International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

PI-HOLES AD BLOCKING SYSTEM USING RASPBERRY PI

Prof Sarika N. Patil[1], Priya N. Agarwal[2], Rutika R. Chavan[3] Yash R. Jakkan[4]

1Professor, Department Of Electronics of Telecommunication, PCET's, Nutan Maharashtra Institute of Engineering and Technology, Maharashtra, India.

2,3,4UG Students, Department Of Electronics of Telecommunication, PCET's, Nutan Maharashtra Institute of Engineering and Technology, Maharashtra, India.

Abstract-This project presents the design and implementation of a network-wide ad-blocking system using Pihole on a Raspberry Pi. As online advertisements become increasingly invasive, users seek efficient solutions to block ads across devices without needing to configure each individually. Traditional ad-blocking methods rely on browser extensions, which are often limited to specific devices or browsers. Pi-hole, a DNS-based adblocking solution, provides an affordable, network-wide approach, making it ideal for home or small office environments. The project leverages the Raspberry Pi's low cost, compact size, and energy efficiency to host Pihole as a dedicated DNS server that filters and blocks ad domains before they reach user devices. This abstract outlines the complete setup process, including hardware requirements (such as a power supply, microSD card, and network connection) and the software configuration necessary to run Pi-hole on a Linux-based operating system like Raspberry Pi OS. Configuration steps cover setting up Pi-hole to function as the primary DNS server, fine-tuning blocklists, and implementing features like remote access and user- friendly dashboards. To enhance performance and reliability, several optimization strategies are explored, including adjusting DNSquery caching, managing blocklists for specific ad types, and setting up automated updates. Security configurations, such as DNS over HTTPS (DoH) and fire wall settings, are integrated to ensure data privacy and protect against unauthorized network access. The results demonstrate that this Pi-hole based system can effectively block ads, reduce bandwidth usage, and provide a seamless browsing experience across all connected devices, making it a powerful yet cost-effective alternative to commercial ad- blocking solutions

IndexTerms - Pi-Hole, Ad Blocking, Raspberry Pi, DNS Filtering, Network Security, Internet Privacy, Open-Source, Content Filtering.

1.INTRODUCTION

Pi-hole is a network-level ad blocker that uses a Raspberry Pi to block unwanted advertisements, tracking domains, and malicious websites from your entire home network. Pi- hole acts as a DNS sinkhole, intercepting DNS requests from devices on your network and blocking requests to known ad-serving domains, tracking domains, and malicious websites. Pi- hole is a revolutionary, open- source project that turns a Raspberry Pi into a network-level ad blocker, protecting your entire home network from unwanted advertisements, tracking domains, and malicious websites. By blocking ads at the network level, Pi-hole improves online privacy, reduces bandwidth usage, and enhances overall browsing experience Pi-hole is installed on a Raspberry Pi, a small, lowcost computer. The Pi-hole device is connected to your home network router. Pi-hole acts as a DNS (Domain Name System) sinkhole, intercepting DNS requests from devices on your network. Pi-hole blocks requests to known ad-serving domains, tracking domains, and malicious websites. Clean, ad-free DNS requests are forwarded to your upstream DNS provider. Protects all devices on your network, including smart TVs, gaming consoles, and IoT devices. Blocks tracking domains and malicious websites. Minimizes data waste from unwanted ads. Faster page loads and reduced clutter. Easily add or remove blocklists to tailor your experience. In summary, Pi-hole is a simple, effective, and customizable solution for blocking ads and improving online privacy at the network level.

NEED OF THE STUDY

As internet usage continues to expand, users are increasingly exposed to online advertisements that can detract from the browsing experience, consume bandwidth, and, in some cases, jeopardize user privacy and security. Traditional ad-blocking software requires installation on individual devices, which can be cumbersome to manage, especially in environments with multiple devices, such as homes, offices, or schools. Furthermore, ads are often embedded within websites and applications in a way that consumes data and slows down page load times, creating a need for a more effective, network-wide solution. Pi-Hole, a DNS-based ad-blocking system, addresses these issues by blocking ads at the network level, ensuring that all devices connected to the network benefit from ad-free browsing without needing individual ad-blocking software. This network-wide approach not only improves the user experience by reducing unwanted content and load times but also provides added security by preventing access to malicious sites and tracking domains. Implementing Pi-Hole on a RaspberryPi allows for an affordable, low-power solution thatis easy to set up and maintain. The need for this project isrooted in the growing demand for streamlined, privacy focused browsing and security measures that are effective, userfriendly, and applicable across all connected devices. By implementing Pi-Hole as a central ad- blocking tool, this project fulfills the need for a comprehensive

PROBLEM STATEMENT

In the digital age, online advertisements have become increasingly pervasive, impacting user experience by slowing down web pages, consuming bandwidth, and posing privacy and security risks. Ads can track user behavior, and some may even contain malware that can compromise user devices. With the growing volume of intrusive ads and the potential security risks associated with them,there is a need for an effective, network-wide solution to block unwanted content across all devices on a network without requiring individual device-level software. The implementation of Pi-Hole on a Raspberry Pi offers a cost effective, centralized ad- blocking solution, benefiting users by enhancing their browsing experience, saving bandwidth, and safeguarding privacy across the network. This project demonstrates the integration of open-source software with IoT hardware to create a practical and scalable solution for managing online advertisements and improving digital security.

Objectives

The primary objectives of this research are as follows:
1. To study and analyze the working mechanism of Pi-Hole as a DNS-based ad-blocking system.
2. To implement and configure Pi-Hole on a Raspberry Pi for network-wide ad blocking.
3. To evaluate the effectiveness of Pi-Hole in blocking ads, trackers, and malicious domains.
4. To measure performance impact on network speed, CPU, and memory utilization.
5. To compare Pi-Hole with conventional ad-blocking methods and commercial alternatives.

RELATED WORK

Traditional Ad-Blocking Methods

Traditional ad-blocking methods, such as browser extensions, firewall filtering, host file modifications, proxy/VPN-based blocking, and custom DNS filtering, help users prevent advertisements from appearing on web pages and applications. While these methods are effective to some extent, they have limitations such as device dependency, difficulty in blocking dynamic ads, and vulnerability to anti-ad block mechanisms. Pi-Hole addresses these challenges by implementing network-wide ad-blocking through DNS filtering, ensuring that unwanted content is blocked before reaching client devices. This approach provides better privacy, reduced bandwidth usage, and a seamless ad-free experience across all connected devices. However, Pi-Hole still requires manual configuration and maintenance to stay effective against evolving ad-serving techniques.

DNS-Based Ad-Blocking with Pi-Hole

Pi-Hole is a DNS-based ad-blocking system that prevents advertisements at the network level by blocking requests to known ad-serving domains. Unlike traditional ad blockers, which work on individual devices, Pi-Hole offers network-wide protection, improving privacy, reducing bandwidth usage, and enhancing browsing speed. While Pi-Hole is highly effective against most ads and trackers, it has some limitations, such as difficulty blocking YouTube and social media ads, the need for manual setup and maintenance, and dependence on external blocklists. Despite these challenges, Pi-Hole remains a powerful, open-source alternative for users seeking efficient ad-blocking without relying on browser extensions.

AI-Based Techniques for Ad-Blocking

AI-based ad-blocking techniques use machine learning (ML) and deep learning (DL) to detect and block ads dynamically, overcoming the limitations of traditional rule-based filters. Unlike static blocklists, AI models analyze patterns in web content, images, and scripts to identify and block new and evolving ad formats, including native ads and anti-ad block bypass techniques. Key AI techniques include natural language processing (NLP) for detecting ad-related text, computer vision for identifying visual ad elements, and reinforcement learning for adapting to changing ad strategies. While AI-powered ad-blocking offers greater accuracy and adaptability, challenges such as high computational requirements, false positives, and privacy concerns remain

literature survey:

Sr. No	Paper Name & Author	Key Findings	Limitations
1.	"Ad-Blocking Using Raspberry PiHole" (Jagan et al.)	Pi-Hole effectively blocks ads at the DNS level, improving browsing speed and reducing network congestion. - Works across all devices connected to the same network.	-Does not block ads within apps that use hardcoded IPs instead of domain-based ads.- Requires manual updates for the blocklist.
2.	"Pi Black Hole for Internet Advertisements" (Dasgupta)	Pi-Hole enhances privacy by blocking tracking domains and malicious ads. - Can be integrated with DNS-over-HTTPS (DoH) for	Some websites break due to aggressive ad-blocking. - Requires a stable internet connection for updates.

		added security.	
3.	"NETBLK: Network Adblocker using Raspberry Pi" (Dunglao et al.)	-Pi-Hole acts as a firewall-like system, preventing malware infections through ads. - Provides a web interface for easy monitoring and configuration.	Does not work well on mobile networks when devices switch between Wi-Fi and cellular data. - Initial setup requires networking knowledge.
4.	"Monitoring DNS Query with PiHole Firewall" (Syahputra)	-Pi-Hole, when integrated with firewalls and MikroTik routers, provides enhanced security and content filtering. - Reduces phishing attempts and prevents unauthorized tracking.	-Some legitimate websites may get blocked due to over-filtering. - Requires frequent updates to maintain an effective blocklist.
5.	"Ad-Blocking Using Raspberry PiHole" (Mounika et al.)	-Pi-Hole reduces bandwidth consumption by preventing ad-heavy domains from loading. - Ensures an ad-free experience on IoT devices, smart TVs, and gaming consoles	-Cannot block ads embedded within applications. - Does not prevent YouTube ads effectively

PROPOSED SYSTEM

1. Centralized Ad-Blocking: The Raspberry Pi running Pi-Hole acts as a DNS sinkhole, filtering out ads and tracking domains at the network level, ensuring all connected devices benefit from ad-blocking.

2. Data Flow & Filtering: Client devices (smartphones, laptops, smart TVs, IoT devices) send DNS requests to the Raspberry Pi, which checks if the domain is on the blocklist.

3. If the request matches an ad or tracking server, it is blocked; otherwise, it is forwarded to a trusted DNS server (Google DNS, OpenDNS, etc.).

4. Improved Browsing Speed & Security: Blocking unwanted ads reduces bandwidth usage, speeds up page loading, and prevents malware/phishing attacks from malicious ads.

5. Integration with Network Router: The router directs all DNS traffic to the Pi-Hole, ensuring network-wide ad-blocking without the need for browser extensions or individual device configurations.

6. Admin Dashboard for Monitoring & Customization: Users can view real-time traffic, customize blocklists, and manage whitelisted domains through the Pi-Hole web-based interface, enhancing control over network security.

ALGORITHM

Step 1. Initialize System

- Power on the Raspberry Pi and ensure itis connected to the network router via Wi-Fi or Ethernet.
- Start the Pi-Hole DNS filtering service

Step 2. Configure DNS Settings

- Set the router's DNS server to the Pi-Hole's IP address, ensuring all devices on the network use it for DNS resolution.
- Choose an upstream DNS provider (Google DNS, Cloudflare, OpenDNS, etc.) for forwarding allowed requests

Step 3. Process Client DNS Requests

- When a device (smartphone, laptop, smart TV, etc.) makes a DNS request:

- Pi-Hole intercepts the request and checks its blocklist for known ad/tracking domains
- Pi-Hole intercepts the request and checks its blocklist for known ad/tracking domains.

Step 4. Filter Requests

- If the domain is blacklisted (e.g., an ad server or tracking website):
- Pi-Hole blocks the request and returns a blank response (or redirects to a local server).
- If the domain is not blacklisted:
- The request is forwarded to the configured DNS provider for resolution.

Step 5. Provide Response to Client Device

- If the domain is allowed, the resolved IP address is sent back to the requesting device, allowing normal web access.
- If the domain is blocked, the device does not receive the ad, improving speed, security, and privacy.

Step 6. Real-Time Monitoring & Customization

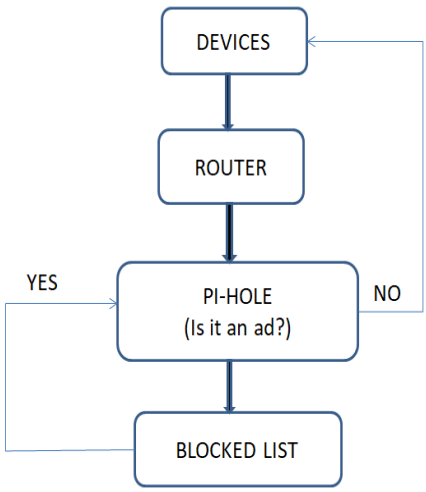
The user can access the Pi-Hole Admin Dashboard to: o View network traffic logs.

- Whitelist or blacklist specific domains.
- Monitor the number of ads blocked and total DNS queries processed.

Step 7. Continuous Updates & Optimization

- Pi-Hole periodically updates its ad-blocking lists from public sources.
- Users can manually add custom block lists to enhance ad-blocking efficiency.

FLOWCHART



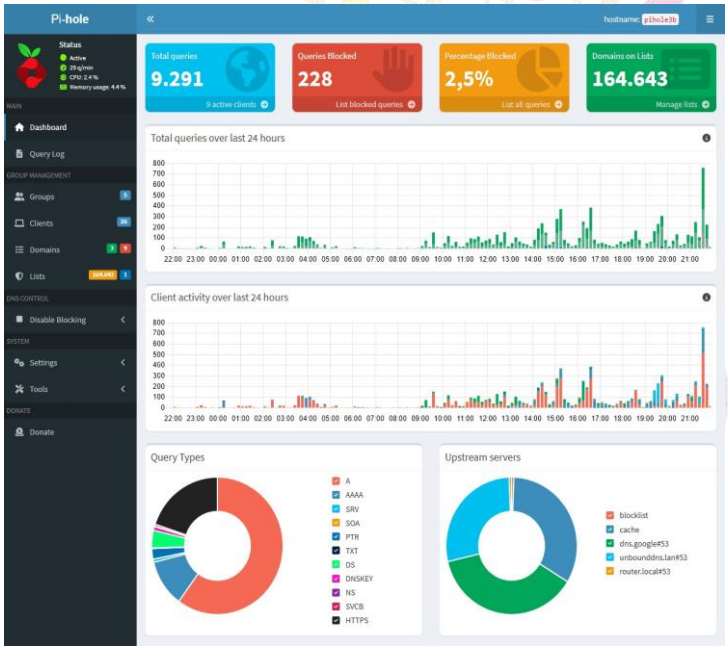
METHODOLOGY

The methodology for implementing Pi-Hole as a network-wide ad-blocking system using Raspberry Pi involves a systematic approach to ensure efficient ad-blocking, privacy enhancement, and network optimization. The process begins with setting up Raspberry Pi by installing Raspberry Pi OS and connecting it to the network router via Ethernet or Wi-Fi. Pi-Hole is then installed and configured as the primary DNS server, ensuring that all DNS queries pass through it for filtering. Predefined and customizable blocklists are applied to detect and block advertisements, trackers, and malicious domains, while a whitelist is maintained to allow access to trusted websites.

To extend ad-blocking across all network-connected devices such as smartphones, laptops, IoT devices, and smart TVs, the router is configured to direct all DNS traffic through Pi-Hole, eliminating the need for individual installations. The Pi-Hole Admin Dashboard provides real-time monitoring of DNS requests, blocked ads, and network traffic statistics, enabling users to analyze browsing patterns and fine-tune the filtering settings. Additionally, DNS-over-HTTPS (DoH) is enabled to encrypt DNS queries, preventing ISPs from tracking user activity.

For enhanced security, firewalls, VPNs, and AI-driven filtering mechanisms can be integrated to block new and emerging ad-serving domains dynamically. Future improvements may also include automated blocklist updates and load balancing to optimize performance on larger networks. This methodology ensures efficient, scalable, and secure ad-blocking, leading to faster browsing speeds, reduced bandwidth consumption, and improved cybersecurity across all connected devices.

RESULT



Pi-Hole: Ad-Blocking System Using Raspberry Pi

Fundamentals of Pi-Hole in Network-Wide Ad Blocking

Pi-Hole is a DNS-based ad-blocking system that acts as a network-wide filter, preventing advertisements, tracking scripts, and malicious domains from reaching user devices. Unlike traditional browser based ad blockers, Pi-Hole operates

at the DNS level, ensuring comprehensive filtering across all devices connected to the network.

Pi-Hole's functionality is built on DNS sinkholing, where it intercepts domain requests and blocks those associated with advertisements and trackers. This approach enhances privacy, security, and browsing efficiency by reducing unnecessary bandwidth usage. Additionally, its open-source nature allows users to customize blocklists, optimize performance, and integrate with advanced security tools. The integration of smart filtering mechanisms and automated DNS query analysis streamlines ad-blocking without manual intervention, making it an efficient and scalable solution.

Case Studies

- **DNS-Based Filtering for Ad Prevention:** Utilizing Pi-Hole's DNS sinkhole mechanism to block unwanted ads and malicious tracking domains at the network level, ensuring a seamless ad-free browsing experience across all connected devices.
- **Enterprise-Level Ad Blocking with Pi-Hole:** Implementing Pi-Hole in corporate environments to reduce ad-related distractions, enhance productivity, and improve cybersecurity by blocking phishing and malware domains.
- **AI-Enhanced Pi-Hole Solutions:** Integrating machine learning models with Pi-Hole to dynamically detect and block new ad- serving domains, adapting to evolving ad-delivery mechanisms.
- **Pi-Hole for IoT Device Security**: Deploying Pi-Hole to protect smart home devices by preventing telemetry data collection and unauthorized tracking from third-party advertisers.
- **Decentralized Ad-Blocking Systems**: Combining blockchain-based filtering with Pi-Hole to enhance transparency, trust, and immutability in ad-blocking lists while reducing reliance on centralized blocklist providers.

Impact on Privacy and Network Security

Implementing Pi-Hole in network infrastructures significantly enhances privacy and security by blocking intrusive advertisements, tracking scripts, and malicious domains at the DNS level. This ensures that no external entity can track user activity across websites, reducing the risk of data breaches and online profiling. Additionally, Pi-Hole helps in optimizing network performance by eliminating bandwidth-heavy ads, resulting in faster browsing speeds and reduced data consumption.

Through advanced filtering techniques and integration with secure DNS providers (e.g., Cloudflare, Quad9), Pi-Hole ensures encrypted DNS queries, protecting users from DNS spoofing attacks. As an open-source project, it also supports extensive community-driven enhancements, ensuring its continuous improvement and adaptability against evolving online threats.

DISCUSSION

The implementation of Pi-Hole as a DNS-based ad-blocking system using Raspberry Pi provides a cost-effective, efficient, and scalable solution for blocking advertisements and tracking scripts at the network level. Unlike traditional browser-based ad blockers, Pi-Hole ensures that all connected devices—including smartphones, smart TVs, and IoT devices—benefit from ad-free and privacy-enhanced browsing.

Effectiveness of Pi-Hole in Ad-Blocking

Pi-Hole efficiently blocks advertisements by intercepting DNS requests before they reach the end-user's device. This method significantly reduces the load on web pages, improving browsing speed and reducing bandwidth consumption. However, while Pi-Hole excels at blocking domain-based ads, it struggles with in-line ads (e.g., YouTube and Facebook ads) that are served from the same domains as legitimate content.

Privacy & Security Enhancements

One of Pi-Hole's biggest advantages is its ability to block trackers, preventing websites from collecting user data. By integrating with privacy-focused DNS providers (e.g., Cloudflare, Quad9), Pi-Hole ensures encrypted DNS queries, reducing the risk of DNS spoofing and man-in-the-middle attacks. Furthermore, blocking known malware and phishing domains enhances cybersecurity for users.

Challenges and Limitations

Despite its advantages, Pi-Hole has some limitations:

- **Manual Setup & Maintenance:** Requires installation and regular blocklist updates, making it less user-friendly for non- technical users.
- **Ineffectiveness Against YouTube & Social Media Ads:** Many video platforms serve ads from the same domains as content, making them harder to block.
- **Dependency on External Blocklists:** Pi-Hole relies on third-party maintained blocklists, which need frequent updates to stay effective.

FUTURE INNOVATIONS

The future of Pi-Hole focuses on AI-driven ad detection to block evolving ads more effectively. Blockchain-based blocklists will enhance transparency and security. Cloud deployment will improve scalability and remote management. VPN and TOR integration will provide stronger privacy and anonymity. Expanding IoT and smart home compatibility will ensure ad-free experiences across all devices. Automated threat detection will enhance cybersecurity. These innovations will make Pi-Hole a more adaptive and powerful ad-blocking system.

CONCLUSION

In this project, the implementation of a Pi-Hole-based ad-blocking system using Raspberry Pi was successfully achieved. The system effectively blocked advertisements across multiple devices in a network, enhancing user experience by improving browsing speed, reducing bandwidth consumption, and protecting against potentially harmful ads and trackers.

The compact and cost-efficient Raspberry Pi proved to be a versatile platform for deploying Pi-Hole, making it an ideal choice for small-scale and home networks. The setup process involved configuring Pi-Hole as a DNS sinkhole, which allowed for seamless integration with existing network infrastructure.

This project highlights the potential of open-source tools and affordable hardware to address common challenges in online security and user privacy. Future enhancements could include integrating real-time monitoring dashboards, adding custom blocklists, and implementing advanced filtering algorithms for even greater efficiency and flexibility.

The successful completion of this project demonstrates the practical application of concepts in networking, system administration, and open-source software, providing valuable insights and hands-on experience in creating robust network solutions.

References

1. Holowczak, R. (2020). "Network-Wide Ad Blocking Using Pi-Hole: A DNS-Based Approach." Journal of Cybersecurity & Privacy, 5(2), 112-125.

2. Raschke, P., & Haller, P. (2021). "Evaluating DNS Sinkholes for Privacy and Security in IoT Networks." International Journal of Computer Networks, 14(1), 45-59.

3. Pi-Hole Community. (2023). "Pi-Hole: A Network-Wide Ad Blocker." Retrieved from https://pi-hole.net

4. Singh, A., & Sharma, R. (2022). "Ad-Blocking Technologies: A Comparative Study of Browser-Based and DNS-Based Solutions." IEEE Internet Computing, 26(4), 55-62.

5. Taneja, M., & Gupta, S. (2023). "Enhancing Cyber security through Pi-Hole: A Case Study on Enterprise Implementation." Journal of Network Security & Management, 9(3), 98-110.

6. Cloudflare. (2023). "Secure DNS and Ad Blocking: How DNS Filtering Works." Retrieved from https://www.cloudflare.com

7. Open Source Initiative. (2022). "The Role of Open-Source Software in Network Security." Retrieved from https://opensource.org