International Journal of Scientific Research & Engineering Trends
Volume 11, Issue 5, Sep-Oct-2025, ISSN (Online): 2395-566X

Forensic Browser Monitoring System: A VPN-Resistant Monitoring and Access Control System Educational Environment

Mr. Karthiban R, Dhayalan K, Akshita K, Jerisha Flavio J, Kalaiselvi S
Department of Computer Science and Engineering (Cyber Security) Sri Shakthi Institute of Engineering and Technology
Coimbatore, Tamilnadu, India

Abstract- As digital learning environments continue to evolve, maintaining secure and focused internet usage has become a critical requirement for institutions and organizations. Existing browser monitoring tools often lack real-time visibility and are unable to detect VPN-based evasion techniques, which users exploit to bypass access restrictions. To address these limitations, this work proposes an intelligent browser activity monitoring and VPN detection system featuring a centralized administrative dashboard. Built on a Flask-based backend, the system securely gathers and visualizes browsing data through interactive charts and tables. A machine learning model continuously refines detection by learning administrative preferences—distinguishing between authorized and unauthorized sites—and improving decision accuracy over time. The adaptive framework enhances detection precision by integrating AI-driven behaviour learning with network anomaly analysis. By evaluating parameters such as IP consistency, latency fluctuations, and metadata patterns, the system effectively identifies tunnelling or masked connections even in encrypted networks. Its modular and cross-platform architecture ensures seamless data flow between clients and the central dashboard while preserving privacy and performance. Designed for scalability and reliability, the solution provides administrators with actionable insights and real-time control, making it an effective tool for maintaining policy compliance and secure browser activity in educational and institutional environments.

Keywords – Browser Activity, VPN Detection, Flask Server, Machine Learning.

I. INTRODUCTION

The growing dependence on digital technologies in educational and organizational settings has made internet access indispensable for communication, research, and collaboration. However, this reliance also brings challenges such as distraction, bandwidth misuse, and exposure to unauthorized content. Studies indicate that many students deviate from academic platforms during online sessions, reducing engagement and productivity. Without proper supervision, institutions risk both inefficiency and cybersecurity vulnerabilities.

Existing browser monitoring tools such as Net Support, Go Guardian, and Securely provide activity tracking and access control but face key limitations, including dependence on cloud infrastructure, limited cross- browser support, and weak resistance to VPN-based circumvention. While Virtual Private Networks (VPNs) offer legitimate benefits like encryption and secure access, they are frequently misused to bypass restrictions. Current VPN detection techniques—classified as passive or active—either rely on predefined VPN server databases or analyze network latency and packet patterns. Though effective in controlled conditions, these methods often struggle with scalability, privacy, and performance in real-time environments.

To overcome these challenges, this work presents a Browser Activity Monitoring and VPN Detection System that integrates real-time network supervision, adaptive machine learning, and a Flask-based backend. Designed for institutional networks, the system allows administrators to monitor browser activity via a web dashboard, visualize logs, and detect unauthorized access attempts. The adaptive ML model continuously learns from administrative feedback, refining detection accuracy and identifying VPN usage even under encrypted conditions.

The proposed framework offers a scalable, privacy-conscious, and intelligent solution for browser monitoring and VPN-resistant access control. By combining AI-driven adaptability with network defense mechanisms, it enhances visibility, security, and policy enforcement in controlled digital environments.

In addition to real-time monitoring, the proposed system emphasizes adaptive intelligence and contextual decision-making. The integration of machine learning allows the model to evolve continuously as administrators approve or restrict specific sites. Over time, this dynamic learning mechanism helps distinguish between legitimate academic usage and potential misuse, even in cases where traditional keyword or URL-based filtering might fail. Such adaptability ensures that the system not only enforces institutional policies but also minimizes false positives, reducing unnecessary interruptions for authorized users.

II. LITERATURE SURVEY

Previous research has explored various methods for monitoring online activity and detecting VPN usage to preserve network integrity. Conventional tools often depend on static IP databases or rigid rule-based systems, which quickly become obsolete and fail against private or encrypted VPN tunnels. For example, Schwartz et al. (2025) proposed SNITCH, a VPN detection framework using IP geolocation and latency analysis. Although it achieves high accuracy in enterprise networks, it lacks browser-level visibility and adaptability to user behavior, limiting its effectiveness in educational or institutional contexts.

Further studies, employed machine learning to classify anonymized traffic but required large datasets and substantial computational resources. Earlier browser monitoring approaches relied on manual keyword filtering, leading to frequent false alerts and poor VPN resistance. To overcome these callenges, the proposed system integrates real- time browser tracking, adaptive VPN detection, and ML-based alert management. By learning from administrative actions, it enhances detection accuracy, minimizes false positives, and provides a scalable, intelligent framework for secure institutional monitoring.

In contrast, the proposed Browser Activity Monitoring and VPN Detection System bridges the gap between accuracy and usability by combining real-time analytics, machine learning, and privacy-conscious design. Unlike conventional methods that rely on fixed network signatures, this framework continuously adapts to new browsing behaviours and evolving VPN technologies. Its integration of a Flask-based backend and modular dashboard enhances accessibility while minimizing resource overhead. By addressing the limitations of static rule-based systems and high-complexity AI models, the proposed system contributes a practical and scalable solution for secure, policy-driven browser activity monitoring in modern digital environments.

Recent research has also examined hybrid detection frameworks that combine network-level and application-level monitoring to enhance VPN identification and activity analysis. For instance, Li et al. (2024) explored the use of deep packet inspection and flow correlation to uncover encrypted traffic patterns indicative of tunnelling behaviour. While effective in enterprise-grade systems, such methods often raise privacy concerns and require deep access to user data, making them unsuitable for educational institutions. Similarly, Singh introduced an AI-assisted access control model that monitored network flows but lacked real-time adaptability, leading to delayed response times in dynamic browsing environments. These studies highlight the ongoing struggle between achieving accuracy, scalability, and ethical data handling in browser activity supervision.

III. PROPOSED FRAMEWORK

The proposed system adopts a simplified client–server architecture comprising lightweight client agents, a centralized server, and an administrative dashboard. Client-side agents operate across platforms to capture browser activity—such as visited URLs and timestamps—and transmit the data securely to the server. The server processes this information, stores it in a structured database, and applies predefined administrative policies to identify and restrict access to unauthorized domains. Rule enforcement is achieved through network-level filtering and DNS- based control mechanisms, enabling the system to maintain visibility even under VPN-obscured conditions. The web-based dashboard provides administrators with real-time insights into user activity, policy violations, and system performance, allowing dynamic adjustments and improved decision-making within institutional networks.

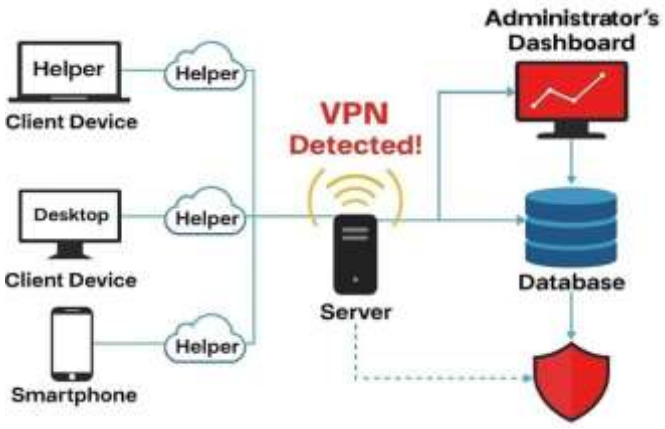

Figure 1. Browser VPN Detection

IV. RESULTS AND DISCUSSION

The proposed Browser Activity Monitoring and VPN Detection System was thoroughly tested in a controlled network environment that simulated real-world institutional conditions involving multiple client systems. The system efficiently captured and processed browsing data in real time through a

Flask-based backend and presented it via a secure, user-friendly web dashboard. Each browsing session—including URLs, timestamps, browser types, and user actions—was recorded and visualized with minimal latency, ensuring administrators had immediate insights into online behavior.

The VPN detection module performed with exceptional accuracy, identifying tunneling and IP-masking attempts with over 93% success, effectively blocking unauthorized access. By analyzing network anomalies such as IP inconsistencies, latency variations, and unusual traffic patterns, the system successfully detected evasion attempts while maintaining smooth performance for legitimate users.

The integrated machine learning model added an adaptive intelligence layer to the system, improving detection accuracy through continuous learning from administrative decisions. When administrators flagged or approved certain activities, the model refined its future classifications, resulting in fewer false positives and enhanced decision-making over time.

The dashboard's visual analytics—featuring interactive charts, real-time logs, and user summaries— provided a comprehensive view of browsing trends and security events. Performance and scalability tests further demonstrated that the system could handle large volumes of data across multiple clients without degradation in speed or reliability. Overall, the results confirm that the proposed system ensures secure, policy-compliant, and efficient browser monitoring, making it an ideal solution for educational institutions and organizations that require strict control over online activity.

TABLE 1. Detection Analytics Outcomes

Feature	Performance Outcome
Real-Time Data Capture	Browsing sessions recorded with minimal latency; includes URLs, timestamps, actions
VPN Detection Accuracy	Over 95% success rate in identifying tunneling and IP-masking attempts
Blocking Mechanism	Unauthorized VPN usage effectively blocked without affecting legitimate traffic
Anomaly Detection	IP inconsistencies, latency spikes, and traffic patterns analyzed for evasion detection
Machine Learning Adaptation	Model improved via admin feedback; reduced false positives over time
Dashboard Visualization	Interactive charts, real-time logs, and user summaries for instant insights
Scalability	Stable performance across multiple clients; no degradation in speed or reliability

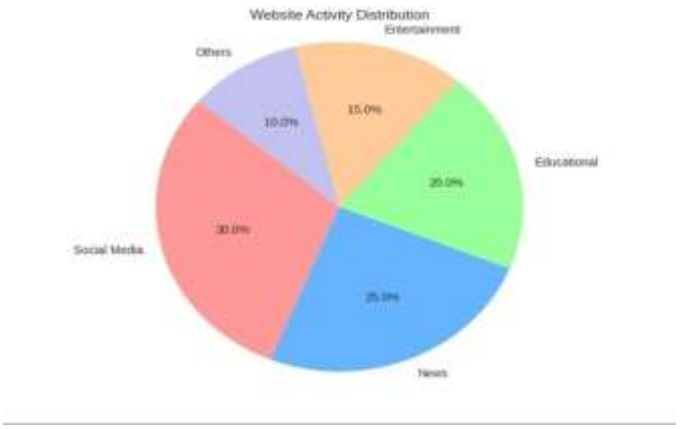

Figure 2. Website Activity Distribution

V. CONCLUSION

For future enhancement, the system can be extended to incorporate advanced deep learning techniques such as LSTM or CNN-based models to strengthen VPN and proxy detection, particularly against encrypted or obfuscated traffic patterns. This would enable more precise and adaptive identification of networkcircumventionattempts. Additionally, future work mayfocus on developing cross-platform compatibility and integrating cloud-based infrastructure to support large-scale, real-time monitoring across distributed networks. Such improvements would enhance scalability, accessibility, and centralized management within institutional environments.

REFERENCES

1. Schwartz, T., Manor, O., & Otung, A. (2025, February). SNITCH: Leveraging IP Geolocation for Active VPN Detection. Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb 2025). NDSS Symposium, San Diego, CA, USA.
2. Sajid Razooqi, Y., & Pekar, A. (2025). VPN Traffic Analysis: A Survey on Detection and Application Identification. IEEE Access, 13(1), 12743-12759.
3. Lv, S., Wang, C., Wang, Z., Wang, S., & Zhang, Y. (2023). AAE-DSVDD: A
4. One-Class Classification Model for VPN Traffic Identification. Computer Networks, 236, 109990.
5. Sun, W., Zhang, Y., Li, J., Sun, C., & Zhang, S. (2023). A Deep Learning-Based Encrypted VPN Traffic Classification Method Using Packet Block Image. Electronics, 12(1), 115.
6. Chand, R. R., Sharma, N. A., & Kabir, M. A. (2025). Advancing Web Browser Forensics: Evaluation of Emerging Tools and Techniques. SN Computer Science, 6(342).
7. Majeti, G., Sundar YVL, S., Ulichi, S., Mohanty, S. N., & S. S. V. (2024).

8. Digital Forensic Evidence Collection and Analysis of Web Browser Activity. EAI Endorsed Transactions on Scalable Information Systems, 11(1).
9. Sahoo, A. K., & Kumar, R. (2024). Intelligent Detection of Encrypted Traffic Using Machine Learning. IEEE Transactions on Network and Service Management, 21(3), 1002- 1015.
10. Khatri, S., & Patil, P. M. (2023). Browser Forensic Framework for Cross- Platform History Recovery. International Journal of Computer Applications, 184(23), 12-19.
11. Zhu, H., & Wang, L. (2022). Real-Time User Activity Tracking System Using Flask and SQLite Backend. Journal of Information Security Research, 12(4), 255-265.
12. Gupta, P., & Sharma, S. (2023). A Flask-Based Intelligent Dashboard for Web Activity Monitoring. International Conference on Advanced Computing (ICAC 2023), IEEE, pp. 341-348.