PISECURE: INTEGRATED SOLUTION FOR NETWORK PROTECTION

B. E. Electronics and Telecommunication Engineering

By

Sakshi Aghav **01**
Arya Chowkekar **04**
Aaryan Gorana **21**
Vishal Gupta **22**

Supervisor:

Dr. Jyoti Mali
Associate Professor

Department of Electronics and Telecommunication Engineering
Atharva College of Engineering
Malad West Mumbai
University of Mumbai
2024-2025

PISECURE: INTEGRATED SOLUTION FOR NETWORK PROTECTION

B. E. Electronics and Telecommunication Engineering

By

Sakshi Aghav	**01**
Arya Chowkekar	**04**
Aaryan Gorana	**21**
Vishal Gupta	**22**

Supervisor:

Dr. Jyoti Mali
Associate Professor

Department of Electronics and Telecommunication Engineering
Atharva College of Engineering
Malad West Mumbai
University of Mumbai
2024-2025

AET'S

ATHARVA COLLEGE OF ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"PiSecure: integrated firewall solution for network protection"** is a Bonafide work of **"Sakshi Aghav (01), Arya Chowkekar (04), Aaryan Gorana (21), Vishal Gupta (22)"** submitted to the University of Mumbai in partial fulfilment of the requirement for the award of the degree of B.E. in Electronics and Telecommunication.

Dr. Jyoti Mali
Project Guide

(Name and sign)
External Examiner

College Seal

Prof.Ammu Striney	**Dr. Bhavin Shah**	**Dr. Ramesh Kulkarni**
Internal Examiner	**Head of Department**	**Principal**

Project Report Approval for B.E.

This project report entitled **"PiSecure: integrated firewall solution for network protection"** By **"Sakshi Aghav (01), Arya Chowkekar (04), Aaryan Gorana (21), Vishal Gupta (22)"** is approved for the degree of ***B.E. in Electronics and Telecommunication.***

Examiners

1.----------

2.----------

Date:

Place:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Signature)

(Sakshi Aghav Roll no. 01)

(Arya Chowkekar Roll no.04)

(Aaryan Gorana Roll No.21)

(Vishal Gupta Roll No.22)

Date:

ABSTRACT

In today's digital landscape, network security threats such as unauthorized access, malware, Denial of Service (DoS) attacks, and Man-in-the-Middle (MITM) attacks have become increasingly prevalent. To address these risks, our project introduces a **hardware-based firewall** integrated with a **DNS-based ad blocker and an Intrusion Detection System (IDS)**, all built on a **Raspberry Pi**. This solution provides a **cost-effective, scalable, and customizable** security framework designed for home and small business networks.

The firewall enforces strict **traffic filtering policies** using **iptables**, allowing administrators to block or allow traffic based on **IP addresses, domains, and network protocols**. The **DNS-based ad blocker**, utilizing the **DNS Sinkhole** concept, effectively blocks advertisements, trackers, and malicious domains at the DNS level, improving security and browsing performance. The **Intrusion Detection System (IDS)** continuously monitors network activity, detecting **brute-force attacks, DoS attempts, active reconnaissance, ARP spoofing, and MITM attacks**.

Instead of relying on a database, all detected threats and logs are stored in **log files**, allowing network administrators and security engineers to analyse traffic using **Wireshark**. The system is managed via a **centralized web-based dashboard**, enabling easy configuration and real-time monitoring. This project offers a **comprehensive, user-friendly, and powerful cybersecurity solution** tailored to evolving network security challenges.

List of Figures

Table no :01(Figures)

List of Tables

Table no : 02(Tables)

List of Abbreviations

Sr. No.	Abbreviations	Expanded form
1	IDS	Intrusion detection system
2	DDOS	Distributed Denial of Service
3	DOS	Denial of Service
4	DPI	Deep Packet Inspection
5	VPN	Virtual Private Network
6	DNS	Domain Name System
7	MITM	Man-in-the-Middle
8	ARP	Address Resolution Protocol
9	IP	Internet Protocol
10	USB	Universal Serial Bus
11	CSI	Camera Serial Interface
12	DSI	Display Serial Interface
13	LED	Light Emitting Diode
14	HTTP	Hypertext Transfer Protocol
15	HTTPS	Hypertext Transfer Protocol Secure
16	SSH	Secure Shell
17	ICMP	Internet Control Message Protocol
18	SQL	Structured Query Language

Table no :03(Abbreviations)

INDEX

Table no :04(Index)

Chapter 1
INTRODUCTION

The hardware-based firewall built using a **Raspberry Pi** is a cost-effective, efficient, and scalable solution designed to **secure networks** by filtering incoming and outgoing traffic. Unlike traditional software firewalls that run on individual computers, this firewall operates at the network level, acting as a security gateway between internal devices and the external internet.
This project aims to design and implement a comprehensive Raspberry Pi-based firewall that integrates multiple security components to provide robust network protection. The firewall leverages Intrusion Detection Systems (IDS) like Snort or Suricata to actively monitor network traffic and identify threats such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. By analysing network packets in real-time, the system can detect suspicious patterns and respond promptly to mitigate potential risks.

To enable centralized and real-time management, a web-based monitoring console built using Flask is included. This dashboard allows users to visualize network traffic, view threat alerts, configure firewall rules, and manage security policies with ease. The system is designed to be flexible, enabling the creation of customizable firewall rules that can adapt to specific network environments.
By utilizing Raspberry Pi as the core hardware, this firewall solution is both affordable and scalable, making it accessible for a wide range of users, from small businesses to home networks. With a combination of IDS and real-time monitoring, this project offers a holistic security solution that enhances network protection while being cost-effective and easy to deploy.

In addition to its core firewall capabilities, the Raspberry Pi-based security solution incorporates deep packet inspection (DPI) techniques to analyze network traffic at a granular level. This enables the identification of potentially malicious payloads, unauthorized data transfers, and policy violations. By leveraging libraries like PyShark for packet capture and Pandas for data processing, the system can generate detailed insights into network behavior, allowing administrators to proactively respond to anomalies. Furthermore, integration with threat intelligence feeds ensures that the firewall stays updated with the latest attack signatures, enhancing its ability to detect and mitigate emerging cyber threats.

Another key feature of this project is its modularity, allowing users to expand its functionality based on specific security needs. Additional security measures such as an ad-blocking system, Virtual Private Network (VPN) support, and automated threat response mechanisms can be incorporated to strengthen network defenses. The firewall can also be configured for content filtering, enabling businesses or households to restrict access to specific websites or categories. Moreover, its energy-efficient nature makes it a sustainable and cost-effective alternative to commercial firewalls, offering a powerful security solution without excessive power consumption.

1.1 Description

A hardware-based firewall is a network security solution designed to filter, monitor, and control **incoming** and **outgoing** traffic at the network level. Unlike traditional software firewalls, which operate on individual devices, a hardware firewall acts as a central security gateway, protecting all connected devices from cyber threats.

With the rising cybersecurity threats, home and small business networks require a **robust, cost-effective, and customizable security solution**. Our project leverages a **Raspberry Pi-based hardware firewall** that integrates **firewall rules, DNS-based ad blocking, and an Intrusion Detection System (IDS)** into a single, efficient system.

The firewall provides **advanced protection against threats** like **Denial of Service (DoS), Man-in-the-Middle (MITM), ARP spoofing, and reconnaissance attacks**. Users can monitor and control network traffic using a centralized web dashboard, accessible via the Raspberry Pi's IP address. The user-friendly interface allows easy **configuration of firewall rules, real-time traffic analysis, and attack detection logs**.
This affordable, scalable, and customizable security solution ensures **enhanced network security, privacy, and control**, making it ideal for small-scale deployments.

1.2 Problem Formulation

With the increasing reliance on the internet, cyber threats such as malware infections, unauthorized access, Denial of Service (DoS) attacks, and Man-in-the-Middle (MITM) attacks have become a growing concern for home and small business networks. Traditional security measures such as software firewalls and ad-blockers provide partial protection but often lack integration, require multiple installations, and are complex to configure. Additionally, existing solutions may not effectively detect network reconnaissance, ARP spoofing, brute-force attacks, or unauthorized remote access attempts.

Furthermore, most commercial firewalls and security appliances are expensive, lack customization options, and require professional expertise for configuration. Small businesses and home users often struggle with managing network security and monitoring threats in real time due to the absence of an intuitive interface and centralized management system.

This project aims to bridge this security gap by developing a cost-effective, hardware-based firewall using Raspberry Pi that integrates firewall functionalities, DNS-based ad-blocking, and an Intrusion Detection System (IDS). The system will provide real-time network traffic analysis, automatic threat detection, and a web-based dashboard for simplified management.

1.3 Motivation

With the rise in **cyber threats, intrusive ads, and network vulnerabilities**, traditional firewalls are often **complex, expensive, and lack integration**. Small businesses, home users, and educational institutions need an **affordable, easy-to-use, and powerful** security solution.

This project aims to develop a **hardware-based firewall** that combines **traffic control, intrusion detection, and ad blocking** into a single, **cost-effective, and scalable** system. By leveraging **Raspberry Pi and open-source tools**, we provide **enterprise-level security** with **simple management** through a web-based console.

Furthermore, this firewall solution is designed to be highly customizable, allowing users to define specific security policies based on their unique network requirements. With features such as deep packet inspection (DPI), real-time traffic monitoring, and automated threat detection, the system ensures proactive defence against cyber threats. The inclusion of ad blocking not only enhances security by preventing malicious advertisements but also improves browsing speed and user experience. By integrating these capabilities into a compact and energy-efficient Raspberry Pi-based setup, this project delivers an all-in-one security solution that is both powerful and accessible to non-technical users.

1.4 Proposed Solution

To address the challenges of **complex configuration, lack of integration, and high costs** in existing firewall solutions, we propose a **hardware-based firewall** using **Raspberry Pi**. This firewall will provide **real-time network security, traffic monitoring, and ad blocking** in an easy-to-use and cost-effective manner.

- **Integrated Security:** A Raspberry Pi-based firewall, DNS-based ad-blocking, and Intrusion Detection System (IDS), combined into a single, cost-effective solution for seamless protection.
- **Customizable Traffic Filtering:** Allows users to block or allow traffic based on IP addresses, domains, and Protocols, ensuring fine-grained control over network security.
- **Advanced Threat Protection:** Detects and mitigates cyber threats such as:

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks Brute-force attacks**
- **Man-in-the-Middle (MITM) attacks**
- **Active reconnaissance (port scanning, fingerprinting attempts, etc.)**
- **Ping of Death attack (excessively large ping packets used to crash systems)**
- **ARP Spoofing (malicious redirection of network traffic)**
- **Real-Time Monitoring & Alerts**
- **User-Friendly Web Interface (Centralized Web Console)**

1.5 Scope of a Project

This project aims to develop a **hardware-based firewall** using **Raspberry Pi**, integrating **traffic filtering, intrusion detection, and ad blocking** into a single cost-effective solution.

1. **Network Security Enhancement:**
   The firewall provides **advanced security** for **home networks, small businesses, and educational institutions** by monitoring and filtering network traffic.

2. **Traffic Control & Management:**
   It regulates network access, **blocks unauthorized traffic**, and prevents malicious activities such as **DDoS attacks, brute-force attempts, and phishing**.

3. **Intrusion Detection & Prevention (IDS/IPS):**
   Integrated **IDS** detects cyber threats and suspicious activities, ensuring real-time protection.

4. **Ad Blocking for Safer Browsing:**
   Pi-hole integration blocks unwanted ads, tracking, and malicious domains, improving privacy and network performance.

5. **Scalability & Customization:**
   Designed to **adapt to growing security needs**, the firewall allows users to modify filtering rules, IDS configurations, and logging mechanisms based on network requirements.

6. **Cost-Effective Alternative to Commercial Firewalls:**
   Provides **enterprise-level security features** at a fraction of the cost, making it an ideal solution for users with limited budgets.

7. **User-Friendly Web Interface:**
   A **Flask-based web dashboard** simplifies firewall rule configuration, monitoring, and security alerts for non-expert users.

8. **Real-Time Network Monitoring & Alerts:**
   Tracks live network traffic, **bandwidth usage, active connections, and security threats**, ensuring proactive threat mitigation.

9. **Cross-Platform Support:**
   Primarily designed for **Raspberry Pi**, but adaptable for **Linux-based** systems, making it a **versatile firewall solution**.

10. **Future Expansion Possibilities:**
    Potential future enhancements include **VPN support, AI-based threat detection, multi-network support, and cloud-based logging**.

Chapter 2
LITERATURE SURVEY

1. A New Method of Hardware Firewall Implementation on SOC

Authors: Saeed Ezzati, Hamid Reza Naji, Amir Chegini, Payam HabibiMehr

This research paper presents an FPGA-based hardware firewall designed to improve packet filtering efficiency, processing speed, and power consumption. Unlike traditional software-based firewalls, this hardware implementation leverages pipeline architecture and embedded memory to enhance performance.

The firewall classifies network packets using predefined security rules stored in FPGA memory, reducing latency and external memory access time. The design utilizes a Finite State Machine (FSM) to control packet processing, decision-making, and filtering. By implementing the system on ALTERA FPGA families (STRATIX III, CYCLONE III, CYCLONE II) and using VHDL programming, the researchers achieved lower power consumption and higher processing speed compared to existing architectures.

The study demonstrates that hardware-based firewalls outperform software-based solutions, particularly in high-speed network environments where real-time packet filtering is required. The proposed system offers scalability, flexibility, and security improvements by allowing dynamic firewall rule updates without modifying hardware components.

2. Visual Firewall: Real-time Network Security Monitor

Authors: Chris P. Lee, Jason Trost, Nicholas Gibbs, Raheem Beyah, John A. Copeland

This research paper introduces VisualFirewall, a tool designed to enhance firewall monitoring and intrusion detection through real-time visualization. The system provides four different views—Real-Time Traffic, Visual Signature, Statistics, and IDS Alarm—to help system administrators monitor network activity and detect threats more efficiently.

The paper highlights the challenges of firewall misconfigurations and overwhelming IDS logs, proposing a graphical approach to simplify traffic analysis and security monitoring. By integrating firewall logs, IDS alerts, and real-time network data, VisualFirewall helps users differentiate between normal and malicious traffic patterns. The system was implemented using Java, OpenGL (JOGL), and JFreeChart for portability and flexibility.

The study demonstrates that real-time visualization improves network security monitoring by allowing both experts and non-experts to quickly identify and respond to cyber threats such as DDoS attacks, port scans, and worm infections.

3. Critical Analysis on Web Application Firewall Solutions

Authors: Abdul Razzaq, Ali Hur, Sidra Shahbaz, Muddassar Masood, H. Farooq Ahmad

This research paper analyzes Web Application Firewall (WAF) solutions, focusing on their effectiveness in mitigating web-based security threats such as SQL injection, cross-site scripting (XSS), and zero-day attacks. The study highlights how traditional network firewalls are insufficient for protecting web applications, as most attacks target application-layer vulnerabilities.

The paper evaluates 15 different WAF solutions, including ModSecurity, Imperva SecureSphere, Barracuda, F5-Big IP, Web Sniper, Citrix WAF, and others. It compares them based on features like traffic monitoring, attack prevention, deep inspection, authentication, encryption support, and session protection.

The research finds that no single WAF provides complete security, as some lack zero-day attack protection, load balancing, or real-time monitoring.

The study concludes that a combination of WAFs and secure coding practices is essential for web application security. It also recommends customized WAF deployment based on an organization's specific requirements to achieve optimal protection.

4. A Firewall for Internet of Things

Authors: Naman Gupta, Srishti Sengupta, Vinayak Naik

This research paper presents a firewall solution for securing IoT devices in a home network environment. The study highlights the growing concerns of privacy and security in IoT systems, where devices often communicate with cloud databases over the internet, making them vulnerable to attacks like packet sniffing, unauthorized access, and DDoS attacks.

To address these threats, the authors propose a cost-effective, open-source firewall implemented on a Raspberry Pi. The firewall is configured to:

- Filter network traffic using iptables rules.
- Enable NAT and packet tracking to monitor device behavior.
- Prevent MITM attacks by blocking ICMP redirects.
- Mitigate DDoS threats using TCP SYN cookies and traffic profiling.

The paper also discusses case studies on IoT vulnerabilities, including Mirai malware attacks, and suggests using whitelisting techniques to block unauthorized traffic.

Future work includes enhancing traffic profiling and deploying multiple firewalls to improve .

5. Modeling and Management of Firewall Policies

Authors: Ehab S. Al-Shaer and Hazem H. Hamed, DePaul University

This research paper presents a rule management framework aimed at simplifying firewall policy administration and minimizing misconfigurations. Unlike traditional manual approaches, this system leverages automated techniques to detect policy anomalies and conflicts, ensuring improved security and efficiency.

The framework utilizes advanced algorithms to analyze firewall filtering rules, automatically identifying inconsistencies and potential vulnerabilities. By providing

structured rule organization and conflict resolution, the system reduces the complexity of rule management while maintaining policy integrity. The proposed solution is implemented in a user-friendly tool called "Firewall Policy Advisor," which enables seamless rule insertion, modification, and removal without introducing security risks. The study demonstrates that automated firewall rule management significantly reduces human error, enhances policy accuracy, and strengthens network security. The proposed system offers scalability, flexibility, and reliability by enabling anomaly-free policy editing while streamlining firewall administration.

6. Firewall Security: Policies, Testing and Performance Evaluation
Authors:Michael R. Lyu and Lorrien K. Y. Lau

This research paper explores the relationship between firewall security levels and system performance in distributed environments. Unlike conventional assumptions that higher security leads to lower performance, this study systematically evaluates the impact of varying firewall security levels on transaction time and latency.

The study formulates, designs, implements, and tests seven distinct firewall security levels under controlled experimental conditions. Performance metrics are analyzed phase by phase, comparing the trade-offs between security enhancements and network efficiency. The results indicate that increased security does not always correspond to reduced performance; significant impacts are observed only in specific scenarios.

The findings challenge the traditional security-performance trade-off assumption, offering insights into optimizing firewall configurations for both protection and efficiency. This research provides a structured approach for organizations to balance security and performance, ensuring an optimal firewall setup tailored to their operational needs.

7. Firewall Policy Queries
Authors: Alex X. Liu, Member, IEEE, and Mohamed G. Gouda, Member, IEEE

This research paper presents an efficient firewall query processing framework designed to assist administrators in analyzing and managing firewall policies. Unlike traditional manual inspections, this approach leverages a structured query language and algorithmic processing to enhance accuracy and efficiency.

The study introduces the Structured Firewall Query Language (SFQL), an SQL-like language specifically designed for describing firewall queries. It also establishes the Firewall Query Theorem as the theoretical foundation for query processing. The proposed system utilizes decision diagrams as its core data structure, enabling efficient query execution and optimization. Additionally, the framework supports operations such as union, intersection, and subtraction on query results.

Experimental results demonstrate that the firewall query processing algorithm significantly improves policy analysis, processing queries in under 10 milliseconds for firewalls with up to 10,000 rules. The proposed system enhances security by detecting policy errors, preventing misconfigurations, and ensuring firewall rules effectively safeguard private networks.

8. Enhancing Windows Firewall Security Using Fuzzy Reasoning
Authors: Nitin Naik and Paul Jenkins

This research paper presents an enhanced Windows Firewall designed to improve network traffic monitoring and analysis using a fuzzy reasoning approach. Unlike the standard Windows Firewall, which primarily relies on basic inbound and outbound

rule filtering, this enhanced version provides advanced detection and prevention capabilities.

The proposed system integrates fuzzy logic to analyze network traffic patterns, allowing for the identification of complex attack scenarios beyond simple rule-based filtering. A simulated ICMP flooding attack demonstrates the limitations of default firewall rules, whereas the enhanced firewall successfully detects and mitigates such threats. Additionally, the system can be extended to prevent other denial-of-service attacks, including TCP and UDP flooding.

Experimental results show that incorporating fuzzy reasoning significantly improves firewall effectiveness, making it a more robust security tool for Windows users. The proposed enhancement increases the firewall's adaptability, enabling real-time threat detection and improved network protection.

9. Next Generation Firewall for Network Security: A Survey

Authors: Kishan Neupane*, Rami Haddad*, Lei Chen

This research paper presents a comprehensive survey of traditional and next-generation firewalls (NGFWs), analyzing their functionalities, advantages, and role in modern network security. Unlike conventional firewalls that rely on predefined rules for traffic filtering, NGFWs incorporate advanced security mechanisms to counter emerging cyber threats.

The study explores various technologies integrated into NGFWs, including deep packet inspection, intrusion prevention systems (IPS), and application-aware filtering. A comparative analysis highlights the limitations of traditional firewalls in addressing sophisticated attacks such as botnets and targeted intrusions. Additionally, the paper discusses primary network security goals, emerging threats, and potential solutions for enhancing firewall effectiveness.

Findings indicate that organizations must adopt next-generation firewalls to strengthen their security posture, offering proactive protection against evolving cyber threats. The proposed insights emphasize the need for continuous firewall advancements to safeguard networks against modern attack vectors.

10. Vulnerabilities in Personal Firewalls Caused by Poor Security Usability

Authors: Bander Alfayyadh, James Ponting, Mohammed Alzomai, Audun Jøsan

This research paper examines the usability challenges of personal firewalls and their impact on overall IT security. While personal firewalls serve as a crucial defense mechanism against cyber threats, their effectiveness is often compromised by poor usability, making them difficult for non-expert users to manage correctly.

The study employs a cognitive walkthrough approach to evaluate the design of personal firewall systems, identifying elements that violate established usability principles. Findings highlight that many security vulnerabilities stem from user errors, misconfigurations, and a lack of intuitive design. The research emphasizes the need for improved user-friendly firewall interfaces that minimize complexity while maintaining robust security.

Recommendations for enhancing personal firewall usability are provided, including better guidance, automation, and simplified configuration options. The paper concludes by suggesting future research directions to improve the usability of security tools and reduce user-induced vulnerabilities in network protection system

Chapter 3

METHODOLOGY

3.1 Block Diagram for Proposed Solution

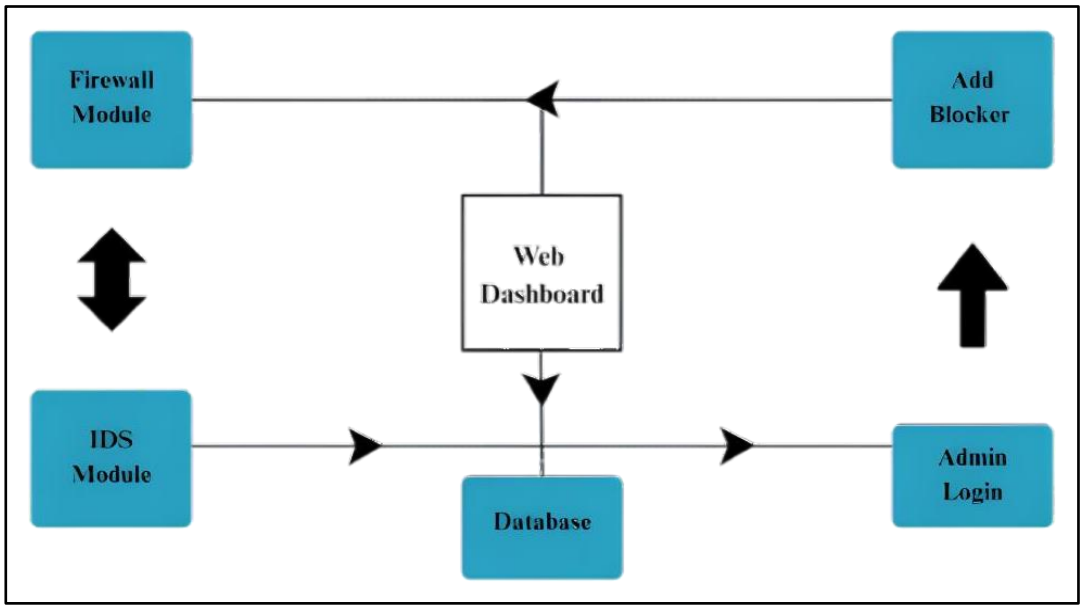


Fig no: 01 **(Block Diagram)**

Description:

The given diagram represents the architecture of a Raspberry Pi-based hardware firewall system, integrating multiple security components for comprehensive network protection. At the core of the system is the Web Dashboard, which serves as the centralized interface for managing firewall rules, intrusion detection alerts, and ad-blocking functionalities. The Firewall Module is responsible for monitoring and filtering network traffic, ensuring that only legitimate data packets are allowed while blocking suspicious or unauthorized connections. The IDS (Intrusion Detection System) Module actively analyzes network traffic patterns to detect and prevent cyber threats such as Denial of Service (DoS) attacks, malware, and unauthorized access attempts. These modules work in tandem, with the IDS providing real-time alerts and insights that can be acted upon by the firewall to strengthen security measures.

A Database component is included in the architecture to store logs, security events, and user-defined rules, ensuring persistent data availability for analysis and reporting. The Admin Login module grants authorized users access to the system, allowing them to configure security policies, monitor traffic, and review threat reports through the web-based interface.

The Ad Blocker module enhances security and user experience by preventing malicious advertisements and reducing unwanted network traffic. The entire system is designed to be highly interactive and efficient, allowing users to manage network security seamlessly through a simple yet powerful web dashboard.

1. Web Dashboard (Central Component)

- Acts as the main interface for managing and monitoring different security modules.
- Facilitates interaction between modules and the database.

2. Firewall Module (Top Left)

- Helps in filtering incoming and outgoing network traffic based on security rules.
- Connected to the Web Dashboard, allowing monitoring and control.
-

3. Add Blocker (Top Right)

- A module designed to block advertisements, potentially preventing malicious ads from affecting the system.
- Interacts with the Web Dashboard for management.

4. IDS Module (Bottom Left)

- Intrusion Detection System (IDS) monitors network traffic for suspicious activities.
- Sends data to the Web Dashboard and interacts with the Database.

5. Admin Login (Bottom Right)

- Allows authorized administrators to log in and access the system.
- Interacts with the Web Dashboard for authentication and control.

6. Database (Bottom Centre)

- Stores logs, user credentials, security data, and settings.
- Interacts with the Web Dashboard, IDS Module, and Admin Login.

The database component in our firewall architecture ensures persistent storage of critical data such as traffic logs, security events, and user-defined firewall rules, enabling comprehensive analysis, historical tracking, and report generation. It serves as the backbone for maintaining system intelligence and supporting data-driven decision-making.

3.2 Functional & Non-Functional Requirements

Functional Requirement

The firewall must filter and control network traffic using iptables/nftables, allowing or blocking access based on IP, port, protocol, and domain rules. It should integrate an Intrusion Detection System (IDS) using Snort/Suricata to detect and log cyber threats like DoS and brute-force attacks. A DNS-based ad-blocking module (Pi-hole) must prevent ads and malicious domains. The system should provide real-time monitoring and logging through a Flask-based web dashboard, allowing administrators to view network activity, security alerts, and manage firewall rules. User authentication and role-based access must be implemented for secure configuration. Additionally, the solution should be optimized for scalability and performance, ensuring low resource consumption while maintaining high efficiency on Raspberry Pi.

The firewall system should support automated rule updates to adapt to evolving security threats, ensuring dynamic protection without manual intervention. It must include logging and reporting capabilities that generate detailed insights into network traffic, detected threats, and blocked connections. Additionally, the system should allow administrators to create scheduled security scans and automated responses to identified threats, such as temporarily blocking suspicious IPs or notifying administrators of potential risks via email or dashboard alerts.

Non-Functional

The firewall must be fast, reliable, and secure, ensuring low-latency traffic filtering and efficient resource usage on Raspberry Pi. The web dashboard should be responsive and user-friendly, with secure authentication to prevent unauthorized access. The system must be scalable for future upgrades like cloud monitoring and AI-driven threat detection. It should also provide real-time logging and alerts for network anomalies while maintaining lightweight performance.

The solution should be designed with fault tolerance and minimal downtime, ensuring continuous network security even in case of failures or updates. Backup and restore functionalities should be implemented to safeguard firewall rules, IDS configurations, and system logs. Moreover, the system should adhere to cybersecurity best practices, incorporating encryption for sensitive data, secure API communication, and periodic security updates to protect against emerging vulnerabilities.

The firewall solution must be optimized for speed, reliability, and security, ensuring low-latency traffic filtering and efficient resource utilization on Raspberry Pi. The web dashboard should be responsive, user-friendly, and secured with strong authentication to prevent unauthorized access.

3.3 Specific Requirements

1. Hardware Components

a) Raspberry Pi 3B

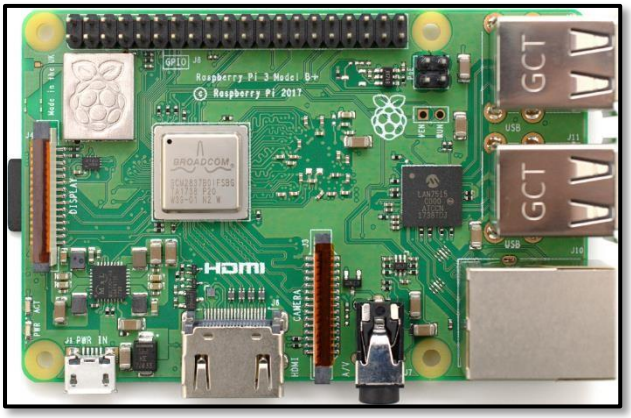


Fig no: 02 **(raspberry Pi 3B)**

The **Raspberry Pi 3B+** is a compact, powerful **single-board computer** designed for a wide range of applications, from DIY projects to IoT and cybersecurity solutions.

Key Specifications:

- **Processor:** 1.4GHz 64-bit Quad-Core ARM Cortex-A53 (Broadcom BCM2837B0)
- **RAM:** 1GB LPDDR2 SDRAM
- **Networking:**
  - ❖ Gigabit Ethernet (via USB 2.0, max ~300 Mbps)
  - ❖ 2.4GHz & 5GHz Dual-Band Wi-Fi (802.11 b/g/n/ac)
  - ❖ Bluetooth 4.2 / BLE
- **Ports & Connectivity:**
  - ❖ 4 × USB 2.0 ports
  - ❖ HDMI output
  - ❖ 3.5mm audio jack
  - ❖ CSI (Camera Serial Interface) and DSI (Display Serial Interface)
  - ❖ GPIO (40-pin header for hardware interfacing)
- **Storage:** MicroSD card slot for OS and storage
- **Power:** 5V/2.5A micro-USB power supply

The **Raspberry Pi 3B+** is ideal for projects like **firewalls, IoT devices, network monitoring, and embedded computing**, making it a great choice for **cost-effective and scalable solutions**.

The **Raspberry Pi 3B+** is a versatile and cost-effective **single-board computer** that balances performance, connectivity, and energy efficiency. Designed for hobbyists, developers, and professionals, it serves as an excellent platform for embedded systems, automation, and cybersecurity applications. With its compact size and extensive community support, the Raspberry Pi 3B+ has become a popular choice for educational purposes, DIY electronics, and low-power computing solutions.

b) USB To Ethernet Adapter

Fig no: 03 **(Ethernet Adapter)**

A **USB to Ethernet adapter** is a device that allows a computer or single-board computer (like a Raspberry Pi) to connect to a wired network via a USB port. It is commonly used when a built-in Ethernet port is unavailable or when additional network interfaces are required.

This adapter is a crucial component for **enhancing wired network connectivity**, especially in **firewall projects, IDS/IPS systems, and IoT applications** where reliable and stable network access is essential.

The image shows a **UGREEN USB to Ethernet adapter**, a compact and efficient networking device designed to provide **wired internet connectivity** to devices that lack an Ethernet port. This adapter features a **USB 3.0 connector** on one end and an **RJ45 Ethernet port** on the other, allowing users to establish a high-speed and stable network connection. It is particularly useful for laptops, ultrabooks, Raspberry Pi, and other devices that rely on wireless connectivity but require a **faster and more reliable wired connection** for tasks such as online gaming, video streaming, and large file transfers.

This adapter supports **Gigabit Ethernet speeds (up to 1000 Mbps)**, ensuring seamless data transmission with minimal latency. The built-in **LED indicators** labeled "ACT" and "LINK" help users monitor network activity and connection status in real time. Its **plug-and-play compatibility** with Windows, macOS, Linux, and even Raspberry Pi makes it a versatile solution for users who need quick and hassle-free networking. The **durable and lightweight** design makes it easy to carry, making it an excellent addition for professionals who work in different network environments.

One of the key advantages of using this adapter with a **Raspberry Pi-based firewall project** is that it enables dual Ethernet interfaces, which is essential for setting up **network filtering, intrusion detection, and traffic monitoring**.

2. Software Components

a. Ad Blocker

Fig no: 04 **(Adblocker graph)**

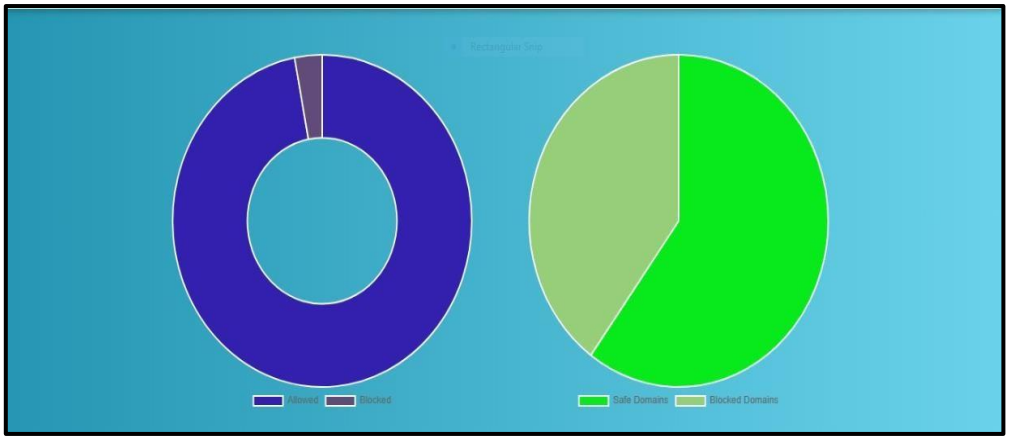


Fig no: 05**(Adblocker pie charts)**

The **Ad Blocker** in our firewall project **operates at the network level** using the **DNS Sinkhole technique** to block ads, pop-ups, and YouTube ads. It intercepts DNS requests and redirects known ad-serving domains to a **non-routable IP**, preventing ads from loading.

- When a user visits a website, their device sends a DNS request to resolve domain names (e.g., ads.example.com).
- Our custom DNS server (running on Raspberry Pi) intercepts these requests.
- If the request is for a known ad-serving domain, it is redirected to a sinkhole (a non-routable IP), effectively blocking the ad.
- If the request is for a legitimate website, it is forwarded to the correct DNS server for resolution.
- This method ensures that ads are blocked at the source, leading to faster browsing, reduced data usage, and enhanced privacy.

The Ad Blocker in our firewall project operates at the network level using the DNS Sinkhole technique to block ads, pop-ups, tracking scripts, and even YouTube ads across all connected devices. By intercepting DNS requests on the Raspberry Pi's custom DNS server, known ad-serving.

b. Firewall Rules

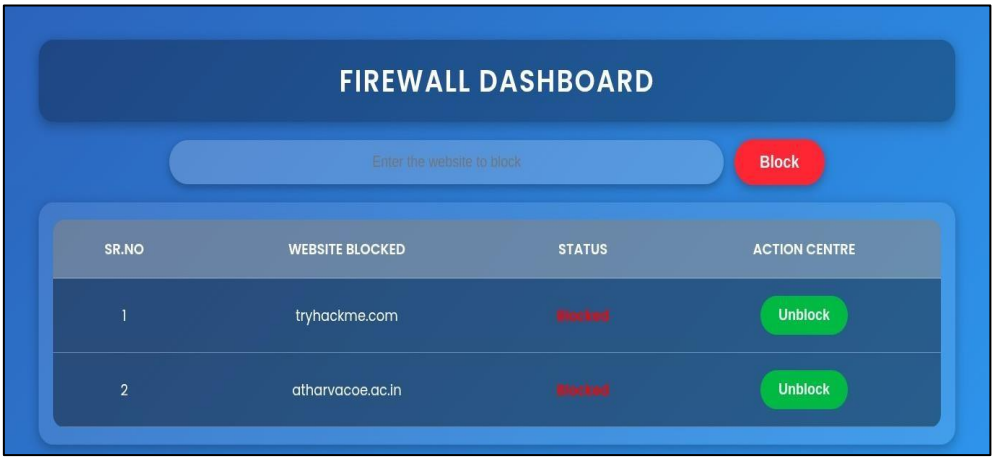


Fig no: 06 **(Firewall Dashboard)**

The firewall in our project **regulates network traffic** by enforcing **custom-defined security rules** to **allow or block specific connections** based on IP, domain, and protocol. It acts as a **first line of defense** against unauthorized access and cyber threats.
A firewall operates by **monitoring, filtering, and controlling incoming and outgoing network traffic** based on predefined security rules. In our project, the firewall is implemented using **iptables** on a Raspberry Pi, allowing us to **enforce traffic filtering, restrict unauthorized access, and mitigate cyber threats** effectively. The rules define what type of network traffic should be allowed or blocked based on specific conditions.

- **IP & Domain-Based Filtering** – Blocks or allows traffic from specific IP addresses or domain names.
- **Protocol-Based Rules** – Controls access to services like HTTP, HTTPS, SSH, DNS, and more.
- **Port Restrictions** – Prevents unauthorized use of open ports to stop malicious activity.
- **DoS & Brute-Force Prevention** – Detects excessive connection attempts and **limits traffic** from suspicious sources.
- **Blocking Unauthorized Packet Forwarding:** Prevents attackers from intercepting and modifying network traffic.
- **Detecting ARP Spoofing:** The firewall checks for abnormal changes in ARP (Address Resolution Protocol) tables to prevent MITM attacks.
- **Real-Time Packet Logging:** Captures details of all blocked and allowed connections for security analysis.
- **Log Storage for Traffic Analysis:** All detected anomalies and security events are saved in log files, which can be analyzed later using **Wireshark**.
- **Protocol-Based Filtering:** Controls access to different network services such as HTTP (web browsing), HTTPS (secure browsing), SSH (remote access), FTP (file transfer), and DNS (domain resolution).
- **IP-Based Filtering:** Blocks or allows traffic from specific IP addresses (both incoming and outgoing).
- **Restricting Access to Specific IPs:** Limits access to critical services, such as SSH, to only trusted IP addresses to prevent unauthorized remote access.

c. Intrusion Detection System

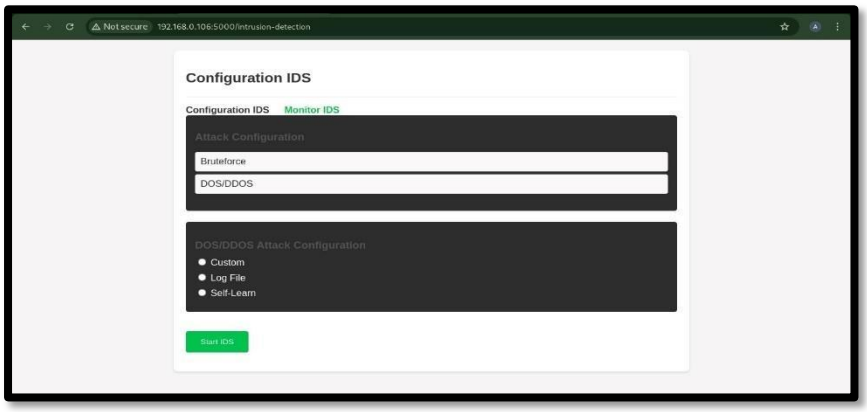


Fig no: 07 **(Intrusion detection system)**

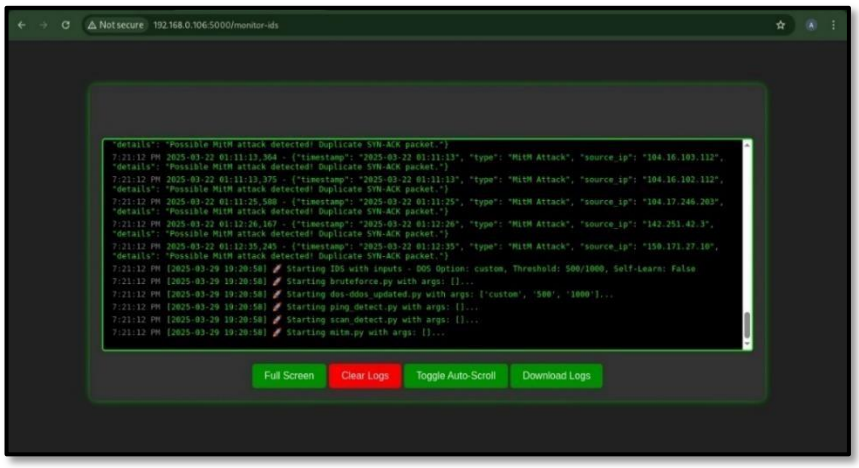


Fig no: 08 **(Intrusion Detection System Dashboard)**

The **Intrusion Detection System (IDS)** in our firewall is designed to **monitor, analyse, and detect suspicious network activities** in real time. It acts as a **security surveillance system** that identifies potential cyber threats and alerts administrators to take action before damage occurs.

- **Denial of Service (DoS/DDoS) Attacks** – Detects excessive traffic (10,000+ requests/sec) from a single source.
- **Brute Force Attacks** – Monitors repeated login attempts (10-15 attempts per minute).
- **Man-in-the-Middle (MITM) Attacks** – Detects unauthorized interception of network traffic.
- **Active Reconnaissance** – Identifies unauthorized scanning or probing of network ports.
- **Ping of Death** – Detects oversized ICMP packets used to crash systems.
- **ARP Spoofing** – Identifies fake ARP responses to prevent unauthorized access
- **Suspicious Payload Signatures** – Analyses packet payloads for known malware patterns, exploit attempts, or injection scripts.
- **Unauthorized Protocol Use** – Detects unexpected or unapproved protocols (e.g., SSH, Telnet) in environments where they shouldn't be used.
- **Data Exfiltration Attempts** – Identifies abnormal outbound traffic patterns that may indicate sensitive data is being leaked.
- **Zero-Day Exploit Behaviour** – Through anomaly detection, the IDS flags previously unknown attack patterns based on unusual network activity.

Chapter 4

DESIGN

4.1. Architectural Design

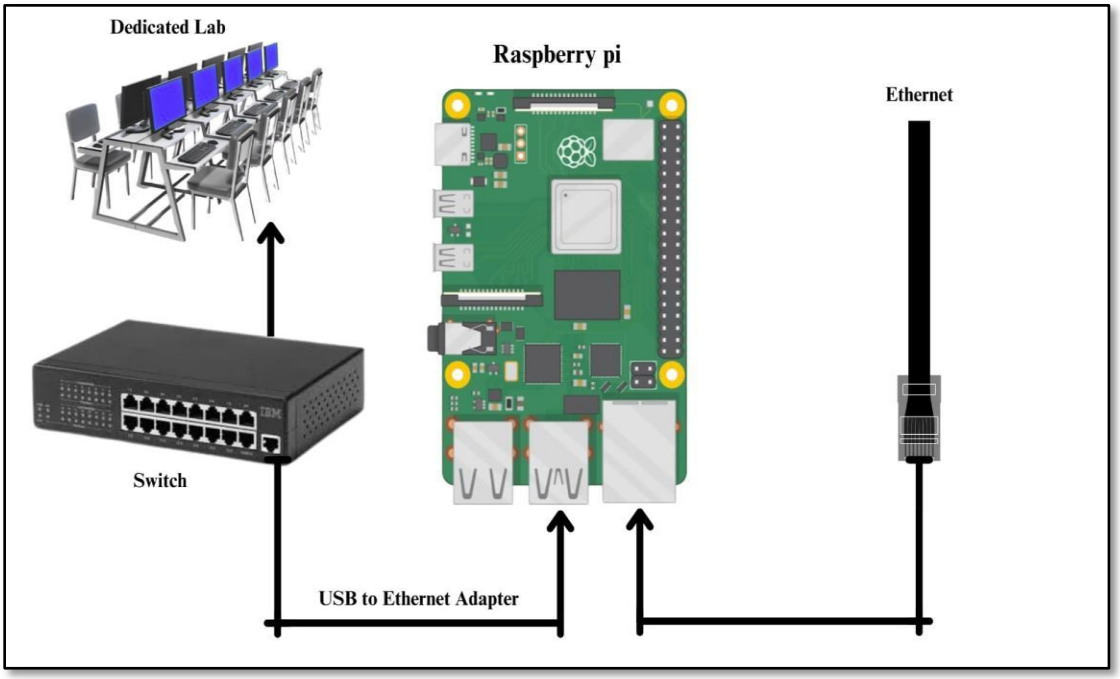


Fig no: 09 **(Design)**

Connections

1. **Internet**

- Raspberry Pi (Ethernet Port): The Pi is connected to the internet via an Ethernet cable, receiving external traffic.
- The internet enters the **Raspberry Pi first**, ensuring all incoming and outgoing traffic passes through security filtering before reaching the lab computers.

2. **Raspberry Pi**

- The **Raspberry Pi** is the **core** of this security system, implementing the firewall, IDS, and ad blocker. It has two key network interfaces:

- Switch (USB to Ethernet Adapter): A USB-to-Ethernet adapter connects the Pi to a network switch, allowing it to filter traffic.
- Acts as the second network interface to forward filtered traffic to the switch.

3. Secure Access for Lab Computers

- The lab computers now receive **only safe and authorized** network access.
- Any blocked requests (malicious sites, unwanted domains, or unauthorized access attempts) **will not be forwarded** to the lab.

4.2. Comparison with Existing system

1. Existing Solution

a) **Complexity in Configuration**: Existing firewalls like pfSense and OpenWRT require technical expertise, making them hard for small businesses and home users. Misconfiguration risks can lead to security vulnerabilities or loss of internet access.
b) **Lack of Integration:** Firewalls, IDS, and ad blockers work separately, creating security gaps and inefficiencies. Logs and alerts are scattered, making unified threat monitoring difficult.
c) **High Costs**: Enterprise security tools are costly, while cheaper alternatives lack advanced features. Licensing fees and hardware requirements add to the total cost of ownership.
d) **Limited Threat Detection:** Standard firewalls only filter packets but fail to detect modern threats like DoS and MITM attacks. Many systems lack anomaly-based detection and AI-driven analysis.
e) **No Real-Time Traffic Insights:** Users cannot see live network activity, making it hard to detect intrusions or unusual traffic. Delayed log access limits timely response to threats.
f) Most open-source tools prioritize functionality over usability. Cluttered or outdated interfaces confuse users.
g) **HardwareLimitations:** Many home users rely on outdated or underpowered hardware. Existing firewall solutions may require x86 machines with high resource demands.

2. Proposed Solution

a) **Integrated Security:** A Raspberry Pi-based firewall, DNS-based ad-blocking, and Intrusion Detection System (IDS), combined into a single, cost-effective solution for seamless protection.
b) **Customizable Traffic Filtering:** Allows users to block or allow traffic based on IP addresses, domains, and protocols, ensuring fine-grained control over network security.
c) **Advanced Threat Protection:** Detects and mitigates cyber threats such as:

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks Brute-force attacks**
- **Man-in-the-Middle (MITM) attacks**
- **Active reconnaissance (port scanning, fingerprinting attempts, etc.)**
- **Ping of Death attack (excessively large ping packets used to crash systems)**
- **ARP Spoofing (malicious redirection of network traffic)**
- **Real-Time Monitoring & Alerts**
- **User-Friendly Web Interface (Centralized Web Console)**

4.3 working of the project

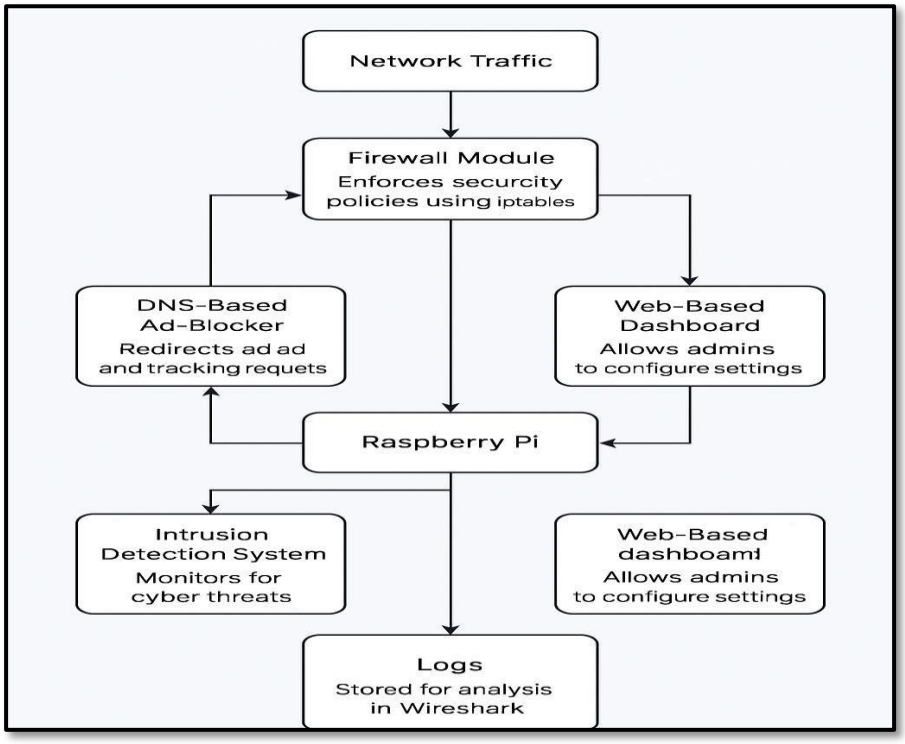


Fig no: 10 **(Working)**

Our project offers an integrated network security solution combining a **firewall, DNS-based ad-blocker (using the DNS Sinkhole concept), and an Intrusion Detection System (IDS)** on a single **Raspberry Pi**. It enhances security, blocks ads, and detects cyber threats while allowing administrators to analyze traffic using log files in **Wireshark**.

The **web-based dashboard** serves as a centralized control panel, allowing admins to configure **firewall rules, ad-blocking, and network monitoring** via the Raspberry Pi's IP. The **firewall module** enforces security policies using **iptables**, filtering traffic based on **IP, domain, and protocol**, while detecting threats like **active reconnaissance, Ping of Death, ARP spoofing, and MITM attacks**.

The **DNS-based ad-blocker** redirects ad and tracking requests to a sinkhole, blocking ads **at the DNS level** for a cleaner browsing experience. Administrators can manage **whitelisting and blacklisting of domains** via the web dashboard.

The **IDS continuously monitors network traffic** to detect attacks like **brute force, DoS, and MITM attacks**, storing logs for analysis using Wireshark. No database is used—**all detections are logged** for forensic study and security enhancements. The **USB-to-Ethernet adapter** ensures proper traffic filtering, making this solution suitable for both **wired and wireless networks**.

In conclusion, this Raspberry Pi-based firewall and IDS solution effectively strengthens network security by integrating custom firewall rules, a DNS Sinkhole-based ad blocker, and real-time intrusion detection into a single device. By leveraging log files for traffic analysis, security professionals can study network behavior, detect cyber threats, and improve security defenses using tools like Wireshark. This cost-effective and scalable solution ensures strong cybersecurity protection while maintaining ease of use and efficient network monitoring.

4.4 code of the main function of the project

1) App code

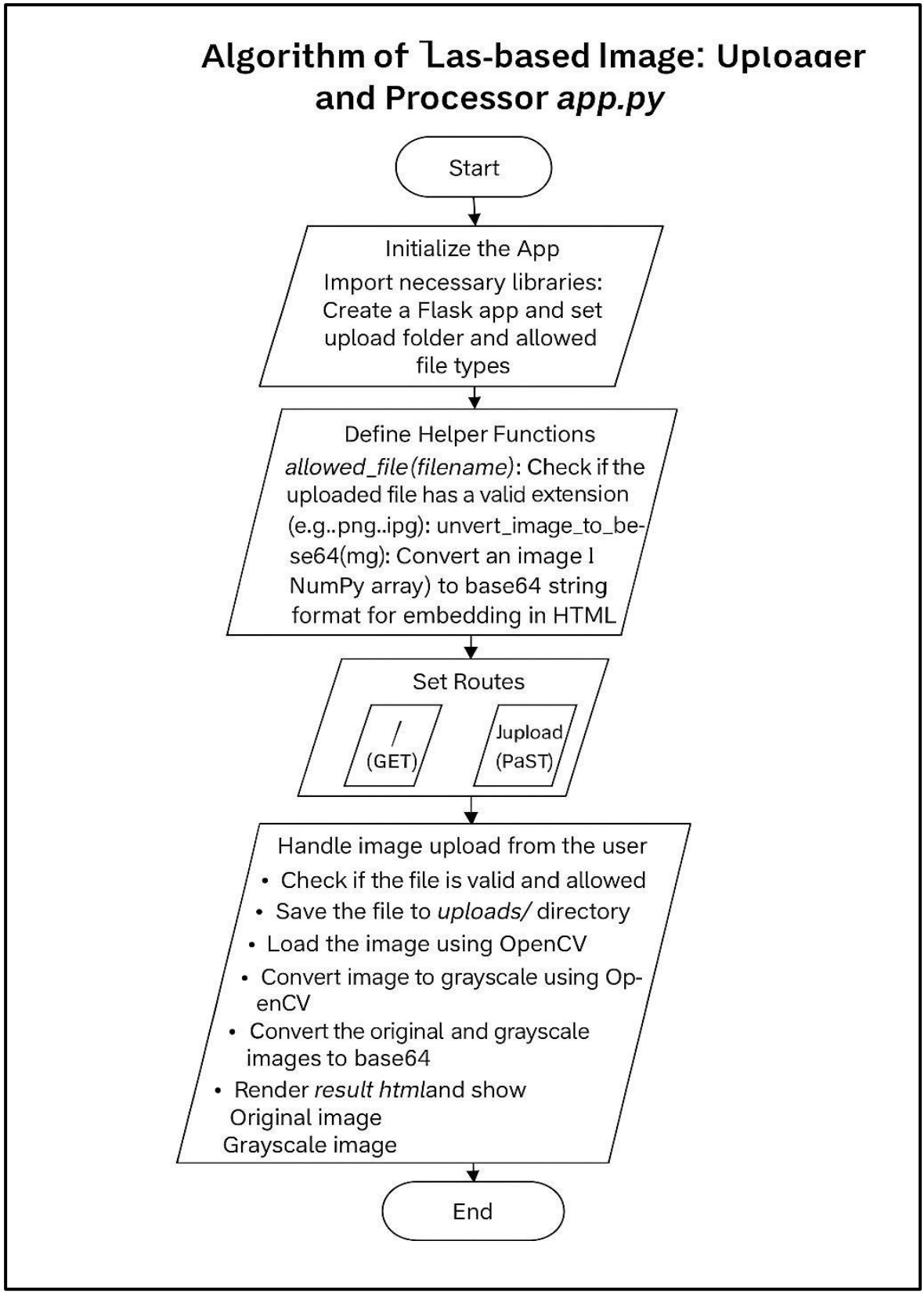


Fig no: 11 (**App algorithm**)

2) Index code

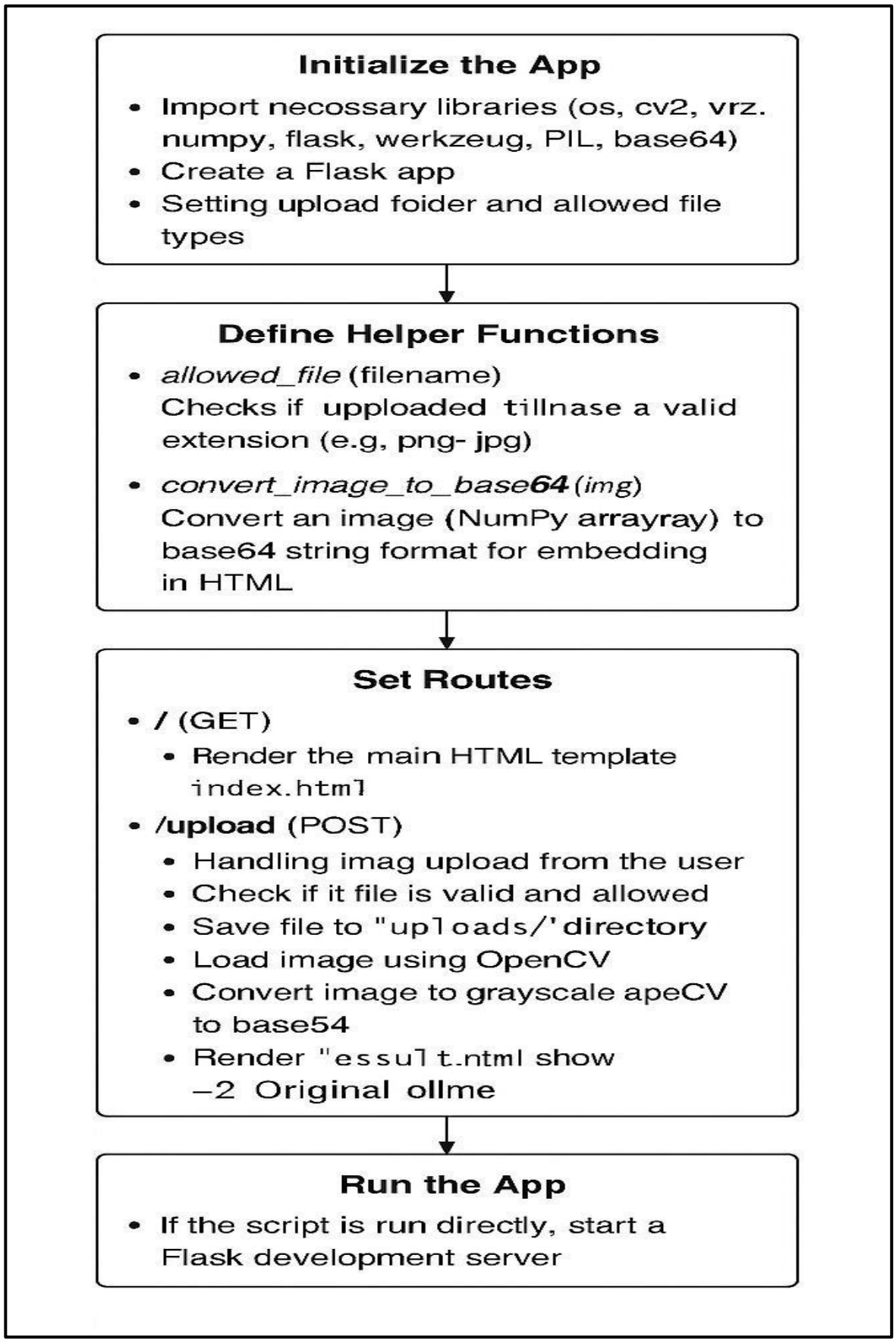


Fig no: 12(**Index algorithm**)

3) Adblocker code

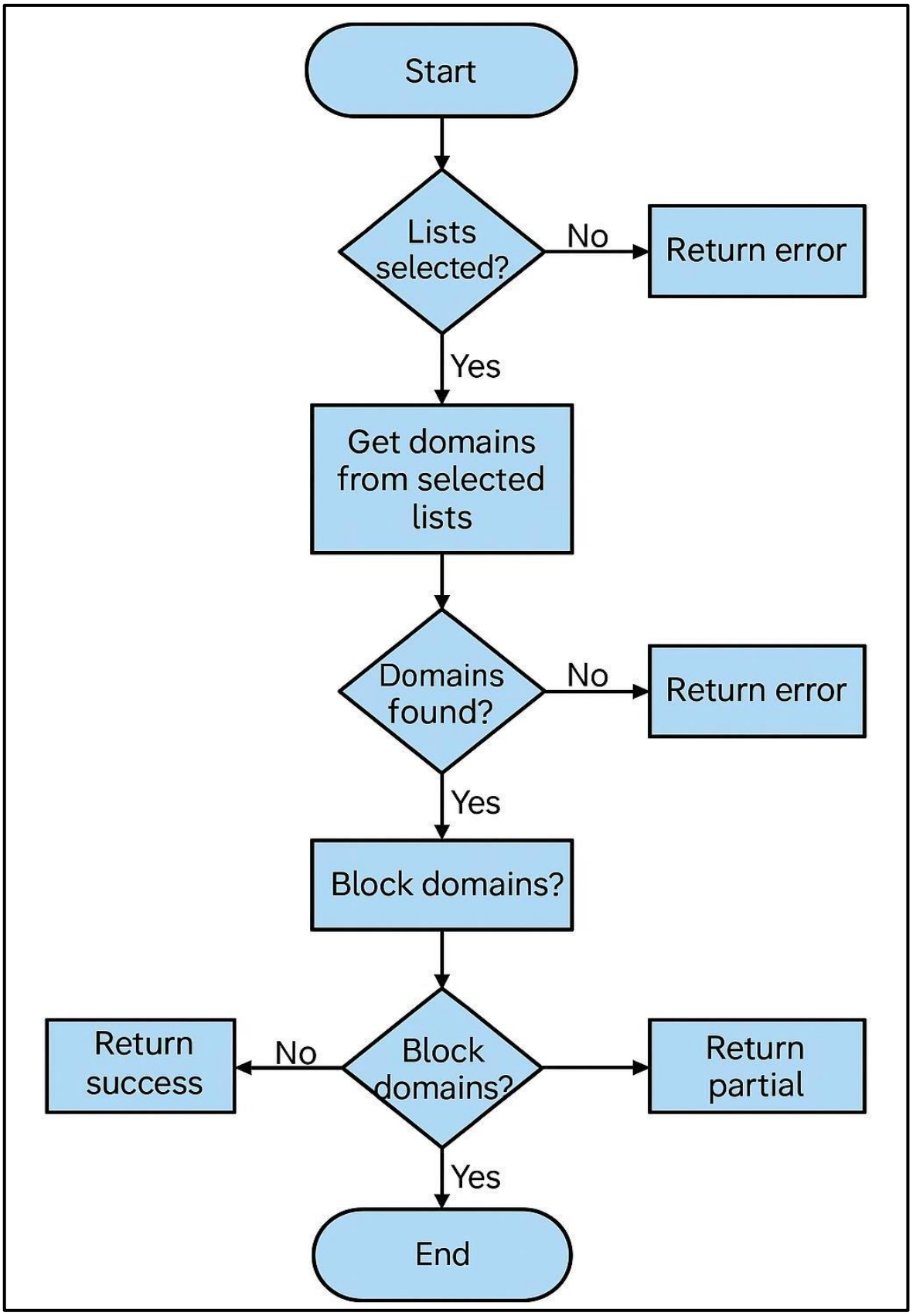


Fig no: 13(**Ad blocker algorithm**)

4) IDS code

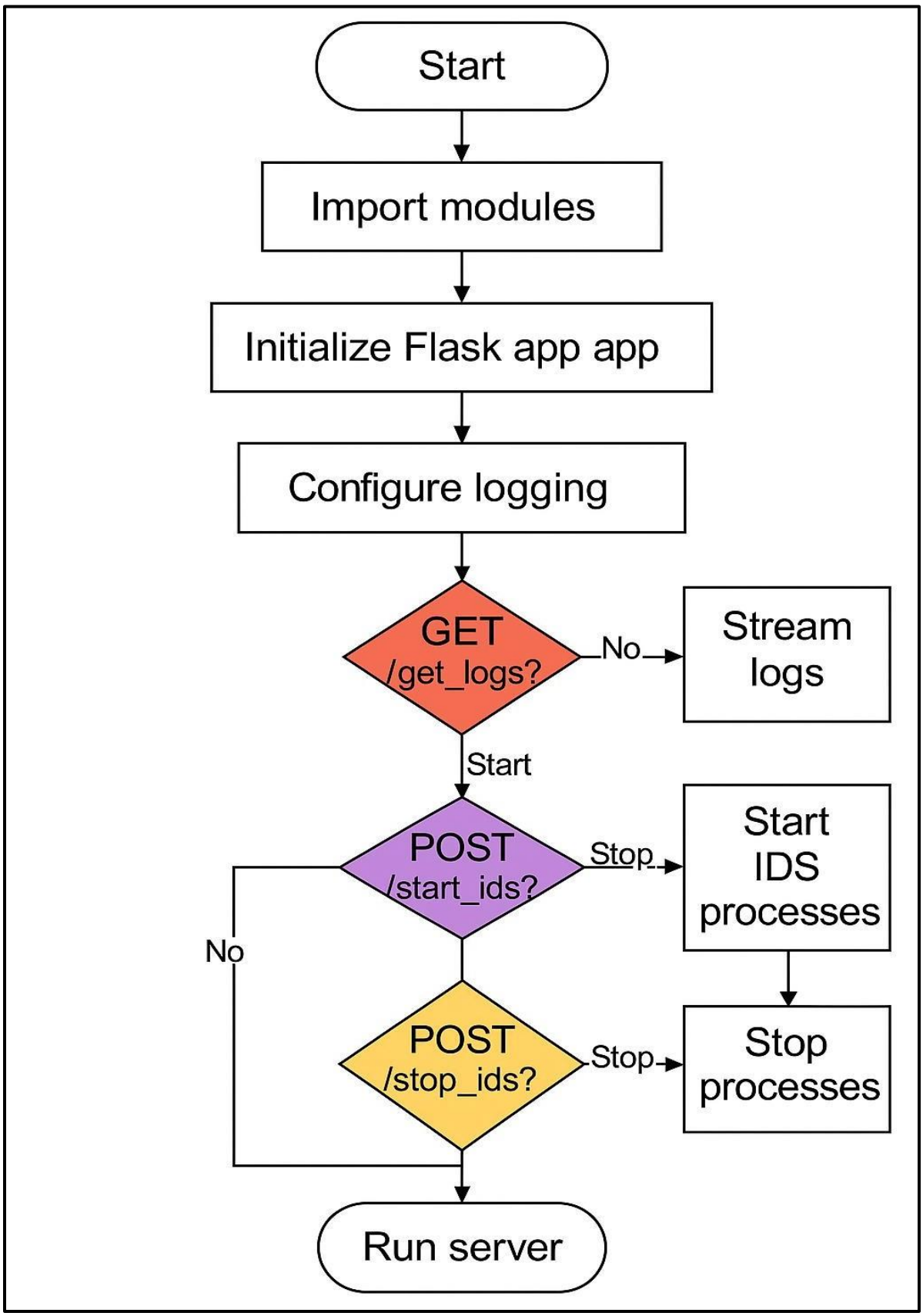


Fig no: 14 (**IDS algorithm**)

4.5 timeline chart of entire year

Week	Tasks
(July 8-12)	Finalizing the project idea: Developing a Raspberry Pi-based integrated cybersecurity system combining Firewall, IDS, and DNS Sinkhole-based Ad Blocker.
(July 15-19)	Studying cybersecurity threats: Researching DoS, brute-force, MITM, active reconnaissance, ARP spoofing, and Ping of Death attacks.
(July 22-26)	Understanding Raspberry Pi 3B+ and its networking capabilities.
(Aug 1-7)	Researching existing firewall solutions like iptables, IDS tools like Snort, and ad-blocking techniques using DNS sinkholes.
(Aug 5-9)	Designing high-level architecture and preparing an implementation roadmap.
(Aug 12-16)	Implementing custom firewall rules using iptables to block unauthorized traffic.
(Aug 19-23)	Developing a (CLI) for adding firewall rules like blocking IPs, domains, and specific ports.
(Aug 26-30)	Implementing basic network packet filtering to allow/block specific traffic.
(Sept 16-20)	Logging firewall events into log files (instead of a database) for further analysis in Wireshark.
(sept 30-4)	Enhancing **firewall filtering rules** to detect and prevent attacks like Dos/DDos
(oct 7-11)	**Brute-force attacks** (tracking failed login attempts).
(oct 14-18)	**MITM attacks** (detecting ARP poisoning attempts).
(oct 28-31)	Implementing **Intrusion Detection System (IDS)** to monitor network packets for suspicious activity.
(Nov 3-7)	Developing **real-time logging and alert generation** for detected threats.
(Nov 10-14)	implementing a **DNS Sinkhole-based ad-blocking system** to block unwanted ads, pop-ups, and YouTube ads.
(Nov 17-22)	Creating a **custom blacklist of ad-serving domains**.
(Jan 1- 4)	Testing the ad blocker against different websites and video platforms.

(Jan 7- 11)	Logging all blocked requests for analysis.
(Jan 14- 18)	Developing a **web-based centralized console** to manage firewall and IDS rules.
(Jan 21- 25)	Features of the dashboard: **Live traffic monitoring** with network activity graphs.
(Jan 28- 31)	**Firewall rule management** (adding, removing, modifying rules).
(Feb 5- 8)	**IDS alert visualization** (displaying detected threats).
(Feb 11- 16)	**Ad blocker settings** for managing domain blacklists.
(Feb 19- 24)	Implementing **secure authentication (Admin Login) to access the dashboard**.
(Feb 27)	Hardening the system security preventing unauthorized access, **Securing log files etc**
(March 2-6)	Enhancing **UI/UX of the web dashboard like 3d animation of raspberry pi** for better usability
(March 9-13)	Deploying the system on a **home/small business network** for real-time testing.
(March 16-20)	Monitoring **network performance** and **ad-blocking effectiveness**.
(March 23-25)	Adjust firewall rules dynamically
(March 26-29)	Analyze **firewall logs** using **Wireshark**.
(April 1-3)	Interpret **IDS alerts** and respond to threats
(April 7-11)	Gathering feedback and making **final adjustments**.
(April 13-15)	Begin User Testing & Feedback collection, Begin Preparing the Black Book
(April 16)	**Finalizing the project report** for submission.
(April 19)	Final Demo of Project in college Finalize the soft copy of Black book.
(April 20)	Finalize and Submit Research paper. Begin Preparing for Project Demonstration
(April 21-25)	Final presentation to external and internal

Table no :05 (**Timeline**)

Chapter 5

IMPLEMENTATION

5.1 Testing in Phases

1) Security Testing

Test Case	Expected Result
Try unauthorized dashboard access	Unauthorized users should be denied
Test SQL injection or XSS on the web console	The system should prevent injection attacks
Simulate network sniffing attempts	Simulate network sniffing attempts

Table no :06(Security Testing)

2) Integration Testing

Test Case	Expected Result
Simulate a normal internet connection	Devices behind the firewall should access the internet
Block specific IPs/websites	Blocked addresses should be inaccessible
Allow only specific applications (e.g., SSH, HTTP)	Only whitelisted applications should communicate

Table no :07I(ntegration Testing)

3) System Testing (End-to-End Functionality)

Test Case	Expected Result
Simulate an external attack (DoS, brute-force)	**Firewall should detect, log, and alert the admin**
Test firewall under network load	**It should function efficiently without crashing**
Verify role-based access for admin/user	**Only authorized users should modify firewall rules**

Table no :08(System Testing)

5.2 Types of Testing used:

a) Unit Testing

- Tests **individual components** like **iptables**, IDS (Snort/Suricata), and the web dashboard.
- Ensures that firewall rules, logging mechanisms, and traffic filtering work as expected.

b) Integration Testing

- Verifies the interaction between different modules (firewall, IDS, ad blocker, monitoring dashboard).
- Ensures that blocked sites remain inaccessible and that traffic logs are properly recorded.

c) System Testing

- **End-to-end** testing of the complete firewall setup.
- Tests internet access, rule enforcement, attack detection, and user management.

d) Performance & Load Testing

- Identifies vulnerabilities such as DoS, brute-force attacks, and SQL injections.
- Ensures unauthorized users cannot access or modify firewall settings.

e) Recovery & Failover Testing

- Simulates **system crashes, network failures, and power outages** to assess recovery mechanisms.
- Ensures **logs and security configurations persist** even after unexpected shutdowns or reboots.

f) False Positive & False Negative Testing

- Evaluates the accuracy of the Intrusion Detection System (IDS) in detecting real threats while minimizing false alerts.
- Tests how well the firewall differentiates between legitimate traffic and malicious activity, ensuring low false positives (blocking legitimate users) and low false negatives (failing to detect attacks).

g) Logging & Audit Testing

- Verifies that all critical events (e.g., blocked packets, intrusion attempts, rule changes) are **accurately logged**.
- nsures **log integrity**, proper timestamps, and that logs are **readable and compatible with analysis tools like Wireshark**.

Chapter 6

RESULT ANALYSIS & DISCUSSION

6.1 Result

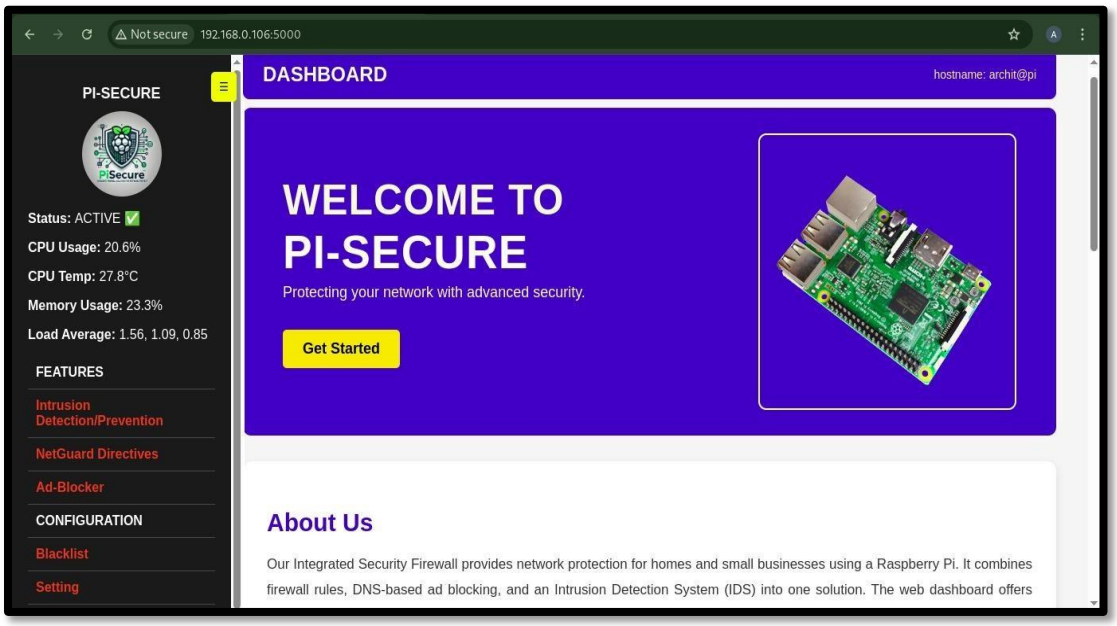


Fig no: 15(**Actual Dashboard**)

This is the **web-based dashboard** for the **PI-SECURE firewall system**, which integrates **firewall rules, an Intrusion Detection/Prevention System (IDS/IPS), a NetGuard module, and an Ad-Blocker** into a single Raspberry Pi security solution. The interface allows **network administrators** to monitor and configure network security settings.

1) Left Sidebar - System Status and Features

(A) System Status Panel (Live Monitoring)

This section provides real-time statistics of the Raspberry Pi firewall:

- **Status: ACTIVE** – Indicates that the firewall system is running.
- **CPU Usage: 20.6%** – Shows the current processor usage of the Raspberry Pi.
- **CPU Temperature: 27.8°C** – Displays the temperature of the CPU to prevent overheating.
- **Memory Usage: 23.3%** – Represents the RAM consumption, ensuring smooth operation.
- **Load Average: 1.56, 1.09, 0.85** – System load over different time intervals (1, 5, and 15 minutes). A lower value suggests the system is running efficiently.

(B) Features Panel (Security Modules)

The **PI-SECURE** system integrates multiple security mechanisms,

- Intrusion Detection/Prevention
- NetGuard Directives

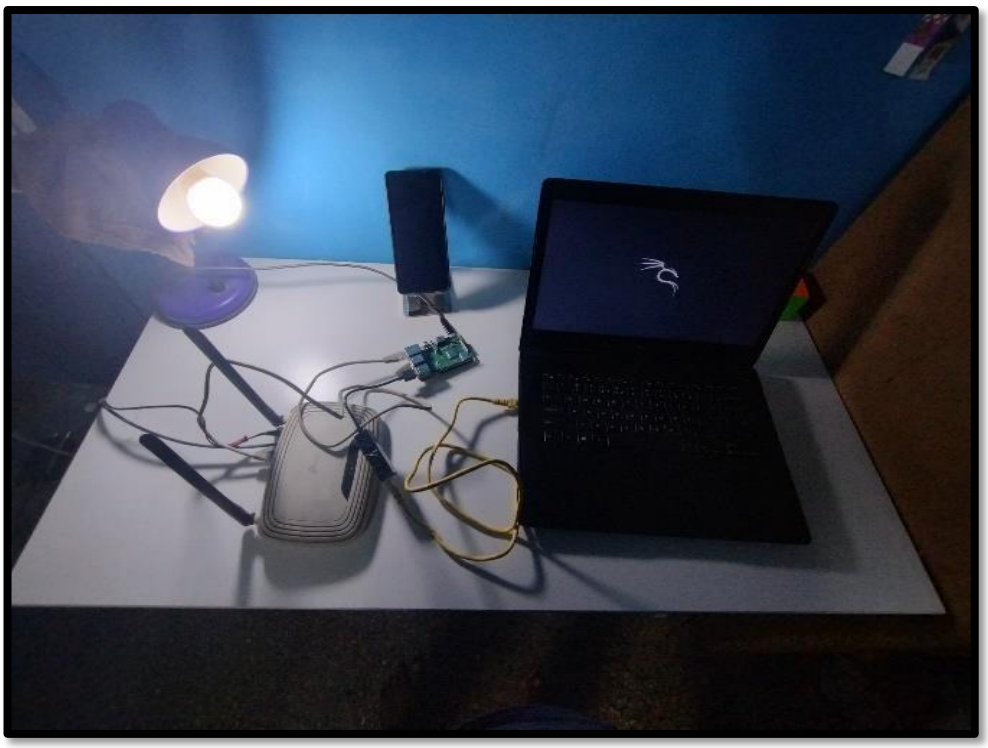


Fig no: 16(**Setup**)

Step-by-Step Connection Flow

I. Internet Source (ISP) → Wi-Fi Router

- The main internet connection originates from the Internet Service Provider (ISP).
- The ISP modem/router provides an internet connection via Ethernet or Wi-Fi.
- The router assigns IP addresses to connected devices via DHCP.
- It acts as a gateway between the local network and the external internet.

II. Wi-Fi Router → Raspberry Pi (Ethernet Connection)

- The Wi-Fi router's Ethernet port is connected to the Raspberry Pi's Ethernet port.
- This ensures that all internet traffic first reaches the Raspberry Pi firewall before going to other devices.
- The Raspberry Pi acts as a transparent bridge or NAT router to filter or inspect traffic.
- Static IP configuration may be used for consistent management and monitoring.

III. Raspberry Pi (Firewall) → USB-to-Ethernet Adapter

- Since Raspberry Pi has only one built-in Ethernet port, a USB-to-Ethernet adapter is used.
- The USB-to-Ethernet adapter is connected to the Raspberry Pi's USB port, adding an extra Ethernet interface.

IV. USB-to-Ethernet Adapter → Laptop (Ethernet Connection)

- The adapter's Ethernet port is connected to the laptop's Ethernet port.
- The laptop receives the filtered network traffic from the Raspberry Pi.

6.2 Advantages

- **Enhanced Security** - Hardware firewalls operate independently of the system they protect, making them less vulnerable to malware, viruses, or system failures,

- **Efficient Network Traffic Filtering** - Unlike software firewalls, hardware firewalls filter traffic before it reaches connected devices, reducing the risk of cyber threats such as unauthorized access, DoS attacks, and malware infiltration.

- **No Performance Impact on End Device**s - Since processing is handled externally, there is no strain on individual computers, unlike software firewalls that consume system resources.

- **Centralized Protection** - A single hardware firewall protects the entire network, eliminating the need for separate firewalls on each device.

- **Custom Firewall Rules** - Allows custom traffic filtering based on IP, domain, or protocol, providing tailored security configurations for businesses and home networks.

- **Intrusion Detection & Prevention** - Integrated IDS/IPS features help detect and mitigate cyber threats in real-time without relying on host-based security measures

6.3 Disadvantages

- **Complex Configuration** – Setting up and managing a hardware firewall **requires technical knowledge**, especially when defining firewall rules, IDS configurations, and network filtering settings.

- **Limited Flexibility** – Unlike software firewalls, which can be updated or customized with new features easily, **hardware firewalls have fixed capabilities** and may require hardware upgrades for additional functionality.

- **Single Point of Failure** – If the hardware firewall fails or crashes, **the entire network security could be compromised** unless a backup system is in place.

- **Device Dependency** – Since all network traffic must pass through the firewall, **a hardware failure could disrupt the entire network**, requiring immediate troubleshooting and replacement.

Despite these challenges, a hardware firewall remains one of the most effective security solutions for network protection, providing superior control, filtering, and intrusion prevention.

Chapter 7
References

1. Ali, M. Q., Al-Shaer, E., & Samak, T. (2014). Firewall Policy Reconnaissance: Techniques and Analysis. IEEE Transactions on Information Forensics and Security, 9(2), 296–308. doi:10.1109/tifs.2013.2296874
2. Liu, A. X., Torng, E., & Meiners, C. R. (2008). Firewall Compressor: An Algorithm for Minimizing Firewall Policies. IEEE INFOCOM 2008 - The 27th Conference on Computer Communications. doi:10.1109/infocom.2008.44
3. Liu, A. X., & Gouda, M. G. (2008). Diverse Firewall Design. IEEE Transactions on Parallel and Distributed Systems, 19(9), 1237–1251. doi:10.1109/tpds.2007.70802
4. Golnabi, K., Min, R. K., Khan, L., & Al-Shaer, E. (2006). Analysis of Firewall Policy Rules Using Data Mining Techniques. 2006 IEEE/IFIP Network Operations and Management Symposium NOMS 2006. doi:10.1109/noms.2006.1687561
5. Al-Haj, S., & Al-Shaer, E. (2011). Measuring firewall security. 2011 4th Symposium on Configuration Analytics and Automation (SAFECONFIG). doi:10.1109/safeconfig.2011.61116
6. Radoglou-Grammatikis, P., Sarigiannidis, P., Liatifis, T., Apostolakos, T., & Oikonomou, S. (2018). An Overview of the Firewall Systems in the Smart Grid Paradigm. 2018 Global Information Infrastructure and Networking Symposium (GIIS). doi:10.1109/giis.2018.8635747
7. Cobb, S. (n.d.). Establishing firewall policy. Southcon/96 Conference Record. doi:10.1109/southc.1996.53500
8. Acharya, H. B., Joshi, A., & Gouda, M. G. (2010). Firewall modules and modular firewalls. The 18th IEEE International Conference on Network Protocols. doi:10.1109/icnp.2010.5762766
9. Maldonado-Lopez, F. A., Calle, E., & Donoso, Y. (2015). Detection and prevention of 9)9)firewall-rule conflicts on software-defined networking. 2015 7th International Workshop on Reliable Networks Design and Modeling (RNDM). doi:10.1109/rndm.2015.7325238
10. Goddard, S., Kieckhafer, R., & Yuping Zhang. (n.d.). An unavailability analysis of firewall sandwich configurations. Proceedings Sixth IEEE International Symposium on High Assurance Systems Engineering. Special Topic: Impact of Networking. doi:10.1109/hase.2001.966815
11. Al-Shaer, E. S., Hamed, H. H. (2004). Modeling and Management of Firewall Policies. IEEE Trans- actions on Network and Service Management, 1(1), 2–10.
12. Lyu, M. R., Lau, L. K. Y. (n.d.). Firewall secu- rity: policies, testing and performance evaluation. Proceedings 24th Annual International Computer Software and Applications Conference. COMP- SAC2000.
13. Liu, A. X., Gouda, M. G. (2009). Firewall Policy Queries. IEEE Transactions on Parallel and Dis- tributed Systems, 20(6), 766–777.
14. Naik, N., Jenkins, P. (2016). Enhancing Windows Firewall Security Using Fuzzy Reasoning. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure

Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress
15. Neupane, K., Haddad, R., Chen, L. (2018). Next Generation Firewall for Network Security: A Sur- vey. SoutheastCon 2018.
16. Razzaq, A., Hur, A., Shahbaz, S., Masood, M., Ahmad, H. F. (2013). Critical analysis on web application firewall solutions. 2013 IEEE Eleventh International Symposium on Autonomous Decen- tralized Systems (ISADS).
17. Adao, P., Focardi, R., Guttman, J. D., Luccio, F.
18. L. (2016). Localizing Firewall Security Policies. 2016 IEEE 29th Computer Security Foundations Symposium (CSF).
19. Lee, C. P., Trost, J., Gibbs, N., Beyah, R., Copeland,
20. J. A. (n.d.). Visual firewall: real-time network secu- rity monitor. IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05).
21. Alfayyadh, B., Ponting, J., Alzomai, M., Josang, A. (2010). Vulnerabilities in personal firewalls caused by poor security usability. 2010 IEEE International Conference on Information Theory and Information Security.
22. Firkhan Ali Bin Hamid Ali. (2011). A study of technology in firewall system. 2011 IEEE Sym- posium on Business, Engineering and Industrial Applications (ISBEIA).
23. Abdul Aziz, M. Z., Ibrahim, M. Y., Omar, A. M., Ab
24. Rahman, R., Md Zan, M. M., Yusof, M. I. (2012). Performance analysis of application layer firewall. 2012 IEEE Symposium on Wireless Technology

RESEARCH PAPER

Pisecure: Integrated Firewall solution for Network Protection

Sakshi Aghav
EXTC Department
Atharva College of engineering
Mumbai,India
aghavsakshi-extc@atharvacoe.ac.in

Arya chowkekar
EXTC Department
Atharva College of engineering
Mumbai,India
chowkekararya-extc@atharvacoe.ac.in

Aaryan Gorana
EXTC Department
Atharva College of engineering
Mumbai,India
goranaaaryan-extc@atharvacoe.ac.in

Vishal Gupta
EXTC Department
Atharva College ofengineering
Mumbai,India
guptavishal-extc@atharvacoe.ac.in

Dr. Jyoti Mali
Associate Professor, EXTC Department
Atharva College of Engineering
Mumbai, India
jyotimali@atharvacoe.ac.in

***Abstract*—The paper focuses on developing an affordable and effective firewall solution for network security using the Raspberry Pi, a compact and versatile computing platform. By leveraging open-source tools like iptables, nftables, and intrusion detection systems (IDS) such as Snort or Suricata, the firewall offers features like packet filtering, deep packet inspection, and real-time traffic monitoring. A custom Python-based firewall is also integrated to allow dynamic, rule-based network traffic control, managed via a user-friendly web-based dashboard built with Flask.**

This dashboard enables users to configure firewall settings, view traffic logs, and receive alerts for unusual network activities easily. Performance testing, including measurements of network throughput, latency, and resource usage under different load conditions, confirmed that the Raspberry Pi is a reliable and efficient firewall for small-scale networks, including home or small business setups.

The design effectively tackles challenges such as managing high traffic volumes and optimizing the Raspberry Pi's constrained resources. Additionally, it ensures flexibility and scalability for diverse applications. Future enhancements may involve integrating VPN functionality and incorporating AI-driven anomaly detection for advanced threat identification, further improving the firewall's capability to safeguard networks and provide a robust, customizable security solution.

***Keywords*—Network security, Intrusion prevention, Secure network architecture, Threat Mitigation, Centralized Firewall Management, Cyber Threat Analysis.**

I. Introduction

Firewalls have been integral to network security since their inception, evolving to counteract the ever-increasing complexity and frequency of cyber threats. Recent advancements in affordable, compact computing platforms, like the Raspberry Pi, have created opportunities for designing innovative, cost-effective firewall systems tailored for small-scale networks, including home users, small offices, and educational institutions.

Deep packet inspection intrusion prevention systems (IPSs) can protect against known attacks that target operating systems and software but cannot successfully detect or block the misuse of applications. Gartner Research uses the term "next generation firewall" to indicate the evolution of firewall that deals with the emerging network security threats compromising the network systems [5] Firewalls have been the frontier defense for secure networks against attacks and unauthorized traffic by filtering out unwanted network traffic coming into or going from the secured network. The filtering decision is taken according to a set of ordered filtering rules written based on predefined security policy requirements.[1]

II. Objective

To design a cost-effective firewall solution using Raspberry Pi that provides essential network security features. Implement a scalable architecture that can be adapted for various network environments, such as home, small office, and educational institutions.

1) In order to achieve the objective of resolving conflicts effectively and efficiently, our conflict resolution mechanism adopts a combination algorithm 4 incorporating features from both permutation and greedy algorithms. A threshold N for selecting a suitable rule reordering algorithm to resolve a conflict can be predefined in the combination algorithm. When the number of conflicting rules is less than N, the permutation algorithm is utilized for resolving conflicts. Otherwise, the greedy algorithm is applied to resolve conflicts.[15]

2) The commercial solutions are expensive and the technical details are not open source. Therefore, our aim is to design a cost-effective and open-source system. We setup a firewall using a Raspberry Pi as a gateway, through which all the things send their data. This will help us in activity/behavior detection of the things. Public requests like HTTP pass through it, giving us the freedom to create our own LAN.[12]

3) A Raspberry Pi is configured as a WiFi access point using hostapd and dnsmasq to setup the DHCP server [5]. We aim to support profiling of traffic generated by the things connected

in the home network. To initiate the efforts, we tried to profile the behavior of just one IoT device, Motorola FOCUS 66: a smart security camera which streams audio and video to a remote application.[12]

4) In order to achieve the objective of resolving conflicts effectively and efficiently, our conflict resolution mechanism adopts a combination algorithm4 incorporating features from both permutation and greedy algorithms. A threshold N for selecting a suitable rule reordering algorithm to resolve a conflict can be predefined in the combination algorithm. When the number of conflicting rules is less than N, the permutation algorithm is utilized for resolving conflicts. Otherwise, the greedy algorithm is applied to resolve conflicts.[15]

5) The objective is to highlight the importance of firewalls in securing networks for organizations. It emphasizes that firewalls are commonly used as the first line of defense and are critical for protecting computer networks. Proper firewall configuration is essential for ensuring security, but it can be challenging to predict the results of the configuration before the firewall is deployed.[13]

III. Block Diagram

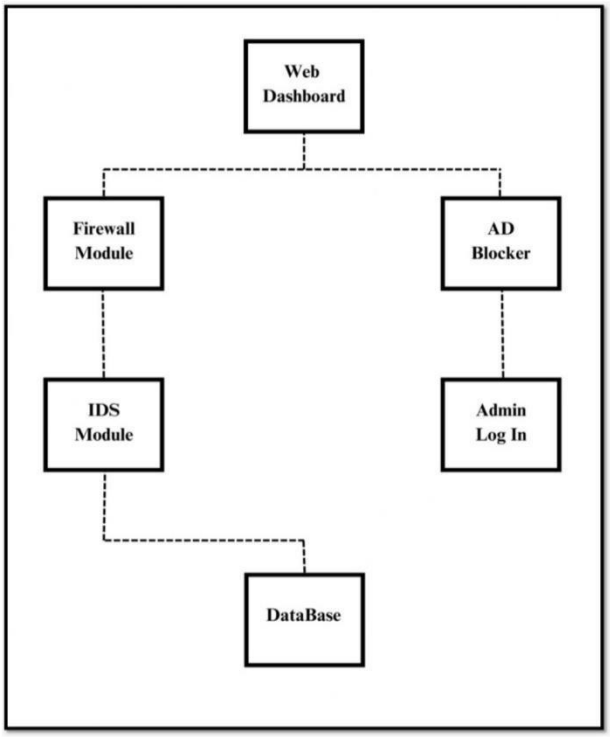


Fig. 1. Block Diagram Of firewall

This block diagram represents the architecture of a Raspberry Pi-based hardware firewall solution. It includes the following key components:

- Web Dashboard: A centralized interface for monitoring and managing all firewall operations.

Fig. 2. Optimization Cycle

- AD Blocker: A DNS-based advertisement blocker to filter ads on websites and YouTube.
- Firewall Module: Enforces rules for traffic filtering based on IPs, domains, and protocols.
- IDS Module: An Intrusion Detection System for identifying and alerting about network threats.
- Admin Log-In: Provides secure access for authorized users to manage and configure the firewall.
- Database: Stores logs, rules, and configurations for firewall, IDS, and ad-blocking operations.

These components work together to provide a comprehensive, customizable network security solution.

This diagram (Fig.2) illustrates the key benefits of implementing a comprehensive security solution. It begins by minimizing hardware reliance and enhancing overall security. By improving endpoint security and enabling real-time threat detection, it ensures proactive protection. Simplified policy management optimizes operational efficiency, while reducing cyber incident costs builds trust with customers. Additionally, it helps optimize network resources, creating a robust and reliable cybersecurity framework for organizations.

IV. Methodology and Results

A. *Hardware Components*

1) *Raspberry Pi:*

- **Model**: Raspberry Pi 4 (or any other version with sufficient resources) is recommended for its improved processing power, RAM (up to 8GB), and enhanced network interfaces.
- **Storage**: A microSD card (at least 16GB) is required to store the operating system (Raspberry Pi OS) and firewall software, including configuration files and logs.

2) *Network Interface Cards (NICs):*

- **Onboard Ethernet Port**: The Raspberry Pi 4 features a Gigabit Ethernet port, which serves as one of the primary

network interfaces (either for external Internet connection or internal LAN).

- **USB to Ethernet Adapter**: Since the Raspberry Pi only has one built-in Ethernet port, you will need an additional network interface for managing both incoming and outgoing traffic .

*3) **Power Supply**:*

- **Official Raspberry Pi Power Supply**: A 5V 3A power supply is required to power the Raspberry Pi 4.

B. Software Components

Intrusion Detection System: Intrusion detection in firewalls enhances security by monitoring network traffic and system activities to identify suspicious or malicious behavior. Integrating an IDS with a firewall strengthens defenses by detecting sophisticated attacks that may bypass traditional rule-based filtering. This combination ensures comprehensive network protection.

*1) **Components of Intrusion Detection in Firewalls**:*

- **Traffic Monitoring**: The IDS actively monitors the network traffic that passes through the firewall.
- **Analysis Engine**: This core component analyzes traffic to detect patterns that match known attack signatures or anomalies.
- **Alert Mechanism**: Generates alerts for administrators upon detecting suspicious activity.
- **Logging**: Records all flagged events for further analysis and investigation.
- **Response Mechanism**: Can automatically block or restrict the source of suspicious traffic when integrated with the firewall.

The ad-blocking module functions intercepting DNS requests to block ads and unwanted content by preventing access to known ad-serving domains. It offers customizable options to enhance filtering based on your specific needs.

C. Results

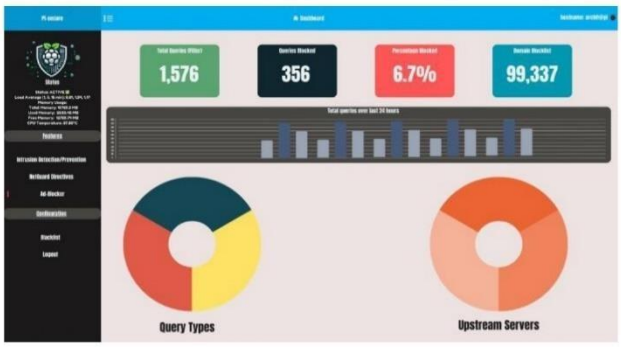


Fig. 3. Centralized Web Console

The image (Fig. 3) depicts a centralized web-based management console for a cybersecurity solution named "Pi-Secure," designed for real-time network monitoring and threat mitigation. It provides an overview of key metrics, including the total queries processed, blocked queries, the percentage of blocked traffic, and the total number of domains in the blocklist. System status details, such as load averages, memory usage, and CPU temperature, are displayed alongside features like Intrusion Detection/Prevention, NetGuard directives, and ad-blocking. Configuration options, such as blacklisting, enhance security controls. The interface also includes graphical visualizations, such as pie charts for query types and upstream servers, as well as a bar graph showing query activity over the last 24 hours. This offers an intuitive and comprehensive view of the system's operations for a Raspberry Pi-based network security appliance.

V. Futurescope and Applications

A. Futurescope

Firewall security, like any other technology, requires proper management to provide the desired security service. Thus, just having a firewall on the boundary of a network may not necessarily make the network more secure. One reason for this is the complexity of managing firewall rules and the potential network vulnerability due to rule conflicts. The Firewall Policy Advisor presented in this paper provides user-friendly tools for purifying and protecting the firewall policy from anomalies. The administrator can use the Firewall Policy Advisor to manage a general firewall security policy without prior analysis of the filtering rules that compose the policy. In this work, we formally defined all possible firewall rule relations and used this to classify firewall policy anomalies.[10] We implemented a system to secure the home network against privacy breaches, confidentiality threats, and related attacks. The future plan is to set up a generalized, intelligent heuristics-based traffic profiling dashboard running on the Raspberry Pi. This dashboard would provide information such as the frequency of data transmission, the location of devices, and other classifications for each device in the home network.[12]

B. Applications

Fifteen web application solutions have been selected for comparison. These include F5, Barracuda, Web Sniper, i-Sentry, Secure IIS, Easy Guard, Web Defend, Secure Sphere, Anchiva, Profanes, Citrix, WebApp Secure, eServer Secure, Server Defender AI, and Mod Security. A detailed comparison has been carried out by selecting the criteria of 'defense mechanism.' This includes security policy control, monitoring, blocking, response filtering, attack prevention, authentication, website cloaking, deep inspection, session protection, and overall security performance. [6]

VI. Conclusion

This project leverages a Raspberry Pi to create a cost-effective, scalable, and customizable hardware-based firewall for home and small office networks. It integrates features like DNS-based ad-blocking, intrusion detection, and real-time monitoring into a single, user-friendly system, offering advanced protection typically found in enterprise solutions.

Building on tools like Pi-Hole, pfSense, and Snort, the project addresses their limitations by providing a comprehensive security framework against threats such as DoS/DDoS and unauthorized access. The web-based GUI simplifies management and monitoring, while the modular design ensures scalability and adaptability for growing network demands.

In conclusion, this project demonstrates how low-cost, open-source hardware can deliver robust network protection and serve as an educational tool for cybersecurity innovations.

VII. References

1) Al-Shaer, E. S., Hamed, H. H. (2004). Modeling and Management of Firewall Policies. IEEE Transactions on Network and Service Management, 1(1), 2–10.
2) Lyu, M. R., Lau, L. K. Y. (n.d.). Firewall security: policies, testing and performance evaluation. Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000.
3) Liu, A. X., Gouda, M. G. (2009). Firewall Policy Queries. IEEE Transactions on Parallel and Distributed Systems, 20(6), 766–777.
4) Naik, N., Jenkins, P. (2016). Enhancing Windows Firewall Security Using Fuzzy Reasoning. 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress
5) Neupane, K., Haddad, R., Chen, L. (2018). Next Generation Firewall for Network Security: A Survey. SoutheastCon 2018.
6) Razzaq, A., Hur, A., Shahbaz, S., Masood, M., Ahmad, H. F. (2013). Critical analysis on web application firewall solutions. 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS).
7) Adao, P., Focardi, R., Guttman, J. D., Luccio, F. L. (2016). Localizing Firewall Security Policies. 2016 IEEE 29th Computer Security Foundations Symposium (CSF).
8) Lee, C. P., Trost, J., Gibbs, N., Beyah, R., Copeland, J. A. (n.d.). Visual firewall: real-time network security monitor. IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05).
9) Alfayyadh, B., Ponting, J., Alzomai, M., Josang, A. (2010). Vulnerabilities in personal firewalls caused by poor security usability. 2010 IEEE International Conference on Information Theory and Information Security.
10) Firkhan Ali Bin Hamid Ali. (2011). A study of technology in firewall system. 2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA).
11) Abdul Aziz, M. Z., Ibrahim, M. Y., Omar, A. M., Ab Rahman, R., Md Zan, M. M., Yusof, M. I. (2012). Performance analysis of application layer firewall. 2012 IEEE Symposium on Wireless Technology
12) Mayer, A., Wool, A., Ziskind, E. (n.d.). Fang: a firewall analysis engine. Proceeding 2000 IEEE Symposium on Security and Privacy. SP 2000.
13) Khan, B., Khan, M. K., Mahmud, M., Alghathbar, K. S. (2010). Security Analysis of Firewall Rule Sets in Computer Networks. 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies.
14) Gupta, N., Naik, V., Sengupta, S. (2017). A firewall for Internet of Things. 2017 9th International Conference on Communication Systems and Networks (COMSNETS).
15) Hu, H., Ahn, G.-J., Kulkarni, K. (2012). Detecting and Resolving Firewall Policy Anomalies. IEEE Transactions on Dependable and Secure Computing, 9(3), 318–331.

ACHIVEMENTS

ATHARVA EDUCATIONAL TRUST'S
ATHARVA COLLEGE OF ENGINEERING
(Approved by AICTE, Recognized by Government of Maharashtra
& Affiliated to University of Mumbai - Estd. 1999 - 2000)
ISO 21001:2018 ISO 14001:2015 ISO 9001:2015
NAAC Accredited A+

CERTIFICATE
OF PARTICIPATION

This Certificate is Awarded to

Sakshi Aghav

for successfully presenting a Paper entitled

Pisecure: integrated firewall solution for network protection

at the 3rd edition of International Conference on Science Technology Engineering & Mathematics for Sustainable Development (ICSTEMSD-2025) held on 21st February, 2025

Dr. Kavita Bani	Dr. Ramesh Kulkarni	Dr. Pravin Nemade
Conference Organizing Chair	Principal	Director

ATHARVA EDUCATIONAL TRUST'S
ATHARVA COLLEGE OF ENGINEERING
(Approved by AICTE, Recognized by Government of Maharashtra
& Affiliated to University of Mumbai - Estd. 1999 - 2000)
ISO 21001:2018 ISO 14001:2015 ISO 9001:2015
NAAC Accredited A+

CERTIFICATE
OF PARTICIPATION

This Certificate is Awarded to

Arya Chowkekar

for successfully presenting a Paper entitled

Pisecure: Integrated Firewall solution for Network Protection

at the 3rd edition of International Conference on Science Technology Engineering & Mathematics for Sustainable Development (ICSTEMSD-2025) held on 21st February, 2025

Dr. Kavita Bani	Dr. Ramesh Kulkarni	Dr. Pravin Nemade
Conference Organizing Chair	Principal	Director

ATHARVA EDUCATIONAL TRUST'S
ATHARVA COLLEGE OF ENGINEERING
(Approved by AICTE, Recognized by Government of Maharashtra
& Affiliated to University of Mumbai - Estd. 1999 - 2000)
ISO 21001:2018 ISO 14001:2015 ISO 9001:2015
NAAC Accredited A+

CERTIFICATE
OF PARTICIPATION

This Certificate is Awarded to

Aaryan Gorana

for successfully presenting a Paper entitled

Pisecure: integrated firewall solution for network protection

at the 3rd edition of International Conference on Science Technology Engineering & Mathematics for Sustainable Development (ICSTEMSD-2025) held on 21st February, 2025

Dr. Kavita Bani	Dr. Ramesh Kulkarni	Dr. Pravin Nemade
Conference Organizing Chair	Principal	Director

ATHARVA EDUCATIONAL TRUST'S
ATHARVA COLLEGE OF ENGINEERING
(Approved by AICTE, Recognized by Government of Maharashtra
& Affiliated to University of Mumbai - Estd. 1999 - 2000)
ISO 21001:2018 ISO 14001:2015 ISO 9001:2015
NAAC Accredited A+

CERTIFICATE
OF PARTICIPATION

This Certificate is Awarded to

Vishal gupta

for successfully presenting a Paper entitled

Pisecure: integrated firewall solution for network protection

at the 3rd edition of International Conference on Science Technology Engineering & Mathematics for Sustainable Development (ICSTEMSD-2025) held on 21st February, 2025

Dr. Kavita Bani, Conference Organizing Chair | Dr. Ramesh Kulkarni, Principal | Dr. Pravin Nemade, Director

ATHARVA EDUCATIONAL TRUST'S
ATHARVA COLLEGE OF ENGINEERING
(Approved by AICTE, Recognized by Government of Maharashtra
& Affiliated to University of Mumbai - Estd. 1999 - 2000)
ISO 21001:2018 ISO 14001:2015 ISO 9001:2015
NAAC Accredited A+

CERTIFICATE
OF PARTICIPATION

This Certificate is Awarded to

Dr. Jyoti Mali

for successfully presenting a Poster entitled

Pisecure: integrated firewall solution for network protection

at the 3rd edition of International Conference on Science Technology Engineering & Mathematics for Sustainable Development (ICSTEMSD-2025) held on 21st February, 2025

Dr. Kavita Bani, Conference Organizing Chair | Dr. Ramesh Kulkarni, Principal | Dr. Pravin Nemade, Director

ABVP | SRIJAN | DIPEX

CERTIFICATE
OF APPRECIATION

This certificate is awarded to

Prof./Dr./Mr./Mrs./Ms. Dr Jyoti Mali from Atharva College of Engineering for guiding the project and participated in the Idea Presentation Round of DIPX-2025, MMR Region held at Bharati Vidyapeeth Deemed University, Department of Engineering and Technology, Kharghar, Maharashtra.

आपका वर्धमान कर्तृत्व भारतमाता के चरणो में समर्पित हो।

Shri. Ram Bhogale, President, SRIJAN Trust
Dr. Mohan Awasthy, Principal, Bharati Vidyapeeth, Department of Engineering and Technology, Kharghar.
Shri. Sankalp Phaldesai, Convenor, DIPEX - 2025

In Association with

RAMKY | re Sustainability

Shot on OnePlus
Thane | 5 March 2025 at 3:27 pm

CERTIFICATE

OF PARTICIPATION

ABVP SRIJAN DIPEX 34

This is to certify that Mr./Ms. Aghav Sakshi Sanjay

from Atharva College Of Engineering participated in the Idea Presentation Round of DIPEX-2025, MMR Region held in association with Bharati Vidyapeeth Deemed University, Department of Engineering and Technology, Kharghar, Maharashtra.

आपका वर्धमान कर्तृत्व भारतमाता के चरणो में समर्पित हो।

Shri. Ram Bhogale, President, SRIJAN Trust

Dr. Mohan Awasthy, Principal, Bharati Vidyapeeth, Department of Engineering and Technology, Kharghar.

Shri. Sankalp Phaldesai, Convenor, DIPEX - 2025

In Association with

CERTIFICATE

OF PARTICIPATION

ABVP SRIJAN DIPEX 34

This is to certify that Mr./Ms. Chaudhekar Arya Anil

from Atharva College Of Engineering participated in the Idea Presentation Round of DIPEX-2025, MMR Region held in association with Bharati Vidyapeeth Deemed University, Department of Engineering and Technology, Kharghar, Maharashtra.

आपका वर्धमान कर्तृत्व भारतमाता के चरणो में समर्पित हो।

Shri. Ram Bhogale, President, SRIJAN Trust

Dr. Mohan Awasthy, Principal, Bharati Vidyapeeth, Department of Engineering and Technology, Kharghar.

Shri. Sankalp Phaldesai, Convenor, DIPEX - 2025

In Association with

Sustainability

CERTIFICATE

OF PARTICIPATION

ABVP SRIJAN DIPEX 34

This is to certify that Mr./Ms. Gohana Aaryan Manoj

from Atharva College Of Engineering participated in the Idea Presentation Round of DIPEX-2025, MMR Region held in association with Bharati Vidyapeeth Deemed University, Department of Engineering and Technology, Kharghar, Maharashtra.

आपका वर्धमान कर्तृत्व भारतमाता के चरणो में समर्पित हो।

Shri. Ram Bhogale, President, SRIJAN Trust

Dr. Mohan Awasthy, Principal, Bharati Vidyapeeth, Department of Engineering and Technology, Kharghar.

Shri. Sankalp Phaldesai, Convenor, DIPEX - 2025

In Association with

Sustainability

ABVP
AKHIL BHARATIYA VIDYARTHI PARISHAD

SRIJAN
DIPEX CENTER FOR ENTREPRENEURSHIP DEVELOPMENT

CERTIFICATE

OF PARTICIPATION

DIPEX 2025

This is to certify that Mr./Ms. Gupta Vishal Santosh
from Atharva College Of Engineering participated in the Idea Presentation Round of DIPEX-2025, MMR Region held in association with Bharati Vidyapeeth Deemed University, Department of Engineering and Technology, Kharghar, Maharashtra.

आपका वर्धमान कर्तृत्व भारतमाता के चरणो में समर्पित हो।

Shri. Ram Bhogale
President, SRIJAN Trust

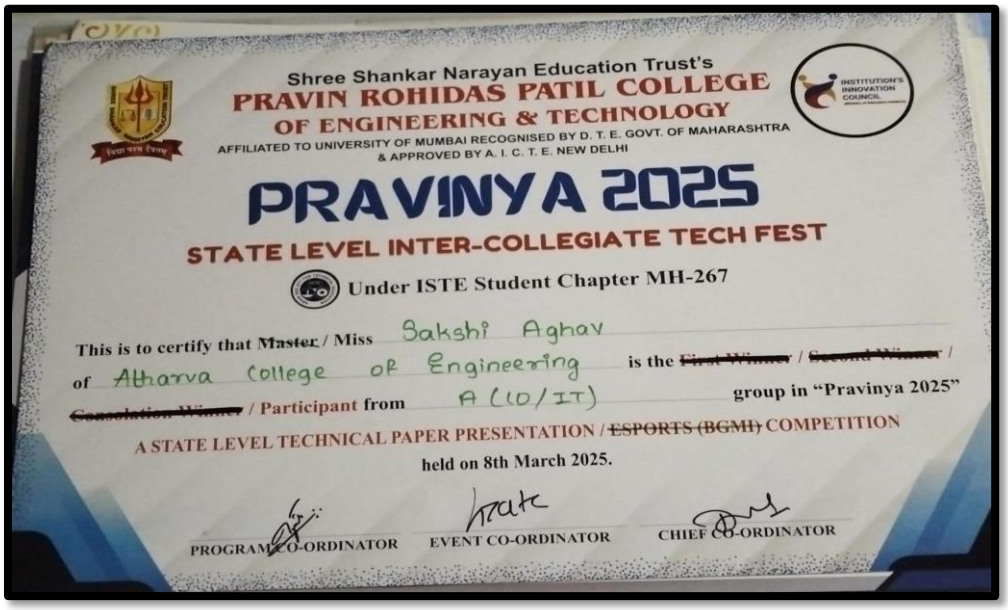
Dr. Mohan Awasthy
Principal, Bharati Vidyapeeth, Department of Engineering and Technology, Kharghar.

Shri. Sankalp Phaldesai
Convenor, DIPEX - 2025

In Association with

RAMS

Sustainability



Shree Shankar Narayan Education Trust's
PRAVIN ROHIDAS PATIL COLLEGE
OF ENGINEERING & TECHNOLOGY
AFFILIATED TO UNIVERSITY OF MUMBAI RECOGNISED BY D. T. E. GOVT. OF MAHARASHTRA
& APPROVED BY A. I. C. T. E. NEW DELHI

INSTITUTION'S INNOVATION COUNCIL

PRAVINYA 2025

STATE LEVEL INTER-COLLEGIATE TECH FEST

Under ISTE Student Chapter MH-267

This is to certify that ~~Master~~ / Miss Sakshi Aghav
of Atharva College of Engineering is the ~~First Winner~~ / ~~Second Winner~~ / ~~Consolation Winner~~ / Participant from A (IO/IT) group in "Pravinya 2025"
A STATE LEVEL TECHNICAL PAPER PRESENTATION / ~~ESPORTS (BGMI)~~ COMPETITION
held on 8th March 2025.

PROGRAM CO-ORDINATOR | EVENT CO-ORDINATOR | CHIEF CO-ORDINATOR

Shree Shankar Narayan Education Trust's
PRAVIN ROHIDAS PATIL COLLEGE
OF ENGINEERING & TECHNOLOGY
AFFILIATED TO UNIVERSITY OF MUMBAI RECOGNISED BY D. T. E. GOVT. OF MAHARASHTRA
& APPROVED BY A. I. C. T. E. NEW DELHI

INSTITUTION'S INNOVATION COUNCIL

PRAVINYA 2025

STATE LEVEL INTER-COLLEGIATE TECH FEST

Under ISTE Student Chapter MH-267

This is to certify that Master / ~~Miss~~ ARYA CHOWKEKAR
of Atharva College of Engineering is the ~~First Winner~~ / ~~Second Winner~~ / ~~Consolation Winner~~ / Participant from A (IO/IT) group in "Pravinya 2025"
A STATE LEVEL TECHNICAL PAPER PRESENTATION / ~~ESPORTS (BGMI)~~ COMPETITION
held on 8th March 2025.

PROGRAM CO-ORDINATOR | EVENT CO-ORDINATOR | CHIEF CO-ORDINATOR

ACKNOWLEDEMENT

We would like to thank our project guide **Dr. Jyoti Mali** for her enormous co-operation and guidance. We have no words to express our gratitude for person who whole heartedly supported the project and gave freely of her valuable time while making this project. All the inputs given by her have found a place in the project.

The technical guidance provided by her was more than useful and made the project successful. She has always been a source of inspiration for us. It was memorable experience learning under such a highly innovative, enthusiastic and hardworking teacher. We are also thankful to our **Principal Dr. Ramesh Kulkarni** and our head of department **Dr. Bhavin Shah** and all the staff members of the **Electronics & Telecommunication Department** who have provided us various facilities and guided us to develop a very good project idea. Finally, we would also like to thank the non-teaching staffs, friends and seniors who guided and helped us while working on this project.