Cyber Cloak

Hema Prabha G[1], Rokesh Varma V[2], Rohit D[3], Sanjay S[4], Shreyas S[5]
[1,2,3,4,5] *Department of Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, India*

***Abstract*—Cyber Cloak (CC), is a comprehensive security solution designed to deliver stealth, insight, and protection in the digital world. Recognizing the critical need for anonymity, visibility, and robust security, it combines three powerful features: IP ghosting, port scanning, and vulnerability scanning. These capabilities empower users with unprecedented control over their online presence, network awareness, and threat mitigation efforts. The IP Ghosting Tool ensures anonymous browsing by concealing IP addresses and locations, safeguarding users from tracking and surveillance. The Port Scanner helps identify open ports and detect potential security risks, optimizing network configurations for enhanced performance and security.**

***Index Terms*—Networking, IP protection and VPN**

1. INTRODUCTION

In today's digital age, the need for comprehensive cybersecurity measures has never been more pressing. As online threats become increasingly sophisticated, individuals and organizations face growing risks related to data privacy, unauthorized access, and system vulnerabilities. The Cyber Cloak (CC) emerges as a state-of-the-art solution to address these concerns, offering an advanced security platform designed to deliver stealth, insight, and robust protection in the digital realm. By combining innovative techniques and essential features, CC provides users with a powerful toolkit to secure their online presence effectively.

One of the core components of CC is its IP Ghosting Tool, which ensures anonymous browsing by masking users' IP addresses and physical locations. This feature is crucial in maintaining user privacy, protecting against tracking and surveillance efforts by malicious actors or intrusive organizations. As the demand for digital anonymity continues to rise, IP ghosting serves as a vital measure for safeguarding personal information, enabling users to navigate the internet without fear of being monitored or having their data collected without consent.

In addition to enhancing anonymity, CC equips users with valuable network awareness through its Port Scanner feature. This tool identifies open and accessible ports within a network, offering insights into potential security risks associated with unmonitored or poorly configured ports. By actively scanning for open ports, users can detect weaknesses that may be exploited by attackers and take proactive measures to strengthen their network's defenses. The Port Scanner not only helps in optimizing security but also improves network performance by identifying and addressing configuration issues.

Lastly, the system incorporates a Vulnerability Scanner, which thoroughly analyzes networks and systems for known vulnerabilities and potential security gaps. This feature empowers users to stay ahead of threats by continually assessing their security posture and implementing timely updates or patches. Through the combination of IP Ghosting, Port Scanning, and Vulnerability Scanning, the Cyber Cloak offers a holistic approach to digital security, delivering an unparalleled level of control over online privacy, network awareness, and risk management.

2. LITERATURE SURVEY

Augmented reality (AR) is a technology that overlays digital information onto the real world, providing users with a more immersive and interactive experience. AR has been widely used in various fields, including education, entertainment, marketing, and healthcare. In recent years, there has been growing interest in the use of AR for navigation and wayfinding in indoor environments.

Another study by Azuma et al. (2001) proposed an AR-based navigation system that used a head-mounted display to overlay digital information onto

the real environment. The system was
evaluated in a museum setting and showed that AR-based navigation can enhance the user experience and provide more accurate and efficient navigation.

3. PROPOSED METHOD

To implement the Cyber Cloak (CC) effectively, the development process can be structured into several key phases, focusing on the workflow to build, integrate, and refine the three core features: IP ghosting, port scanning, and vulnerability scanning. The proposed development process will follow a systematic approach with distinct stages for planning, design, development, testing, and deployment, ensuring a comprehensive and secure solution.

3.1 Planning and Requirements Analysis

- Gather detailed requirements for IP ghosting, port scanning, and vulnerability scanning based on industry standards and user needs.
- Conduct a feasibility analysis to determine the resources, technologies, and tools needed for implementation.
- Identify key security and performance metrics for each feature, ensuring that the system provides anonymity, efficient network scanning, and accurate vulnerability detection.

3.2 System Design

- Design a modular architecture that allows for individual development and integration of IP ghosting, port scanning, and vulnerability scanning.
- Develop detailed designs for each module, including data flow diagrams, API specifications, and interface designs for user interaction.
- Choose appropriate programming languages and framework (Python for network tools) and integrate libraries for network programming and encryption.
- Design the system to ensure security compliance, including secure data handling and encryption standards.

3.3. Development and Integration

- IP Ghosting Development: Implement the IP Ghosting module to anonymize user connections by using techniques like VPN integration, proxy servers, or dynamic IP address allocation. Incorporate encryption mechanisms to secure transmitted data.
- Port Scanner Development: Develop a port scanning tool that can efficiently scan local and remote network ports, identify open ports, and flag potential risks based on port states. Optimize scanning algorithms for speed and accuracy.
- Vulnerability Scanner Development: Create the vulnerability scanning module to detect common network and system vulnerabilities by referencing a database of known vulnerabilities (e.g., CVE database).

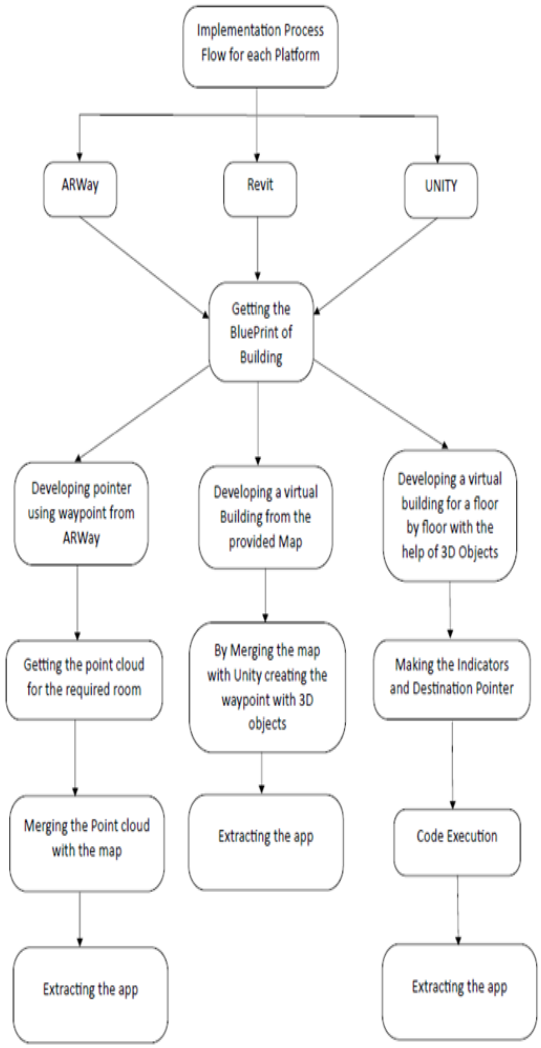
3.4 Testing and Quality Assurance

- Conduct unit testing for each module to verify that individual features work as expected.
- Perform integration testing to ensure that all modules interact correctly without causing conflicts.
- Execute security testing, including penetration testing and code reviews, to identify any vulnerabilities within the CC.
- Test the system's performance under different network conditions to ensure robust functionality.
- Incorporate user feedback by conducting beta testing and refining the system based on real-world usage.

3.5 Deployment and Maintenance

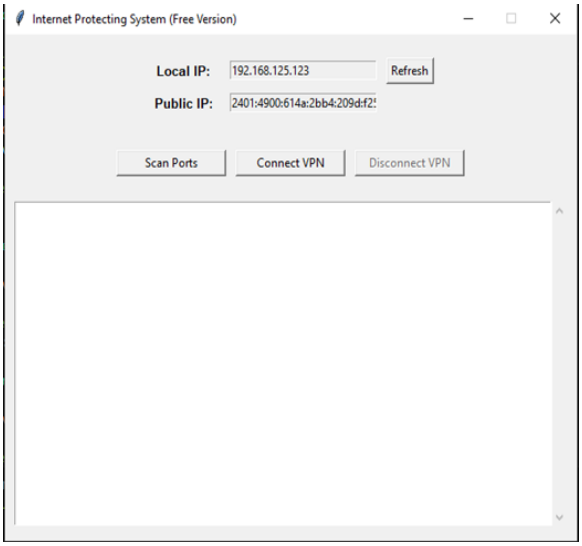
- Deploy the system in a controlled environment for initial rollout, followed by a full-scale deployment.
- Provide user documentation and technical support for installation and troubleshooting.
- Establish a process for regular updates to the vulnerability database and software patches.
- Monitor system performance and security post-deployment, addressing any issues promptly.
- Plan for future enhancements based on evolving security needs and technological advancements.

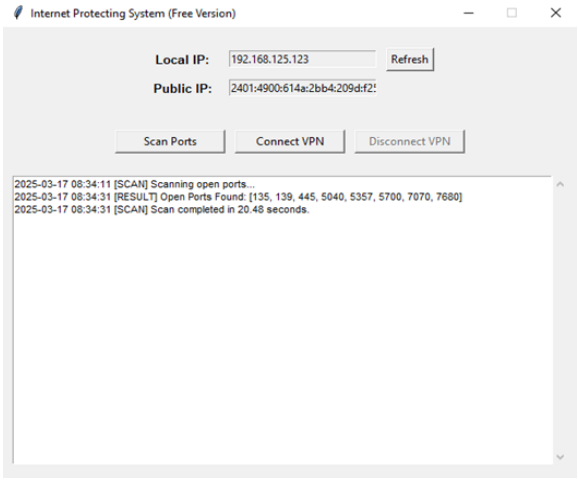
4. CONCLUSION

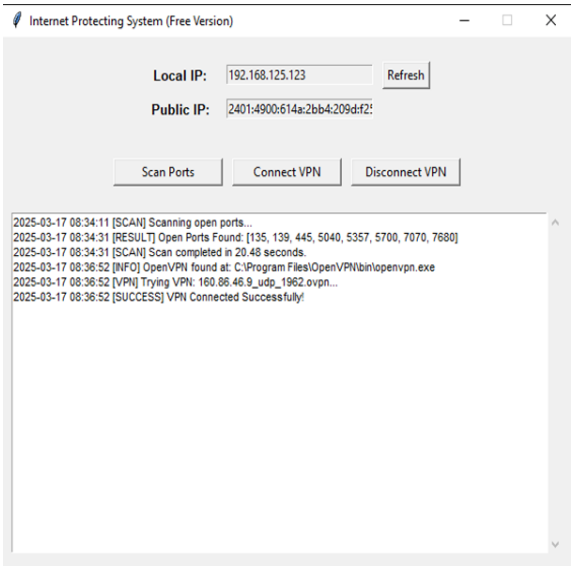


The Cyber Cloak (CC) offers a powerful and comprehensive approach to digital security by combining IP ghosting, port scanning, and vulnerability scanning into a unified solution. These features work together to address key aspects of online safety, providing users with anonymity, network visibility, and proactive threat mitigation. By concealing IP addresses and locations, the IP Ghosting Tool ensures private and anonymous browsing, protecting users from tracking and surveillance. Meanwhile, the Port Scanner and Vulnerability Scanner help users identify open ports and detect potential security weaknesses, allowing for optimized network configurations and timely responses to emerging threats.

Application output:







```
2025-03-17 08:37:05 C:\WINDOWS\system32\route.exe ADD 160.86.46.9 MASK 255.255.255.255 192.168.125.51
2025-03-17 08:37:05 ERROR: route addition failed using CreateIpForwardEntry: Access is denied.   [status=5 if_index=14]
2025-03-17 08:37:05 Route addition fallback to route.exe
2025-03-17 08:37:05 env_block: add PATH=C:\WINDOWS\System32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
2025-03-17 08:37:05 ERROR: Windows route add command failed [adaptive]: returned error code 1
2025-03-17 08:37:05 C:\WINDOWS\system32\route.exe ADD 0.0.0.0 MASK 128.0.0.0 10.211.1.222
2025-03-17 08:37:05 ERROR: route addition failed using CreateIpForwardEntry: Access is denied.   [status=5 if_index=10]
2025-03-17 08:37:05 Route addition fallback to route.exe
2025-03-17 08:37:05 env_block: add PATH=C:\WINDOWS\System32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
2025-03-17 08:37:05 ERROR: Windows route add command failed [adaptive]: returned error code 1
2025-03-17 08:37:05 C:\WINDOWS\system32\route.exe ADD 128.0.0.0 MASK 128.0.0.0 10.211.1.222
2025-03-17 08:37:05 ERROR: route addition failed using CreateIpForwardEntry: Access is denied.   [status=5 if_index=10]
2025-03-17 08:37:05 Route addition fallback to route.exe
2025-03-17 08:37:05 env_block: add PATH=C:\WINDOWS\System32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
2025-03-17 08:37:05 ERROR: Windows route add command failed [adaptive]: returned error code 1
2025-03-17 08:37:05 Initialization Sequence Completed
```

vpn_log.txt - Notepad

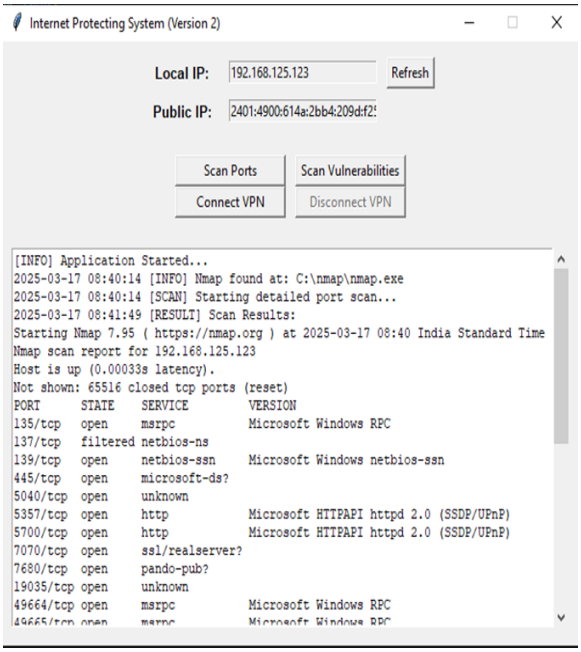
File Edit Format View Help

```
2025-03-08 12:05:06 [INFO] OpenVPN found at: C:\Program Files\OpenVPN\bin\openvpn.exe
2025-03-08 12:05:06 [VPN] Trying VPN: 73.127.60.145_tcp_1814.ovpn...
2025-03-08 12:05:06 [SUCCESS] VPN Connected Successfully!
2025-03-08 12:05:43 [VPN] Disconnecting VPN...
2025-03-08 12:05:43 [SUCCESS] VPN Disconnected.
2025-03-08 12:09:07 [INFO] Nmap found at: C:\nmap\nmap.exe
2025-03-08 12:09:07 [SCAN] Starting detailed port scan...
2025-03-08 12:11:05 [RESULT] Scan Results:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-08 12:09 India Standard Time
Nmap scan report for 192.168.164.123
Host is up (0.0039s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE    SERVICE       VERSION
135/tcp   open     msrpc         Microsoft Windows RPC
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds?
5040/tcp  open     unknown
5357/tcp  open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5700/tcp  open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
6646/tcp  open     tcpwrapped
49664/tcp open     msrpc         Microsoft Windows RPC
49665/tcp open     msrpc         Microsoft Windows RPC
49666/tcp open     msrpc         Microsoft Windows RPC
49667/tcp open     msrpc         Microsoft Windows RPC
49668/tcp open     msrpc         Microsoft Windows RPC
49670/tcp open     msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.45 seconds

2025-03-08 12:16:53 [INFO] Nmap found at: C:\nmap\nmap.exe
2025-03-08 12:16:53 [SCAN] Starting vulnerability check...
2025-03-08 12:19:42 [RESULT] Vulnerability Scan Results:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-08 12:16 India Standard Time
Nmap scan report for 192.168.164.123
```

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8



REFERENCES

[1] Xiaopei Liu, Zhaoyang Lu, Jing Li and Wei Jiang, “Detection and Segmentation Text from Natural Scene Images Based on Graph Model”, WSEAS Transactions on Signal Processing, Vol. 10, No. 1, pp. 124-135, 2014.

[2] Monika Xess and S. Akila Agnes, “Survey on Clustering Based Color Image Segmentation and Novel Approaches to FCM Algorithm”, International Journal of Research in Engineering and Technology, Vol. 2, No. 12, pp. 346-349, 2013.

[3] A.J. Jadhav, Vaibhav Kolhe and Sagar Peshwe, “Text Extraction from Images: A Survey”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 3, pp. 333-337, 2013.

[4] Chengquan Zhang, Cong Yao, Baoguang Shi and Xiang Bai, “Automatic Discrimination of Text

and Non-Text Natural Images", Proceedings of International Conference on Document Analysis and Recognition, pp. 886-890, 2015.

[5] Qiong Xu, Zongliang Gan, Changhong Chen and Feng Liu, "Novel Chinese Text Localization Method for Natural Images through SVM Classification", Journal of Computational Information Systems, Vol. 9, No. 18, pp. 7291-7298, 2013.

[6] Lluis Gomez and Dimosthenis Karatzas, "Multi-script Text Extraction from Natural Scenes", Proceedings of International Conference on Document Analysis and Recognition, pp. 1-5, 2013.

[7] Stanley Sternberg, "Biomedical Image Processing", IEEE Computer, Vol. 16, No. 1, pp. 22-34, 1983.

[8] Lalit Prakash Saxena, "An Effective Binarization Method for Readability Improvement of Stain-Affected (Degraded) Palm Leaf and Other Types of Manuscripts", Current Science, Vol. 107, No. 3, pp. 489-496, 2014.

[9] Rapeeporn Chamchong, Chun Che Fung and Kok Wai Wong, "Comparing Binarisation Techniques for the Processing of Ancient Manuscripts", Proceedings of International Symposium on Entertainment Computing, pp. 55-64, 2010.

[10] Salem Saleh Al Amri, N.V. Kalyankar and S. Khamitkar, "Deblured Gaussian Blurred Images", Journal of Computing, Vol. 2, No. 4, pp. 132-139, 2010

[11] C. Li, S. Anwar and F. Porikli, "Underwater Scene Prior Inspired Deep Underwater Image and Video Enhancement", Pattern Recognition, Vol. 98, pp. 1-13, 2020.

[12] A. Jalal, A. Salman and F. Shafait, "Fish Detection and Species Classification in Underwater Environments using Deep Learning with Temporal Information", Ecological Informatics, Vol. 57, pp. 1-16, 2020.