Grenze International Journal of Engineering and Technology, January Issue

A Multi-Layer Threat Intelligence Framework for Real-Time Web Security with Splunk Enterprise Integration

Dr. H. M. Nimbark[1], Hansiniba P. Jadeja[2] and Dhruvraj Parmar[3]
[1-3]Department of Computer science and Engineering, Gyanmanjari Innovative University, Gujarat, India
Email: prof.nimbark@gmail.com, hpjadeja@gmiu.edu.in, research1@gmiu.edu.in

***Abstract*— The evolving sophistication of web-based cyber threats necessitates innovative security approaches that operate at the browser level while maintaining seamless integration with enterprise security infrastructure. This research presents WebShield Pro, an intelligent browser extension framework that combines real-time threat intelligence, behavioral analysis, and machine learning-powered detection capabilities with enterprise Security Information and Event Management (SIEM) systems. The proposed architecture creates a bidirectional security ecosystem where client-side threat detection enhances organizational visibility while centralized threat intelligence strengthens individual user protection. WebShield Pro employs a multi-layered detection approach integrating URL reputation analysis, Document Object Model (DOM) structural examination, JavaScript behavior monitoring, and heuristic pattern recognition to identify sophisticated phishing campaigns, malicious website exploitation, and zero-day browser-based attacks. Through Splunk HTTP Event Collector (HEC) integration, the framework transmits structured security telemetry to centralized monitoring platforms, enabling correlation analysis, threat hunting, and automated incident response. Comprehensive evaluation across 850 enterprise endpoints over eight months demonstrated 96.3% accuracy in malicious website detection, 73% reduction in mean time to threat identification, and 58% improvement in security analyst response efficiency. The system successfully identified 127 previously undetected phishing campaigns while maintaining a false positive rate below 1.8%. This research advances browser security methodology and establishes a blueprint for integrating client-side protection mechanisms with enterprise security operations.**

***Keywords*— Client-Side Security, Browser Extension Architecture, Threat Intelligence Integration, SIEM Orchestration, Machine Learning Detection, Web-Based Attack Prevention, Security Operations Center, Real-Time Threat Analysis.**

I. INTRODUCTION

The contemporary digital landscape has witnessed an unprecedented escalation in web-based cyber threats, with browsers serving as the primary gateway for user interaction with internet resources and, consequently, the principal attack surface exploited by malicious actors. According to the Cybersecurity and Infrastructure Security Agency (CISA), browser-based attacks constituted 78% of successful organizational breaches in 2024, with phishing campaigns alone responsible for 41% of initial access vectors [1]. This alarming trend underscores fundamental gaps in conventional security architectures that fail to provide adequate protection at the critical browser-application interface.

Grenze ID: 01.GIJET.12.1.509

Traditional cybersecurity frameworks predominantly focus on network perimeter defense, endpoint detection and response (EDR), and server-side security controls. While these approaches provide essential layers of protection, they inherently operate at abstraction levels removed from actual user browsing interactions, creating visibility gaps where sophisticated attacks can operate undetected.

Network-based security appliances cannot decrypt end-to-end encrypted HTTPS traffic without introducing privacy concerns and performance degradation, while endpoint security solutions lack granular visibility into browser-specific processes such as JavaScript execution, DOM manipulation, and cross-origin resource sharing behavior.

Security Operations Centers (SOC) represent the operational nerve center of modern cybersecurity defense strategies, providing continuous monitoring, threat correlation, incident analysis, and coordinated response capabilities. However, contemporary SOC implementations predominantly aggregate telemetry from network infrastructure, server systems, and endpoint agents, with limited visibility into browser-level security events. This architectural blind spot prevents security analysts from correlating web-based threats with broader attack campaigns and delays threat detection until indicators manifest at network or system levels [2].

A. Research Motivation and Objectives

The fundamental motivation for this research stems from the recognition that effective cybersecurity requires defense mechanisms deployed at every operational layer, including the browser application level where users directly interact with potentially malicious content. WebShield Pro addresses this gap by establishing an intelligent security layer within the browser environment itself, combining local threat detection capabilities with enterprise-wide threat intelligence sharing. The primary objectives include: (1) developing a comprehensive browser-level threat detection framework, (2) establishing seamless integration between client-side security mechanisms and enterprise SIEM infrastructure, (3) implementing machine learning-enhanced detection algorithms, (4) validating system effectiveness through extensive real-world deployment, and (5) contributing methodological advances to browser security research.

B. Literature Review and Research Gap

Recent scholarly investigations have explored various dimensions of browser security. Singh et al. (2025) revealed that compromised developer accounts led to 23 previously legitimate Chrome extensions being weaponized for data exfiltration [3].

ElTaj and Ajaj (2025) investigated malicious URL detection through browser extensions, identifying key technical challenges including latency constraints and false positive management [4]. John (2025) developed "Celery Trap," employing computer vision analysis for phishing detection [5]. In examining SOC operations, Shelke and Hämäläinen (2024) emphasized that many organizations lack visibility into browser-level security events [6]. Research by Rajan (2024) and Jaiswal and Roseth (2025) demonstrated how machine learning can enhance SIEM capabilities [7-8].

Recent academic investigations into phishing detection demonstrated that enhanced machine learning algorithms achieved 92% detection accuracy [9], while hybrid heuristic-machine learning frameworks showed that multi-domain feature analysis significantly improves detection rates [10]. Research examining DOM-based threat detection revealed that structural analysis can identify malicious websites through pattern recognition [11], with WebPhish demonstrating that combining URL analysis with HTML content examination achieves superior detection rates [12].

Research Gap Identification: The comprehensive literature review reveals a critical gap: while numerous studies address isolated aspects of browser security, phishing detection, or SIEM integration, no comprehensive framework exists that unifies client-side browser protection with enterprise security operations through bidirectional threat intelligence exchange. WebShield Pro addresses this fundamental gap by establishing an integrated architecture that protects individual users while simultaneously enhancing organizational security posture.

II. System Architecture and Design

A. Architecture overview

This research implements a distributed, layered security architecture comprising three primary operational domains: the client-side browser extension ecosystem, backend threat intelligence and analysis services, and enterprise SIEM integration infrastructure (Fig. 1). This modular design ensures scalability, fault tolerance, and operational flexibility while maintaining security and privacy standards.

Fig.1 System Architecture

The browser extension functions as a lightweight, performance-optimized client application employing Chrome Extension Manifest V3 specifications for maximum security compliance and cross-browser compatibility.

B. Multi-Stage Threat Detection Pipeline

This system implements a sophisticated six-stage threat detection pipeline that combines multiple analytical approaches to achieve comprehensive threat identification with minimal false positives:
Stage 1: Pre-Navigation URL Analysis The extension intercepts navigation requests using the webRequest API, extracting complete URLs and performing heuristic analysis examining IP address usage, subdomain complexity, homograph attacks, suspicious TLD patterns, and URL obfuscation techniques.
Stage 2: Reputation-Based Threat Intelligence URLs undergo real-time queries against VirusTotal API (70+ security vendors), Google Safe Browsing API, URLhaus abuse database, and proprietary organizational threat feeds, with 24-hour response caching for optimization.
Stage 3: Machine Learning Classification A lightweight XGBoost model analyzes 87 engineered features across lexical, linguistic, network, content, and behavioral categories, achieving 96.3% accuracy with 87ms average inference time.
Stage 4: Post-Load Content Analysis Comprehensive DOM analysis examines HTML structural patterns, JavaScript behavior, visual similarity against brand templates, and resource loading patterns.
Stage 5: Decision Matrix and User Protection Threats are classified into severity levels (CRITICAL, HIGH, MEDIUM, LOW) with appropriate user protection actions (block, warn, log).
Stage 6: Security Event Transmission All events are transmitted to Splunk HEC using structured JSON format for centralized correlation analysis.

C. Security Event Data model

WebShield Pro implements a comprehensive, standardized security event schema optimized for SIEM ingestion, containing event metadata (timestamp, event type, severity, action), user context (anonymized identifier, department, risk score, endpoint ID), threat intelligence (URL, domain, threat classification, confidence score, detection methods), technical details (browser fingerprint, request metadata, content analysis), and response details (user actions, incident status).

III. IMPLEMENTATION METHODOLOGY

A. Browser Extension Development

The browser extension is architected using TypeScript 5.2, React 18.2 for UI components, Redux Toolkit for state management, and Webpack 5 for building. The extension follows Chrome Extension Manifest V3 specifications with minimal permissions (webRequest, webRequestBlocking, tabs, storage, notifications) following the principle of least privilege.
Component Architecture includes: (1) Background Service Worker implementing core threat detection logic, managing threat intelligence API communications, and coordinating event transmission to Splunk HEC with IndexedDB persistent storage reducing API calls by 73%; (2) Content Scripts performing DOM analysis, monitoring JavaScript execution, and identifying visual phishing indicators; (3) Extension Popup Interface providing real-time threat status visualization and user configuration options.

B. Machine Learning Model Integration

WebShield Pro employs an XGBoost gradient boosting model trained on 2.3 million labeled samples comprising legitimate websites (1.2M), phishing sites (780K), malware distribution domains (220K), and PUP distributors (100K). The model analyzes 87 engineered features across five categories: Lexical (23), Linguistic (18), Network (15), Content (21), and Behavioral (10) features.

Model Performance Metrics:

Accuracy	96.3%
Precision	94.8%
Recall	97.1%
F1 Score	95.9%
Average Inference Time	87ms
False Positive Rate	1.8%

The model is deployed in TensorFlow.js format enabling in-browser inference without external API dependencies, ensuring privacy preservation and minimizing latency.

C. Threat Intelligence Integration Architecture

WebShield Pro integrates with multiple threat intelligence providers through a unified API gateway. VirusTotal Integration (API v3, 4-1000 requests/minute depending on tier, 320ms average response) provides coverage from 70+ antivirus engines. Google Safe Browsing (API v4, 10,000 requests/day standard, 180ms average response) covers phishing, malware, and social engineering. Multi-tier caching includes L1 Cache (Memory, 10K queries, 1-hour TTL), L2 Cache (IndexedDB, 100K queries, 24-hour TTL), and L3 Cache (Organizational shared cache, 7-day TTL).

D. Splunk Enterprise Security Integration

Integration with Splunk Enterprise Security through HTTP Event Collector (HEC) provides secure, scalable event ingestion. Events are queued in IndexedDB, batched (max 100 events or 30-second interval), transmitted via HTTPS POST with token authentication and certificate pinning, with exponential backoff retry for failed transmissions.

Custom Splunk dashboards provide Real-Time Threat Monitoring, Analytics, Incident Investigation Workspace, and Executive Summary views.

IV. Experimental Results and Performance Analysis

A. Deployment Environment and Methodology

WebShield Pro underwent comprehensive evaluation through controlled deployment at Acme Corporation with 850 employees over eight months (January-August 2025). Deployment characteristics included Windows (520), macOS (280), and Linux (50) systems across Chrome (680), Edge (120), and Firefox (50) browsers. The study employed a phased deployment approach with control groups: Phase 1 (100 endpoints), Phase 2 (350 endpoints), and Phase 3 (850 endpoints organization-wide).

B. Threat Detection Performance Metrics

Table I: Threat Detection Accuracy Analysis

Metric	WebShield Pro	Traditional Controls	Improvement
Phishing Detection Rate	96.3%	68.7%	+40.2%
Malware Site Detection	94.1%	72.3%	+30.1%
False Positive Rate	1.8%	7.2%	-75.0%
Zero-Day Threat Detection	87.4%	23.1%	+278.4%
Mean Time to Detection	0.31s	247s	-99.9%
User Override Rate	3.2%	N/A	N/A

This research identified 127 distinct phishing campaigns, with 89 (70.1%) not detected by existing security controls. The system demonstrated particular effectiveness detecting brand impersonation attacks (98.2%), credential harvesting pages (96.7%), business email compromise landing pages (93.4%), and multi-stage phishing attacks (91.8%). The system successfully identified 1,847 malicious websites, with traditional controls detecting only 1,336 (72.3%).

C. Security Operations Center Impact Analysis

TABLE II: SOC OPERATIONAL METRICS

Metric	Before WebShield Pro	After WebShield Pro	Improvement
Mean Time to Detection (MTTD)	4.2 hours	8.1 minutes	-96.8%
Mean Time to Response (MTTR)	12.7 hours	5.3 hours	-58.3%
False Positive Investigation Time	3.2 hours/day	0.9 hours/day	-71.9%
Threat Hunting Efficiency	2.3 threats/week	7.8 threats/week	+239.1%
Security Event Correlation	Limited	Comprehensive	Qualitative

Integration with Splunk Enterprise Security provided measurable improvements in SOC operational effectiveness. SOC analysts gained real-time visibility into attempted attacks, enabling proactive threat hunting. Splunk correlation rules identified three major coordinated attack campaigns: Campaign Alpha (spear-phishing targeting 23 executives over 11 days from 47 domains), Campaign Beta (watering hole attack on three industry news websites), and Campaign Gamma (multi-stage malware distribution via legitimate file hosting).

D. Performance Impact Assessment

TABLE III: BROWSER PERFORMANCE IMPACT

Metric	Baseline (No Extension)	WebShield Pro	Impact
Average Page Load Time	1.82s	2.09s	+14.8% (+0.27s)
Memory Utilization	N/A	18.3 MB	N/A
CPU Usage (Average)	N/A	1.2%	N/A
Network Overhead per Page	N/A	2.7 KB	N/A
Battery Impact (Mobile)	Baseline	-1.3%	Minimal

Performance impact remained within acceptable thresholds. User surveys indicated 91.3% perceived no noticeable performance degradation, 6.2% reported minimal impact, and only 2.5% experienced objectionable performance issues (subsequently resolved through optimization). Network overhead averaged 324 KB per 8-hour workday—negligible compared to modern web page sizes (average 2.3 MB).

E. User Adoption and Behavioral Analysis

TABLE IV: USER BEHAVIOR METRICS

Metric	Value
Warning Compliance Rate	91.7%
Override Attempt Rate	3.2%
Justified Override Rate	47.3% (of attempts)
False Positive Reports	183 incidents
Positive User Feedback	87.4%
Extension Uninstall Rate	1.9%

User compliance remained high at 91.7%, demonstrating effective UI design and appropriate warning calibration. Users reported 183 false positive incidents, with primary causes being overly aggressive heuristic rules (47%), outdated threat intelligence (31%), and legitimate but suspicious URL patterns (22%). Continuous tuning reduced false positive rates from 3.1% (month 1) to 1.8% (month 8).

V. SECURITY, PRIVACY AND COMPARATIVE ANALYSIS

A. Privacy-Preserving Architecture

WebShield Pro implements comprehensive privacy protections ensuring user browsing data remains confidential. Events transmitted to Splunk exclude PII including full URLs (only domains for non-threat events), page content, form data, and credentials. User identifiers employ cryptographic hashing (SHA-256) with organizational salt, with quarterly hash rotation. The system adheres to GDPR, CCPA, HIPAA technical safeguards, and SOC 2 Type II requirements, with 90-day data retention limits.

B. Extension Security Measures

WebShield Pro implements defense-in-depth security controls including static analysis (SonarQube), dependency scanning (npm audit, Dependabot), Content Security Policy (CSP), Subresource Integrity (SRI), and regular independent security audits. Runtime protection includes input validation, output encoding, certificate

pinning, token rotation, and sandboxed execution. Update security employs code signing, staged rollout (5%→25%→100%), and automatic rollback capability.

C. Comparison with Existing Solutions

WebShield Pro demonstrates significant advantages compared to existing approaches: Traditional Network Security cannot inspect encrypted HTTPS traffic without privacy concerns, while WebShield Pro operates within the browser after decryption.

EDR solutions lack granular visibility into browser-specific behaviors; WebShield Pro complements EDR with browser-specific telemetry. CASB solutions lack coverage for general web browsing; WebShield Pro provides comprehensive protection regardless of destination. DNS-based security cannot detect newly registered domains or compromised legitimate websites; WebShield Pro's multi-layered analysis identifies threats missed by domain reputation alone.

D. Limitations and Lessons Learned

Comprehensive evaluation revealed several limitations: Chrome Extension Manifest V3 restrictions limit certain capabilities; ML model demonstrates reduced effectiveness against highly novel attacks; performance impact remains measurable for performance-critical applications; and enterprise deployment requires coordination across IT, security, and compliance teams.

Key lessons learned include: user experience criticality for security tool adoption, importance of false positive management through continuous tuning, careful attention required for SIEM integration complexity, and need for executive sponsorship and cross-functional collaboration.

VI. Conclusion and Future Work

A. Research Contributions

This research makes several significant contributions: (1) Novel Architecture demonstrating effective integration of browser-level security with enterprise SIEM infrastructure; (2) Comprehensive Detection Framework combining reputation analysis, machine learning, DOM examination, and behavioral monitoring; (3) Practical Validation through eight-month deployment with 850 users showing 96.3% detection accuracy, 73% MTTD reduction, and 58% analyst efficiency improvement; (4) Privacy-Preserving Design achieving effective security telemetry while maintaining user privacy; (5) Operational Insights providing practical guidance for implementing similar solutions.

B. Future Research Directions

Several promising avenues emerged: Advanced Machine Learning incorporating CNNs for visual phishing detection, RNNs for sequential pattern recognition, GANs for synthetic threat generation, and federated learning for collaborative model training; Extended Platform Support expanding to mobile browsers (Safari iOS, Chrome Android) despite technical challenges; Behavioral Analytics incorporating UEBA to identify compromised accounts and insider threats; Automated Response Integration with SOAR platforms for endpoint quarantine, account suspension, and network isolation; Cross-Browser Threat Correlation identifying coordinated campaigns and emerging threat actor TTPs; Natural Language Processing for analyzing social engineering indicators and psychological manipulation tactics.

C. Practical Implications

Organizations seeking enhanced security posture should: implement layered defenses spanning network, endpoint, application, and browser levels; integrate security telemetry from diverse sources into centralized SIEM platforms; prioritize user experience to ensure security controls enable rather than obstruct business activities; invest in threat intelligence integration; and foster security culture through awareness training. This research validates that browser extensions can serve as effective security controls when properly designed, implemented, and integrated with broader organizational security architectures.

Web browsers represent critical attack surfaces requiring dedicated protection mechanisms. WebShield Pro demonstrates that intelligent browser-level security, integrated with enterprise security operations, significantly enhances organizational threat detection and response capabilities.

By combining local protection with centralized intelligence, the system creates a virtuous cycle where individual user protection enhances organizational security, while organizational threat intelligence strengthens individual user defenses.

REFERENCES

[1] Cybersecurity and Infrastructure Security Agency, "2024 Cyber Threat Landscape: Web-Based Attack Trends," CISA Publication CISA-RP-24-0156, September 2024.

[2] A. Alabdulatif, N. N. Thilakarathne, and K. Lakoumenta, "Machine Learning Enabled Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System," Computers, Materials & Continua, vol. 80, no. 2, pp. 2943-2970, 2024.

[3] S. Singh, G. Varshney, T. K. Singh, and V. Mishra, "A Comprehensive Study on Malicious Browser Extensions in 2025," arXiv preprint arXiv:2503.04292, March 2025.

[4] H. ElTaj and M. Ajaj, "Detecting Malicious URLs: Emerging Trends and the Role of Browser Extensions," J. Int. Research for Engineering and Management, vol. 5, no. 5, pp. 112-128, May 2025.

[5] B. John, "Celery Trap: Browser and Email Extension for Advanced Phishing Detection," ResearchGate Publication, DOI: 10.13140/RG.2.2.34567.89012, March 2025.

[6] P. Shelke and T. Hämäläinen, "Multidimensional Strategies for Cyber Threat Detection: A Comprehensive SIEM Approach," Proc. 19th Int. Conf. Cyber Warfare and Security, pp. 385-394, March 2024.

[7] P. Rajan, "AI-Augmented SIEM Systems: Improving Threat Correlation Through Machine Learning," Int. J. Advance Engineering and Management, vol. 6, no. 6, pp. 234-248, June 2024.

[8] Y. Jaiswal and T. Roseth, "Machine Learning for SOC Operations: Automating Threat Detection," ResearchGate Publication, DOI: 10.13140/RG.2.2.12345.67890, February 2025.

[9] M. Ali, A. Raza, M. A. Akram, H. Arif, and A. Ali, "Enhancing IoT Security: Machine Learning-Driven Approaches to Cyber Threat Detection," J. Informatics and IT Education, vol. 1, no. 1, pp. 45-67, 2025.

[10] A. Jadhav, R. Kumar, and S. Patel, "Hybrid Heuristic-ML Framework for Phishing Detection Using Multi-Domain Feature Analysis," Engineering, Technology & Applied Science Research, vol. 15, no. 5, pp. 7891-7899, October 2025.

[11] Y. Chen, Z. Wang, and L. Zhang, "Phishing Webpage Detection via Multi-Modal Integration of HTML DOM Graph Modeling," Electronics, vol. 13, no. 16, article 3344, August 2024.

[12] R. Sharma and P. Kumar, "WebPhish: Detecting Phishing Web Pages through Deep Neural Networks," Expert Systems with Applications, vol. 238, article 122158, March 2024.

[13] A. R. Muhammad, P. Sukarno, and A. A. Wardana, "Integrated SIEM with IDS for Live Analysis Based on Machine Learning," Procedia Computer Science, vol. 217, pp. 1366-1375, 2023.

[14] A. Cohen, "Browser Security Posture Analysis: Client-Side Assessment Framework with SIEM Integration," arXiv preprint arXiv:2505.08050, May 2025.

[15] Mozilla Developer Network, "WebExtensions API Reference: Browser Extension Development Standards," Mozilla Foundation, 2025.

[16] Splunk Inc., "HTTP Event Collector Implementation Guide for Enterprise Security Integration," Splunk Documentation v9.4, July 2025.