International Journal of Electrical, Electronics and Computer Systems
ISSN: 2347-2820
Volume 15 Issue 01 (2026) | Pages: 67-73

Local Selfie: A Web-Based Application for Digital Footprint Visualization and Privacy Awareness

K. N. Agalave[1], Swapnil Pawar[2], Omkar Deshmukh[3], Yogesh Jadhav[4], Dinesh Thorat[5]

[1,2,3,4,5]Department Of Computer Engineering, S.B.Patil College of Engineering, Indapur, Pune, Maharashtra, India.
[1]*Kimaya8890@gmail.com*, [2]*swapnilpawarofficial@gmail.com*, [3]*omkard3490@gmail.com*, [4]*yogeshnj.9999@gmail.com*, [5]*dineshthorat6886@gmail.com*

Peer Review Information

Type: *Article*
Received: *22 March 2026*
Revised: *06 April 2026*
Accepted: *24 May 2026*
Published: *05 June 2026*

Abstract

The rapid growth of digital systems has increased concerns regarding user privacy, security, and transparency. Local Selfie is a web-based application designed to monitor and visualize a user's local digital footprint in real time. It tracks system parameters such as CPU usage, memory consumption, processes, file activities, and network connections to provide comprehensive insights into system behavior. The system integrates machine learning using the Isolation Forest algorithm to detect anomalies, along with behavioral analysis to identify deviations from normal patterns. AI-generated explanations enhance user understanding of potential threats. All data is stored locally using SQLite, ensuring privacy. The platform delivers real-time analytics and intuitive dashboards, enabling users to effectively monitor and secure their computing environment.

Keywords: System Monitoring; Privacy Awareness; Anomaly Detection; Machine Learning; Isolation Forest; Behavioral Analysis; Digital Footprint; Cybersecurity; Real-Time Analytics; Network Monitoring; File Activity Tracking; Local Data Processing.

How to Cite This Article

Agalave, K. N., Pawar, S., Deshmukh, O., Jadhav, Y., & Thorat, D. (2026). Local Selfie: A web-based application for digital footprint visualization and privacy awareness. *International Journal of Electrical, Electronics and Computer Systems*, 15(1), 67–73.

Introduction

In the modern digital era, personal computing devices continuously generate and process large volumes of data, often without explicit user awareness. Background processes, network communications, and file operations collectively form a user's digital footprint. However, most users lack visibility into these activities, which can lead to potential privacy risks, security vulnerabilities, and inefficient system usage.[1]

Traditional system monitoring tools provide raw metrics such as CPU usage, memory consumption, and process lists. While useful, these tools often fail to deliver meaningful insights or actionable intelligence for non-technical users. Moreover, with the increasing sophistication of cyber threats, static monitoring approaches are insufficient to detect anomalies or malicious behavior effectively.[2]

To address these challenges, the Local Selfie system is developed as an integrated, web-based monitoring solution that emphasizes real-time visibility, intelligent analysis, and user-centric design. The application captures system-level data using monitoring modules that track processes, file activities, and network connections. These modules operate continuously and store structured data in a local database for further analysis.[3]

A key innovation of this system lies in its hybrid detection mechanism. It combines rule-based evaluation with machine learning techniques to identify anomalies. The machine learning engine leverages the Isolation Forest algorithm to detect outliers in system behavior, while a behavioral engine generates system fingerprints and measures deviation from normal patterns. This dual approach improves detection accuracy and reduces false positives.[4]

Furthermore, the system introduces an AI-based explanation module that interprets suspicious activities and provides human-readable insights. This feature transforms complex technical data into understandable information, enabling users to make informed decisions regarding system security.[5]

The application is designed with privacy as a core principle. Unlike cloud-based monitoring tools, Local Selfie operates entirely on the local machine, ensuring that sensitive data never leaves the user's environment. The backend is implemented using Flask, while the frontend utilizes modern web technologies for interactive visualization.[6]

In summary, Local Selfie aims to provide an intelligent, privacy-focused monitoring platform that not only tracks system activity but also interprets it, thereby enhancing user awareness and control over their digital environment.[7]

Literature Survey

1. Mistry et al. (2023) – Privacy-Preserving On-Screen Activity Tracking Using Federated Learning: This study focuses on monitoring user activity while preserving privacy using federated learning techniques. The key contribution is performing analysis locally without transferring sensitive data to centralized servers. From this work, the concept of privacy-preserving local processing has been adopted in the proposed system. Unlike cloud-based monitoring, Local Selfie ensures that all computations and data analysis occur on the user's device. Additionally, the idea of analyzing user activity patterns without exposing raw data inspired the system's design for secure monitoring. This research supports the importance of maintaining user trust while implementing intelligent tracking systems.[1]

2. Aquino et al. (2021) – User Privacy and Data Protection: Analysis of Social Media Platform Policies and User Awareness: This paper highlights the gap between user awareness and actual privacy practices on digital platforms. It emphasizes that users often do not fully understand how their data is accessed or used. From this study, the proposed system adopts the concept of enhancing user awareness through visualization and feedback mechanisms. The Local Selfie dashboard provides clear insights into system behavior, helping users understand their digital footprint. The research also influenced the inclusion of privacy scores, enabling users to evaluate their system's security level effectively and make informed decisions regarding their digital activities.[2]

3. Schreiber et al. (2021) – Digital Privacy Awareness and Behavior Modification Through Real-Time Monitoring Systems: This research focuses on improving user awareness through real-time monitoring dashboards. It demonstrates how continuous feedback can influence user behavior and improve privacy practices. The proposed system adopts the idea of real-time monitoring and visualization, where system metrics are continuously tracked and displayed through an interactive interface. Additionally, the concept of behavior modification through insights is implemented in Local Selfie using AI-generated explanations and alerts. This ensures that users not only observe data but also understand its implications and take appropriate actions to maintain system security and privacy.[3]

4. Padmavathi & Mohanlal (2021) – A Study on Extent of Awareness Among College Students in Security and Privacy Issues: This study analyzes the level of privacy awareness among students and identifies a significant lack of understanding regarding digital risks. The proposed system utilizes this insight by focusing on user-friendly design and simplicity, ensuring that even non-technical users can interpret system data easily. The concept of bridging the gap between technical monitoring tools and user understanding has been adopted. Local Selfie addresses this issue by providing intuitive dashboards, privacy scores, and simplified insights, making privacy awareness accessible to a broader audience, including students and general users.[4]

5. Koidl et al. (2018) – The BigFoot Initiative: Digital Footprint Awareness in Social Media: This paper introduces a system for tracking and visualizing digital footprints in social media environments. It highlights the importance of making users aware of their online activities. From this research, the idea of digital footprint visualization has been extended to local system activities. Unlike the original focus on social media, Local Selfie applies similar principles to system-level behavior, including processes, files, and network interactions. The concept of representing user activity through visual dashboards has been directly adopted, enabling users to better understand and manage their digital footprint in a local computing environment.[5]

6. Bushuyev et al. (2021) – Conceptual Model of Project Digital Footprint: This study provides a theoretical framework for understanding digital footprints, distinguishing between active and passive data generation. The proposed system adopts this conceptual understanding to monitor both explicit user actions (active) and background system processes (passive). By integrating multiple activity sources such as file access, process execution, and network communication, Local Selfie builds a comprehensive view of system behavior. This research influenced the system's design to consider multiple dimensions of digital activity rather than focusing on a single aspect, resulting in a more holistic monitoring solution.[6]

7. Marwick & Ellison (2012) – Privacy in Social Networks: Understanding Privacy Perceptions and Behaviors: This paper explores user privacy concerns and behavioral patterns in social networks. It highlights the complexity of privacy perception and the need for better awareness mechanisms. From this research, the proposed system adopts the idea of context-aware privacy insights, where users are informed about potential risks based on system activity. The concept of translating complex data into understandable insights influenced the inclusion of AI-based explanations in Local Selfie. This helps users interpret system behavior without requiring technical expertise, thereby improving usability and awareness.[7]

8. Young & Quan-Haase (2009) – Information Revelation and Internet Privacy Concerns on Social Network Sites: This study investigates how users disclose information and the risks associated with it. It emphasizes that users often underestimate privacy threats. The proposed system incorporates this insight by implementing real-time alerts and anomaly detection to highlight potential risks immediately. Instead of relying solely on user awareness, Local Selfie proactively identifies unusual system behavior and informs users. This approach ensures that users are not only aware of risks but are also guided in identifying and mitigating them effectively through system-generated insights and recommendations.[8]

9. Taddicken (2014) – The Privacy Paradox in the Social Web: This research discusses the contradiction between users' privacy concerns and their actual behavior. It shows that users often act inconsistently with their stated concerns. From this, the proposed system adopts the concept of behavioral analysis and pattern recognition. Local Selfie tracks system activity over time and compares it with baseline behavior to detect deviations. This helps identify risky behavior patterns even when users are unaware of them. The study influenced the development of the behavioral engine, which plays a crucial role in anomaly detection and system monitoring.[9]

10. Dwork (2008) – Differential Privacy: A Survey of Results: This paper introduces the concept of differential privacy for protecting sensitive data during analysis. Although the proposed system does not directly implement differential privacy algorithms, it adopts the principle of data minimization and local processing. All data in Local Selfie is stored and analyzed locally without sharing with external systems, ensuring strong privacy protection. This research influenced the system's architecture to prioritize privacy-first design, reducing exposure of sensitive information while still enabling meaningful analysis and insights.[10]

Proposed System

Problem Statement

Users are largely unaware of how applications on their personal devices access and manipulate their data, creating significant privacy risks. Existing tools track online activities but fail to monitor local system behaviors such as application usage, file access, and network communications, which often involve sensitive information. Current local monitoring solutions either expose data to external servers or lack real-time, actionable insights. There is a need for a privacy-preserving solution that provides real-time local system monitoring, clear visualizations, and empowers users to take control of their digital footprint.

Requirements

Hardware Requirements

- Processor: Intel Core i3 or equivalent (i5 recommended for optimal performance)
- RAM: Minimum 4 GB (8 GB recommended for smooth real-time monitoring)
- Storage: At least 500 MB free disk space for application and database storage
- Network: Internet connection (optional, required only for external API usage or updates)
- Display**:** Standard monitor with minimum resolution of 1366 × 768

Software Requirements

- Operating System: Windows 10/11 (primary), Linux/macOS (with minor modifications)
- Programming Language: Python 3.10 or higher
- Framework: Flask (for backend development)
- Database: SQLite (for local data storage)
- Libraries/Packages: psutil (system monitoring), watchdog (file system monitoring), scikit-learn (machine learning – anomaly detection), openai (AI-based explanations)
- Frontend Technologies: HTML, Tailwind CSS, JavaScript
- Browser: Google Chrome / Microsoft Edge.
- Development Tools: Visual Studio Code, MySQL Workbench

Architecture Diagram

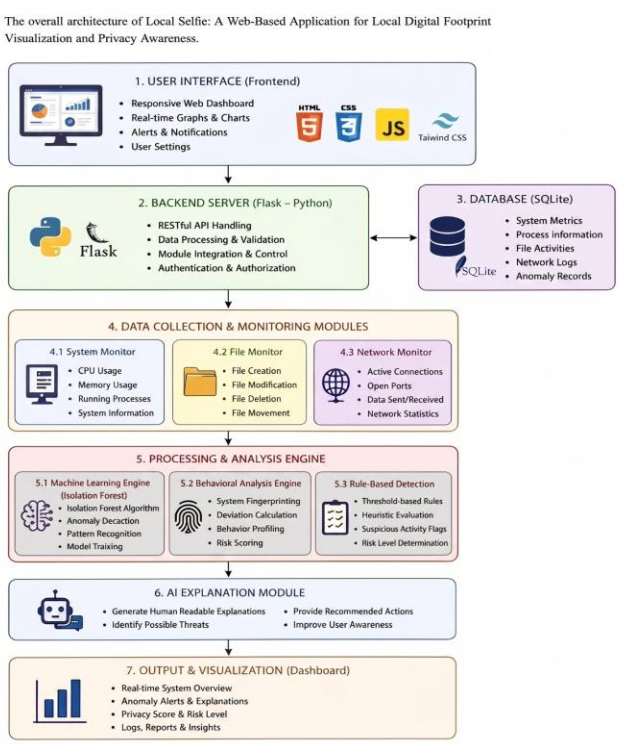

Fig. 1. *Architecture Diagram*

Work Flow of System

The Local Selfie system follows a structured workflow to monitor, analyze, and visualize system activities in real time. Initially, the system initializes all components including the backend server, database, and monitoring modules. Once activated, system, file, and network monitors continuously collect data such as CPU usage, memory consumption, active processes, and network connections. This data is stored locally in the SQLite database for further processing.

The collected data is then analyzed using a hybrid approach combining machine learning, behavioral analysis, and rule-based logic to identify abnormal patterns. When anomalies are detected, contextual information is processed and passed to the AI module, which generates human-readable explanations and recommendations. Finally, all results including system metrics, alerts, and privacy scores are displayed on an interactive web dashboard, enabling users to understand system behavior and respond to potential risks effectively.

Result Discussion

Figure 2 - The presented figures illustrate the operational outcomes of the Local Selfie system, demonstrating its capability to monitor, analyze, and interpret system-level activities in real time. The dashboard visualizes key performance indicators including CPU usage, memory utilization, active network connections, and computed privacy score.

The privacy score reflects the overall system security posture, derived from multiple parameters such as resource utilization, file access frequency, and network activity. A moderate score, as observed, indicates controlled system behavior with no critical anomalies detected.

The system dynamically adjusts this score based on threshold-based and machine learning–driven evaluations.

The process monitoring section highlights active processes along with their CPU consumption, enabling identification of resource-intensive applications. This facilitates detection of abnormal or suspicious processes contributing to potential system risk.

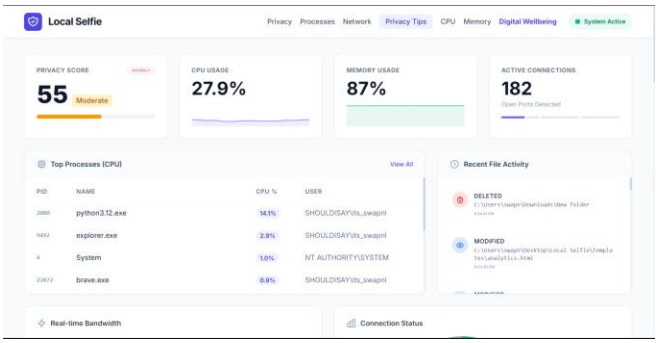

Fig. 2. *Dashboard of Local Selfie System.*

Figure 3 - The network analysis module provides detailed visibility into active connections, including IP addresses, ports, and connection states. Connections are categorized based on security characteristics, such as encrypted or potentially risky, allowing users to interpret network behavior effectively. The presence of standard encrypted connections alongside local internal traffic indicates normal operational conditions.

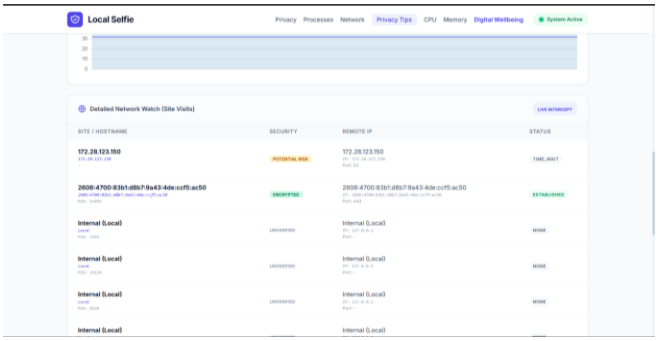

Fig. 3. *Network Monitoring of Local Selfie System*

Figure 4 - The Digital Wellbeing interface presents user-centric analytics by evaluating application usage patterns. Metrics such as focus score, productive time, and distraction index are computed to assess user productivity. The observed low focus score and minimal productive time suggest limited engagement with productive applications during the monitored interval.

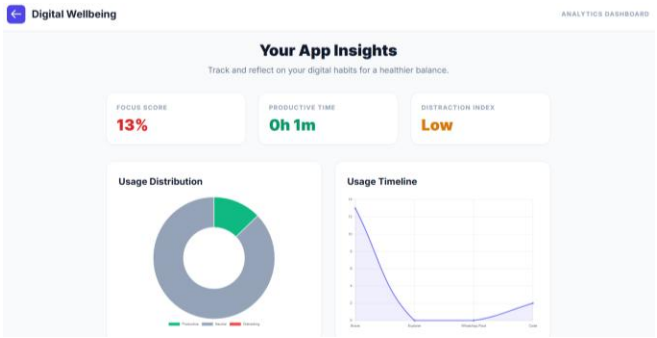

Fig. 4. *Applications Usage Insights of Local Selfie System*

Figure 5 - Furthermore, the system incorporates an AI-driven anomaly detection mechanism combining machine learning and behavioral analysis. The results indicate no significant anomaly or behavioral deviation, confirming that the system activity aligns with its baseline operational profile.

Overall, the results validate that the proposed system effectively integrates system monitoring, privacy assessment, network analysis, and behavioral intelligence into a unified platform, providing both security insights and user behavior analytics without relying on external data sources.

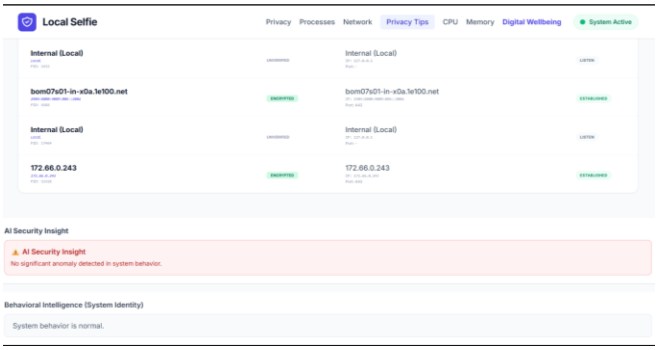

Fig. 5. *AI Security Insight and Behavioral Intelligence of Local Selfie System*

Conclusion

The Local Selfie system successfully demonstrates a unified approach to real-time system monitoring, privacy assessment, and behavioral analysis within a local, privacy-preserving environment. By integrating system-level data collection with machine learning–based anomaly detection and rule-based evaluation, the system provides meaningful insights into both system performance and potential security risks.

The results indicate that the application is capable of continuously tracking critical parameters such as CPU usage, memory consumption, file activity, and network connections, while transforming this data into an interpretable privacy score and actionable insights. The incorporation of an Isolation Forest–based model enhances the system's ability to detect anomalies efficiently, while the behavioral analysis component further improves detection accuracy by identifying deviations from normal system patterns .

Additionally, the inclusion of AI-generated explanations bridges the gap between complex technical analysis and user understanding, making the system accessible to non-technical users. Operating entirely on local infrastructure ensures data security and eliminates dependency on external services.

Overall, the proposed system provides an effective, scalable, and user-centric solution for monitoring digital footprints, enhancing privacy awareness, and improving system security in real time.

References

1. J. Padmavathi and S. A. K. Mohanlal, "A Study on Extent of Awareness Among College Students in Security and Privacy Issues in Social Media," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 7, no. 3, pp. 676–682, 2021.
2. J. C. Aquino et al., "User Privacy and Data Protection: Analysis of Social Media Platform Policies and User Awareness," J. Inf. Secur. Privacy Res., vol. 15, no. 2, pp. 145–162, 2021.
3. D. Mistry et al., "Privacy-Preserving On-Screen Activity Tracking and Classification Using Federated Learning," IEEE Access, vol. 11, pp. 79315–79329, 2023.
4. K. Koidl et al., "The BigFoot Initiative: Digital Footprint Awareness in Social Media," Proc. ACM Conf. Supporting Group Work, pp. 285–294, 2018.
5. R. Lambiotte and M. Kosinski, "Tracking the Digital Footprints of Personality," Proceedings of the IEEE, vol. 102, no. 12, pp. 1934–1939, 2014.
6. S. Bushuyev et al., "Conceptual Model of Project Digital Footprint," IEEE CSIT, pp. 327–332, 2021.
7. P. Schreiber et al., "Digital Privacy Awareness and Behavior Modification Through Real-Time Monitoring Systems," Privacy and Security in Digital Communications, vol. 8, no. 4, pp. 112–128, 2021.
8. L. A. Marwick and N. B. Ellison, "Privacy in Social Networks: Research Opportunities and Challenges," Information, Communication & Society, vol. 15, no. 4, pp. 543–570, 2012.
9. A. L. Young and A. Quan-Haase, "Information Revelation and Internet Privacy Concerns on Social Network Sites," Proc. Communities and Technologies, pp. 265–274, 2009.
10. M. Taddicken, "The Privacy Paradox in the Social Web," Journal of Computer-Mediated Communication, vol. 19, no. 2, pp. 248–273, 2014.
11. C. Dwork, "Differential Privacy: A Survey of Results," Springer, pp. 1–19, 2008.
12. B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," AISTATS, pp. 1273–1282, 2017.
13. F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," IEEE International Conference on Data Mining (ICDM), pp. 413–422, 2008.
14. F. Pedregosa et al., "Scikit-learn: Machine Learning in Python," Journal of Machine Learning Research, vol. 12, pp. 2825–2830,

2011.
15. G. Rodola, “psutil: Cross-platform Library for Process and System Monitoring in Python,”
16. S. Axelsson, “The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection,” *ACM CCS*, 1999.
17. R. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” *IEEE Symposium on Security and Privacy*, 2010.
18. E. Gelenbe and Y. Caseau, “The Impact of Information Technology on Energy Consumption and Carbon Emissions,” *Ubiquity*, 2015.
19. T. L. Saaty, “Decision Making with the Analytic Hierarchy Process,” *Int. J. Services Sciences*, 2008.
20. M. Bishop, “Computer Security: Art and Science,” Addison-Wesley, 2003.
21. W. Stallings, “Network Security Essentials: Applications and Standards,” Pearson, 2017.