IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

Smart Personal Privacy & Safety Assistant

Prof. Vikas Gaikwad[1], Hrishikesh Kshirsagar[2], Vinit Borawake[3], Rushikesh Kadlag[4], Yashraj Gavhane[5]
Professor, Department of Artificial Intelligence & Data Science[1]
Students, Department of Artificial Intelligence & Data Science[2-5]
Shree Ramchandra College of Engineering, Pune, India

Abstract: *The Smart Personal Privacy & Safety Assistant is an AI-powered cybersecurity solution designed to enhance user privacy, online safety, and threat awareness during web browsing. With the rapid increase in phishing attacks, malicious websites, online tracking, and data theft incidents, traditional browser protection mechanisms often fail to provide adaptive and real-time security. This system integrates a browser extension, cloud-based artificial intelligence engine, and interactive analytics dashboard to provide comprehensive protection against evolving cyber threats. The browser extension continuously monitors URLs, webpage content, trackers, and user interactions while maintaining privacy through encrypted and anonymized data processing. Machine Learning and Natural Language Processing techniques are employed to identify phishing attempts, malicious domains, deceptive dark patterns, and suspicious web activities.*

Keywords: Artificial Intelligence, Virtual Mouse, Hand Gesture Recognition, Eye Tracking, Voice Control.

I. INTRODUCTION

Personalized medicine has emerged as a revolutionary approach in healthcare, aiming to provide treatments tailored toan individual's genetic and biological characteristics. Traditional drug treatments often follow a "one-size-fits-all" approach, which may result in ineffective treatment or adverse drug reactions in different patients. The variation in drug response is mainly influenced by genetic factors, environmental conditions, and individual biological differences.

II. PROBLEM STATEMENT

To design and implement an AI-powered Smart Personal Privacy & Safety Assistant that detects phishing attacks, malicious websites, online tracking activities, and privacy threats in real time while providing secure browsing, cloud-based threat intelligence, personalized privacy analytics, and emergency safety assistance through an integrated browser extension and dashboard platform.

OBJECTIVES

- Implement privacy-preserving monitoring techniques that protect user data during analysis.
- Design a cloud-based threat intelligence module for advanced risk analysis and continuous model improvement.
- Implement privacy-preserving monitoring techniques that protect user data during analysis.

SCOPE

The Smart Personal Privacy & Safety Assistant is designed to provide comprehensive protection against online threats and privacy risks during web browsing.

DOI: 10.48175/IJARSCT-37264

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

III. LITERATURE SURVEY

TABLE I

Sr. No	Title	Author	Year	Methodology Used	Conclusion
1.	Privacy Preserving Data Sharing	Zhang et al.	2021	Machine Learning	Improved data privacy protection.
2.	Smart Safety Monitoring System	Kumar et al.	2020	IoT and Sensors	Enhanced user safety monitoring.
3.	AI-Based Cyber Security System	Lee et al.	2022	Deep Learning	Detected security threats effectively.
4.	Browser Security using AI	Sharma et al.	2023	Machine Learning	Improved malicious website detection.

IV. METHODOLOGY

The proposed system is designed as an intelligent privacy and safety assistant that monitors browsing activities, detects malicious websites, and provides real-time security alerts. The development process is divided into the following stages:

i. Data Collection

The system collects URLs, website information, and security-related data from browser activities and threat detection APIs. This data is used to identify potential security risks.

ii. URL Analysis and Feature Extraction

The system analyzes website URLs and extracts important features such as domain information, HTTPS status, suspicious keywords, and security indicators to identify harmful websites.

iii. Threat Detection Module

Machine learning algorithms are used to classify websites as safe or malicious based on extracted features. The system detects phishing, unsafe links, and suspicious web activities.

iv. Real-Time Browser Monitoring

The browser extension continuously monitors user browsing activity and checks visited websites against the trained model and security databases.

v. System Integration

All three modules are integrated into a unified system. A priority-based approach is used to handle inputs efficiently, ensuring smooth and responsive interaction without conflicts.

V. MODELING & ANALYSIS

The proposed system analyzes website URLs, browser activities, and security indicators to identify privacy threats and provide real-time protection to users.

i. URL Feature Analysis

The system extracts features from URLs such as domain length, HTTPS status, suspicious keywords, and special characters. [F = {f_1, f_2, f_3, ..., f_n}] where (F) represents the extracted feature set used for threat detection.

ii. Threat Classification

Machine learning algorithms classify websites as safe or malicious based on the extracted features.[P(T) = \frac{\text{Malicious URLs}}{\text{Total URLs}}] This helps the system predict potential security threats accurately.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

iii. Browser Activity Monitoring

The browser extension continuously monitors visited websites and compares them with predefined security rules and threat databases.

iv. Alert Generation

When a suspicious website is detected, the system generates warning notifications and security recommendations to the user.

v. Performance Analysis

The system provides real-time detection with minimal response time and high accuracy, ensuring effective privacy protection and safe browsing experience

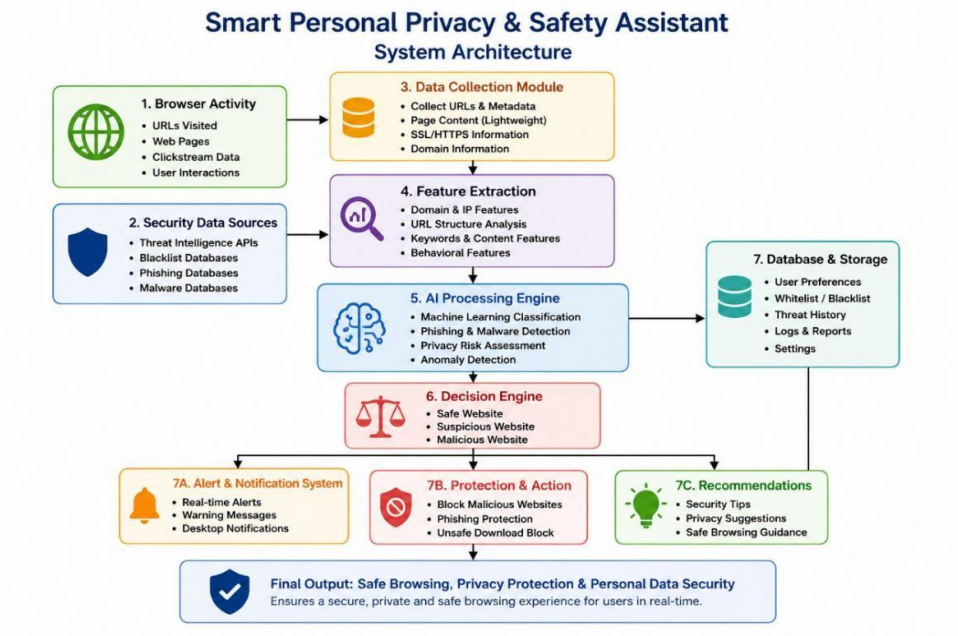


Figure 1. SYSTEM ARCHITECTURE

1. Data Monitoring Module
• Continuously monitors user activities and system events.
• Collects information from files, applications, and network usage.
• Detects suspicious or unauthorized activities in real time.

2. Privacy Protection Module
• Identifies sensitive information such as passwords and personal data.
• Monitors application permissions and data access requests.
• Prevents unauthorized access to private information.

3. Threat Detection Module
• Detects malicious websites, phishing links, and unsafe downloads.
• Analyzes system behavior to identify potential security threats.
• Provides early warnings against cyber attacks and privacy risks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

4. AI Processing Core
• Acts as the central intelligence unit of the system
• Performs:
i. Threat analysis
ii. Privacy risk assessment
iii. User behavior analysis
• Uses machine learning techniques to identify suspicious activities
• Generates security recommendations and alerts

5. Database & Storage Module
• Stores user preferences and security configurations
• Maintains threat logs and alert history
• Records detected privacy risks and security events
• Supports future analysis and system improvement

6. Decision Engine
• Evaluates detected threats and privacy risks
• Determines appropriate security actions
• Controls:
i. Alert generation
ii. Access restrictions
iii. Security recommendations
• Helps users make informed security decisions

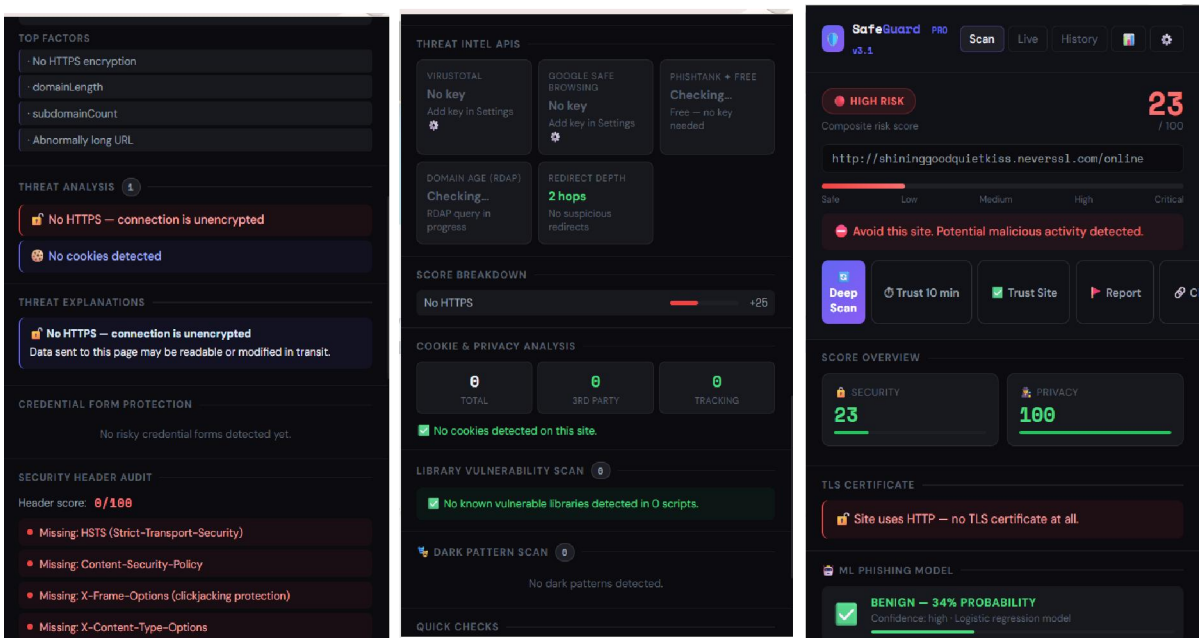
7. Alert & Response Module
• Displays real-time security notifications and warnings

VI. RESULTS & DISCUSSION

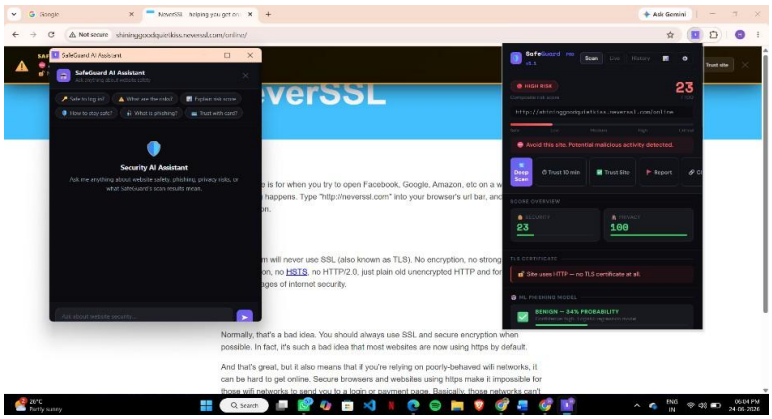
i. The proposed Smart Personal Privacy & Safety Assistant was successfully implemented and tested in a real-time environment, demonstrating effective monitoring and protection of user privacy and security.
ii. The privacy protection module accurately detected sensitive information and unauthorized access attempts, helping users safeguard personal data.
iii. The threat detection module successfully identified suspicious websites, unsafe activities, and potential security risks, providing timely alerts to users.
iv. The AI processing unit effectively analyzed user activities and generated appropriate security recommendations based on detected risks.
v. Real-time notifications and warning alerts improved user awareness regarding privacy threats and potential cyber attacks.
vi. The integration of privacy monitoring, threat detection, and intelligent decision-making provided a more secure and efficient user experience compared to conventional security approaches.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

INTERFACE

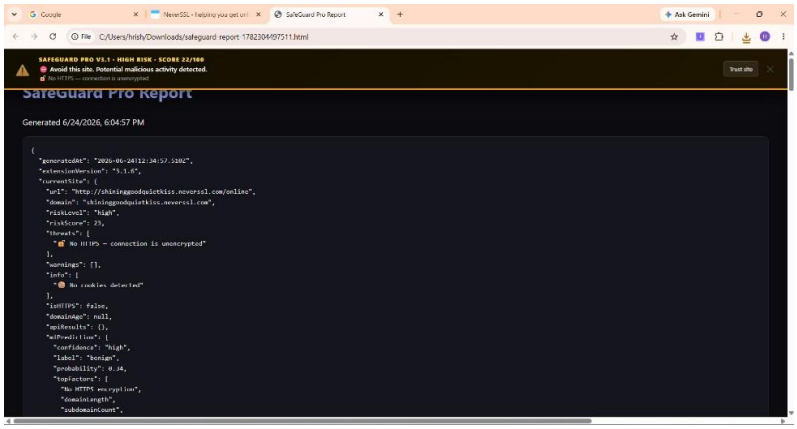


AI INTEGRATION

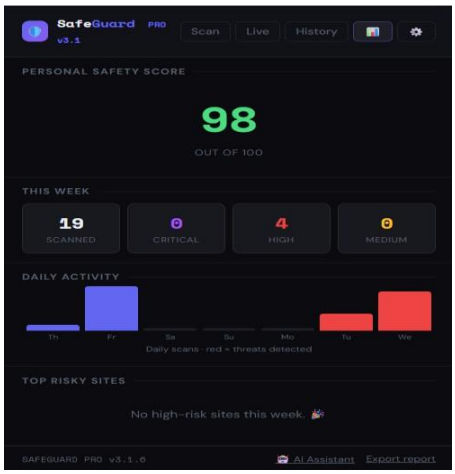


IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

• **EXPORT REPORT**



• **VISUAL REPORT**



• **ACCURACY AND PERFORMANCE ANALYSIS**

The performance of the Smart Personal Privacy & Safety Assistant was evaluated based on detection accuracy, response time, and system reliability. Various test cases were conducted under different operating conditions to assess the effectiveness of the privacy monitoring and threat detection modules.

The privacy protection module achieved high accuracy in identifying sensitive information and unauthorized access attempts. The threat detection module successfully detected suspicious websites, unsafe activities, and potential security risks with minimal false alerts.

The AI processing unit analyzed user activities in real time and generated appropriate security recommendations with low response time. The alert system provided immediate notifications, enabling users to take preventive actions against potential threats.The overall system demonstrated reliable performance with low latency and efficient resource utilization. The experimental results indicate that the proposed system offers an effective, accurate, and cost-efficient solution for enhancing personal privacy and digital security.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 10, June 2026
Impact Factor: 8.2

VII. CONCLUSION

The Smart Personal Privacy & Safety Assistant provides an effective solution for online privacy and cybersecurity. By integrating AI-based threat detection, browser security monitoring, and cloud intelligence, the system enhances user safety and protects against modern cyber threats. The proposed solution contributes to a safer and more secure browsing experience.

ACKNOWLEDGEMENT

We express our sincere gratitude to our project guide and faculty members of the Department of Artificial Intelligence and Data Science for their valuable guidance, encouragement, and continuous support throughout the development of this project. We would also like to thank our institution for providing the necessary facilities, resources, and technical environment required for the successful completion of this work.

Special thanks are extended to our friends and classmates for their suggestions and cooperation during the project development process.

REFERENCES

i. S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, 2021.
ii. W. Stallings, Network Security Essentials: Applications and Standards, 7th ed., Pearson, 2020.
iii. N. Daswani, C. Kern, and A. Kesavan, Foundations of Security: What Every Programmer Needs to Know, Apress, 2007.
iv. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed., Wiley, 2020.
v. O. Chapelle, B. Scholkopf, and A. Zien, Semi-Supervised Learning, MIT Press, 2006