frontiers | Frontiers in Computer Science

TYPE Correction
PUBLISHED 17 November 2025
DOI 10.3389/fcomp.2025.1673393

OPEN ACCESS

EDITED AND REVIEWED BY
Stelvio Cimato,
University of Milan, Italy

*CORRESPONDENCE
Muhammad Arshad
✉ Muhammad.arshad@tudublin.ie

RECEIVED 25 July 2025
ACCEPTED 28 October 2025
PUBLISHED 17 November 2025

CITATION
Arshad M, Ahmad A, Onn CW and Sam EA (2025) Correction: Investigating methods for forensic analysis of social media data to support criminal investigations. *Front. Comput. Sci.* 7:1673393. doi: 10.3389/fcomp.2025.1673393

Correction: Investigating methods for forensic analysis of social media data to support criminal investigations

Muhammad Arshad[1]*, Ashfaq Ahmad[2], Choo Wou Onn[3] and Emmanuel Arko Sam[4,5]

[1]School of Informatics and Cybersecurity, Technological University Dublin, Dublin, Ireland, [2]Faculty of Basic Sciences, Lahore Garrison University, Lahore, Pakistan, [3]Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia, [4]Unicaf, Larnaca, Cyprus, [5]University of East London, London, United Kingdom

KEYWORDS

AI in forensics, cybercrime investigation, food security, forensic analysis, gender injustices, social media forensics

A Correction on
Investigating methods for forensic analysis of social media data to support criminal investigations

by Arshad, M., Ahmad, A., Onn, C. W., and Sam, E. A. (2025). *Front. Comput. Sci.* 7:1566513. doi: 10.3389/fcomp.2025.1566513

The below references for were erroneously written as:

Smith, R. & Patel, T. (2023). "Cross-Border Data Access in Digital Forensics". Digital Investigation, 45, 101678.

Zhang, Y., et al. (2023) "Secure Federated Learning for Digital Forensics: A Provable Framework with Differential Privacy." IEEE Transactions on Information Forensics and Security, 18, 4503-4517.

Liu, Y., et al. (2023). "Adversarial Validation for Bias Mitigation in Forensic Machine Learning". IEEE Transactions on Information Forensics and Security, 18, 2105-2118.

The correct references are:

Zuo, Z. (2024). Cross-border data forensics: challenges and strategies in the belt and road initiative digital era. *Editor. Board* 20:49. doi: 10.5539/ass.v20n2p49

Zhang, Z., Wu, L., Ma, C., Li, J., Wang, J., Wang, Q., et al. (2022). LSFL: a lightweight and secure federated learning scheme for edge computing. *IEEE Trans. Inf. Forensics Secur.* 18, 365–379. doi: 10.1109/TIFS.2023.3331274

Pagano, T. P., Loureiro, R. B., Lisboa, F. V. N., Peixoto, R. M., Guimarães, G. A. S., Cruz, G. O. R., et al. (2023). Bias and unfairness in machine learning models: a systematic review on datasets, tools, fairness metrics, and identification and mitigation methods. *Big Data Cogn. Comput.* 7:15. doi: 10.3390/bdcc7010015

Zuo (2024) was not cited in the article. The citation has now been inserted into section *3.2 Data collection, 3.2.3 Ethical and legal compliance*, First Paragraph and should read:

"The data collection strictly adhered to privacy laws such as GDPR and country jurisdiction guidelines. Where necessary, legal warrants or subpoenas were acquired

to access restricted or private data. Kerr's (2022) seminal work on Computer Crime Law establishes the foundational standards for lawful acquisition of social media data, emphasizing chain of custody protocols that informed our blockchain-based preservation system (Section 6.2). For jurisdiction challenges, we reference the Zuo (2024) empirical study in Digital Investigation, which evaluates GDPR/CCPA compliance in 200+ cross-border cases, directly supporting our warrant-based data access procedures."

Zhang et al. (2022) and Pagano et al. (2023) were not cited in the article. The citations have now been inserted in section *5.4 Bias, fairness, and responsible AI* Second Paragraph and should read:

"While federated learning architectures show promise for privacy-preserving forensics, we prioritise peer-validated methods such as those formalized by Zhang et al. (2022) in their IEEE Transactions on Information Forensics and Security study, which demonstrated provable security guarantees for distributed forensic analysis while maintaining GDPR compliance. For adversarial robustness testing, we cite Pagano et al. (2023) an MDPI study, which formalizes bias-mitigation frameworks for forensic AI—an approach mirrored in our SHAP analysis."

The original version of this article has been updated.

Publisher's note