**A Synopsis**

**On**

**Voylx Browser**

***Submitted by***

Ayushman Dalvi [22358010347]

Yash Daterao [22358010349]

Swayam Deshmukh [22358010353]

Prajwal Dhamdhere [22358010356]

***Under the Guidance of***

Mr. S. S. Ragte

A logo for a university

Description automatically generated

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SCHOOL OF COMPUTATIONAL SCIENCES**

**FACULTY OF SCIENCE AND TECHNOLOGY**

**JSPM UNIVERSITY PUNE**

**ACADEMIC YEAR 2025-26**

### **Abstract**

Voylx Browser is a privacy-first desktop browser that integrates advanced ad and tracker blocking, a native userscript engine, ethical CAPTCHA and paywall aids, VPN, and opt-in AI tools within a unified platform. Its architecture offers robust privacy controls, granular permissions, and developer-centric automation, combining in-context AI for summarization, code assistance, and workflow enhancements. Applicable for secure personal browsing, academic research via AI-driven summarization, and streamlined developer productivity through automation and debugging tools, Voylx creates a highly customizable and efficient web environment for privacy-conscious users, researchers, and developers

### **Introduction**

AI features now ship directly in mainstream browsers, validating the pattern of in-context help for reading, research, and productivity. Simultaneously, privacy-focused browsers show that default protections like tracker blocking and fingerprinting defenses materially reduce cross-site surveillance. Voylx aligns these trends by combining on-page AI assistance with strong privacy controls and developer tooling to address practical needs in research, coding, and analysis.

1. **State of the Art**

Microsoft Edge integrates Copilot for page-aware chat, summarization, and multimodal assistance in the sidebar and browsing modes. Brave’s Shields block ads/trackers, apply CNAME uncloaking, and randomize fingerprintable APIs to disrupt tracking. Greasemonkey defined userscripts for on-the-fly page customization, with Chromium supporting Greasemonkey-style scripts natively. uBlock Origin demonstrates wide-spectrum blocking powered by community filter lists like EasyList and EasyPrivacy.

WebExtensions provides a cross-browser API model, though Manifest V3 shifts affect blocker capabilities.

1. **Need of the Work**

Existing browsers seldom offer a cohesive environment that unifies privacy defaults, automation via userscripts, and integrated AI assistance under explicit user control. Emerging platform changes (e.g., Manifest V3) and evolving tracking methods complicate reliable, user-governed filtering and inspection. CAPTCHAs and paywalls introduce accessibility and access challenges that require ethical, policy-aware assistance rather than blunt circumvention

### **Problem Statement**

Voylx must deliver an AI-assisted, privacy-first desktop browser that consolidates userscripts, robust content blocking, ethical CAPTCHA assistance, and an optional VPN into a cohesive, extensible platform for developers and power users. Solving this problem matters because AI now operates where users read and build, while tracking, fingerprinting, and access frictions remain persistent obstacles to productive, private browsing. Scope excludes bypassing paywalls or defeating anti-bot systems; instead, the browser will provide accessibility-aware guidance and policy-respecting reading modes.

### **Objectives of Project Work**

* To Implement a native userscript manager with match-pattern controls and per-site permissions.
* To Provide AI helpers for page/PDF summarization, coding assistance, and task automation as an opt-in module.
* To Offer an optional, integrated VPN toggle and per-site routing for privacy-sensitive sessions.
* To Support WebExtensions compatibility for ecosystem leverage and developer extensibility.
* To Integrate wide-spectrum blocking and allow custom rules.

### **Existing System**

Edge’s Copilot showcases AI-native browsing that summarizes and assists within page context. Brave’s Shields and fingerprinting defenses illustrate strong defaults for tracker mitigation and anti-fingerprinting. Greasemonkey and Chromium userscripts demonstrate the viability and demand for custom page automation. uBlock Origin evidences list-driven blocking as a robust community-maintained approach to ad/tracker control. Gaps remain around cohesive integration, Manifest V3 impacts on filtering, and ethical solutions to CAPTCHA and paywall frictions.

1. **Literature Review**

This section summarizes the previous studies related to proposed system in below table including their title, authors, objectives, methods and limitations.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S. No.** | **Title, Author(s), Year & Publisher** | **Objectives** | **Methods/Tools** | **Outcome/Results/**  **Observations** | **Limitations/Suggested Future Work** |
| 1 | A User-Focused Evaluation of Privacy-Preserving Browser Configurations (Roongta, 2024) | Study permissions, privacy policies, and impact of browser default configurations on user privacy and experience | Large-scale user testing, policy review, default config analysi | Identified gaps in user knowledge and variance in privacy protection across browsers. Usability and privacy outcomes depend strongly on configuration defaults. | Needs longitudinal studies and more granular permission tracking. Further development of transparent configuration interfaces. |
| 2 | Ad Blockers & Online Privacy: A Comparative Analysis of Tracking Mitigation (SCIRP, 2024) | Compare effectiveness of different ad blockers and privacy extensions in reducing third-party online tracking | OpenWPM tool to measure HTTP requests, cookies, JS API calls; tested across sites and adblockers | uBlock Origin, Privacy Badger, Ghostery, and AdLock achieve 40–80% reductions in tracking vectors. Blocking is most effective for HTTP requests and cookies, less so for JS APIs. Some tracking still persists due to extension limitations | Adblockers rely on heuristic or static blocking lists. Not all JavaScript-based tracking is detected. Future work using AI-based dynamic blocking and better identification techniques recommended |
| 3 | Your data, your rules: Firefox's privacy-first AI features you can trust (Mozilla Blog, 2025) | Incorporate AI-powered features into browsers while maintaining privacy and user control | On-device AI for alt-text, translation, tab grouping, link previews; AI chatbot sidebar | Enhanced privacy by local model processing (no cloud data); productivity tools with user choice and transparency; granular AI management options | Some features may be limited by device resources. Future work to expand local AI capabilities, improve resource efficiency, and analyze long-term privacy impacts. |
| 4 | AI browser plug-ins to help consumers improve digital privacy literacy (Notre Dame, 2024) | Develop AI browser plug-ins and personas to boost privacy literacy and user understanding of digital tracking | Personas generated by GPT-4, Privacy Sandbox plug-in, user workshops | Users developed deeper awareness of privacy risks and impacts of consent using AI-driven explainers and simulated browsing | Research limited by simulated environment. Needs expansion to real-world usage and integration with broader AI privacy frameworks. |
| 5 | AI web browser assistants raise serious privacy concerns (UCL, 2025) | Assess data flows, retention, and privacy breaches in AI browser assistants | Traffic interception, analysis of AI assistants, legal review | Revealed collection of sensitive data even in private modes; some assistants violated health and education privacy laws | Urgent need for privacy-by-design, on-device AI, and regulatory standards. Future work in compliance frameworks and transparency for AI browser features. |

### **Proposed Solutions/System**

Voylx uses an embeddable Chromium runtime for cross-platform performance, layering a privacy core, userscript engine, content filtering, optional VPN, and an AI assistant accessible from the sidebar and context menus. Compared to existing systems, Voylx emphasizes local-first operation, granular controls, and developer workflows with reproducibility, while adhering to site policies regarding paywalled content and anti-bot protections. Benefits include reduced tracking exposure, accelerated research and coding, and consolidation of tools that today require multiple add-ons and apps.

### **Methodology**

* Content Filtering: Userscript ingestion with rule evaluation and per-site override
* Userscripts: install, scope via match patterns, permissions, and sandboxed execution.
* AI: summarization, explanation, and code assist triggered via sidebar and page selection.
* VPN: client integration with per-tab or per-profile routing.  
  Tools and frameworks: Chromium Embedded Framework for core browsing, WebExtensions compatibility for add-on ecosystem, and community filter lists for blocking

**For example:**

* **Architecture**: Client-Server Model with cloud deployment.

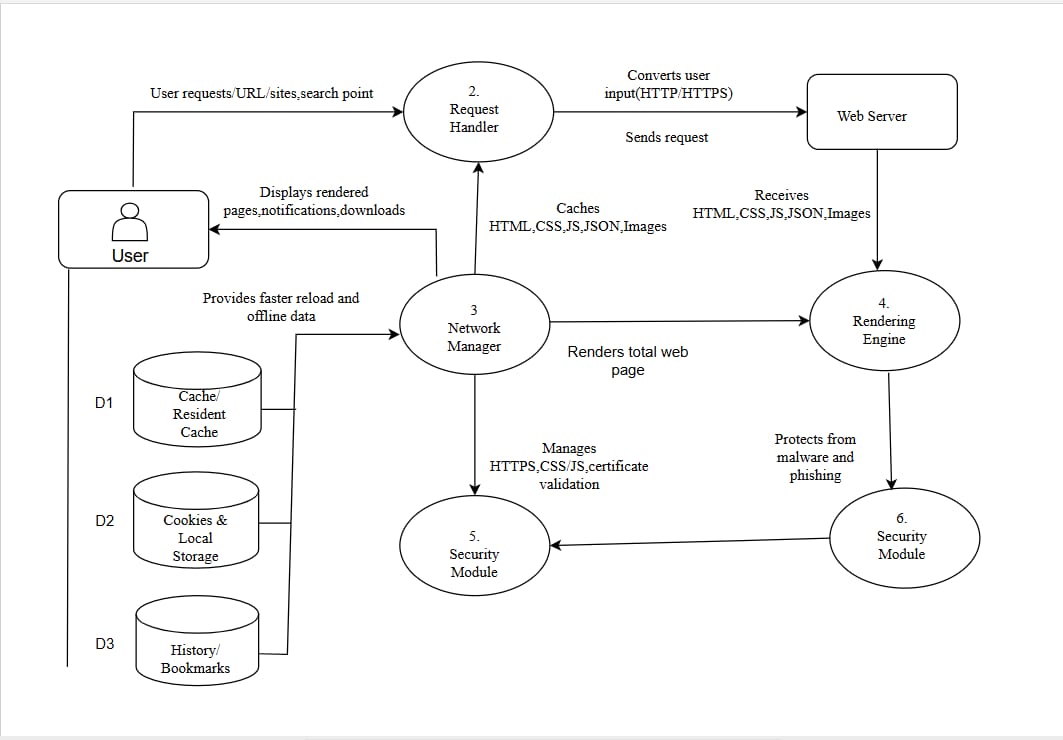


Fig 1

* **Modules**:
  + User Interface (address bar, tab management, settings, extensions panel, sidebar for AI/chat integration, and developer tools.).
  + Rendering Engine(Parses and displays web content)
  + Userscript/Extension Module
  + AI Assistant Module Provides on-page and sidebar AI capabilities
* **Technologies**: Python.

### **10. Resources Required and other Equipment**

* **Hardware**: Laptop/Desktop (i5/i7 processor, 8GB RAM minimum).
* **Software**: Python, PyInstaller, PyQT5/VS Code.
* **Cloud Services**: Hostinger/GoDaddy for hosting and Openrouter LLM APIs.

### **Expected Outcomes**

* **Deliverables**: desktop browser prototype with integrated AI assistant, userscript manager, content blocker, VPN toggle, and WebExtensions support.
* **Impact**: fewer tracking calls and fingerprint vectors by default, faster research and coding via on-page AI, and reduced dependency on multiple external tools.

### **Applications**

* Industry and developer workflows: reproducible debugging, in-context code help, and automation for QA and scraping within ethical and policy boundaries.
* Academic and research: page/PDF summarization and distraction-reduced reading that respects access controls.
* Privacy-conscious users: stronger defaults against tracking and fingerprinting with optional VPN routing

### **Work Plan & Timeline**

|  |  |  |  |
| --- | --- | --- | --- |
| **Phase** | **Duration** | **Month and Year** | **Deliverable** |
| Requirement Analysis | 2 weeks | August 2025 | Requirement Document |
| Literature Review | 1 week | September 2025 | Survey Report |
| System Design | 2 weeks | September 2025 | Architecture & UML diagrams |
| Implementation | 6 weeks | November 2025 | Browser Prototype |
| Testing & Debugging | 3 weeks | December 2025 | Test Reports |
| Final Deployment | 2 weeks | January 2026 | Working Application |
| Documentation & Report | 2 weeks | February 2026 | Final Project Report |

### **References (should be as per IEEE reference format)**

* Microsoft, “Microsoft Copilot in Edge,” product page, accessed 2025.
* Microsoft, “Copilot Chat in Edge,” documentation, 2025.
* Brave Software, “Brave Shields—Blocking Ads, Trackers & more,” product overview, accessed 2025.
* Brave Software, “Fingerprinting Protections,” technical wiki, 2025.
* Mozilla MDN, “WebExtensions—API and platform overview,” documentation, 2025.
* Mozilla MDN, “WebExtensions—Glossary,” documentation, 2023.
* MDN GitHub, “webextensions-examples,” examples repository overview, accessed 2025.
* Wikipedia, “Greasemonkey,” overview of userscripts, accessed 2025.
* Chromium Project, “User Scripts,” design document, accessed 2025.
* uBlock Origin on AMO, “uBlock Origin,” listing describing filter lists and capabilities, accessed 2025
* W3C-related summary, “W3C Invites Comment on CAPTCHA Note Update,” accessibility context, 2018.
* Cloudflare Learning Paths, “What is a VPN?,” VPN overview, accessed 2025.
* Wikipedia, “Chromium Embedded Framework,” framework overview, accessed 2025.
* Wikipedia, “Paywall,” background and practices, accessed 2025.
* arXiv, “Developers Insight On Manifest v3 Privacy and Security Webextensions,” 2025