Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 199-207

AI Based Privacy Analyzer

[1]Deependra Singh, [2]Pawan Kumar Jaiswal
[1]Student, B. Tech CSE, 6th Semester, [2]Assistant Professor
[1,2]Amity University Chhattisgarh Raipur, Chhattisgarh
[1]deependra.singh3@s.amity.edu, [2]pkumar@rpr.amity.edu

Abstract

With the increasing use of web applications in everyday life, users unknowingly share large amounts of personal data while browsing. Most websites rely on trackers, cookies, and third-party services to monitor user activity, often without clear visibility to the user. This creates serious concerns around privacy and data misuse.

This project presents a Browser Privacy Analyzer with a Local Intelligence Engine, designed to monitor browser network activity in real time and identify potential privacy risks. The system captures outgoing HTTP/HTTPS requests through a Chrome extension and processes them locally using a FastAPI-based backend. It analyzes request metadata such as domains, cookies, and request patterns to detect trackers, identify third-party communication, and highlight possible data exposure.

Instead of relying on cloud services, the system performs all analysis locally, ensuring that user data remains private. A risk scoring mechanism is used to classify websites into different privacy levels, and the results are displayed through a live dashboard.

The project demonstrates how a lightweight, local-first system can provide meaningful insights into web tracking behavior and help users better understand their online privacy.

Keywords – Browser Privacy, Tracker Detection, FastAPI, Chrome Extension, Local Analysis, Privacy Risk Score

1. INTRODUCTION

Today, web browsers are central to almost every digital activity, from social media to online banking. While this convenience has improved user experience, it has also led to increased tracking of user behavior. Websites often collect data using cookies, scripts, and third-party services, and most users are not fully aware of how their data is being used.

Although tools like ad blockers exist, they mainly focus on blocking content rather than explaining what is happening behind the scenes. Users still lack a clear understanding of which websites are tracking them and how much data is being shared.

This project focuses on solving that problem by building a system that can monitor browser activity in real time and provide insights into privacy risks. By capturing network requests and

ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 199-207

analyzing them locally, the system gives users transparency into tracking behavior without compromising their own data.

1.1 OBJECTIVE OF THE STUDY

The main objective of this project is to build a system that can analyze browser activity and highlight privacy risks in real time. The key goals include:

- Capturing live browser network requests using a Chrome extension
- Extracting useful metadata such as domain, cookies, and request type
- Identifying tracker domains and suspicious endpoints
- Differentiating between first-party and third-party requests
- Analyzing tracking behavior over time
- Detecting possible sharing of sensitive data
- Assigning a privacy risk score to websites
- Displaying results in a simple and understandable dashboard

1.2 SCOPE OF THE WORK

This project focuses on analyzing browser-level network activity to understand how websites interact with user data. The system works entirely on a local machine, which means user data is not sent to any external server.

The analysis is based on request metadata and observable patterns rather than deep inspection of encrypted content. While this limits access to payload-level data, it still provides meaningful insights into tracking behavior.

The system is designed mainly for learning and analysis purposes and can be extended in the future with more advanced models or broader browser support.

2. LITERATURE REVIEW

Over the years, several approaches have been proposed to improve online privacy. Early tools mainly relied on blocking known tracker domains using predefined lists. While effective to some extent, these approaches struggle with new or unknown trackers.

More recent methods use machine learning techniques to classify tracking behavior based on patterns such as request frequency, domain relationships, and cookie usage. These approaches provide better adaptability but often depend on cloud-based systems, which raises additional privacy concerns.

Another important direction is behavior-based analysis, where systems study how domains behave across different websites. This helps in identifying cross-site tracking and repeated data collection patterns.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 199-207

However, many existing systems either lack real-time capabilities or do not provide clear explanations to users. This project aims to bridge that gap by combining real-time monitoring, local processing, and simple visualization.

3. PROBLEM STATEMENT

Users interact with websites daily without knowing how their data is being tracked or shared. Most privacy policies are difficult to understand, and existing tools do not clearly explain tracking behavior.

Current solutions either block trackers silently or rely on external servers for analysis. This creates a lack of transparency and, in some cases, introduces additional privacy risks.

The challenge is to build a system that can monitor browser activity, analyze tracking behavior locally, and present the results in a way that is easy to understand.

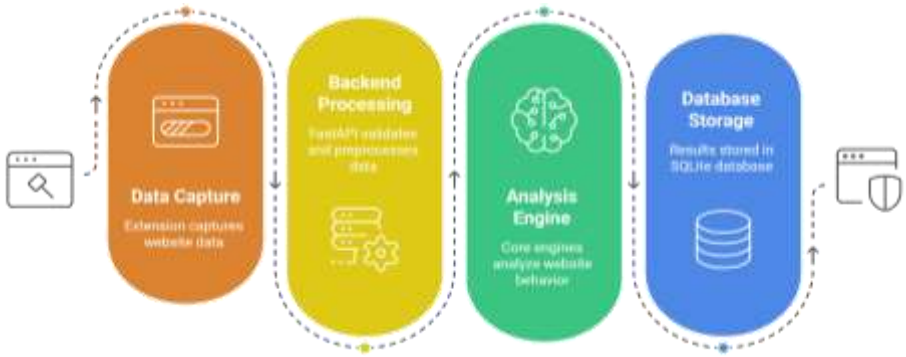
4. PROPOSED METHODOLOGY / MODEL

The system is designed as a pipeline that captures browser requests, processes them locally, and analyzes privacy risks using different modules.

Instead of relying on complex AI models alone, the system combines rule-based logic and behavioral analysis to provide practical and interpretable results.

4.1 SYSTEM ARCHITECTURE / DESIGN

Architecture Flow:



Working Steps:

1. Data Capture
   The browser extension captures outgoing HTTP/HTTPS requests
2. Metadata Extraction
   Important fields like URL, domain, cookies, and timestamp are extracted

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 199-207

3. Backend Processing
   Data is sent to a FastAPI backend for further processing
4. Analysis Engine
   - Detects tracker domains
   - Identifies third-party requests
   - Analyzes request patterns
5. Data Storage
   Results are stored in a local SQLite database
6. Visualization
   A dashboard displays risk scores, alerts, and insights

4.2 ALGORITHMS / TECHNIQUES USED

Tracker Detection

- Matching domains against known tracker patterns
- Identifying suspicious keywords in URLs
- Detecting third-party domains

Behavior Analysis

- Tracking request frequency
- Identifying repeated patterns
- Detecting cross-site activity
- Analyzing cookie usage

Risk Scoring

- Number of trackers
- Third-party interactions
- Frequency of requests
- Presence of sensitive indicators

5. IMPLEMENTATION

The system is implemented as a combination of a browser extension and a local backend.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 199-207

The Chrome extension listens to network requests and sends relevant data to the backend. The FastAPI server processes this data using different analysis modules and stores the results in SQLite.

A simple web dashboard is used to display the results. It updates automatically and shows information such as tracker domains, risk levels, and alerts.

The implementation focuses on keeping the system lightweight, fast, and easy to run locally.

5.1 TOOLS & TECHNOLOGIES

Software

- Python
- FastAPI
- SQLite
- SQL Alchemy
- JavaScript
- Chrome Extension APIs

Hardware

- Processor: Intel i5 or above
- RAM: Minimum 8 GB
- Storage: 256 GB

6. RESULTS AND DISCUSSION

The system was tested on multiple websites and successfully captured and analyzed browser requests in real time. It was able to detect tracker domains, identify third-party communication, and assign meaningful risk scores.

During testing, over 678 requests were processed, and the dashboard updated continuously with new data. The system provided clear insights into tracking behavior and highlighted potentially risky websites.

6.1 PERFORMANCE ANALYSIS

- Real-time request processing
- Dashboard refresh every 5 seconds
- Local data storage for fast access
- No dependency on external services

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 199-207

7. TESTING AND VALIDATION

The system was tested using different browsing scenarios to ensure accuracy and reliability.

Testing included:

- Individual module testing
- Full pipeline testing
- Real-time browser activity testing

Validation focused on:

- Correct detection of trackers
- Consistency of risk scores
- Stability of the system during continuous usage

8. CONCLUSION

This project presents a practical approach to understanding browser privacy by analyzing real-time network activity. The system provides users with visibility into tracking behavior and helps them understand how their data is being used.

By keeping the entire process local, the system avoids additional privacy risks and ensures faster processing. It serves as a useful tool for both learning and improving awareness about online privacy.

9. FUTURE SCOPE

The project can be extended in several ways:

- Adding support for more browsers
- Using advanced machine learning models
- Implementing automatic blocking of trackers
- Improving visualization and analytics
- Extending to mobile platforms

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 199-207

References

[1] Sim, K., Heo, H., & Cho, H.,
"Combating Web Tracking: Analyzing Web Tracking Technologies for User Privacy," *Future Internet*, 2024.

[2] Liu, Z., Dani, J., Wu, S., Cao, Y., & Saxena, N.,
"Identified-and-Targeted: Privacy-Invasive Use of Browser Fingerprinting," *arXiv*, 2024.

[3] Ukani, A., Haddadi, H., Shamsabadi, A. S., & Snyder, P.,
"Privacy Practices of Browser Agents," *arXiv*, 2025.

[4] Ramasamy, V., Barrett, S., Dorai, G., & Zumbach, J.,
"Unveiling Privacy Policy Complexity Using Graph Mining and NLP," *arXiv*, 2025.

[5] Raibulet, C., & Wang, K.,
"Awareness of Privacy and Data Collection: Privacy Policy Effectiveness," *Frontiers in Computer Science*, 2025.

[6] Achuthan, K., et al.,
"Advancing Cybersecurity and Privacy with Artificial Intelligence," *Frontiers in Big Data*, 2024.

[7] Yu, S., Carroll, F., & Bentley, B.,
"Insights into Privacy Protection Research in AI," *IEEE Access*, 2024.

[8] Paracha, A., et al.,
"Machine Learning Security and Privacy: Threats and Countermeasures," *EURASIP Journal*, 2024.

[9] Mandal, A., Chakraborty, T., & Gurevych, I.,
"Towards Privacy-Aware AI Models," *Nature Computational Science*, 2025.

[10] Sonkar, S.,
"Recent Innovations in AI Privacy: Protecting Data in ML," *IJSCSEIT*, 2025.

[11] Wahhab, B. M. A., et al.,
"Emerging Technologies for Data Privacy Protection," 2025.

[12] "Enhancing IoT Privacy with Artificial Intelligence: Trends and Future Directions," *ScienceDirect*, 2025.

[13] "Machine Learning-Based Web Tracking Detection Systems: A Survey," *IEEE*, 2024.

[14] "Third-Party Tracking and Privacy Risks in Modern Web Systems," *ACM Digital Library*, 2024.

ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 199-207

[15] "Detection of Data Leakage in Web Applications Using ML Techniques," *Springer*, 2024.

[16] "Behavior-Based Detection of Tracking and Data Sharing in Web Browsers," *IEEE Security & Privacy*, 2025.

[17] "Real-Time Network Traffic Analysis for Privacy Risk Detection," *Elsevier*, 2024.

[18] "Designing Privacy-Aware Systems: Principles and Applications," *ACM Computing Surveys*, 2025.

[19] "Local-First Privacy Systems: Architecture and Benefits," *IEEE Software*, 2024.

[20] "Explainable AI for Privacy Risk Assessment in Web Systems," *Springer AI Journal*, 2025.