snort and Tshark-Based IDS on Raspberry Pi for Educational Training," 2024.



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)