Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

Portable Cybersecurity and Data Protection

Aneena Sajad S
Undergraduate
Dept. of ECE
Muslim association
college of engineering

Fathima Hussain S
Undergraduate
Dept. of ECE
Muslim association
college of engineering

Salma Subair
Undergraduate
Dept. of ECE
Muslim association
college of engineering

Nithi S Prem
Undergraduate
Dept. of ECE
Muslim association
college of engineering

Abstract - This project presents the design and development of a Portable Cybersecurity and Data Protection Device using the Raspberry Pi Zero 2 W. The system functions as a portable, hardware-level network security solution that monitors real-time network traffic and protects users from cyber threats such as hacking, phishing, port scanning, brute force attacks, and malicious tracking. Unlike traditional software-based antivirus systems, the device operates at the network level by acting as an intermediate security layer between the router and user devices, performing packet inspection, firewall automation, ad and tracker blocking, and intelligent threat detection. Suspicious IP addresses are automatically identified and blocked using predefined security rules and anomaly detection techniques. An optional AI module further enhances detection accuracy by analyzing traffic behavior to identify abnormal activities. The device also provides real-time alerts through visual indicators and display modules to ensure user awareness. The proposed solution is portable, cost-effective, and suitable for homes, educational institutions, and small offices, demonstrating the practical implementation of cybersecurity concepts using embedded systems to enhance network security and data privacy.

Keywords—Cyber security, Raspberry Pi Zero 2 W, Network Security, Packet Inspection, Embedded Systems.

INTRODUCTION

With the rapid growth of the internet and digital communication, cybersecurity has become a major concern in modern computing environments. People and organizations depend on the internet for communication, data transfer, online transactions, and cloud services.However, this increased usage also exposes users to cyber threats such as malware, phishing, data theft, tracking, and unauthorized access. Therefore, ensuring secure internet usage and protecting user data is essential. Traditional security methods like antivirus software and firewalls provide basic protection, but users are still vulnerable due to unsafe browsing, malicious websites, and hidden data collection.Public networks in places like cafés, airports, and institutions often lack proper security, increasing cyber risks. Hence, a portable and user-friendly cybersecurity solution is needed to monitor and protect network traffic in real time.

With advancements in embedded systems, compact cybersecurity devices can be developed to enhance network safety. These systems can monitor internet traffic, block malicious domains, prevent ads, and detect suspicious connections, providing an extra layer of protection.The Portable Cybersecurity & Data Protection Device is designed to improve internet security and user privacy. It uses a Raspberry Pi Zero 2 W as the main processing unit to monitor and control network activities, analyzing traffic and filtering harmful connections.The system includes an LCD display, LED indicators, and an SD card. The LCD shows real-time system status and alerts, LEDs indicate device operation, and the SD card stores the OS, configurations, and logs.When suspicious activity or malicious connections are detected, the device blocks them automatically and notifies the user. This helps protect personal data and improve browsing privacy.The system is portable, cost-effective, and easy to deploy, making it suitable for homes, educational institutions, and small offices. It provides an efficient solution for enhancing cybersecurity through real-time monitoring and data protection.

EXISTINGSYSTEM

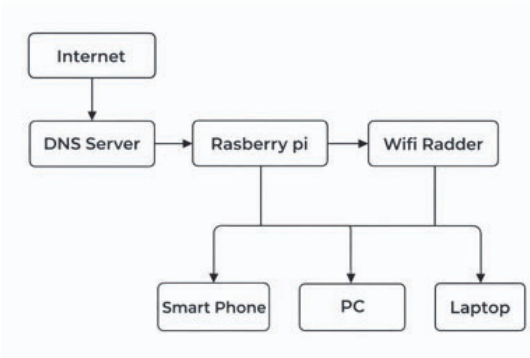

Fig. 1 Block diagram of Existing Portable Cybersecurity & Data protection system

The existing block diagram shown in fig.1,represents a network-based ad-blocking and monitoring system using a Raspberry Pi. The system is designed to control and filter internet traffic for devices connected to a local network. It works by routing all network requests through a central device that manages domain name resolution and blocks unwanted advertisements or malicious domains before they reach the user's device.At the top of the diagram, the Internet acts as the main source of data and online services. When a user tries to access a website or online application, the request first travels from the internet to the DNS Server. The DNS server is responsible for translating website names (domain names) into IP addresses so that devices can communicate with the correct servers on the internet.After the DNS request is processed, the traffic is forwarded to the Raspberry Pi, which acts as the core controller of the system. The Raspberry Pi is configured with ad-blocking software that filters DNS requests. If the request is associated with an advertisement or a blocked domain RaspberryPi prevents it from reaching the user's device. This improves browsing speed and reduces unnecessary data usage.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

From the Raspberry Pi, the filtered internet connection is om sent to the Wi-Fi Router. The router distributes the internet connection to all devices connected to the local network. connection to all Since the filtering process already happens in the Raspberry Pi, every device connected to this router automatically benefits from the ad-blocking system without requiring any additional software installation. The router then provides internet access to different user devices such as Smartphones, PCs, and Laptops. Each of these devices sends its DNS requests through the same network path. As a result, advertisements and unwanted domains are blocked at the network level, level, ensuring a cleaner and safer browsing experience for all connected devices. Overall, this block this bloc diagram illustrates a centralized network filtering architecture where the Raspberry Pi acts as the main control unit. By placing the ad-blocking mechanism between the DNS server and the Wi-Fi router, the system efficiently manages and filters internet traffic for for multiple devices simultaneously, improving network performance, security, and user experience

III. PROPOSED SYSTEM

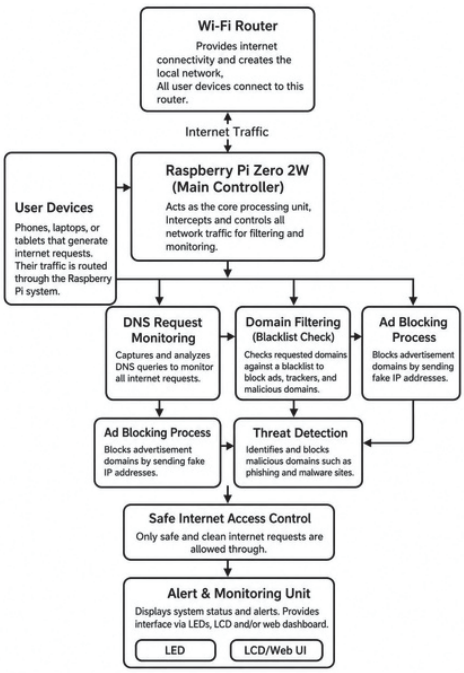

Fig. 2 Block diagram of Proposed Portable Cybersecurity & Data protection system

The advanced block diagram shown in fig. 2 represents an improved network security and ad-blocking system built using a Raspberry Pi Zero 2W. This system is designed to monitor internet traffic, block advertisements, detect potential threats, and provide secure internet access for all connected devices. By placing the Raspberry Pi at the center of the network, the system can analyze and filter requests before they reach the user's devices, improving both security and browsing performance.At the beginning of the network structure is the Wi-Fi Router, which provides internet connectivity and creates the local network environment.

All devices such as smartphones, laptops, and PCs connect to this router to access the internet. The router forwards all internet traffic through the Raspberry Pi so that the requests can be analyzed and filtered before reaching the final destination.

The User Devices block represents devices such as smartphones, laptops, and tablets that generate internet requests. Whenever a user tries to access a website or application, the request is routed through the Raspberry pi system. This ensures that every request passes through the monitoring and filtering stages, allowing the system to manage network activity effectively. The central component of the system is the Raspberry Pi Zero 2W, which acts as the main controller. It processes incoming network traffic and performs several important tasks such as DNS request monitoring, domain filtering, and ad blocking. The Raspberry Pi checks whether the requested domain is safe or potentially harmful and blocks suspicious or unwanted connections. The system includes several filtering mechanisms. DNS Request Monitoring captures and analyzes DNS queries to observe internet usage. Domain Filtering checks requested domains against a blacklist to identify ads or malicious websites. The Ad Blocking Process blocks advertisement domains by redirecting them to fake or null IP addresses, preventing ads from loading. Additionally, the Threat Detection module identifies harmful domains related to phishing, malware, or unsafe websites.Finally, the system ensures Safe Internet Access Control by allowing only secure and clean requests to pass through the network. The Alert and Monitoring Unit provides feedback about the system's status using interfaces such as an LED indicator or an LCD/Web interface dashboard. This allows users or administrators to monitor network activity and confirm that the filtering and protection system is functioning properly

IV. METHODOLOGY

A. Circuit diagram

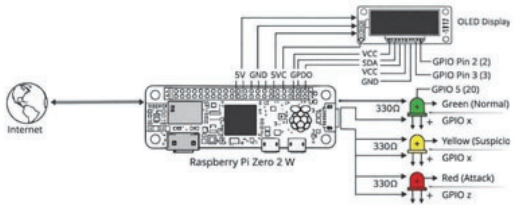

Fig. 3 Circuit diagram of portable cyber security and data protection device

The circuit diagram shown in fig. 3 represents the hardware implementation of the proposed network monitoring and ad-blocking system using a Raspberry Pi Zero 2W. The Raspberry Pi Zero 2W acts as the central processing unit that controls the monitoring system, processes network data, and communicates with output devices such as LEDs and an LCD display. The system is designed to visually indicate the network status and potential threats detected in the internet traffic. The Raspberry Pi Zero 2W is connected to the internet and acts as the main controller of the system. It processes incoming network data and performs functions such as DNS monitoring, ad blocking, and threat detection. The Raspberry Pi uses its GPIO (General Purpose Input Output) pins to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

communicate with external components such as the LCD display and status indicator LEDs.An LCD display module is connected to the Raspberry Pi to show system information and network status. The LCD uses communication pins such as VCC, GND, SDA, and SCL for power supply and data communication. The VCC pin provides the power supply, while the GND pin acts as the ground reference. The SDA and SCL pins are used for I2C communication between the Raspberry Pi and the LCD display, allowing the system to display messages related to network activity, alerts, and system status. The circuit also includes three LED indicators to visually represent different network conditions.

Each LED is connected to the Raspberry Pi through a 330-ohm resistor, which protects the LED by limiting the current flowing through it. These LEDs provide a simple visual indication of whether the network traffic is normal, suspicious, or under attack.The green LED represents normal network operation. When the system detects that internet traffic is safe and no suspicious activity is found, the Raspberry Pi activates the green LED. This indicates that the network is functioning properly and users can safely access the internet.The yellow LED indicates suspicious network activity. If the system detects unusual or potentially unsafe domains during DNS monitoring, the Raspberry Pi triggers the yellow LED to alert the user. This acts as an early warning signal that the system has detected unusual traffic that may require attention.The red LED represents a detected attack or highly malicious activity. When the Raspberry Pi identifies a harmful domain or potential cyber threat, the red LED is activated to alert the user immediately. This warning allows the user or system administrator to take appropriate action to protect the network.Overall, the circuit diagram demonstrates how the Raspberry Pi Zero 2W integrates with an LCD display and LED indicators to create a simple yet effective network monitoring and alert system. The combination of visual indicators and display output helps users easily understand the network status and ensures better monitoring of internet security within the system.

B. Working

The circuit diagram shows the working of a network monitoring and ad-blocking system using a Raspberry Pi Zero 2W. In this system, the Raspberry Pi acts as the main controller that processes internet traffic and provides visual indications of the network status. The system is designed to detect normal traffic, suspicious activity, and potential attacks, and then display the status through LEDs and an LCD displayThe working of the system begins with the internet connection. The Raspberry Pi Zero 2W is connected to the internet and acts as a network controller. It monitors the incoming and outgoing traffic from the connected devices. All network data passes through the Raspberry Pi, allowing it to analyze requests and identify advertisement domains or malicious websites. Once the network traffic is received, the Raspberry Pi processes the data using its internal software. The system checks DNS requests and filters domain names to determine whether they are safe or harmful. Based on the analysis results, the Raspberry Pi decides whether the network traffic is normal, suspicious, or a potential attack.

The LCD display is connected to the RaspberryPi using the I2C communication interface.The pins used include VCC, GND, SDA, and SCL. VCC provides power to the display, while GND acts as the ground connection. The SDA (Serial Data) and SCL (Serial Clock) pins allow the Raspberry Pi to send data to the LCD. Through this display, the system shows messages such as network status, alerts, and system information. The circuit also includes three LEDs that act as visual indicators of the system's status. Each LED is connected to a GPIO pin of the Raspberry Pi through a 330-ohm resistor. The resistor is used to limit the current flowing through the LED and protect it from damage. These LEDs help users quickly understand the condition of the network. The green LED indicates normal network activity. When the Raspberry Pi detects that the internet traffic is safe and no harmful domains are present, it sends a signal through the corresponding GPIO pin to turn on the green LED. This shows that the system is operating normally and the network is secure. The yellow LED represents suspicious activity. If the Raspberry Pi detects unusual traffic patterns or potentially unsafe domains, it activates the yellow LED. This acts as a warning signal that the system has identified suspicious behavior that may require attention or monitoring. The red LED indicates a detected attack or malicious activity. When the system identifies a harmful website, phishing attempt, or malware-related domain, the Raspberry Pi activates the red LED. At the same time, the LCD display may show a warning message. This allows the user or administrator to quickly understand that a security threat has been detected and appropriate action may be required.

C. Algorithm

Step 1: System and Hardware Initialization

1.Start the device and power on the system.
2.Initialize the Raspberry Pi Zero 2 W microcontroller. 3.Load the operating system and start the cybersecurity monitoring program.
4.Initialize all connected components including LCD display, LED indicators, and SD card storage.
5.Establish network connection through Wi-Fi for monitoring internet traffic.

Step 2: Network Monitoring

1.Start continuous monitoring of incoming and outgoing network traffic.
2.Analyze data packets passing through the network. 3.Compare domain requests with the list of known malicious or tracking domains.
4.Display the message “SYSTEM ACTIVE – NETWORK PROTECTED” on the LCD display.

Step 3: Threat Detection

1.Check whether any suspicious or malicious domain is detected.
2.If no threat is detected, continue monitoring the network traffic.
3.If a suspicious request or harmful connection is detected, mark it as a potential threat.

Step 4: Threat Blocking

1.Block the detected malicious domain or harmful website.
2.Prevent the connection from reaching the user device.
3.Update the system log with the blocked request information.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

Step 5: User Notification

1.Display a warning message such as “THREAT BLOCKED – MALICIOUS DOMAIN DETECTED” on the LCD display.
2.Turn on LED indicator to notify the user about the blocked threat.
3.Store the threat details and timestamp in the system log file on the SD card.

Step 6: Data Logging

1.Record all network activities including allowed and blocked requests.
2.Store logs securely in the SD card for analysis and monitoring.
3.Maintain a record of detected trackers, advertisements, and malicious websites.

Step 7: Continuous Protection

1.Resume monitoring the network continuously.
2.Wait for new network requests or suspicious activities.
3.Repeat the monitoring, detection, and blocking process automatically.

D. Flowchart

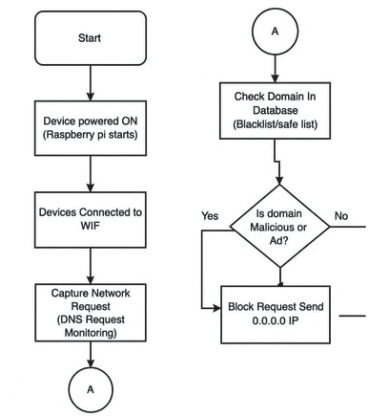

Fig. 4 Flowchart of DNS-Based Malicious Domain Detection and Blocking

V. EXPERIMENTAL RESULT

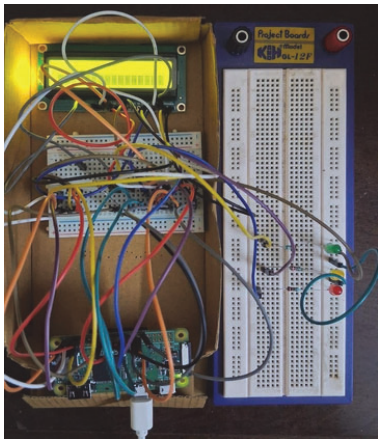

Fig.5Hardware Implementation and Result Display

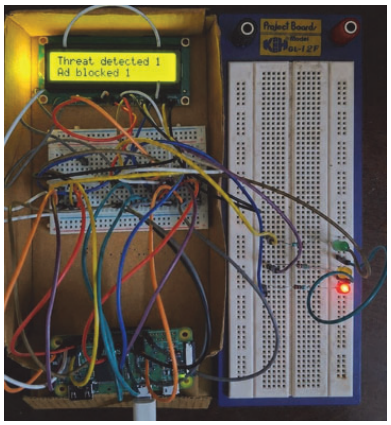

Fig.6Detection of Threatand Activation of Blocking System withLED Indication

The proposed system, developed using the Raspberry Pi Zero 2 W successfully functions as a portable network-level ad blocker and cybersecurity solution, delivering improved performance and enhanced protection By effectively filtering out advertisements, tracking scripts, and heavy media content, the system improves browsing speed, enabling web pages to load faster and providing a smoother user experience. In addition, it reduces overall bandwidth consumption by blocking unnecessary background data, thereby optimizing network usage. The system also demonstrates strong proactive security capabilities by blocking access to known malicious domains, phishing websites, and ad servers at the network level. This ensures that all connected devices are protected from potential cyber threats such as malware attacks and unauthorized data access. Real-time monitoring is achieved through an LCD, which displays information such as blocked advertisements, network activity, and system status, allowing users to continuously monitor the system's operation

Furthermore, LED indicators provide immediate visual feedback by indicating normal conditions, suspicious activity, or potential security threats.Overall, the system operates as a centralized security layer for all connected devices, including smartphones, laptops, and IoT devices, eliminating the need for separate security installations. With its compact design, low power consumption, and effective performance, the system provides a reliable and user- friendly solution for portable cybersecurity and network optimization.

VI .ACKNOWLEDGMENTS

I would like to express my sincere gratitude to professions, department of electronics and communication engineering for there valuable guidance and there encouragement in pursing this paper

VII. CONCLUSION

he development of a portable cybersecurity and data protection device is an important initiative in the modern digital era. As people increasingly rely on smartphones, laptops, and loT devices for communication, work, and data storage, the risk of cyber threats also grows.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 07 , July - 2026

While these technologies offer convenience and mobility, many of them lack strong built-in security systems. This project highlights the need for additional protection to safeguard sensitive information from evolving cyber threats. One of the key findings of the project is the importance of physical security measures. Device theft, lost hardware, and the use of unsecured public Wi-Fi networks can expose personal and professional data to serious risks. A portable security device can create a secure environment or "safe bubble" around connected devices, helping to protect data even when users are in potentially unsafe digital environments. The project also emphasises the need for comprehensive, multi-layered data protection. Effective security solutions should include strong data encryption, secure VPN connectivity, and continuous monitoring of connected devices. By combining these protective layers, the device can reduce the risk of threats such as data theft, unauthorised access, and Man-in- the-Middle attacks, ensuring safer digital communication and storage.In conclusion, this project demonstrates that hardware-based security solutions play a vital role in bridging the gap between mobility and cybersecurity. Future improvements could include Al-driven threat detection systems that analyse behavior patterns to identify advanced malware and cyber attacks. By enabling automatic security protocols and simplifying complex protection methods, such devices empower users to secure their digital information without requiring advanced technical expertise.

VIII. REFERENCES

[1] A. S. Visvanathan, Y. Nathan and M. Abdulnabi, "A Raspberry Pi Security Device Using VPN and Adblocker," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-5.

[2] J. Jeremiah, "Intrusion Detection System to Enhance Network Security Using Raspberry Pi Honeypot in Kali Linux," 2019 Intemational Conference on Cybersecurity (ICoCSec), Negeri Sembilan, Malaysia, 2019, pp. 91-95.

[3] E. H. Sonawane, M. Patil, S. Patil, U. Thakur, B. Patil and A. Marathe, "Middleware Device for Advertisement Blocking." 2022 International Conference on Futuristic Technologies (INCOFT), Belgaum, India, 2022, pp. 1-5

[4] A. M. Nugraha, R. M. R. Erlangga, F. C. Cindy, N. Kana and A. 1. Irawan, "Analysis of Network-Wide Ad Blocker Using Mikrotik RouterBoard and Raspberry Pi for Enhancing Network QoS," 2025 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), Bali, Indonesia, 2025, pp 150-157.

[5] J. Marot and S. Bourennane, "Raspberry Pi for image processing education," 2017 25th European Signal Processing Conference (EUSIPCO), Kos, Greece, 2017, pp. 2364-2366, doi: 10.23919/EUSIPCO.2017.8081633

[6] B. Balon and M. Simić, "Using Raspberry Pi Computers in Education," 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2019, pp. 671-676, doi: 10.23919/MIPRO.2019.8756967.

[7] F. López, F. J. Torres, V. A. Ramírez, D. A. Núñez, R. Corona and A. R. López, "Raspberry Pi for Implementation of Web Technology in an Automation Process," 2019 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC), Ixtapa, Mexico, 2019, pp. 1-6, doi: 10.1109/ROPEC48299.2019.9057040.

[8] A. S. Visvanathan, Y. Nathan and M. Abdulnabi, "A Raspberry Pie Security Device Using VPN and Adblocker," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-5, doi: 10.1109/ICMNWC56175.2022.10031864.

[9] H. Sonawane, M. Patil, S. Patil, U. Thakur, B. Patil and A. Marathe, "Middleware Device for Advertisement Blocking," 2022 International Conference on Futuristic Technologies (INCOFT), Belgaum, India, 2022, pp. 1-5, doi: 10.1109/INCOFT55651.2022.10094371.

[10] A. M. Nugraha, R. M. R. Erlangga, F. C. Cindy, N. Karna and A. I. Irawan, "Analysis of Network-Wide Ad Blocker Using Mikrotik RouterBoard and Raspberry Pi for Enhancing Network QoS," 2025 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), Bali, Indonesia, 2025, pp. 150-157, doi: 10.1109/IAICT65714.2025.1110066

[11] Geary, S. Malware, phishing, spyware and viruses – what's the difference?, August 2017

[12] Mary, L., Dheen, S. N., & Narayanan, S. K. Network-wide range ad-blocker using Raspberry Pi. International Journal of Pure and Applied Mathematics, vol. 119, pp. 1771-1775, 2018.

[13] M. C. Nawej, "Evaluation of virtual private network impact on network performance," 2016.