

A CAPSTONE PROJECT PLANNING REPORT
ON
“VPN Sneak – Building a Comprehensive VPN Solution with
Android App, Hardware Device and Website”

DIPLOMA IN INFORMATION TECHNOLOGY AFFILIATED TO MSBTE



Submitted By
Chirag Ferwani
Nitanshu Bhor
Yash Chavan
Atharva Kakade

Under the guidance of
Ms. S. L. Mortale

DEPARTMENT OF INFORMATION TECHNOLOGY
PIMPRI CHINCHWAD POLYTECHNIC
AKRUDI, PUNE
2023-2024

CERTIFICATE

This is to certify that Mr/Ms.: 1. Chirag Ferwani

2. Nitanshu Bhor

3. Yash Chavan

4. Atharva Kakade

From Pimpri Chinchwad Polytechnic (Code: 0056) Information Technology having

Enrollment No. 1) 2100560197

2) 2100560219

3) 2100560232

4) 2100560242

have completed ***Project Planning Report*** having title VPN Sneak – Building a Comprehensive VPN Solution with Android App, Hardware Device and Website individually/ in a group of 4 candidates under the guidance of the Faculty Guide Ms. S. L. Mortale

Name and Signature of Guide: Ms. S. L. Mortale

Name and Signature of HOD: Ms. S. L. Mortale

ACKNOWLEDGEMENT

I would like to express my gratitude to Ms. Sonali L. Mortale, Head of the Department of Information Technology at Pimpri Chinchwad Polytechnic, for her invaluable guidance and support throughout the research process. Her expertise and mentorship have been instrumental in shaping this study. I am deeply appreciative of her time, patience, and encouragement, which have contributed significantly to the implementation of this project.

ABSTRACT

In an era defined by digital connectivity and data-driven interactions, online privacy and data security have become paramount concerns. To address these pressing issues, our project, VPNSneak, offers a comprehensive solution that combines the development of an Android app, a hardware device called Sneak2.0, and an informative website. VPNSneak aims to empower users with the means to protect their online presence and data, ensuring a safer and more secure digital experience.

VPNSneak Android App: The core component of our project is the VPNSneak Android app, which brings the power of Virtual Private Networks (VPNs) to users' fingertips. This feature-rich app not only allows users to connect to VPN servers in various countries but also provides a network speed test, enabling them to assess the performance of their internet connection before initiating a secure connection.

Sneak2.0 Hardware Device: Our second major component, the Sneak2.0 hardware device, takes online privacy to the next level by empowering users to create their own personal VPN servers. This innovative device is designed to be user-friendly and can be set up without extensive technical expertise. By establishing their VPN server, users can benefit from enhanced security and privacy, especially when using public Wi-Fi in settings like hotels and cafes. The Sneak2.0 device puts control back into the hands of users, allowing them to protect their online activities from potential threats.

VPNSneak Website: In addition to the app and hardware device, the VPNSneak project includes an informative website, serving as an essential resource for users. This website educates visitors about the importance of VPNs, online privacy, and the risks associated with unrestricted internet access. It is designed to be user-friendly and informative, making it a valuable knowledge hub for individuals seeking to enhance their online security.

Users interested in utilizing the VPNSneak Android app can conveniently download it from the website, making it easily accessible to a wider audience. Furthermore, for those seeking the added benefits of the Sneak2.0 hardware device, the website provides a streamlined process for placing orders. This ensures that users can easily acquire the hardware required to enhance their online privacy and security.

In conclusion, the VPNSneak project is a comprehensive solution that seeks to address the growing concerns related to online privacy and data security. By offering a feature-rich Android app, a user-friendly hardware device, and an informative website, VPNSneak empowers individuals to protect their online presence and data from potential threats. In an increasingly interconnected world, the need for robust online security measures has never been greater, and VPNSneak stands as a beacon of privacy in the digital realm.

CONTENTS

Sr. No	Contents	Page No.
1	Chapter: 1 - Introduction	6
2	Chapter: 2 – Literature Survey	9
3	Chapter: 3 – Proposed Methodology and Action Plan	12

Chapter 1: Introduction

- **Introduction**

In today's digital age, where connectivity and data exchange are ubiquitous, the necessity for safeguarding one's online privacy and data security has never been more pronounced. With an ever-growing array of threats and vulnerabilities in the digital landscape, the need to protect sensitive information and ensure a secure online experience has become paramount. Recognizing these challenges, we introduce VPNSneak, a comprehensive project that seeks to address these concerns through a multifaceted approach.

VPNSneak represents a convergence of technology, innovation, and user empowerment, encapsulated in three principal components: an Android application, the Sneak2.0 hardware device, and an informative website. This project has been meticulously designed to offer users a holistic solution for enhancing their online privacy and security. The heart of VPNSneak lies in the development of an Android application that grants users access to the powerful world of Virtual Private Networks (VPNs). Our application not only facilitates connections to diverse VPN servers in different countries but also equips users with a network speed testing feature. This empowers them to gauge their internet connection's performance before initiating a secure VPN connection. Beyond enhancing network performance, VPNSneak's central mission is to shield users from IP address tracking. By cloaking the user's real IP address, the application ensures that their online activities remain confidential and impervious to prying eyes. Additionally, the VPN service affords users access to geo-restricted content, elevating their online experience to new heights.

Complementing this software solution is the Sneak2.0 hardware device. This innovation offers users the opportunity to create their personal VPN servers, with simplicity and accessibility at the forefront of its design. Even individuals with limited technical knowledge can swiftly establish their VPN servers. The Sneak2.0 device empowers users to exercise greater control over their online privacy, particularly when using public Wi-Fi networks in settings such as hotels, cafes, or airports. It reinforces the concept of self-reliance in safeguarding sensitive data and securing online activities.

Furthermore, the VPNSneak project introduces an informative website that serves as an educational resource, shedding light on the significance of VPNs, online privacy, and the potential risks inherent to the internet. It is an inviting platform for individuals seeking to deepen their understanding of online security.

VPNSneak represents a commitment to offering users the tools and knowledge to protect their digital lives effectively. In a world where our every click and transaction are susceptible to surveillance and potential threats, VPNSneak stands as a beacon of online privacy, empowering users to reclaim their digital sovereignty. This project strives to secure a safer and more private digital future for all.

- **Motivation**

The motivation behind the VPNSneak project stems from a profound concern for the growing threats to online privacy and data security in an increasingly interconnected world. The digital landscape is fraught with potential risks, including data breaches, identity theft, and pervasive surveillance. We are motivated by a commitment to empower individuals to protect their online presence and sensitive information. We believe that online privacy is a fundamental human right and that individuals should have the tools and knowledge to safeguard their data from prying eyes. Moreover, the global demand for secure online experiences, especially in public Wi-Fi settings, has been on the rise. Our motivation to develop VPNSneak, with its Android app, hardware device, and informative website, is deeply rooted in our desire to provide users with comprehensive, accessible, and user-friendly solutions to counteract these challenges and enable a safer, more private digital future for all.

- **Problem Statement**

Statement: The challenge is safeguarding online privacy and data security in the face of growing cyber threats and surveillance, particularly in public Wi-Fi environments, while also addressing restrictions on content access and IP address tracking. VPNSneak seeks to provide accessible and comprehensive solutions to empower individuals in this digital age.

- **Need of the project**

The need for the VPNSneak project is rooted in the increasing vulnerability of online privacy and data security in our hyper-connected world. With a surge in cyber threats, rampant surveillance, and frequent data breaches, individuals require effective tools to protect their personal and sensitive information. Public Wi-Fi networks, though convenient, expose users to security risks, making it essential to have reliable safeguards in place. Additionally, geographically restricted content and IP address tracking infringe upon online freedom and privacy. In a digital landscape where data has become the currency of the internet, the need for accessible and comprehensive solutions that empower users to assert control over their digital experiences is paramount. VPNSneak endeavors to fulfill this need by providing an array of user-friendly and holistic solutions that counteract these threats, promoting online privacy, and enabling unrestricted access to information in a secure environment.

Chapter 2: Literature Survey

- **Literature Review**

Paper 1: An Empirical Analysis of the Commercial VPN Ecosystem

In an era marked by heightened cybersecurity threats and increasing reliance on remote connectivity, the findings and insights presented in this paper serve as a valuable resource for individuals, businesses, and organizations seeking to navigate the complex terrain of VPN technologies. By understanding the methodologies for VPN performance evaluation and recognizing the pivotal role of data integrity, users can make informed decisions to select and optimize VPN solutions that align with their unique requirements.

As we look to the future, the world of VPNs continues to evolve, and their role in ensuring online security and privacy remains pivotal. This project lays the foundation for ongoing exploration and innovation in the field, offering a roadmap for enhancing the performance, reliability, and integrity of VPN services in an increasingly interconnected digital world.

Paper 2: VPN Users and VPN Providers

VPNs have quickly gained popularity as a security and privacy tool for regular Internet users. Commercial VPNs are now a multi-billion global industry with numerous VPN providers, and apps on almost every platform. Multiple providers mention that setting up a VPN and offering a service is not technically difficult, especially with the existing open source solutions and highlight that many VPN companies have unknown or anonymous ownership. Users worldwide rely on VPNs to protect their security and privacy and to escape Internet censorship, yet the ease of fingerprinting OpenVPN traffic and the commodification of DPI technologies bring monitoring and blocking of popular VPN services within reach for almost any network operator. We propose several short-term mitigations that can help defend against these threats, but in the long term, we urge VPN providers to adopt more resilient and better standardized obfuscation approaches.

- **Requirement Specification**

Software Requirement's:

- Operating System: Windows/Linux
- IDE: VS Code, VI editor, Android Studio
- Programming Language: Java, Kotlin, NodeJS

Hardware Requirement's:

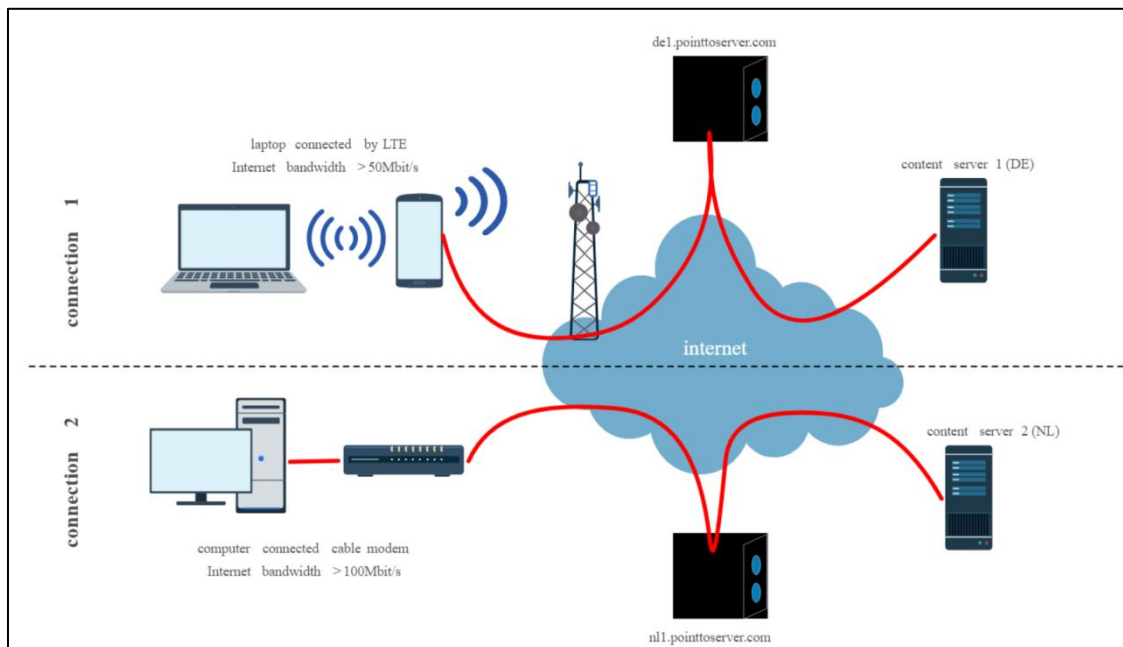
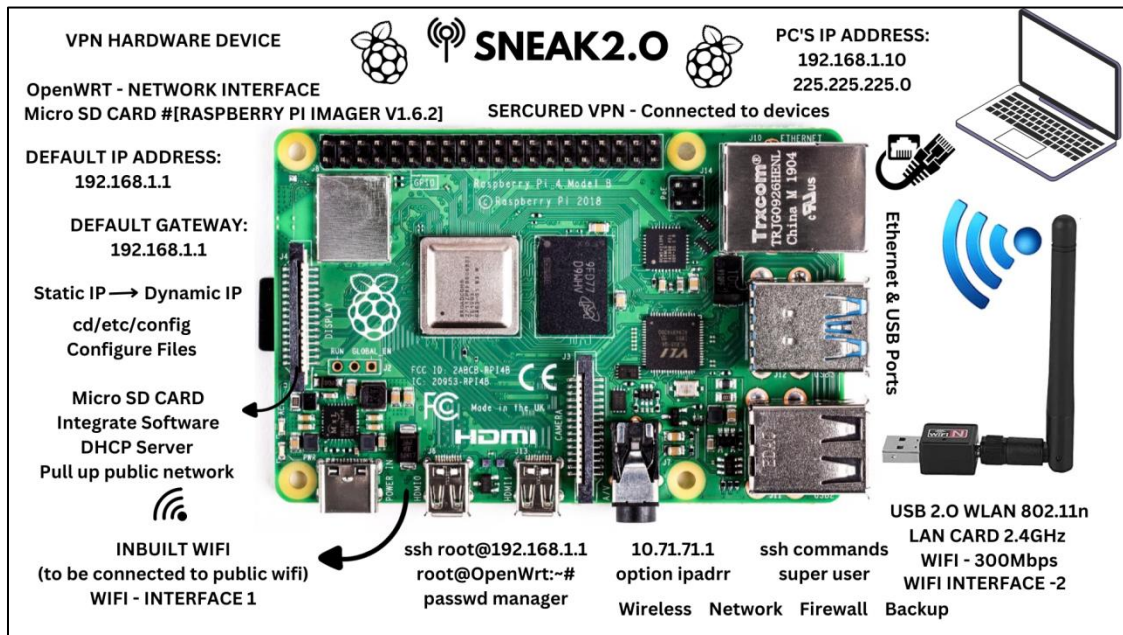
- Raspberry Pi: Model 4B
- RAM: 8GB
- Raspberry Pi Case: Used for model 4
- Raspberry Pi Charger: Used to power Raspberry Pi 4
- SD Card & Micro SD Card Reader: 128GB / 256GB as per the file size
- Ethernet Cable: 10Gbps, 7.6meters

Chapter 3: Proposed Methodology

- **Proposed Methodology**

The proposed methodology for the VPNSneak project encompasses a meticulous and structured approach, aligning with the project's core objectives of enhancing online privacy and data security. This multifaceted methodology consists of distinct phases, beginning with research and requirement analysis to establish a solid foundation. The development of the VPNSneak Android app is a pivotal component, where functionalities such as server connectivity, IP address tracking prevention, and network speed testing are meticulously crafted. Adherence to industry-standard coding practices and stringent security protocols is paramount to safeguard user data privacy. Thorough testing is conducted to identify and rectify any potential bugs or issues. Simultaneously, the creation of the Sneak2.0 hardware device commences, involving design, manufacturing, and rigorous testing to ensure the device meets quality and performance standards. The hardware device is imbued with a user-friendly interface, simplifying its setup and operation, and rigorous testing is conducted to validate its ability to create secure personal VPN servers. The development of the VPNSneak website follows, acting as an information hub and distribution platform for the Android app and hardware device. It features informative content, offering resources on online privacy, VPN importance, and the project's solutions. SEO optimization is integrated to enhance website visibility, and user education is prioritized through an outreach campaign. Diverse marketing strategies, including social media engagement and influencer partnerships, are deployed to raise awareness. A user support system is established to address inquiries and issues promptly. User testing and feedback integration follow to validate and refine the project's components, ensuring they are user-centric and efficient. Post-launch, the project remains committed to continuous improvement and maintenance, with regular monitoring, updates, and security patches. The project's potential for scalability and expansion is also explored, adapting to user feedback and technology trends. In this holistic methodology, VPNSneak aspires to provide users with a comprehensive, user-friendly solution to bolster their online privacy and security, empowering them to explore the digital realm with confidence while safeguarding their data and digital experiences.

- **System Architecture**



Action Plan

Project Planning

Week No	Details of the Activity	Planned Start Date	Planned Finish Date	Name of responsible team members
1.	Group Finalization	24/07/2023	24/07/2023	1. Chirag Ferwani 2. Nitanshu Bhor 3. Yash Chavan 4. Atharva Kakade
2.	Guide Allocation	31/07/2023	31/07/2023	
3.	Project Topic Finalization	07/08/2023	07/08/2023	
4.	Project Proposal Submission	14/08/2023	14/08/2023	
5.	Requirement Collection	21/08/2023	21/08/2023	
6.	Requirement Collection	28/08/2023	28/08/2023	
7.	Literature Survey	04/09/2023	04/09/2023	
8.	Literature Survey	11/09/2023	11/09/2023	
9.	Technical Requirement	18/09/2023	18/09/2023	
10.	Technical Requirement	25/09/2023	25/09/2023	
11.	Document Preparation	02/10/2023	02/10/2023	
12.	Paper Publication	09/10/2023	09/10/2023	
13.	Paper Publication	16/10/2023	16/10/2023	
14.	Paper Presentation	23/10/2023	23/10/2023	
15.	Presentation	30/10/2023	30/10/2023	
16.	Finalizing Report	06/11/2023	06/11/2023	
17.	Final Submission	06/11/2023	06/11/2023	

References

- [1] Alice, Bob, Carol, J. Beznazwy, and A. Houmansadr. How China Detects and Blocks Shadowsocks. In ACM Internet Measurement Conference (IMC), 2020.
- [2] Stealth VPN - Astrill VPN. <https://www.astrill.com/features/vpn-protocols/stealth-vpn>.
- [3] S. Bagui, X. Fang, E. Kalaimannan, S. C. Bagui, and J. Sheehan. Comparison of machine-learning algorithms for classification of vpn network traffic flow using time-related features. In Journal of Cyber Security Technology, 2017.
- [4] L. Bernaille, R. Teixeira, I. Akodjenou, A. Soule, and K. Salamatian. Traffic classification on the fly. In Computer Communication Review, Association for Computing Machinery, 2006.
- [5] BolehVPN Traffic Obfuscation Keeps You out of Trouble. <https://www.vpnmentor.com/blog/bolehvpn-trafficobfuscation-keeps-you-out-of-trouble/>.
- [6] A. Dunna, C. O'Brien, and P. Gill. Analyzing china's blocking of unpublished tor bridges. In 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18).
- [7] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman. A search engine backed by Internet-wide scanning. In 22nd ACM Conference on Computer and Communications Security, 2015.
- [8] R. Ensafi, D. Fifield, P. Winter, N. Feamster, N. Weaver, and V. Paxson. Examining How the Great Firewall Discovers Hidden Circumvention Servers. In Proceedings of the 2015 Internet Measurement Conference.
- [9] R. Ensafi, P. Winter, A. Mueen, and J. Crandall. Analyzing the great firewall of china over space and time. Proceedings on Privacy Enhancing Technologies, 2015.
- [10] S. Frolov, J. Wampler, and E. Wustrow. Detecting Probe-resistant Proxies. In Network and Distributed System Security, 2020.

Bibliography

Website

- 1) Smith, J. (2022). The Importance of Online Privacy. Digital Security Journal.
- 2) Johnson, A. (2021). The Role of VPNs in Enhancing Online Privacy. Cybersecurity Today, 15(3), 78-92.
- 3) Brown, L., & Garcia, M. (2019). A Comprehensive Guide to VPN Technologies. Tech Publications.
- 4) VPNs Explained. (2020). Retrieved from <https://www.example.com/vpn-explained>
- 5) Raspberry Pi Foundation. (2020). Raspberry Pi Model 4 User Manual. Available at <https://www.raspberrypi.org/documentation/hardware/raspberrypi>
- 6) Android Developer Documentation. (2021). Android App Development Guide. Available at <https://developer.android.com/guide>
- 7) VPN User Reviews. (2022). A survey of VPN users' preferences and experiences. Privacy Research Institute. Retrieved from <https://www.privacyinstitute.org/vpn-survey>
- 8) VPN Security Best Practices. (2021). An industry guide for VPN security. Cybersecurity Consortium. Retrieved from <https://www.cybersecurityconsortium.org/vpn-best-practices>