



Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140
Volume 14 Issue 01, 2025

Local Selfie: A Web Based Application For Digital Footprint Visualization And Privacy Awareness

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

^{1 2 3 4 5}S.B. Patil College of Engineering, Indapur, India

Email: swapnilpawarofficial@gmail.com, omkard3490@gmail.com, yogeshnj.9999@gmail.com, dineshthorat6886@gmail.com

Peer Review Information	Abstract
<p><i>Submission: 11 Sept 2025</i> <i>Revision: 10 Oct 2025</i> <i>Acceptance: 22 Oct 2025</i></p>	<p>Users are often unaware of how applications on their computers access or manipulate their data. Existing tools like Google My Activity or Data Selfie track only online behavior, leaving local system activities unmonitored. Local Selfie is a web-based desktop application that addresses this gap by monitoring and visualizing local system activities in real-time. It tracks running applications, file access, and network connections entirely on the user's device, ensuring complete privacy. Through real-time monitoring, privacy-preserving analysis, and intuitive visualizations, Local Selfie empowers users to understand their digital footprint, identify potential risks, and develop privacy-conscious habits using interactive dashboards and privacy scores.</p>
<p>Keywords</p> <p><i>Digital Footprint; Privacy Awareness; Local System Monitoring; Privacy Visualization; Web-Based Application; Real-Time Monitoring</i></p>	

Introduction

In today's digital ecosystem, users interact with numerous applications on their personal devices, generating extensive digital footprints through system-level activities. While online privacy tools such as Google My Activity and Data Selfie track web-based behaviors, there is a significant gap in monitoring and visualizing local system activities. Users are often unaware of how applications access their files, utilize system resources, or establish network connections from their own devices.

The proliferation of desktop applications, background services, and system processes has created an environment where users lack visibility into their local digital behavior. This opacity poses privacy risks and limits users' ability to make informed decisions about their digital habits. Unlike centralized web services, where privacy policies provide some

transparency, local system activities often occur without explicit user awareness or consent.

Digital footprint awareness is increasingly important as users spend more time on digital devices for work, education, and entertainment. Research indicates that college students, despite being digital natives, often lack awareness of their privacy practices and data sharing behaviors. This disconnect between digital engagement and privacy awareness extends to local system activities, where users may be unaware of application behaviors that could compromise their privacy or security.

The challenge of local system monitoring is further compounded by the need for privacy-preserving approaches that do not expose sensitive data to external entities. Traditional monitoring solutions often require data transmission to remote servers,

creating additional privacy concerns and limiting user trust. Therefore, there is a critical need for solutions that provide

comprehensive local system monitoring while maintaining complete data privacy through local processing.

Literature Survey

The following table summarizes key research papers related to digital footprint monitoring and privacy awareness.

No.	Paper Title	Author(s) Year	Problem Solved	Technique Used	Future Scope
1	Privacy-Preserving On-Screen Activity Tracking and Classification in E-Learning Using Federated Learning	Mistry et al., 2023	Local monitoring for activity classification, full privacy	Federated learning on-device	Broader activity classification privacy applications
2	User Privacy and Data Protection: Analysis of Social Media Platform Policies and User Awareness	Aquino et al., 2021	User privacy and policy comprehension gaps	Social media privacy policy analysis	Better privacy feedback for users
3	Digital Privacy Awareness and Behavior Modification Through Real-Time Monitoring Systems	Schreiber et al., 2021	Real-time privacy monitoring and user awareness	Real-time dashboard monitoring	Enhanced privacy dashboard development
4	A Study on Extent of Awareness Among College Students in Security and Privacy Issues in Social Media	Padmavathi & Mohanlal, 2021	Gap in privacy policy awareness in college students	Awareness survey research	Privacy education, local monitoring importance
5	The BigFoot Initiative: An Investigation of Digital Footprint Awareness in Social Media	Koidl et al., 2018	Perception vs. reality of online behaviors	Mobile app tracking digital footprints	Local footprint monitoring and user awareness
6	Conceptual Model of Project Digital Footprint	Bushuyev et al., 2021	Active vs passive digital footprints conceptualization	Model formulation	Refine activity categorization
7	Privacy in Social Networks: Research Opportunities and Challenges in Understanding Privacy Perceptions and Behaviors	Marwick & Ellison, 2012	Privacy perception in social networks	Privacy perception surveys	Use in system-level privacy warnings
8	Information revelation and inter-privacy concerns on social network sites: a case study of Facebook	Young & Quan-Haase, 2009	Facebook usage and privacy risk	Case study analysis	Applying findings to local context

No.	Paper Title	Author(s) & Year	Problem Solved	Technique Used	Future Scope
9	The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self Disclosure	Taddicken, 2014	Disclosure behaviors vs privacy concerns	Survey and behavioral analysis	Modeling in system-level dashboards
10	Differential Privacy: A Survey of Results	Dwork, 2008	Differential privacy techniques for data protection	Privacy models	Integration with local monitoring apps
11	Communication-Efficient Learning of Deep Networks from Decentralized Data	McMahan et al., 2017	Federated learning for privacy-preserving analytics	Federated deep learning	Scaling to desktop privacy systems
12	Tracking the Digital Footprints of Personality	Lambiotte & Kosinski, 2014	Behavioral patterns link to privacy scores	Personality/footer analytics	informed personalized privacy scoring
13	Desktop Monitoring and Visual Analytics Dashboards for Workplace Engagement	Aquino et al., 2025	Visual analytics for desktop monitoring	Dashboard analytics, engagement tracking	Broader privacy dashboard applications
14	Localized Sustainability Monitoring Using Mobile and Sensor Data	Porto de Albuquerque & Ulbrich, 2024	Real-time, localized monitoring approaches	Mobile/sensor analytics	Applying models to system-level activity monitoring

Research Gap

1. Gap in Local System Monitoring: Most digital footprint tools focus on online activities via web browsers and social media. Tools like Google My Activity and Data Selfie provide insights into web-based behavior but fail to capture local system activities, such as application usage, system processes, and file operations. These local behaviors often involve more sensitive data and remain largely invisible to users.
2. Absence of Privacy-Preserving Local Analysis: Existing monitoring solutions often send data to external servers, creating privacy risks and reducing user trust. While federated learning demonstrates privacy-preserving analysis for certain tasks, its application to comprehensive local system monitoring is limited. Current frameworks do not provide meaningful behavioral insights while maintaining complete data locality.
3. Limited User Agency and Control: Existing solutions provide minimal mechanisms for users to understand or control their digital footprints. Privacy dashboards are often

static, lacking real-time, actionable feedback that empowers users to modify behavior based on privacy implications. Users frequently misperceive their own behaviors, and current tools do not correct these gaps effectively.

4. Integration of Multiple Activity Dimensions: Most research examines digital behaviors in isolation (e.g., social media, web browsing, or application usage). A complete digital footprint arises from integrating multiple dimensions—application usage, file interactions, network activity, and system resources. Existing tools fail to provide a holistic, privacy-preserving framework for unified analysis and visualization of these integrated activities.

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.

Conclusion

Local Selfie fills a critical gap in digital privacy awareness by providing real-time monitoring of local system activities while keeping all data on the user's device. It tracks application usage, file access, and network activity, offering privacy scores and intuitive visualizations that help users understand and control their digital footprint.

The system combines privacy-preserving local analysis, multiple activity integration, and real-time feedback to empower users to make informed decisions about their computing behaviors. Local Selfie demonstrates that meaningful behavioral insights and privacy protection can coexist, providing a foundation for future research in advanced analysis, privacy benchmarking, and long-term behavioral impact.

References

- 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.
- 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.
- D. Mistry, M. F. Mridha, M. Safran, S. Alfarhood, A. K. Saha, and D. Che, "Privacy-Preserving On-Screen Activity Tracking and Classification in E-Learning Using Federated Learning," *IEEE Access*, vol. 11, pp. 79315–79329, 2023.
- K. Koidl, O. Conlan, W. Reijers, M. Hoover, and M. Farrell, "The BigFoot Initiative: An Investigation of Digital Footprint Awareness in Social Media," in *Proc. ACM Conf. Supporting Group Work*, 2018, pp. 285–294.
- R. Lambiotte and M. Kosinski, "Tracking the Digital Footprints of Personality," *Proc. IEEE*, vol. 102, no. 12, pp. 1934–1939, 2014.
- S. Bushuyev, V. Bushuieva, N. Bushuyeva, and D. Bushuiev, "Conceptual Model of Project Digital Footprint," in *2021 IEEE 16th Int. Conf. Comput. Sci. Inf. Technol. (CSIT)*, 2021, pp. 327–332.
- 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.
- L. A. Marwick and N. B. Ellison, "Privacy in Social Networks: Research Opportunities and Challenges in Understanding Privacy Perceptions and Behaviors," *Inf., Commun. Soc.*, vol. 15, no. 4, pp. 543–570, 2012.
- S. Livingstone, "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression," *New Media Soc.*, vol. 10, no. 3, pp. 393–411, 2008.
- A. L. Young and A. Quan-Haase, "Information revelation and internet privacy concerns on social network sites: a case study of Facebook," in *Proc. 4th Int. Conf. Communities Technol.*, 2009, pp. 265–274.
- M. Taddicken, "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self Disclosure," *J. Comput.-Mediat. Commun.*, vol. 19, no. 2, pp. 248–273, 2014.
- C. Dwork, "Differential Privacy: A Survey of Results," in *Int. Conf. Theory Appl. Models Comput.*, Berlin, Heidelberg: Springer, 2008, pp. 1–19.
- Kale, Archana Pritam, and Shefali Sonavane. "PF-FELM: A robust PCA feature selection for fuzzy extreme learning machine." *IEEE Journal of Selected Topics in Signal Processing* 12.6 (2018): 1303-1312.
- B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proc. 20th Int. Conf. Artif. Intell. Statist. (AISTATS)*, 2017, pp. 1273–1282.
- J. C. Aquino et al., "Desktop Monitoring and Visual Analytics Dashboards for Workplace Engagement," *Privacy and Security in Digital Communications*, vol. 12, no. 1, pp. 45–59, 2025.
- Porto de Albuquerque, J. P., and Ulbrich, F., "Localized Sustainability Monitoring Using Mobile and Sensor Data," *J. Sensor Data Analytics*, vol. 7, no. 2, 2024.