

CipherNet

¹Het Patel, ²Jay Parekh, ³Sai Suraj Suravajhala, ⁴Ronak Mahidharia

¹Information Systems, Northeastern University

²Information Systems, Northeastern University

³Information Systems, Northeastern University

⁴Information Systems, Northeastern University

{patel.hetas, parekh.jay1, suravajhala.s, mahidharia.r}@northeastern.edu

Abstract: This document presents the development and conceptualization of CipherNet, a web browser meticulously designed with user privacy at its core. The project addresses the growing concerns surrounding personal data security and the pervasive tracking practices of modern browsers. CipherNet integrates features like ad-blocking, tracker prevention, cookie management, and mitigation of browser fingerprinting, ensuring a secure, lightweight, and user-configurable browsing environment. With a commitment to user-centric design, CipherNet delivers an engaging and seamless interface, harmonizing privacy and usability. This initiative epitomizes the fusion of technological innovation and privacy advocacy, aiming to redefine online interactions by emphasizing user control and anonymity while maintaining an enriched browsing experience. CipherNet aspires to establish a new benchmark for privacy-aware digital navigation.

Keywords: *Privacy, Web Browser, User Control, Tracking, Implementation, Evaluation.*

I. PROBLEM DESCRIPTION

In the current digital landscape, safeguarding user privacy has become an urgent priority as existing browsers frequently collect and share personal data without explicit consent. These

practices heighten user concerns over security breaches and intrusive tracking mechanisms, such as cookies and browser fingerprinting, often exploited by websites to amass data for targeted advertising. Web browsers serve as the primary access point to the internet, mediating activities like news consumption, shopping, and online banking. Unfortunately, many browsers and websites rely on trackers to monitor user activity, creating a pervasive environment of data collection. This invasive behavior not only infringes on individual privacy but also underscores the critical need for tools that grant users comprehensive control over their digital footprint.

The core issue lies in the absence of a browser that genuinely prioritizes user-centric privacy. Current solutions often depend on third-party extensions or intricate settings adjustments, resulting in fragmented and reactive approaches to protecting personal information. Users are left grappling with inadequate options, lacking seamless solutions for managing their online data.

This project aims to address this gap by developing a lightweight, privacy-oriented browser that inherently integrates robust mechanisms to curb intrusive tracking and data collection practices. CipherNet is designed to empower users, ensuring they can navigate the web with confidence and control over their personal information. By embedding privacy

features directly into the browser's framework, CipherNet eliminates the dependency on external tools, fostering a browsing experience that prioritizes anonymity and user autonomy.

As we advance with CipherNet, we envision a future where users can engage with the internet without compromising their fundamental right to privacy.

II. ANALYSIS (RELATED WORK)

This section explores prior studies, developments, and limitations in the field of web browser privacy. A thorough review reveals widespread privacy concerns stemming from the data collection and tracking practices employed by mainstream browsers. Research consistently highlights the lack of user control over personal data, which exposes individuals to privacy vulnerabilities and security risks.

Existing solutions, such as third-party browser extensions and plugins, offer limited relief but fail to provide cohesive and integrated privacy protection. For example, mechanisms like "Do Not Track" have proven largely ineffective due to their optional nature and inconsistent implementation across websites. Additionally, advanced tracking techniques, such as browser fingerprinting, exploit unique system configurations to profile users, further amplifying the need for comprehensive solutions.

Despite growing awareness of privacy challenges, progress remains limited. Many approaches fail to strike a balance between robust privacy protection, usability, and system performance. Previous attempts often fall short of delivering seamless browsing experiences while addressing sophisticated tracking methods.

This project aims to fill this gap by designing a web browser that integrates advanced privacy features into its core architecture. By incorporating mechanisms for tracker and ad-blocking, cookie management, and fingerprinting prevention, CipherNet seeks to offer a unified solution that enhances privacy without compromising usability. This initiative contributes to ongoing efforts to safeguard user data and control, bridging the divide between privacy and seamless digital interactions.

III. SYSTEM DESIGN

The foundation of CipherNet rests on a meticulously planned system design that addresses critical privacy concerns while providing a smooth and user-friendly browsing experience. The system's structure focuses on architectural integrity, intuitive user interfaces, and the effective use of modeling tools to achieve its objectives.

A. Architectural Framework

CipherNet's architecture is purpose-built to align with its central mission of privacy preservation and a reimagined browsing experience. The system is organized into distinct layers, each interacting fluidly to enhance privacy functionality. These layers include the user interface, privacy-enhancing modules, data handling systems, and communication protocols. This modular structure ensures seamless integration of privacy features without disrupting the overall user experience.

B. User Interface Design

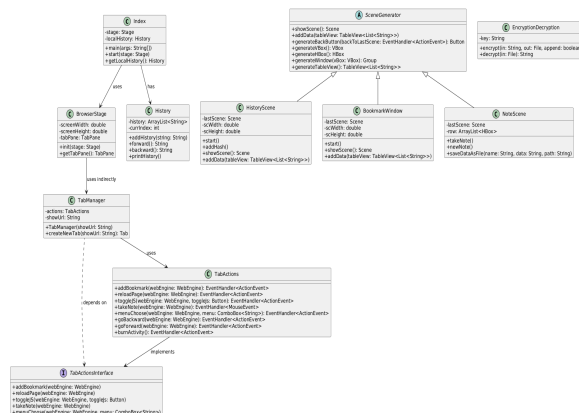
The browser's interface is crafted with simplicity and accessibility in mind, allowing users to easily interact with advanced features like

ad-blocking, tracker prevention, and cookie management. CipherNet's UI adheres to a minimalist aesthetic with intuitive navigation and clear indicators of privacy-focused options. This ensures users can effortlessly customize their privacy settings, reinforcing the browser's user-centric ethos.

C. UML Class Diagrams

Unified Modeling Language (UML) class diagrams were pivotal in structuring CipherNet's architecture. These diagrams illustrate the relationships and interactions between key system components, such as "Index," "BrowserStage," "History," "URL," "HttpURLConnection," "TabManager," and "EncryptionDecryption." This visual representation facilitated efficient collaboration and streamlined the development process, ensuring the seamless integration of privacy-centric features and functional elements.

In conclusion, the design phase laid the groundwork for CipherNet's core mission to redefine user privacy norms. Through a robust architectural framework, intuitive user interface, and comprehensive UML modeling, the browser delivers a secure and empowering web experience.



IV. IMPLEMENTATION

This section outlines the detailed implementation of CipherNet, focusing on the development of its privacy features, tools, and methodologies used to create a secure and user-friendly web browser.

A. Privacy-Enhancing Features

Ad-Blocking and Tracker Blocking

CipherNet integrates advanced filtering mechanisms to block advertisements and tracking scripts effectively. The browser utilizes the WebEngine component of JavaFX to enable browsing functionalities. Since many advertisements and trackers depend on JavaScript, disabling JavaScript serves as an effective method to block these elements. This ensures that user activity remains private and free from intrusive monitoring.

Cookie Management

CipherNet employs robust cookie management using Java's built-in libraries. When a website attempts to store cookies, the browser encrypts the data, preventing other sites from accessing user behavior insights. This feature enables users to clear all cookies and stored data with a single click, offering complete control over personal information.

Encrypted Browser History

Unlike conventional browsers that utilize user history for tailored ads, CipherNet encrypts all browsing history. This ensures that only the user can access their history, eliminating the risk of external exploitation.

Secure Connection Handling

The browser guarantees a secure browsing environment by managing HTTPS connections efficiently. This involves verifying server

certificates, preventing man-in-the-middle attacks, and maintaining a secure data transmission protocol.

Transparent Data Collection Policies

CipherNet features clear data collection policies that inform users about what data is collected, how it is used, and any third-party sharing. Users can opt in or out of data collection, ensuring complete transparency and user empowerment.

B. User-Centric Interface

Dynamic Web Page Rendering

CipherNet uses JavaFX's WebView component for rendering web pages dynamically. This component ensures efficient loading of various content types, delivering a fluid browsing experience. JavaFX, combined with CSS for styling and Eclipse IDE for development, streamlines the creation of an aesthetically pleasing and responsive interface.

Ergonomic Design and Navigation

The browser's interface prioritizes usability, incorporating responsive layouts, intuitive controls, and accessible menu structures. The workflow begins with the user inputting a query, which triggers an HTTP/HTTPS request. Upon receiving a response, the browser renders the web page. This cyclical process ensures a seamless browsing experience. Version control through GitHub, task management via Trello, and communication tools like Microsoft Teams supported the implementation phase.

By meticulously integrating privacy features and user-centric design principles, CipherNet provides an enhanced browsing experience that prioritizes security and ease of use.

V. EVALUATION

Comparison with Existing Solutions

CipherNet's comprehensive privacy features set it apart from mainstream browsers, which often provide limited protection against tracking and data collection. While specific comparisons are not detailed in this report, CipherNet's emphasis on integrated privacy tools highlights its unique contribution to enhancing online user privacy.

User Study and Feedback

Feedback from user studies affirmed CipherNet's success in delivering a privacy-focused and intuitive browsing experience. Features like ad-blocking, tracker prevention, and encrypted browsing history were particularly well-received. However, the feedback also emphasized areas for improvement, such as cross-platform compatibility and refining the user interface to further enhance accessibility. The evaluation phase demonstrated CipherNet's efficacy in addressing privacy concerns and providing a seamless user experience. By combining qualitative and quantitative assessment methods, the project underscored its potential to redefine online privacy standards while identifying opportunities for future refinements.

Here are some screenshots of our web browser showing some of its features:

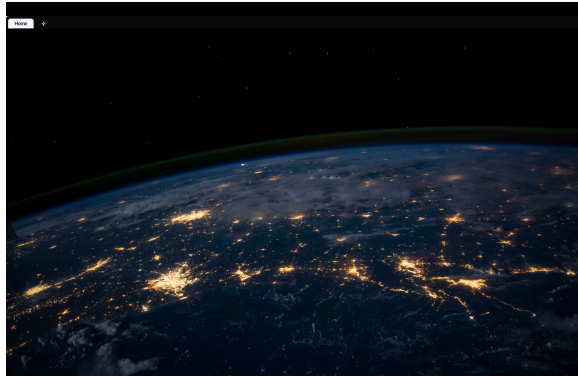


Figure 2. Home Page

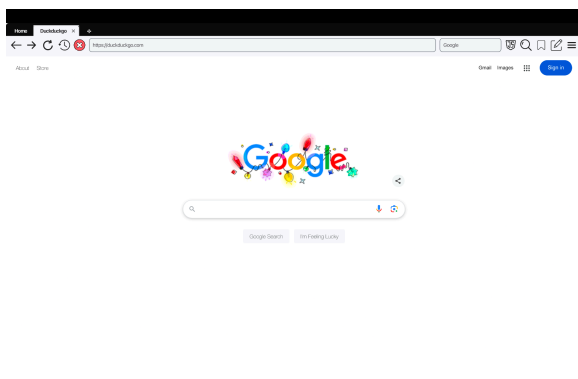


Figure 3. Default Search Engine

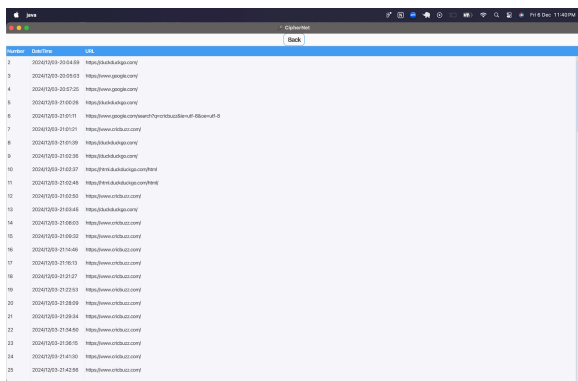


Figure 4. Default Search Engine

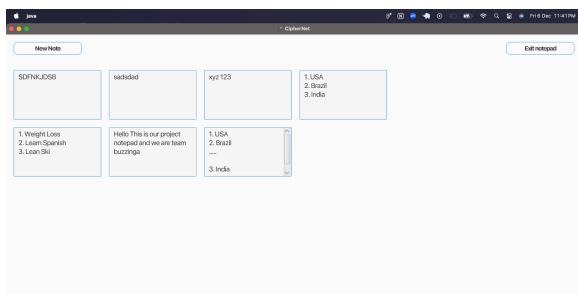


Figure 5. Default Search Engine

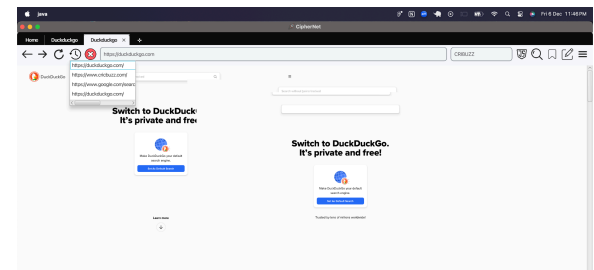


Figure 6. Quick search

VI. DISCUSSION(REFLECTION)

The development of CipherNet transcends technical innovation, making a significant societal impact by promoting awareness of online privacy. Its successful implementation of features like browser fingerprinting prevention and secure connection management demonstrates a commitment to robust security measures in an era of increasing cyber threats.

The inclusion of ad-blocking and tracker-blocking capabilities represents a decisive stance against invasive advertising and third-party tracking practices. These features not only safeguard user privacy but also enhance the overall browsing experience. Positive user feedback validates the browser's capacity to transform the digital landscape into a more secure and engaging environment.

From a technical perspective, CipherNet adheres to established software engineering principles, such as modular design and abstraction. Efficient use of data structures, including lists, stacks, and queues, underscores the importance of optimized resource management in complex software systems.

Future improvements present exciting opportunities for expansion. The integration of

machine learning for predictive privacy controls, achieving full cross-platform compatibility, and improving accessibility features are all avenues for further development. Conducting extensive user studies could offer deeper insights into user preferences, enabling even more tailored enhancements.

This project serves as a testament to the synergy between technological innovation and user-focused design. CipherNet not only addresses pressing privacy concerns but also sparks a broader dialogue about digital ethics and the responsibilities of technology developers. It stands as a foundation for a future where privacy is an inherent right, not a luxury.

VII. CONCLUSION AND FUTURE WORK

The creation of CipherNet marks a significant step in tackling the pervasive privacy violations and tracking practices endemic to mainstream browsers. By embedding advanced features such as ad-blocking, tracker prevention, and robust cookie management, CipherNet ushers in a new era where user privacy and data sovereignty take precedence.

The efficient use of data structures like arrays and array lists supports the browser's ability to handle various modern web functionalities effectively. CipherNet empowers users to navigate the internet confidently, ensuring their digital footprints are shielded from invasive surveillance mechanisms. This privacy-centric design fosters trust and user empowerment in online interactions.

The development process was not without challenges. Integrating cutting-edge privacy technologies while maintaining cross-platform

compatibility required meticulous effort. Additionally, addressing privacy concerns solely within the browser context revealed the broader need for system-wide tracking prevention solutions at the operating system level.

Looking ahead, CipherNet's roadmap includes refining existing features and exploring new avenues for privacy enhancement. In-depth user studies will provide valuable insights into user behavior, driving continuous improvement. Aligning the browser with emerging privacy standards and technologies will further reinforce its capacity to protect user data.

This project stands as a beacon of innovation in privacy-centric web browsing, offering tangible benefits in user experience and data security. CipherNet serves as a guidepost in the digital landscape, advocating for trust, user control, and the sanctity of personal data. As we venture into an increasingly interconnected world, CipherNet illuminates the path toward a future built on privacy-first principles.

VIII. JOB ASSIGNMENT

Member 1: Rendering Web Results and JavaScript Blocking

This member was responsible for designing and implementing the core functionality of CipherNet's web browsing capabilities. They focused on dynamically rendering web pages using the JavaFX WebView component, ensuring a fast and responsive browsing experience. Additionally, they developed mechanisms to block JavaScript, effectively preventing the execution of ads and tracking scripts, which enhanced user privacy and improved browsing speed. Their responsibilities included optimizing HTTP/HTTPS request handling and conducting performance testing to

ensure seamless content rendering across various web formats. They also identified and resolved bugs or performance issues related to rendering and script blocking.

Member 2: Quick Notes and History Management

The second member developed and integrated features that allowed users to create, edit, and manage quick notes within the browser. They also implemented an encrypted browsing history system to ensure that users' past browsing sessions remained private and secure. This member designed user-friendly interfaces for managing notes and browsing history, including search and export options. They conducted extensive testing to ensure the reliability of these features and collaborated with other team members to align history management with CipherNet's privacy-first design principles.

Member 3: Bookmarks and Multi-Tab Functionality

This member led the implementation of multi-tab browsing functionality, enabling users to open, close, and switch between tabs effortlessly. They also created a bookmarking system that allowed users to save, categorize, and access their favorite web pages. The member developed intuitive interfaces for managing tabs and bookmarks, prioritizing user productivity. Ensuring the smooth performance and memory efficiency of multi-tab functionality during testing was a key part of their role. Additionally, they addressed compatibility issues to integrate these features seamlessly into the browser's privacy-centric architecture.

Member 4: Privacy Controls and Cache Management

The fourth member focused on developing privacy-oriented features, such as advanced cookie management, ad-blocking, and tracker

prevention mechanisms. They also implemented cache management functionalities that allowed users to clear browsing data easily. This member ensured transparency by establishing clear data collection policies, allowing users to opt in or out of specific practices. They conducted security audits to identify and address vulnerabilities in privacy controls and cache management. Based on user feedback and evolving privacy standards, this member refined these features to ensure CipherNet upheld its commitment to robust privacy protection.

IX. REFERENCES

1. Poe, D., & Leune, K. (2019). Designing for privacy and security in web-based applications. CRC Press.
2. Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). The web never forgets: Persistent tracking mechanisms in the wild. Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 674-689.
3. Electronic Frontier Foundation. (2020). *Privacy and Modern Web Browsers: An Analysis of Existing Features and Gaps*