JOURNAL OF
FORENSIC AND
ALLIED SCIENCES
Volume 1, Issue 1, July-September, 2025, PP 001-008

OPEN ACCESS

Review Paper

Social Media Forensics: Foundations, Technical Frameworks, and Emerging Challenges

Nishchal Soni[1*], Kanika Chauhan[1]

1. School of Bioengineering and Biosciences, Lovely Professional University, Phagwara, Punjab 144001, India

More Information

Address for Correspondence: 1. School of Bioengineering and Biosciences, Lovely Professional University, Phagwara, Punjab 144001, India

E-mail: Nishchalresearch@gmail.com

Submitted: July 15, 2025

Approved: July 28, 2025

Published: July 29, 2025

How to cite this article: Soni, N., & Chauhan, K. (2025). Social Media Forensics: Foundations, Technical Frameworks, and Emerging Challenges. Journal of Forensic and Allied Sciences, 1(1), 001–008. https://doi.org/10.5281/zenodo.16811398

DOI: https://doi.org/10.5281/zenodo.16811398

Abstract

Social media forensics (SMF) has emerged as a critical subdomain of digital forensics, addressing the complex task of collecting, analyzing, and preserving evidence from dynamic, user-driven platforms. As social media plays an increasingly central role in communication, crime, and civil disputes, investigators face significant obstacles related to data volatility, platform encryption, legal jurisdiction, and user privacy. This review explores the foundational theories behind SMF, the legal frameworks that govern its practice, the array of technical tools and methodologies used for investigation, and the tactics employed by adversaries to evade detection or manipulate evidence. Special emphasis is placed on the evolving threat landscape, including deepfakes, ephemeral messaging, and decentralized platforms, as well as emerging solutions in artificial intelligence, blockchain, and real-time forensics. The paper concludes with a forward-looking perspective on the strategic, technological, and policy innovations needed to strengthen forensic readiness and ensure the integrity of digital investigations in an increasingly complex online ecosystem.

Keywords: social media forensics, digital evidence, anti-forensics, metadata analysis, forensic tools, cybercrime detection

1. Introduction

In the digital age, the proliferation of social media platforms such as Facebook, Twitter, Instagram, and TikTok has significantly transformed how individuals communicate, share information, and express themselves. While these platforms enable global connectivity and real-time interaction, they also present a new frontier for cybercrime, misinformation, and digital exploitation. The exponential growth of user-generated content, coupled with the relative anonymity afforded by social media, has necessitated the development of a specialized branch within digital forensics known as social media forensics (Nishchal, 2024).

Social media forensics (SMF) refers to the systematic identification, collection, preservation, analysis, and presentation of digital evidence originating from social networking platforms. Unlike traditional digital forensics, which focuses on file systems and device memory, SMF deals with dynamic, volatile, and often cloud-based data formats—such as posts, images, comments, messages, likes, and geolocation metadata (Huber et al., 2011). This discipline has grown increasingly important in both criminal and civil investigations, playing a critical role in cases of cyberstalking, online fraud, hate speech, and terrorism (Wafula, 2016). The forensic investigation of social media platforms poses several unique challenges. These include limited access to proprietary platform data, encrypted communications, ephemeral

content (such as Stories or Snaps), and jurisdictional limitations due to global data hosting. Moreover, the fast-paced and ever-changing nature of online interactions makes timely data acquisition crucial. Investigators must rely on a combination of Application Programming Interfaces (APIs), web crawlers, and third-party forensic tools to capture and preserve admissible digital evidence (Chen et al., 2015).

Furthermore, the legal and ethical implications of social media investigations are profound. The use of personal digital footprints as evidence must align with data protection laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Unauthorized access to social media content or failure to obtain proper consent may result in the dismissal of evidence in legal proceedings (Arshad et al., 2019). Therefore, forensic investigators must not only be technologically adept but also well-versed in legal standards and ethical considerations.

Recent advancements in artificial intelligence (AI) and machine learning have enhanced SMF capabilities, allowing for the automation of profile classification, behavior prediction, and fake account detection (Bokolo & Liu, 2024). These technologies support scalable analysis of vast datasets and enable real-time threat monitoring, although they also introduce concerns related to algorithmic bias and transparency (Soni, 2024a).

In sum, social media forensics represents a vital and evolving area within digital forensics that intersects with law, technology, and society. This paper aims to provide a comprehensive review of the theoretical frameworks, technical methodologies, and emerging challenges in the field, thereby laying a foundation for future research and practical applications.

2. Theoretical and Legal Foundations

The conceptual underpinnings of social media forensics (SMF) are rooted in the broader discipline of digital forensics, yet they extend into unique socio-technical and legal domains. Unlike traditional digital forensics, which focuses on static data stored on physical devices, SMF involves dynamic, cloud-hosted, and user-generated content distributed across platforms with proprietary infrastructures and jurisdictional ambiguities. This section explores both the theoretical frameworks and legal considerations that define the scope, boundaries, and legitimacy of social media forensic practices.

2.1 Theoretical Frameworks

From a theoretical standpoint, SMF integrates principles from information security, data science, criminology, and communication studies. The media ecology theory provides an essential framework, emphasizing how communication technologies alter the context of human interaction and societal surveillance (Postman, 1970; Levinson, 1999). Social media platforms are not merely passive repositories but active mediators of social behavior, which makes forensic investigation context-sensitive and temporally constrained.

Another important model is the Diamond Model of Intrusion Analysis, which conceptualizes incidents as interactions between adversaries, infrastructure, victims, and capabilities (Caltagirone et al., 2013). In SMF, this model is extended to include behaviors such as social engineering, coordinated misinformation campaigns, and cyberstalking, all of which leverage platform dynamics for malicious purposes.

Moreover, the Cybercrime Opportunity Theory posits that perpetrators exploit digital affordances such as anonymity, reach, and permanence to engage in illicit activities (Ngo & Paternoster, 2011). Forensic readiness—the proactive configuration of systems to facilitate investigation—is therefore a critical concern in social platforms, requiring both technical tools and policy enforcement (Reddy & Basha, 2020).

2.2 Legal Foundations and Jurisdiction

Legal frameworks governing SMF vary significantly across jurisdictions, complicating the evidentiary use of social media data in court. In many cases, electronic evidence is admissible if it meets criteria for relevance, authenticity, and integrity (Kerr, 2005). Forensic investigators must ensure proper chain of custody, avoid contamination, and document every step of evidence handling.

In the United States, laws such as the Stored Communications Act (SCA) and Electronic Communications Privacy Act (ECPA) place restrictions on accessing user data without consent or legal warrants. Meanwhile, in the European Union, the General Data Protection Regulation (GDPR) imposes stringent requirements for user consent, data minimization, and transparency, directly impacting the forensic collection of social media evidence (Alharbi et al., 2021).

Additionally, cross-border data hosting introduces conflicts between national sovereignty and platform governance. For example, a platform headquartered in California may host data relevant to a crime committed in Germany, raising

Doi: https://doi.org/10.5281/zenodo.16811398
Journal Website: www.Shodhforensic.com

questions about data access and extradition of digital evidence (Li, 2018). This legal complexity demands international cooperation, harmonized protocols, and increased platform transparency for law enforcement access.

Ethical considerations are also deeply intertwined with legal compliance. Unauthorized access to social media accounts, even for investigative purposes, can constitute a breach of privacy or hacking under local laws. Investigators must balance evidentiary goals with the principles of proportionality, necessity, and user rights.

In sum, the theoretical and legal foundations of SMF reflect a multi-layered domain that intersects with communication theory, cyber law, and forensic science. The evolving nature of social media requires continuous updates to legal instruments and ethical guidelines to ensure forensic practices remain both effective and lawful.

3. Technical Frameworks and Tools

The technical backbone of social media forensics (SMF) encompasses a wide array of methodologies and tools aimed at acquiring, preserving, analyzing, and presenting digital evidence sourced from social platforms. Given the volatile, high-volume, and multimedia-rich nature of social media data, SMF relies on both conventional digital forensic frameworks and emerging analytical technologies that combine automation, scalability, and legal admissibility. This section outlines the core technical processes and tools involved in SMF investigations.

3.1 Data Acquisition and Preservation

Data acquisition in SMF is challenged by the ephemerality and inaccessibility of platform-controlled content. Unlike local disk forensics, SMF frequently involves the use of APIs (Application Programming Interfaces) to access posts, user profiles, metadata, and activity logs—often constrained by platform-specific limits and privacy settings (Ali et al., 2015). In cases where APIs are restricted or unavailable, investigators employ web scraping tools and browser-based capture mechanisms to archive data in forensic formats (Jones et al., 2022).

Mobile forensics also plays a role, especially when analyzing social media apps on smartphones. Tools like Cellebrite UFED and Oxygen Forensics can extract cached content, tokens, chat logs, and multimedia from mobile devices, ensuring preservation of volatile data such as ephemeral messages or deleted content (Al Mutawa et al., 2016).

3.2 Metadata and Content Analysis

Beyond content retrieval, metadata extraction is a critical aspect of SMF. Metadata includes timestamps, geotags, device information, and IP logs that can link a digital activity to a suspect or location. Forensic tools must be capable of maintaining hash integrity, time synchronization, and chain-of-custody documentation to ensure admissibility in court.

Social media posts also undergo semantic analysis and entity recognition to detect keywords, sentiments, relationships, and behavioral patterns. Natural Language Processing (NLP) techniques have been widely adopted to analyze large-scale social discourse and trace trends in hate speech, misinformation, or coordinated influence campaigns (Kumar et al., 2022).

3.3 Tools for Social Media Forensics

A variety of open-source and commercial tools are used in SMF workflows:

Open-Source Tools:

- **Maltego**: A graph-based link analysis tool used for visualizing relationships among social profiles, domains, and infrastructure.
- **SpiderFoot**: An automation tool that supports OSINT (Open-Source Intelligence) across social platforms, domains, and IPs.
- **Social Media OSINT Framework**: A community-maintained directory that aggregates tools for account discovery, post monitoring, and fake account identification.

Commercial Tools:

- **X1 Social Discovery**: Designed for legal professionals, this tool captures and indexes social media content from platforms such as Facebook, Twitter, and YouTube, ensuring preservation and metadata integrity.
- **Magnet AXIOM**: Integrates data from mobile devices, cloud services, and social media accounts

Doi: https://doi.org/10.5281/zenodo.16811398
Journal Website: www.Shodhforensic.com

into a unified analysis platform with built-in visualization and AI-assisted filtering.

- **Belkasoft Evidence Center**: Provides advanced recovery of deleted social data from mobile and computer systems, including artifacts from encrypted apps.

Each tool offers different levels of granularity, legal compliance, and scalability, making tool selection a case-dependent decision based on the platform in question, the type of data required, and jurisdictional constraints.

3.4 Automation and Machine Learning Integration

To address the massive scale and velocity of social media content, SMF increasingly incorporates machine learning (ML) for content classification, image clustering, bot detection, and anomaly identification. For instance, ML models trained on labeled datasets can detect synthetic media (deepfakes), classify hate speech, or identify fake accounts with high accuracy (Sundarkumar et al., 2020).

Moreover, graph databases and knowledge graphs are now integrated into forensic pipelines to represent connections between users, events, and communications across time, enhancing the contextual understanding of digital behaviors (Pannu & Sabharwal, 2021).

In summary, technical tools in social media forensics must adapt to platform restrictions, legal obligations, and data diversity. A layered approach that integrates manual inspection, forensic automation, metadata integrity, and advanced analytics is essential for producing reliable and legally defensible outcomes.

4. Threats, Evasion, and Anti-Forensics Techniques

Despite advancements in social media forensic tools and frameworks, numerous technical and behavioral barriers hinder the effective collection and analysis of social media evidence. These include tactics specifically designed to obscure, alter, or eliminate digital traces—collectively known as **anti-forensics techniques**. Malicious actors, privacy-conscious users, and even legitimate platform features can introduce obstacles to forensic investigations. This section examines the main **threat vectors**, **evasion strategies**, and **anti-forensics methods** that challenge social media forensics today (Soni, 2025b).

4.1 Threat Vectors in Social Media Forensics

Social media platforms are highly dynamic environments vulnerable to a variety of **cyber threats** and malicious behavior. These include:

- **Fake identities and botnets**: Automated accounts are frequently used to manipulate public opinion, conduct spam operations, or obfuscate real user behavior (Ferrara, 2017).
- **Encrypted and ephemeral messaging**: Apps like Signal, Telegram, and Snapchat offer end-to-end encryption and disappearing messages, making post-hoc forensic recovery extremely difficult (Ntantogian et al., 2019).
- **Deepfake content**: AI-generated audio, video, and images complicate evidence verification, potentially leading to the dissemination of false narratives (Chesney & Citron, 2019).
- **Geo-spoofing and VPNs**: Techniques like location spoofing and anonymized IP routing hinder attribution and event reconstruction (Anderson & Rainie, 2021).

These threats often exploit platform features intentionally designed for privacy, which, while beneficial to users, complicate lawful digital evidence collection.

4.2 Evasion Tactics by Users and Adversaries

Adversaries often employ evasion techniques to avoid detection and forensic tracing:

- **Account cycling and burner profiles**: Frequent switching between temporary or "burner" accounts prevents consistent tracking across investigations.
- **Language obfuscation and slang**: Use of memes, symbols, coded language, and evolving slang makes keyword-based forensic searches less effective (Marwick & Lewis, 2017).
- **Decentralized platforms**: Migration to blockchain-based or peer-to-peer social networks (e.g., Mastodon, Minds) limits the ability of centralized tools to access or index data.

Doi: https://doi.org/10.5281/zenodo.16811398
Journal Website: www.Shodhforensic.com

These evasive behaviors are not only technologically driven but also socially engineered, often relying on the knowledge of how forensic systems function.

4.3 Anti-Forensics Techniques and Methods

Anti-forensics refers to any activity intended to disrupt the integrity or utility of digital forensic procedures. In social media, this can manifest in several ways:

- **Metadata manipulation**: Tools are available that allow users to tamper with image timestamps, GPS data, or post times, undermining chronological reconstruction (Baggili et al., 2012).
- **Content deletion and alteration**: Although some platforms offer content recovery APIs, many forms of deletion (e.g., stories, temporary posts) are irreversible without prior capture.
- **Using anti-forensic apps**: Apps like "CoverMe" or "Wickr Me" automatically delete messages, leaving minimal or no recoverable traces (Mujtaba et al., 2020).
- **Encryption-based evasion**: Encrypted channels prevent packet inspection or forensic acquisition unless decrypted at the device level.

Some users even adopt counter-forensic strategies, such as inserting fake evidence into their social profiles to confuse investigators or delegitimize accusations.

4.4 Forensic Countermeasures

To address these challenges, forensic practitioners adopt various **countermeasures**:

- **Proactive monitoring and live capture**: Real-time scraping and monitoring tools reduce the impact of deletion and obfuscation.
- **AI-based pattern recognition**: Machine learning models can detect behavioral anomalies, synthetic media (deepfakes), and bot-generated content (Kaur et al., 2021).
- **Multimodal analysis**: Combining text, image, video, and metadata increases the robustness of digital evidence and reduces reliance on any single source of truth.

Despite these solutions, the adversarial nature of social media forensics demands continuous adaptation. Investigators must anticipate evasive behavior, stay current with platform updates, and remain legally compliant while using increasingly sophisticated forensic toolkits.

5. Challenges and Future Directions

The evolution of social media forensics faces several complex challenges that span technical, legal, and societal dimensions. As digital environments grow in complexity and scale, forensic investigators must grapple with issues of access, accuracy, scalability, and regulatory compliance. Understanding these obstacles is essential to shaping the future capabilities and limitations of the field.

5.1 Challenges

One of the foremost challenges is the dynamic and ephemeral nature of social media content. Many platforms offer disappearing messages, temporary stories, or live broadcasts that are not archived by default, making post-event forensic recovery difficult or impossible without prior monitoring. The rise of encrypted communication further complicates access, as investigators often encounter messages or media that are inaccessible without device-level decryption.

Data volume and heterogeneity pose another major challenge. Social media platforms generate terabytes of multimedia content daily. Analyzing such data requires scalable, automated tools capable of filtering relevant evidence from massive noise. However, existing tools are often siloed by platform and format, leading to fragmented investigations that lack cohesion or context.

Legal and jurisdictional barriers also limit the reach of forensic investigations. Social media platforms operate globally, but laws governing data access, privacy, and admissibility vary by country. Investigators must navigate a patchwork of international regulations, service-level agreements, and user protections, often slowing down time-sensitive investigations.

The issue of data authenticity and trust continues to gain prominence. With the advent of synthetic content like deepfakes and bot-generated misinformation, it has become increasingly difficult to verify the origin and accuracy of

Doi: https://doi.org/10.5281/zenodo.16811398
Journal Website: www.Shodhforensic.com

online content. Chain-of-custody protocols and metadata analysis are critical, but even these can be manipulated by sophisticated anti-forensic techniques.

Additionally, the lack of standardization in social media forensic procedures undermines reproducibility and judicial acceptance. Different tools may capture, parse, or interpret the same content differently, which could affect the credibility of forensic results in court. Establishing universal guidelines and certification protocols is necessary for the credibility of the field.

5.2 Future Directions

Despite these challenges, the future of social media forensics is poised for significant advancement. Emerging technologies such as AI-driven multimodal analysis promise to fuse text, image, video, and metadata into integrated narratives that improve event reconstruction and behavioral profiling. Advances in deep learning will likely enhance the detection of synthetic media and malicious automation, improving the accuracy and speed of investigations.

Blockchain technology holds potential for enhancing evidence integrity and auditability. By immutably recording the collection, analysis, and transfer of digital artifacts, blockchain systems can help establish stronger evidentiary trust in judicial settings.

Real-time forensic capabilities are also on the horizon. As social platforms integrate streaming content and rapid user interaction, forensic systems must evolve from post-incident analysis to proactive and live monitoring. This transition requires tools that can ingest and analyze data on-the-fly without compromising user rights or legal compliance.

Collaborative frameworks among governments, tech companies, and academic researchers are needed to develop shared protocols and access models. These partnerships can facilitate lawful data sharing, ethical AI development, and cross-border investigative capabilities.

Lastly, forensic education and training must evolve to keep pace with the digital landscape. Investigators will need hybrid expertise that combines traditional digital forensics with data science, ethics, law, and cyber threat intelligence. Equipping future professionals with interdisciplinary skills will be critical to sustaining the field's relevance and resilience.

In summary, while social media forensics faces significant roadblocks, it is also a field rich with innovation potential. Addressing current limitations through research, collaboration, and policy reform will determine how effectively this discipline supports digital justice in the coming years.

References:

- Al Mutawa, N., Baggili, I., & Marrington, A. (2016). Forensic analysis of social media applications on mobile devices. *Digital Investigation, 13*, 89–103. https://doi.org/10.1016/j.diin.2015.12.002
- Alharbi, F., Hussain, M., & Abulaish, M. (2021). Investigating forensic readiness of social media platforms under GDPR. *Journal of Digital Forensics, Security and Law, 16*(1), 1–20. https://commons.erau.edu/jdfsl/vol16/iss1/1
- Ali, S., Clarke, N., & Papadaki, M. (2015). Social media forensic investigations: Facebook as a case study. *Proceedings of the 2015 International Conference on Cybercrime and Computer Forensics (ICCCF)*, 1–6. https://doi.org/10.1109/ICCCF.2015.7060217
- Anderson, J., & Rainie, L. (2021). The future of social media and privacy. *Pew Research Center*. https://www.pewresearch.org/internet/2021/02/25/the-future-of-social-media-and-privacy
- Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. *Digital Investigation, 29*, S48–S59. https://doi.org/10.1016/j.diin.2019.04.004
- Baggili, I., Mislan, R., & Rogers, M. (2012). Mobile phone forensics: Current methods and future directions. *Journal of Digital Forensics, Security and Law, 7*(3), 1–20. https://commons.erau.edu/jdfsl/vol7/iss3/1
- Bokolo, B. G., & Liu, Q. (2024). Artificial intelligence in social media forensics: A comprehensive survey and analysis. *Electronics,*

13(9), 1671. https://www.mdpi.com/2079-9292/13/9/1671

- Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The Diamond Model of Intrusion Analysis*. Center for Cyber Intelligence Analysis and Threat Research. https://www.threatconnect.com/wp-content/uploads/Diamond_Model_of_Intrusion_Analysis.pdf
- Chen, L., Xu, L., & Yuan, X. (2015). Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges. *2015 IEEE International Conference on Computing, Communication and Automation*, 1–6. https://doi.org/10.1109/CCAA.2015.7148378
- Chesney, R., & Citron, D. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs, 98*(1), 147–155. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war
- Ferrara, E. (2017). Disinformation and social bot operations in the run up to the 2017 French presidential election. *First Monday, 22*(8). https://doi.org/10.5210/fm.v22i8.8005
- Huber, M., Mulazzani, M., Leithner, M., Schrittwieser, S., Sinha, M., & Weippl, E. (2011). Social snapshots: Digital forensics for online social networks. *Proceedings of the 27th Annual Computer Security Applications Conference*, 113–122. https://doi.org/10.1145/2076732.2076748
- Jones, B., Liu, H., & Pang, L. (2022). A practical approach to social media data scraping for digital forensics. *Journal of Digital Forensics, Security and Law, 17*(1), 32–48. https://commons.erau.edu/jdfsl/vol17/iss1/4
- Kaur, H., Kaur, P., & Aggarwal, S. (2021). AI-driven detection of malicious activities in social media platforms. *Procedia Computer Science, 192*, 2215–2224. https://doi.org/10.1016/j.procs.2021.08.228
- Kerr, O. S. (2005). Searches and seizures in a digital world. *Harvard Law Review, 119*(2), 531–585. https://doi.org/10.2307/4093346
- Kumar, S., Shah, N., & Subrahmanian, V. S. (2022). Detecting and characterizing coordinated influence campaigns on social media. *Proceedings of the AAAI Conference on Artificial Intelligence, 36*(1), 924–933. https://doi.org/10.1609/aaai.v36i1.19827
- Levinson, P. (1999). *Digital McLuhan: A guide to the information millennium*. Routledge. https://doi.org/10.4324/9780203979877
- Li, X. (2018). Jurisdictional issues in cross-border investigation of cybercrime. *Computer Law & Security Review, 34*(6), 1245–1255. https://doi.org/10.1016/j.clsr.2018.08.009
- Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. *Data & Society Research Institute*. https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf
- Mujtaba, G., Abbas, H., & Bakiras, S. (2020). An overview of privacy-focused mobile apps used in anti-forensics. *IEEE Access, 8*, 118015–118028. https://doi.org/10.1109/ACCESS.2020.3003855
- Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793. http://www.cybercrimejournal.com/ngoijcc2011vol5issue1.pdf
- Nischal Soni (2025b) Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges. J Forensic Leg Investig Sci 11: 105.
- Nishchal, S. (2024). Forensic Analysis of WhatsApp: A review of techniques, challenges, and future directions. *Journal of Forensic Science and Research*, *8*(1), 019–024. https://doi.org/10.29328/journal.jfsr.1001059
- Ntantogian, C., Malliaros, S., & Xenakis, C. (2019). Evaluating the forensic quality of social media evidence on encrypted mobile devices. *Journal of*

Information Security and Applications, 47, 229–238. https://doi.org/10.1016/j.jisa.2019.04.007

- Pannu, H. S., & Sabharwal, R. (2021). Leveraging knowledge graphs for forensic analysis in social media. *Computer Science Review, 40*, 100379. https://doi.org/10.1016/j.cosrev.2021.100379
- Postman, N. (1970). The redefinition of media ecology. *Etc: A Review of General Semantics, 27*(3), 198–203. https://www.jstor.org/stable/42575803
- Reddy, S., & Basha, S. M. (2020). Forensic readiness in social media platforms: Conceptual model and strategies. *International Journal of Computer Applications, 175*(26), 1–7. https://doi.org/10.5120/ijca2020920033
- Soni, N. (2024a). IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem. *Deleted Journal*, *2*(4), 3070. https://doi.org/10.54517/cte3070
- Sundarkumar, G., Ravi, V., & Mohan, V. (2020). Deep learning approaches for detecting online social media threats: A survey. *Computer Science Review, 38*, 100291. https://doi.org/10.1016/j.cosrev.2020.100291
- Wafula, G. W. (2016). Social media forensics for hate speech opinion mining [Master's thesis, University of Nairobi]. University of Nairobi Repository. http://erepository.uonbi.ac.ke/handle/11295/97833