iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.59745

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

ShieldedLink Application: A Comprehensive Mobile Security Solution

Reddyvari Venkateswara Reddy[1], K Sujitha[2], Batchu Sai Karthik[3], Yaramadi Sai Naveen Kumar[4], Thandra Bhanuprakash[5]

[1]*Associate Professor, Department of CSE (CyberSecurity), CMR College of Engineering and Technology, Hyderabad, Telangana, India*

[2]*Associate Professor, Department of CSE (CyberSecurity), CMR College of Engineering and Technology, Hyderabad, Telangana, India*

[3, 4, 5]*Student, Department of CSE (Cyber Security), CMR College Of Engineering and Technology, Hyderabad, Telangana, India*

Abstract: ***ShieldedLink Application is a robust DNS resolver and firewall solution designed to prioritize speed, security, privacy, and configurability. Operating across over 300 global locations within Cloudflare's data centers, it offers end-to-end median latency as low as 30ms, ensuring swift resolution of domain names to IP addresses. Security is ensured through exclusive response over TLS, safeguarding user data from potential surveillance and DNS manipulation attacks. Each user benefits from a dedicated endpoint, guaranteeing privacy akin to a personalized resolver setup. Transparency is facilitated with optional per-user logs for analytics and reporting. Additionally, users enjoy configurability through preset blocklists, empowering them to define firewall rules based on their preferences. Complemented by the ShieldedLink Application companion app for Android, users can further enhance their security by implementing granular app blocking rules, including blocking by category, app activity, or device status.***

Keywords: DNS resolver, Firewall, Security, Privacy, Configurability, TLS, Cloudflare, DNS Manipulation Attacks, Android app.

I. INTRODUCTION

In today's digital landscape, protecting online privacy and security is more crucial than ever. The Domain Name System (DNS), often referred to as the "internet's address book," plays a vital role in converting human-readable domain names into machine-readable IP addresses, facilitating seamless web navigation. However, conventional DNS services face vulnerabilities that compromise user privacy and expose them to cyber threats.

Responding to these challenges, the ShieldedLink Application emerges as a groundbreaking solution—a fast, secure, private, transparent, and customizable DNS resolver paired with a robust firewall. By harnessing cutting-edge technologies and innovative strategies, the ShieldedLink Application establishes a new benchmark for internet privacy and security, empowering users to regain control over their online experiences.

A. Fast and Efficient

With end-to-end median latency as low as 30ms, ShieldedLink Application ensures swift and responsive resolution of domain names to IP addresses. This remarkable speed is attributed to the extensive network of over 300 locations worldwide, strategically positioned within Cloudflare's data centers. By routing user requests to the nearest server, The ShieldedLink Application minimizes latency and enhances the browsing experience, setting a new benchmark for DNS performance.

B. Security By Design

Security lies at the core of the ShieldedLink Application, underpinned by the adoption of Transport Layer Security (TLS) protocol. By exclusively responding over TLS, ShieldedLink Application mitigates the risk of eavesdropping and DNS manipulation attacks, safeguarding user privacy and integrity of data transmission. By encrypting DNS queries, the ShieldedLink Application ensures that ISPs and governmental agencies are unable to monitor or intercept users' browsing activities, thus preserving their online anonymity and freedom.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

C. Privately Personalized

Unlike conventional DNS resolvers, ShieldedLink Application assigns each user their unique endpoint, fostering a personalized and private browsing environment. This tailored approach ensures that users receive dedicated resolver instances, eliminating the risk of data leakage or interference from other users. By prioritizing user privacy and autonomy, the ShieldedLink Application empowers individuals to navigate the internet with confidence and peace of mind.

D. Transparent and Configurable

The ShieldedLink Application embraces transparency by offering users the option to access per-user logs for analysis and generating insightful analytics and reports. This transparency empowers users to monitor their online activities and gain valuable insights into their browsing patterns. Moreover, the ShieldedLink Application provides extensive configurability, allowing users to customize firewall rules using preset blocklists according to their preferences. Whether it's blocking specific categories of apps or enforcing restrictions based on app usage or device status, the ShieldedLink Application puts the control back into the hands of users.

E. Companion App for Enhanced Protection

To further enhance internet security, ShieldedLink Application offers a companion app for Android devices, doubling up as a powerful firewall. Equipped with advanced features such as blocking apps by category, restricting background app usage, and imposing permanent app blocks, the companion app extends the protective capabilities of the ShieldedLink Application to mobile devices, ensuring comprehensive protection across all platforms.

II. LITERATURE REVIEW

A. "Beal, V. (2019). What is a Virtual Private Network (VPN)"

Beal's paper (2019) succinctly defines Virtual Private Networks (VPNs) are connections that are encrypted and secure that are formed over public networks such as the internet. They play a vital role in safeguarding private information and maintaining privacy. Exploring various VPN types such as remote access and site-to-site configurations, Beal highlights their significance in enabling secure access to resources and maintaining anonymity, particularly in remote work and mobile computing contexts.

B. "Mobile Security. (2022). National Institute of Standards and Technology (NIST)."

The website of the National Institute of Standards and Technology is a great place to gather information regarding mobile security devices (NIST). It offers a summary of the best practices for safeguarding mobile devices and apps in addition to insights into how the risk landscape changes. NIST emphasizes the need to protect personal information and mitigate the hazards associated with mobile computing. Instructions on how to assess risks, implement safety measures, and stay up to date with developments in the mobile industry are provided on the website. This is a great resource for businesses and individuals looking to gain a better understanding of mobile privacy and create robust security policies to protect mobile devices and data.

C. "Solanki, K. (2019). A Guide to DNS Security Best Practices. Infosec Institute."

The Infosec Institute-published Solanki (2019) handbook provides a thorough review of DNS security best practices and offers insightful advice on how to mitigate risks and vulnerabilities connected to DNS. With sections on distributed denial-of-service (DDoS) threats, cache poisoning, and DNS spoofing, this guide offers doable suggestions for strengthening DNS security posture. To provide readers with practical strategies to strengthen their organization's DNS security defense and effectively mitigate potential risks, Solanki emphasizes the significance of implementing secure DNS configurations, monitoring DNS traffic, and utilizing DNSSEC (Domain Name System Security Extensions).

D. "Firewalls. (2022). Cisco."

A thorough explanation of firewall technology and its use in contemporary network security techniques may be found on Cisco's firewall homepage. The website showcases Cisco's assortment of firewall products and solutions made to shield businesses from online dangers like malware, illegal access attempts, and data breaches. Cisco demonstrates how firewalls work to filter network traffic, enforce security standards, and identify and stop malicious activity with thorough explanations and visual aids. For businesses looking to put strong firewall security in place to secure their networks and sensitive data from cyberattacks, this resource is a great resource.

III. OBJECTIVE

The goal of this mobile application project is to create a comprehensive security solution that integrates virtual private networks (VPNs), activity monitoring capabilities, DNS protection, and firewalls. The primary goals are to increase user privacy and mobile security, which are accomplished by providing robust defense mechanisms against cybersecurity risks such as malware infiltration, unauthorized access, data interception, and criminal activity. To accomplish this, the mobile application will leverage VPN features to provide mobile devices with safe, encrypted connections. This will make it possible for people to browse the internet safely and anonymously, especially those who use public Wi-Fi networks. Firewall features will also be implemented to monitor and control network traffic. This will let users enforce security regulations and stop harmful or unauthorized access attempts.

Moreover, the firewall features of the mobile application would be crucial for managing and keeping an eye on network traffic. Users can establish stringent security standards and prevent unauthorized access attempts by implementing robust firewall mechanisms. Through proactive detection and blocking of questionable network activity, the firewall feature provides an extra line of security against potential cyber threats and penetration attempts.

To stop DNS-based attacks like DNS spoofing and DNS cache poisoning, DNS protection will also be a part of the security solution.

IV. SYSTEM REQUIREMENTS

A. Hardware

The system needs sufficient resources like CPU, RAM, and storage, along with dedicated graphics capable of handling the intensive processing demands of Android Studio. Suitable graphics cards include Nvidia graphics series 20, 30, and 40.

B. Operating System

The operating system should be capable of running and managing the high processing demands of Android Studio. Common options include Linux, Windows, Mac, and ChromeOS.

C. Internet Connection

A stable and reliable internet connection is essential to download necessary packages and libraries.

V. PROBLEM DEFINITION

For customers who are worried about control, security, and privacy when using the internet, the mobile application offers a full answer. It provides privacy and anonymity by blocking the monitoring of surfing activities thanks to its powerful VPN features. Furthermore, by preventing access to known harmful URLs, the program reduces the risk of malware and phishing assaults. It also gives users control over the behavior of apps and limits internet access to certain apps, therefore reducing privacy concerns. Users can also get around limitations and visit websites and services that are restricted in areas where internet censorship is in place, which supports the freedom of speech and information.

VI. EXISTING SOLUTIONS

A. Avast Mobile Security

Avast Mobile Security is a popular choice among mobile users concerned about their device's security. It offers essential features like anti-theft, privacy protection, and antivirus capabilities. However, one limitation of the app is its sole provision of a firewall for regulating mobile device network access. Users might seek additional security measures beyond the firewall to enhance their mobile security further. While the firewall is crucial for monitoring and controlling network traffic, supplementing it with other security measures can provide a more comprehensive mobile security solution.

Fig.1Avast Mobile Security

B. 1.1.1.1

With the encryption of DNS requests, Cloudflare's 1.1.1.1 offers a way to improve user security and privacy while providing a quicker and more private DNS service. Nevertheless, the app's disadvantage is that it modifies mobile devices' domain name systems (DNS). Even though this modification attempts to increase security and privacy, some users could experience problems or interruptions while trying to access particular websites or services as a result of the changed DNS settings. Users should thus be aware of any potential effects on their mobile surfing experience, even if the app offers substantial privacy benefits.

Fig.2 1.1.1.1

C. Express VPN

ExpressVPN's robust encryption, quick servers, and extensive global server network make it a popular choice for anyone seeking privacy and security when surfing the internet. However, one drawback of ExpressVPN is that it only concentrates on changing VPN settings on mobile devices. While VPNs are essential for safeguarding user data from prying eyes and securing online connections, the app's exclusive focus on VPN capabilities may obscure other crucial elements of mobile security, including firewall protection, DNS encryption, or anti-malware tools. Because of this, even while ExpressVPN does a great job at offering VPN services, customers might need to adopt other security measures to ensure complete protection from online dangers.

Fig.3 Express VPN

VII. LIMITATIONS OF THE EXISTING SYSTEM

A. Avast Mobile Security

1) *Restricted Feature Set:* Although Avast Mobile Security has privacy, anti-theft, and antivirus functions, its capability could be less than that of complete mobile security suites that are sold today. Users can require extra features like sophisticated malware detection, firewall protection, or VPN services.
2) *Dependency on the Firewall:* The firewall function of Avast Mobile Security is the main tool used to control network access. Firewalls are necessary for network security, but if an app depends just on this feature, it can miss other crucial elements of mobile security, such as DNS encryption or anti-phishing features.
3) *Impact on Performance:* When using Avast Mobile Security, some users may see lags or performance problems on their smartphones, especially if the program uses a lot of system resources or battery life.

B. 1.1.1.1

1) *Restricted Capabilities:* The only purpose of the 1.1.1.1 app is to offer DNS encryption services; it could not include any other security features like firewall defense, VPN support, or anti-malware measures. It's possible that users looking for all-encompassing mobile security solutions won't find the app's restricted feature set enough.
2) *Concerns About Reliability:* There's a chance that some users won't have consistent connectivity or have trouble setting up a secure DNS while using the 1.1.1.1 app.
3) *Compatibility Problems may arise from DNS Changes:* Although the 1.1.1.1 app encrypts DNS queries to improve privacy and security, mobile device DNS settings changes may result in problems accessing specific websites or services. Because of the changed DNS settings, users could have trouble accessing specific content or experience internet connectivity issues.

C. Express VPN

1) *Limited Attention paid to VPN Services:* ExpressVPN succeeds at offering robust encryption, fast servers, and a huge global server network; nevertheless, by concentrating just on VPN services, it may fail to address other important facets of mobile security. To guarantee complete security against online dangers, users might need further features like DNS encryption, firewall protection, or anti-phishing tools.
2) *Cost of Membership:* To utilize ExpressVPN, users must pay a monthly fee. This is a premium VPN service. The price of the subscription may be too much for certain customers, particularly in light of the availability of free or significantly less expensive VPN options.
3) *Dependency on third-party Servers:* ExpressVPN is dependent on third-party servers situated in different nations worldwide. These servers provide high-speed connectivity and geographic variety, but they may also present security and privacy risks.

VIII. WORKFLOW

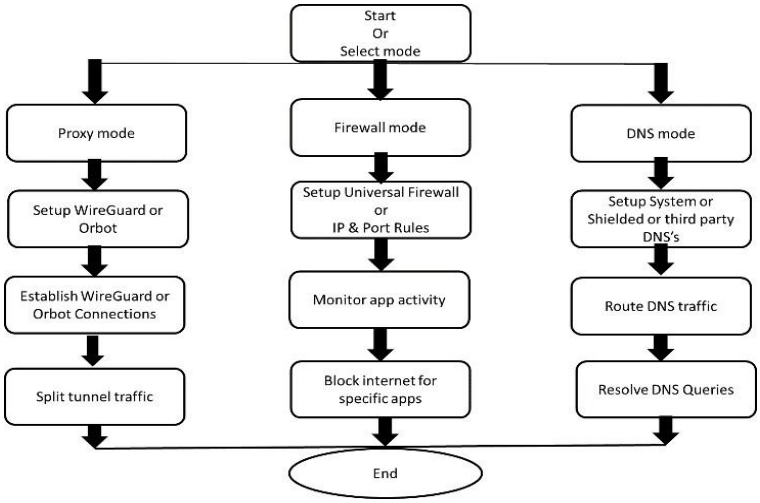


Fig.4 Work Flow

1) *Start of Process:* This is the starting point of the workflow.
2) *Select Mode*
a) DNS (Domain name System).
b) Firewall.
c) Proxy

3) *Setting up Interfaces:* Configure the DNS, Firewall, and Proxy.
4) *Establishment and Maintaining*
a) Block all apps.
b) Route DNS Traffic.
c) Monitoring App Activity.

5) *End of Process:* Signifying the conclusion of the workflow.

IX. ARCHITECTURE

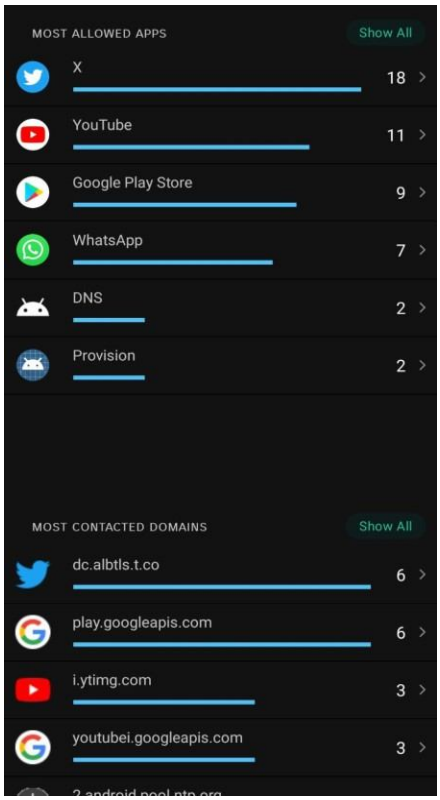


Fig.5: Stats

1) Start Orbot (do not start it in the VPN mode).
2) Take note of Orbot's remarks regarding the "SOCKS5" and "HTTP" fields displayed on its home screen.
3) Open the Shielded Link app; Start it and go to Settings.
4) Enable HTTP Proxy and enter the HTTP port number (as seen in Orbot), if you want just the browsers to use Orbot's Tor bridge.
5) Enable SOCKS5 (TCP) Proxy and enter the port number (from step 2), choose App (as Orbot), and optionally enable Block all UDP traffic except DNS to stop leaking UDP Potential issues may arise with WhatsApp calls, Zoom, and Chromecast functionality, while it's important to note that Orbot does not currently support UDP. By implementing the network firewall rules and usage of tools the network will try to accept or reject the user request.

X. CONCLUSION

In conclusion, the Shielded Link application is a versatile tool that provides a comprehensive solution for enhancing privacy, security, and network control on Android devices. Its multi-mode operation, encompassing VPN, DNS, and Firewall functionalities, caters to a wide range of user needs. The VPN mode's support for multiple Wire Guard up streams in a split-tunnel configuration ensures flexibility and adaptability, while the DNS mode's ability to route DNS traffic to any user-chosen DNS- over-HTTPS or DNSCrypt resolver empowers users with granular control over their DNS resolvers. The Firewall mode's granular application-level control empowers users to restrict internet access based on various criteria, promoting mindful app usage and safeguarding privacy.

XI. RESULTS

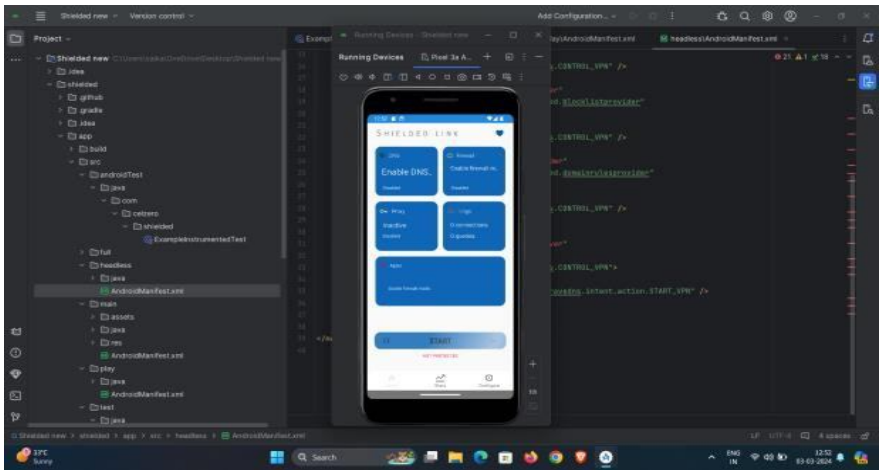


Fig.6: Android Studio Setup

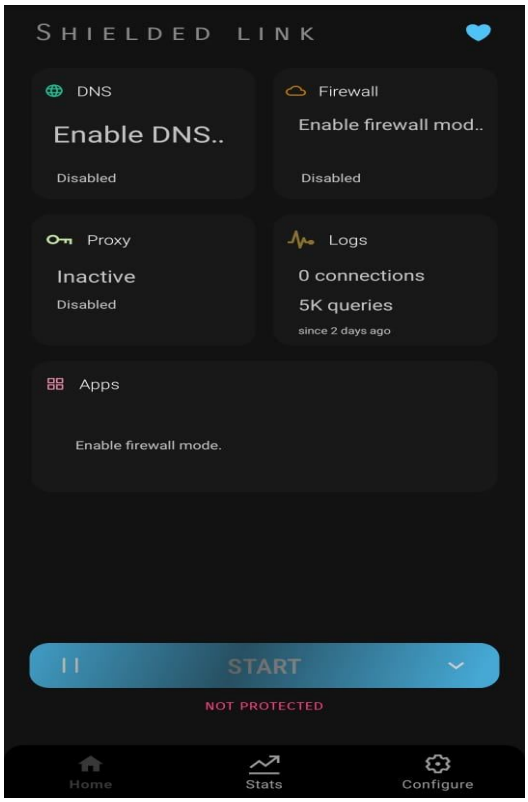
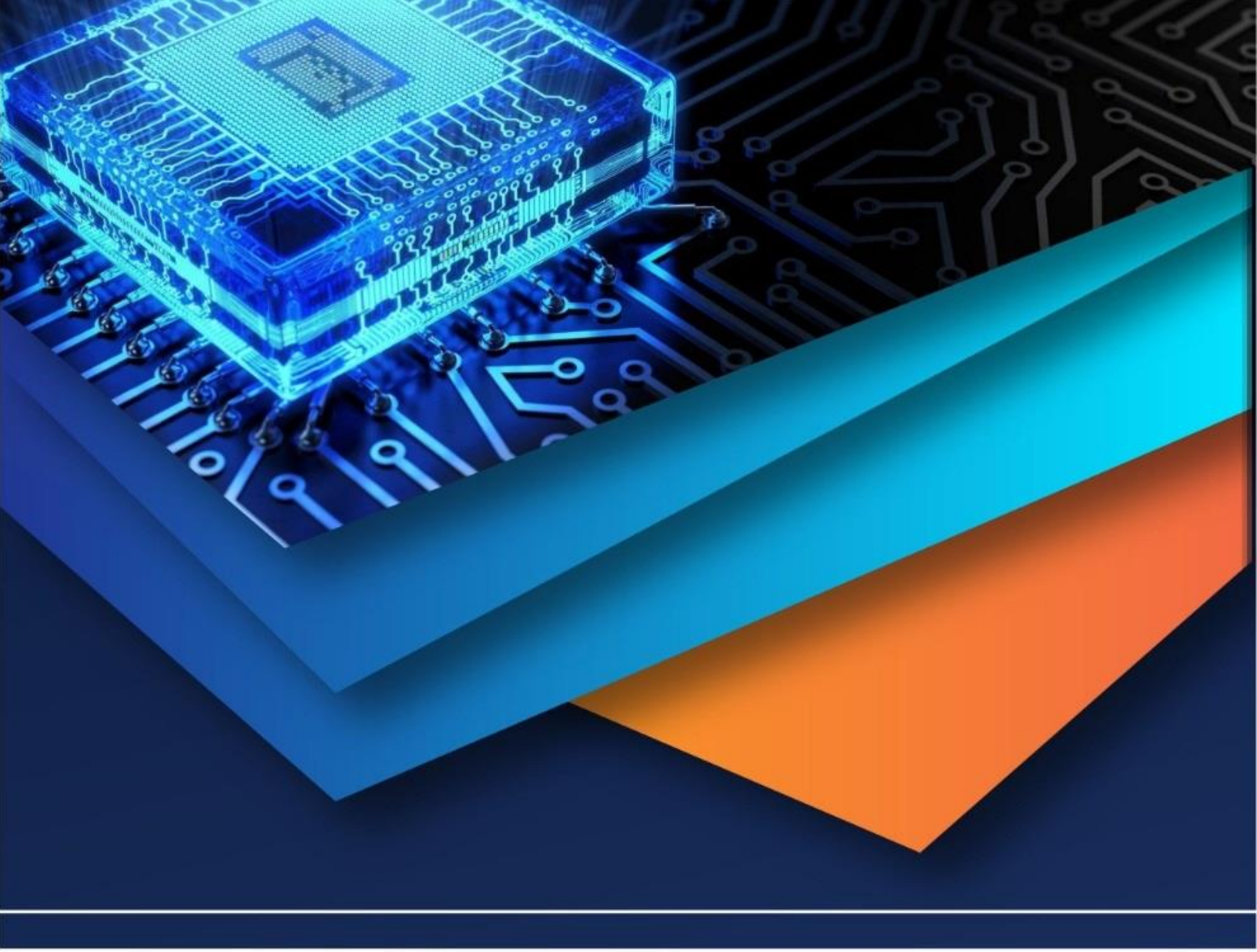


Fig.7: Shielded Link Application

REFERENCES

[1] Beal, V. (2019). What is a Virtual Private Network (VPN)? Webopedia. Retrieved from https://www.webopedia.com/definitions/virtual-private-network-vpn/
[2] Mobile Security. (2022). National Institute of Standards and Technology (NIST). Retrieved from https://www.nist.gov/topics/mobile-security.
[3] Solanki, K. (2019). A Guide to DNS Security Best Practices. Infosec Institute. Retrieved from https://resources.infosecinstitute.com/topic/dns-security-best-practices/
[4] Firewalls. (2022). Cisco. Retrieved from https://www.cisco.com/c/en/us/products/security/firewalls/index.html
[5] DNS Security. (2022). Internet Engineering Task Force (IETF). Retrieved from https://www.ietf.org/wg/dnsop/
[6] Cloudflare. (n.d.). What is DNS? Retrieved from https://www.cloudflare.com/learning/dns/what-is-dns/
[7] RFC 8484 - DNS Queries over HTTPS (DoH). (2018). Internet Engineering Task Force (IETF). Retrieved from https://datatracker.ietf.org/doc/rfc8484/
[8] RFC 7858 - Specification for DNS over Transport Layer Security (TLS). (2016). Internet Engineering Task Force (IETF). Retrieved from https://datatracker.ietf.org/doc/rfc7858/
[9] Fly.io. (n.d.). Fly.io - The Edge Application Platform for Global Apps. Retrieved from https://fly.io/
[10] AWS Security Hub. (n.d.). Amazon Web Services (AWS). Retrieved from https://aws.amazon.com/security-hub/
[11] Stripe. (n.d.). Payments Infrastructure for the Internet. Retrieved from https://stripe.com/
[12] GuardianApp. (n.d.). GuardianApp - Mobile Firewall & VPN for Advanced Privacy. Retrieved from https://guardianapp.com/
[13] Blokada. (n.d.). Blokada - The Best Ad Blocker for Android. Retrieved from https://blokada.org
[14] Pi-Hole. (n.d.). Pi-hole - Network-wide Ad Blocking. Retrieved from https://pi-hole.net/
[15] NextDNS. (n.d.). NextDNS - Secure, Private, and Fast DNS Resolver. Retrieved from https://nextdns.io/
[16] OpenDNS. (n.d.). OpenDNS - Cloud-Delivered Security Solutions. Retrieved from https://www.opendns.com/
[17] Cloudflare Gateway. (n.d.). Cloudflare Gateway - Secure Web Gateway Service. Retrieved from https://www.cloudflare.com/products/cloudflare-gateway/
[18] Warp. (n.d.). Cloudflare Warp - VPN for Secure and Private Browsing. Retrieved from https://developers.cloudflare.com/warp/
[19] Mozilla. (n.d.). Mozilla - DNS over HTTPS (DoH) Explained. Retrieved from https://support.mozilla.org/en-US/kb/firefox-dns-over-https
[20] TLS 1.3 Explained. (2022). Cloudflare. Retrieved from https://blog.cloudflare.com/tls-1-3-explained/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY