A Multi-Functional Web Tool for Comprehensive Threat Detection Through IP Address Analysis

Cebajel Tanan*, Sameer G. Kulkarni§[1], Tamal Das* and Manjesh Kumar Hanawal‡[2]

*Indian Institute of Technology, Dharwad, India
§Indian Institute of Technology, Gandhinagar, India
‡Indian Institute of Technology, Bombay, India
*{210010055, tamal}@iitdh.ac.in, §sameergk@iitgn.ac.in, ‡mhanawal@iitb.ac.in

***Abstract*—In recent years, the advances in digitalisation have also adversely contributed to the significant rise in cybercrimes. Hence, building the threat intelligence to shield against rising cybercrimes has become a fundamental requisite. Internet Protocol (IP) addresses play a crucial role in the threat intelligence and prevention of cyber crimes. However, we have noticed the lack of one-stop, free, and open-source tools that can analyse IP addresses. Hence, this work introduces a comprehensive web tool for advanced IP address characterisation. Our tool offers a wide range of features, including geolocation, blocklist check, VPN detection, proxy detection, bot detection, Tor detection, port scan, and accurate domain statistics that include the details about the name servers and registrar information.**

In addition, our tool calculates a confidence score based on a weighted sum of publicly accessible online results from different reliable sources to give users a dependable measure of accuracy. Further, to improve performance, our tool also incorporates a local database for caching the results, to enable fast content retrieval with minimal external Web API calls. Our tool supports domain names and IPv4 addresses, making it a multi-functional and powerful IP analyser tool for threat intelligence.

***Index Terms*—IP address analysis, Threat intelligence, Cybersecurity tool, IP Geolocation, Blocklist check, VPN detection, Proxy detection, Bot detection, Tor detection, Port scanning.**

I. Introduction

Cybersecurity is a vast field that encompasses strategies for protecting digital assets and information. It includes data collection techniques, network encryption, malicious activity detection, cybercrime analysis, etc. The goal of cyber security is to protect against a wide variety of computer threats, including malware, ransomware, phishing, hacking, data breaches, and various cyber-attacks Analysis, Threat Detection and Response, Encryption, Access control, identity management, and security awareness training. In an increasingly digitized world, where cyber threats continue to evolve, effective security measures are needed to protect individuals, organizations, governments and critical infrastructure from potential injury.

[1]Sameer G. Kulkarni acknowledges funding support from SERB, Govt. of India, through the core research grant: CRG/2023/008021 and the Department of Telecommunications, Govt. of India, 5G Use Case Labs.

[2]Manjesh Kumar Hanawal acknowledges funding support from SERB, Govt. of India, through the Core Research Grant (CRG/2022/008807) and the Bureau of Police Research and Development (BPR&D).

In today's world, cybersecurity is critical in maintaining our data and continuing core business operations and tasks, providing protection against computer systems, networks, and stored data that hackers could steal, compromise, or intercept. Strong cybersecurity measures are needed to protect data privacy, prevent financial loss or reputational damage and prevent business disruptions. This collective action is to combat ever-changing threats aimed at combining clearly defined technical tools and methods with professional efforts.

An Internet Protocol (IP) address is a number assigned to each device connected to a computer network that uses the Internet Protocol to communicate. IP addresses serve two main functions: host or network interface identification and location addressing. There are two main types of IP addresses in use today: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). IPv4 addresses consist of four numbers separated by dots, such as `192.168.0.1`, while IPv6 addresses are long and encoded in hexadecimal, such as `2001:0db8:85a3:0000:0000:8a2e:0370:7334`. IP addresses serve as the digital addresses for routing the data packets to the correct device bearing that IP address.

IP address analysis refers to collecting and assessing relevant details on a particular IP address to explain its source or origin, trustworthiness, risks, activities, and so forth. This procedure is commonplace in computer security, network administration, and electronic investigations, which are focused on establishing the presence of threats, protecting systems from them, or simply understanding where the traffic to a particular resource comes from. Aspects of IP Analysis, like geolocation, proxy check, virtual private network (VPN) check, blocklist check, etc., are critical for varied reasons that we elaborate in the next section (§II).

The rationale behind collecting such data is to form a complete picture of the specific IP address, which should guide the decision whether to permit, deny, or track traffic associated with that IP address. In this regard, IP analysis provides the impetus for preventing attacks, managing threat situations, and protecting the organisation's network against illicit access in cybersecurity teams. By analysing IP addresses, cybersecurity professionals can identify potential threats such as malware, phishing attempts, and hacking attempts. Traffic system mon-

itoring enables the detection of anomalies, such as unusually high activity or connections to known bad areas, indicating potential security breaches. Geolocation data derived from IP addresses helps locate the source of the attack, and restrictions are imposed based on the access point. Integrating threat notification allows you to stay ahead of emerging threats and known malicious IPs, increasing security protection. Analysing IP addresses during incident response efforts helps reconfigure incidents, identify threats that lead to attacks, and assess the scope of a contract. Monitoring IP Data helps analyse incoming reliable connections so organisations can block or disable malicious IP addresses. It is also helpful in the area of digital forensics, where it helps in the identification of offenders and their strategies.

Some of the various fields where IP Analysis is critical are mentioned below:

1) *Threat detection and prevention:* IP reputation databases track the history of IP addresses, identifying those associated with malicious activity like spam or malware distribution. Analysing incoming traffic and blocking connections from flagged IPs helps prevent cyberattacks.
2) *Investigating cybercrimes:* After a security breach, analysing the source IP address can provide a starting point for tracing and potentially identifying the attacker's location.
3) *Law Enforcement:* Analysing IP addresses can help link individuals to specific online activities, aiding investigations into cybercrime, online harassment, or other illegal online activities. With the correct tools, we can identify whether individuals use some services to hide their identities, like Tor (onion routing project) or VPN (a virtual private network).

We have surveyed several online tools available in the market for IP Analysis for Geolocation, Proxy Detection, VPN Detection, Tor Detection, Bot Detection, Threat Detection, Port Scan, Liveness Test, and Whois Information [1]. Out of the 105 tools analysed, we observed that none provided a comprehensive set of features. To address this problem, we are introducing a web tool, a one-stop solution for comprehensive IP address analysis, as it incorporates critical features for IP address analysis, which we will discuss in the next section. On top of that, our tool also provides robust industry-standard user management. We will elaborate on the features of our web tool in the proposed solution Section IV.

II. Background

IP Analysis helps to find several characteristic features of an IP address. In this section, we describe the definitions of these features along with the corresponding methodologies to find them (in Section II-A), as well as the various tools used for IP address analysis (in Section II-B).

A. Features

*1) **IP geolocation**:* This method attempts to determine the geographical location in the form of (country, city) associated with an IP address [2].

Methodology: Using good databases periodically maps IP addresses to their approximate locations [2]–[5].

Accuracy Concerns: Geolocation databases might not always be accurate, especially for mobile devices or due to the anonymization services. Accuracy also depends on the freshness of the information in the database. However, the database update period varies from database to database, typically from 24 hours to a couple of weeks. Some databases, which charge some premium, offer more recent information by updating every minute, whereas community databases are not updated that regularly [4], [6], [7].

Privacy Concerns: Collecting and using geolocation data raises privacy concerns, and hence requires adherence to the relevant regulations [5].

*2) **Tor Detection**:* Tor (The Onion Router) is a privacy-focused network that anonymizes users' Internet traffic by routing it through multiple layers of encryption and volunteer-run relays around the world. Tor detection is the process of identifying traffic originating from the Tor network [8], [9].

Methodology: A few relevant methodologies in this regard are as follows.

- *Public Tor Exit Nodes:* Tor publishes a list of "exit nodes" – the final points from which Tor traffic enters the regular Internet. Organizations can compare incoming IP addresses against this list to identify Tor connections [9]–[12].
- *Browser Fingerprinting:* Using browser fingerprinting methods, one can check for distinct features of the Tor browser. Example: Tor Browser returns a blank image (RGB 255, 255, 255) when extracting the base64-encoded value of an HTML5 canvas element [10].

Accuracy Concerns: The accuracy of Tor detection depends on the methods used and how up-to-date the information is. Detecting listed exit nodes is highly accurate but only catches a portion of overall Tor traffic. Statistical analysis or behavioural fingerprinting can detect Tor traffic even without an exit node list. These methods are less accurate and prone to more false positives [13].

Limitations: Not all Tor traffic can be detected as users can configure Tor to use unlisted "bridges" [14] or obfuscate their traffic, making detection more difficult. While Tor detection can identify traffic belonging to the Tor network, it does not reveal the specific user behind the connection. Some legitimate services or anonymity tools might utilize exit nodes used by Tor, leading to potential false positives [13].

*3) **VPN Detection**:* VPNs (Virtual Private Networks) encrypt a user's Internet traffic and route it through intermediary servers, masking their actual IP address and potentially circumventing geographic restrictions. VPN detection is the process of identifying traffic coming from VPN services [15].

Methodology: A few relevant methodologies in this regard are as follows.

- *Known VPN IP Addresses:* Services maintain databases of IP addresses associated with commercial VPN providers. Comparing incoming traffic to these lists can identify the usage of VPN [15].

- *Port Scanning:* VPNs often use specific ports for communication. Scanning for open ports associated with standard VPN protocols can indicate VPN usage [15].
- *Deep Packet Inspection (DPI):* Analysing the contents of network packets can reveal patterns or signatures that suggest VPN traffic, even if the IP address itself is not recognised [15], [16].
- *TCP/IP Fingerprinting:* Comparing the Operating System (OS) induced from the TCP/IP fingerprint with the OS advertised by the User-Agent. From analysing the TCP/IP packets exchanged between the device and the web server, we can discover the device's operating system, which indicates an OS mismatch compared to the browser's operating system. Inconsistencies detected in this case may indicate the presence of a VPN, proxy server, or Apple's iCloud Private Relay [15].

Accuracy Concerns: Basic IP-based detection can be highly accurate for well-known commercial VPNs but less effective for custom or lesser-known VPN providers. Deep Packet Inspection (DPI) and behavioural analysis offer a higher detection rate, especially for sophisticated techniques, but may have a higher likelihood of false positives [15].

Limitations: VPN providers actively change tactics to avoid detection, making it an ongoing challenge. Legitimate services might use techniques similar to VPNs, leading to potential false positives in detection. Some VPNs offer obfuscation options to mask traffic, making detection even more challenging, *e.g.*, changing header fields in packets to simulate non-VPN-like behaviour. Also, port scanning is not straightforward, as a firewall can drop packets sent to the device. The same goes for identifying the device's OS using custom packets apart from TCP packets sent to the device's browser.

*4) **Proxy Detection**:* Proxy detection is the process of identifying Internet traffic originating from a proxy server. Proxy servers act as intermediaries between a user's device and the Internet, masking the user's IP address and sometimes location [17].

Methodology: A few relevant methodologies in this regard are as follows.

- *Latency Analysis:* Compare latency from browser to server with the latency from a web server to an external IP address. If both latency measurements differ significantly (namely, the Browser to Server Latency is significantly higher than the Server to Browser Latency), it is possible to conjecture that there is an intermediate host between the browser and the web server [18], [19].
- *Port Scanning:* Specific ports are often associated with proxy communication protocols. Scanning for open ports used by known proxy protocols can indicate their use [19].
- *WebRTC Leaks:* WebRTC (Web Real-Time Communication) is a technology that can inadvertently reveal a user's actual IP address even when using a proxy if not configured correctly [18], [19].
- *DNS Leaks:* Network configurations on the user device can lead to DNS (Domain Name System) requests that can sometimes leak the user's actual IP address, even when they are using a proxy [18]–[20].
- *TCP/IP Fingerprinting:* Compare the OS induced from the TCP/IP fingerprint with the OS advertised by the User-Agent. From analysing the TCP/IP packets exchanged between the device and the web server, we can discover the device's operating system, which indicates an OS mismatch compared to the browser's operating system. Inconsistencies detected in this case may indicate the presence of a VPN, proxy server, or Apple's iCloud Private Relay [18], [19].
- *Datacenter IP:* Check if the IP address belongs to a datacenter. Datacenter proxies are often hosted in public data centres like AWS or Digitalocean. Those cloud providers publish their IP ranges, making it possible to check whether a proxy belongs to a data center [18], [19].
- *HTTP Proxy Headers Analysis:* Many HTTP proxy servers add additional HTTP headers to each HTTP request. The presence of those headers indicates that a proxy server is used [18], [19].

Accuracy Concerns: Simple database checking can be practical for identifying basic proxies but less effective for more advanced ones. Combining techniques like port scanning, traffic analysis, and leak detection can improve accuracy but may still have limitations [21].

Limitations: Datacenter-based detection only catches known proxies. New proxies emerge constantly, requiring regular list updates. Some legitimate services or network configurations might use similar protocols or ports as proxies, leading to false positives. Proxy providers employ various techniques to mask their signatures, making detection more challenging. Some methods, like WebRTC or DNS leak detection, might raise privacy concerns if not implemented carefully. Also, port scanning is not straightforward, as an intermediate firewall can be easily configured to drop packets sent for port scanning. Similarly, the packets sent to identify the device's OS apart from the TCP connection can be quickly dropped using a properly configured firewall.

*5) **Bot Detection**:* Bots are automated software programs that perform tasks online. While some bots are helpful, malicious bots can pose security threats. Bot detection identifies and differentiates between human users and automated bots [22], [23].

Methodology: A few relevant methodologies in this regard are as follows.

- *Behavioural Analysis:* Monitoring user activity patterns for signs of automation, such as inhumanly fast clicking or repetitive actions [23]–[25].
- *CAPTCHA Challenges:* Requiring users to solve challenges (like identifying images) that are difficult for bots but easy for humans [24], [25].
- *Device Fingerprinting:* Analysing device characteristics (like browser type, operating system) to identify patterns associated with known bots [24].
- *IP Reputation Analysis:* Checking IP addresses against databases of known malicious bots [23]–[25].

Accuracy Concerns: Simple rule-based detection can be effective for identifying basic bots but less effective for advanced ones that adapt their behaviour. Analysing user behaviour patterns with machine learning can improve accuracy but may still have limitations [22], [25].

Limitations: Sophisticated bots constantly adapt their behaviour to mimic human activity, making detection more challenging. Legitimate users with unusual browsing habits might be flagged as bots, leading to disruptions. Some techniques, like device fingerprinting, might raise privacy concerns if not implemented carefully. Advanced bots can utilise techniques like machine learning to solve CAPTCHAs, rendering them less effective [22].

*6) **Blocklist Check**:* A blocklist check is a security technique used to identify and potentially block malicious or suspicious IP addresses, URLs, or email addresses. These blocklists are essentially large databases containing known threats compiled by security vendors, government agencies, or collaborative efforts [26].

Methodology: The IP address, URL, or email address in question is compared against entries in a blocklist database [27]–[29].

Accuracy Concerns: Reputable, regularly updated blocklists offer higher accuracy but might still have occasional false positives. On the other hand, free or less-maintained blocklists have a higher chance of errors and outdated information, reducing their effectiveness [26].

Limitations: Blocklists may contain inaccurate or outdated information, leading to the blocking of legitimate traffic. New threats emerge constantly, and blocklists might not include them immediately, creating a window of vulnerability. Blocklists often focus on specific threat types, and a clean blocklist check does not guarantee complete security. Malicious actors can use techniques to avoid being blocklisted, like using constantly changing IP addresses.

*7) **Threat Detection**:* This method checks an IP address against databases of known malicious IPs associated with spam, malware, or other threats. This helps to identify potentially risky connections and implement mitigation strategies [30].

Methodology: By checking databases which provide reputation details of IP addresses based on their behaviour and Internet history [31], [32].

Accuracy Concerns: The accuracy of the reputation database itself is crucial. Regularly updated and well-maintained databases with reliable sources are more likely to provide accurate information. The frequency of database updates is essential. Outdated information can lead to "false positives," where legitimate traffic gets blocked, or "false negatives," where malicious activity goes undetected.

Limitations: Malicious actors can mask their actual IP address using techniques like spoofing. This can make it difficult for IP reputation analysis to identify the correct source of threats. The database's coverage of different geographical regions can impact accuracy. Some regions might have less comprehensive data available, leading to potential gaps in identifying threats originating from those areas. Organizations configuring IP reputation systems need to carefully set thresholds for blocking or flagging suspicious activity. Overly aggressive settings can lead to false positives, while overly lax settings might miss actual threats.

B. Tools

*1) **Port Scan**:* Port scan is a technique used to identify active services (programs) running on a computer or network device [33], [34].

Methodology: It works by sending specially crafted packets to different ports on the target device and analysing the response. Each port has a designated purpose (e.g., port 80 for web traffic, port 22 for Secure Shell access). [33], [34]

Accuracy Concerns: TCP SYN scan is a basic scan which checks for open ports by sending a connection request (SYN packet) and analysing the response. It is fast but might miss some services or be susceptible to evasion techniques like firewalls. Techniques like TCP scan, UDP scan, or stealth scans offer more information but might be slower or require more specialised tools. Also, they are not entirely immune to firewalls and similar protection methods. [33]

Limitations: Port scanning only reveals open ports, not necessarily the specific vulnerabilities associated with those services. Malicious actors might use techniques to mask open ports or deflect scans, making them harder to detect. Scanning techniques may misinterpret responses or miss certain open ports depending on the configuration of the target device. Scanning large networks with many devices can be time-consuming and resource-intensive. [33]

*2) **WHOIS**:* The WHOIS (pronounced "who is") service is a query and response protocol used to find information about a specific domain name registration [35]–[37].

Methodology: When you enter a domain name in a WHOIS tool, it acts like a client, contacting the relevant server based on the domain extension (e.g., .com) and sending the name as a query. The server searches its database and sends back information like the registrant (depending on privacy settings), registration date, and nameservers. The tool then displays this information [36].

Accuracy Concerns: The information displayed might not always be wholly accurate or up-to-date, depending on the registrant's data entry [37].

Limitations: Many domain registrars offer privacy protection services that mask the registrant's contact information in WHOIS results. WHOIS does not reveal ownership details for some domain name extensions (like .gov or .edu). Also, the information might not always be accurate if not updated regularly [36], [37].

*3) **Liveness Check (Ping Test)**:* The ping service, also referred as "pinging," acts like a digital echolocation tool for networks. Ping measures the round-trip time (RTT) – the total time it takes for the packet to travel from your device, reach the destination, and return with a response [39].

Tool	Whois	Geolocation	Port Scan	Liveness Test	Proxy Detection	Blocklist Check	VPN Detection	Tor Detection	Bot Detection	Threat Detection	IPv6?	Web App	API
https://www.ipqualityscore.com		F			F	F	F	F	F	F	TRUE	F	F
https://ipinfo.io	F	F	F	F	F		F	F		F	FALSE	F	F
https://www.neutrinoapi.com		F			F	F	F	F	F	F	TRUE	F	F
https://ipapi.com		F	F	F	F			F	F		TRUE	F	F
https://www.maxmind.com/en/geoip-databases		P			P						TRUE	P	P
https://ipanalyzer.in (Our tool [38])	F	F	F	F	F	F	F	F	F	F	TRUE	F	F

TABLE I: The table shows 5 out of 105 surveyed tools. F means free feature, P means paid feature whereas blank means feature is missing. For a complete survey, please check [1].

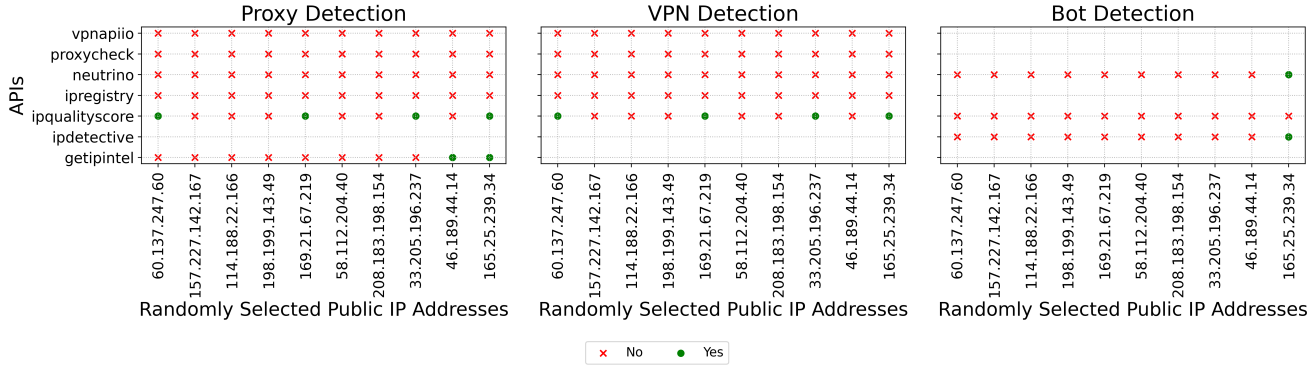


Fig. 1: Output of API Calls from different web tools of 10 random public IP addresses for Proxy, VPN, and Bot Detection.

Methodology: It operates by sending a small data packet, like a digital ping, from your device to a specific destination (identified by an IP address) on the Internet. This destination could be a website, another computer, or any device connected to the Internet. Once the packet reaches the target, it sends a response back to your device [39], [40].

Accuracy Concerns: High network traffic can affect the RTT value, potentially making it appear higher than the actual responsiveness. This can lead to misinterpretations of network performance. Firewalls or other security policies might filter out ping requests, resulting in inaccurate results or no responses. The absence of a response from the host can sometimes be misinterpreted as the host not being live, even though that might not be true [41].

Limitations: Ping measures the round-trip time and does not provide detailed information about the network path, potential bottlenecks, or the cause of connectivity issues. Ping only tests the reachability of the target device or service based on the provided IP address. It does not delve deeper into the internal health or functionality of the target system or application [41].

III. Related Work

In this section, we present a comprehensive survey of various tools related to IP address analysis. [1] presents the complete survey, while Table I provides its snippet. Each row represents a specific tool, while columns represent distinct features. Within this framework, the designation "F" signifies features included at no additional cost, "P" denotes features requiring a premium subscription, and blank cells indicate a feature's absence.

Several key observations can be drawn from this systematic evaluation. Geolocation and WHOIS lookup functionalities are identified as the most common, with little to no deviation in results observed across the analysed tools. Conversely, features like Bot detection, Tor detection, and Threat Detection are encountered less frequently. Interestingly, no single tool provides a complete suite of all evaluated features.

Furthermore, the analysis reveals that a significant majority (96.36%) of tools function solely through web interfaces, while a minority (21.82%) offer access through Application Programming Interfaces (APIs). Notably, a substantial proportion (96.07%) of features are offered free of charge, albeit with potential limitations on usage. It is essential to

acknowledge that much deviation in results is observed across multiple tools analysed for features like Threat Detection, VPN detection, and IP Geolocation. These variations likely stem from discrepancies in the underlying data sources employed.

Figure 1 showcases a few test results. For ten randomly selected public IP addresses across seven IP address analysis web tools, we check the existence of three features in them – namely, whether each of them is behind a proxy, VPN or is a bot. A ● represents *presence*, whereas a ✕ represents *absence* of the feature tested by the respective web tool for the respective IP address.

These observations highlight the complex nature of the tool landscape and shed light on potential factors influencing discrepancies in analysis outcomes, particularly for features like IP reputation and geolocation.

IV. Proposed Solution

In this section, we present a comprehensive tool which has been developed using Python [42], Angular framework [43] for frontend and Django web framework for the backend [44]. Our tool provides robust user management with a suite of functionalities crucial to IP address analysis. On top of that, our tool implements various measures to counteract various threats, including but not limited to Cross-Site Request Forgery (CSRF) [45] attacks, Cross-Site Scripting (XSS) [46] and JavaScript Injection Attacks [47]. In addition, the two-factor authentication feature is included in the solution to make the application more secure. Moreover, our tool is designed to provide an intuitive user experience, even for users with limited technical expertise.

Our tool [38] focuses on delivering functionalities for the comprehensive analysis of IP addresses. Our application queries several databases through APIs to detect anonymisation services like proxies, VPNs and the Tor network, which people use to disguise actual IP addresses. The tool can also identify whether IP is linked to a human or a bot. Moreover, our tool can detect whether that bot was involved in malicious activities by utilising the history of that IP address in databases. Furthermore, our tool has an option for port scans. While scanning an IP address, by analysing particular ports, it finds out the open services. Integration with WHOIS databases provides easy access to the publicly available registration information associated with the domain name of interest. Additionally, our tool can verify whether a specific IP address is listed in any blocklist known to maintain a list of malicious IP addresses so that the user may evaluate the dangers of encountering the IP address.

In addition to this, our tool computes a confidence score for each of the outputs based on the API responses received. Our tool uses several APIs that act as gateways to various global databases. This makes it possible to extract key data points. After receiving the responses for each functionality requested, our tool computes the weighted average of the responses based on predefined weights to give a confidence score to each of the predicted outputs.

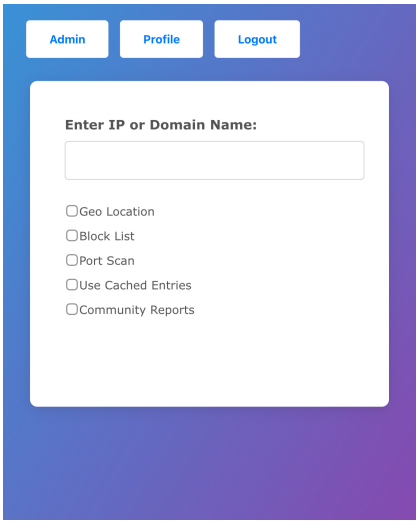
Operating as a web application, our tool can be deployed on a single server to be accessible over the network from any point. It can be accessed globally if our tool is connected to the internet. In a private network, a predefined set of users can access the tool using the user management system it incorporates, which is usually beneficial for corporate and academic institutions. As we have used the Angular framework for our front end, we are able to achieve a high level of responsiveness, while on the server side, we use Django, ensuring scalability.

In addition, to provide a second opinion for the purpose of verifying the results obtained, there is also an option to compute the abuse score of a particular IP address. For this purpose, we use the AbuseIPDB API [48] to fetch user reports and abuse scores for an IP address or domain name, which are elegantly incorporated into the web interface of our tool. One of the appealing features of AbuseIPDB is the vast community of people who provide reports for IP addresses. Our tool integrates user reports from the past 90 days for an IP address through AbduseIPDB, including the report time, report place, report categories [49], and comments. Only registered users can add reports to an IP address in the AbuseIPDB. Assigned abuse score to an IP address is defined based on user reports, with each report being weighted according to the respective user's weight. Although the formula for weighted sum and abuse score calculation is not clearly mentioned in the AbuseIPDB documentation, the weighted user scoring system ensures that no single user can highly influence the abuse score of an IP. The abuse score is provided on a scale of 0 to 100, with higher scores meaning the IP address is more likely to be associated with malicious activity. The API also indicates whether the given IP address belongs to a Tor network or an Internet service provider.

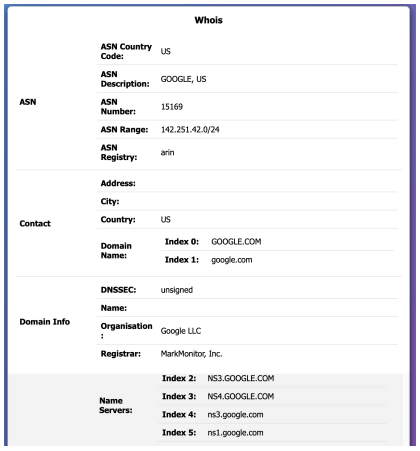
Finally, our tool includes a local database that improves its performance and allows offline usage. For this, we have chosen MongoDB [50], ascribing to its scalability and resilience. It saves the users' records along with the logs of searched IP addresses and domain names with their information. In case of poor API communication or to save API calls, a user can choose to get the latest information saved in the logs, as it is less likely that the information would have changed in that short period of time. This ensures the smooth functioning of the system and facilitates informed decision-making, even with poor API connectivity. For reference, please see Figure 2 for some images of our tool.

V. Conclusion and Future Scope

In this work, we have conducted a thorough review of the public and proprietary tools available to analyse and characterize the IP addresses and presented feature-based comparison and statistical evaluation of different tools. Our work tries to explore the rarity of a specific set of features and how challenging they are to implement. In addition, we have developed and proposed the IP analysis tool, which has a well-balanced range of functionalities and is backed by a modern architecture and a superior user management system.

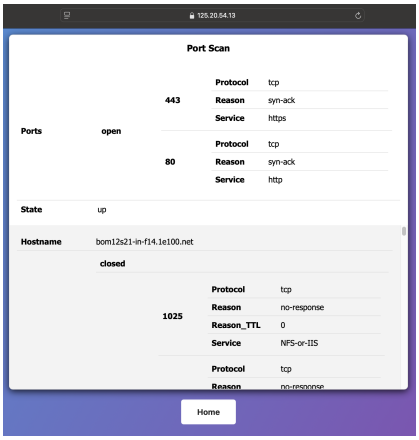


(a) Dashboard

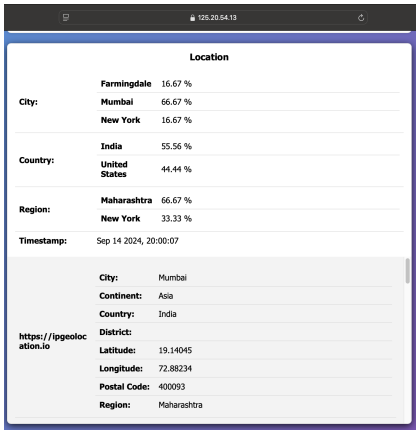


(b) WHOIS Output Summary

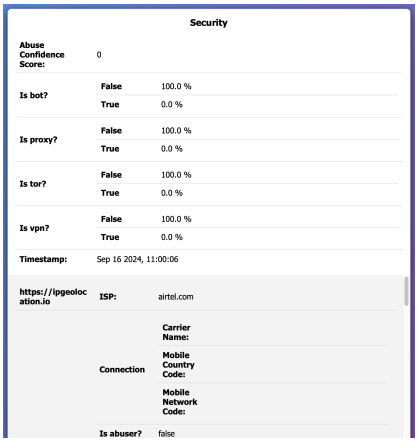
(c) WHOIS Output Details



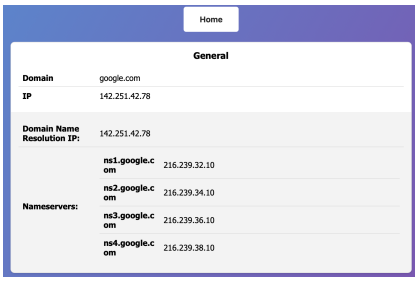
(d) Port Scan Output



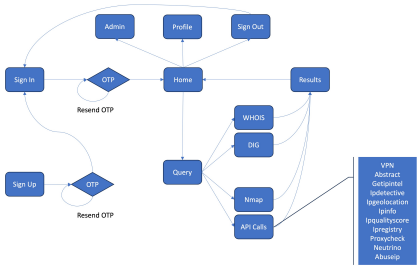
(e) Location Information



(f) Security Information



(g) General Information



(h) Block Diagram

Fig. 2: Snapshots of our tool. Figure 2a shows dashboard of our tool with all the available features and user management tools. Figure 2b shows summary of WHOIS output. Figure 2c shows a gist of detailed information returned by WHOIS databases. Figure 2d shows the states of ports and services running on open ports. Figure 2e shows location information of IP address queried using the responses received from API calls. Figure 2f shows security information of IP address queried using API calls. Figure 2g gives general information of IP address and Figure 2h gives the flow diagram of our tool.

However, there is ample scope to enhance the features and transparency of the tool.

Although the current instrument we employ is useful, there are many other features that could enhance its range and depth. Employing a historical database of registered domain names would, for instance, allow the users to see the changes in ownership and registration over a given period for a particular IP address. In addition, the growing advancement

of the network makes it imperative to include support for IPv6 – a protocol with additional networking that enables the assessment of more internet devices and networks. The introduction of visualisation tools in the report generation process will significantly improve the user experience because they will be able to see trends and patterns more quickly. In order to enhance security management practices, an automated notification system that measures certain user-specified conditions and informs the user whenever a certain IP or domain becomes available should be put in place.

Overall, these changes would enhance the tool's flexibility and would further strengthen its reputation as an advanced and reliable IP analysis tool.

References

[1] Survey table link. Accessed: 2024-05-24. [Online]. Available: https://docs.google.com/spreadsheets/d/1tQcEFkUygEJbKDMkUVCawtYDMy9Ydo-X/

[2] Maxmind geolocation services. Accessed: 2024-10-19. [Online]. Available: https://www.maxmind.com/en/solutions/ip-geolocation-databases-api-services

[3] What is IP geolocation? Accessed: 2024-05-24. [Online]. Available: https://fingerprint.com/blog/what-is-ip-geolocation/

[4] Everything you need to know about IP based geolocation. Accessed: 2024-10-19. [Online]. Available: https://www.if-so.com/geo-targeting/

[5] IP geolocation - how it works. Accessed: 2024-10-19. [Online]. Available: https://geotargetly.com/blog/how-ip-geolocation-works

[6] Maxmind geolocation accuracy blog. Accessed: 2024-10-19. [Online]. Available: https://blog.maxmind.com/2021/07/how-accurate-is-ip-geolocation/

[7] IP geolocation accuracy: How reliable is it. Accessed: 2024-10-19. [Online]. Available: https://www.abstractapi.com/guides/ip-geolocation/how-accurate-is-ip-geolocation

[8] Tor. Accessed: 2024-10-19. [Online]. Available: https://www.torproject.org

[9] What is tor and how can we detect tor users? Accessed: 2024-10-19. [Online]. Available: https://ipdata.co/blog/tor-detection/

[10] How to detect tor traffic. Accessed: 2024-05-24. [Online]. Available: https://focsec.com/blog/how-to-detect-tor-traffic

[11] How to detect tor network connections with falco. Accessed: 2024-10-19. [Online]. Available: https://sysdig.com/blog/detect-tor-network-connection-falco/

[12] New to google secops: Detecting tor exit nodes and remote access tools. Accessed: 2024-10-19. [Online]. Available: https://www.googlecloudcommunity.com/gc/Community-Blog/New-to-Google-SecOps-Detecting-Tor-Exit-Nodes-and-Remote-Access/ba-p/735064

[13] A review on classification of tor-nontor traffic and forensic analysis of tor browser. Accessed: 2024-10-19. [Online]. Available: https://www.academia.edu/download/63249359/a-review-on-classification-of-tor-nontor-traffic-and-IJERTV9IS040701202005509-121751-13tzszq.pdf

[14] Tor-bridge. Accessed: 2024-10-19. [Online]. Available: https://support.torproject.org/glossary/bridge/

[15] VPN detection: How it works. Accessed: 2024-05-24. [Online]. Available: https://fingerprint.com/blog/vpn-detection-how-it-works/

[16] How easy is it to detect if a vpn is being used? Accessed: 2024-10-19. [Online]. Available: https://www.bleepingcomputer.com/vpn/guides/detect-vpn-use/

[17] What is a proxy network? learn about cybersecurity [updated 2023]. Accessed: 2024-10-19. [Online]. Available: https://www.idenfy.com/blog/proxy-detection/

[18] Proxy detection via api: How to detect fraudulent ips. Accessed: 2024-10-19. [Online]. Available: https://seon.io/resources/proxy-detection-via-api/

[19] 7 different ways to detect proxies. Accessed: 2024-05-24. [Online]. Available: https://incolumitas.com/2021/10/16/7-different-ways-to-detect-proxies/

[20] Dns leak test. Accessed: 2024-10-19. [Online]. Available: https://browserleaks.com/dns

[21] The challenges of proxy detection: Addressing database aging and accuracy issues. Accessed: 2024-10-19. [Online]. Available: https://gosecure.ai/blog/2024/08/20/the-challenges-of-proxy-detection-addressing-database-aging-and-accuracy-issues/

[22] Bot detection: What it is and how to enable it. Accessed: 2024-10-19. [Online]. Available: https://www.arkoselabs.com/anti-bot/bot-detection/

[23] Bot detection: What it is and how to block bad bots. Accessed: 2024-10-19. [Online]. Available: https://fingerprint.com/blog/bot-detection/

[24] Bot detection and management. Accessed: 2024-05-24. [Online]. Available: https://www.radware.com/cyberpedia/bot-management/bot-detection/

[25] Bot detection – how to detect bots on your website, apps, & apis. Accessed: 2024-10-19. [Online]. Available: https://datadome.co/guides/bot-protection/bot-detection-how-to-identify-bot-traffic-to-your-website/

[26] Blacklist check: How to solve problems. Accessed: 2024-10-19. [Online]. Available: https://supporthost.com/blacklist-check/

[27] IP blacklist check. Accessed: 2024-05-24. [Online]. Available: https://glockapps.com/blog/ip-blacklist-check/

[28] The ultimate guide to IP blacklist checking and removal. Accessed: 2024-05-24. [Online]. Available: https://inguide.in/the-ultimate-guide-to-ip-blacklist-checking-and-removal/

[29] Realtime blacklist check. Accessed: 2024-10-19. [Online]. Available: https://www.site24x7.com/tools/blacklist-check.html

[30] How to check your sending ip reputation. Accessed: 2024-10-19. [Online]. Available: https://postmarkapp.com/blog/how-to-check-your-ip-reputation

[31] IP reputation check. Accessed: 2024-05-24. [Online]. Available: https://www.ipqualityscore.com/ip-reputation-check

[32] IP reputation and IP location information. Accessed: 2024-05-24. [Online]. Available: https://www.ibm.com/docs/en/sss/3.1.1?topic=events-ip-reputation-ip-location-information

[33] What is a port scan? how to prevent port scan attacks? Accessed: 2024-10-19. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-port-scan

[34] What is port scanning? Accessed: 2024-10-19. [Online]. Available: https://www.avast.com/en-in/business/resources/what-is-port-scanning

[35] Whois protocol specification. Accessed: 2024-10-19. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc3912

[36] What is WHOIS and how is it used? Accessed: 2024-05-24. [Online]. Available: https://www.domain.com/blog/what-is-whois-and-how-is-it-used/

[37] What is whois information and why is it valuable? Accessed: 2024-10-19. [Online]. Available: https://www.domaintools.com/support/what-is-whois-information-and-why-is-it-valuable/

[38] Ip analyser tool. Accessed: 2024-11-15. [Online]. Available: https://ipanalyzer.in

[39] Ping-definition. Accessed: 2024-10-19. [Online]. Available: https://www.techtarget.com/searchnetworking/definition/ping

[40] Ping networking utility. Accessed: 2024-05-24. [Online]. Available: https://en.wikipedia.org/wiki/Ping_(networking_utility)

[41] How to enable & disable ping (icmp echo requests) in windows server 2022 firewall. Accessed: 2024-10-19. [Online]. Available: https://www.layerstack.com/resources/tutorials/How-to-Enable-Disable-Ping-ICMP-Echo-Requests-in-Windows-Server-2022-Firewall

[42] Python. Accessed: 2024-10-19. [Online]. Available: https://www.python.org

[43] Angular. Accessed: 2024-10-19. [Online]. Available: https://angular.dev

[44] Django. Accessed: 2024-10-19. [Online]. Available: https://www.djangoproject.com

[45] Cross site request forgery (csrf) attack. Accessed: 2024-10-19. [Online]. Available: https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/

[46] Cross site scripting (xss). Accessed: 2024-10-19. [Online]. Available: https://owasp.org/www-community/attacks/xss/

[47] What is a javascript injection attack and how is it orchestrated? Accessed: 2024-10-19. [Online]. Available: https://sudip-says-hi.medium.com/what-is-a-javascript-injection-attack-and-how-is-it-orchestrated-abf5d9b044c2

[48] AbuseIPDB apiv2 documentation. Accessed: 2024-05-24. [Online]. Available: https://docs.abuseipdb.com/#introduction

[49] AbuseIPDB report categories. Accessed: 2024-05-24. [Online]. Available: https://www.abuseipdb.com/categories

[50] Mongoddb. Accessed: 2024-10-19. [Online]. Available: https://www.mongodb.com