JOURNALS | Journal of Collective Sciences and Sustainability

Volume 1 Issue 1 (June 2025)
J. Collect. Sci. Sustain., 2025, 1(1), 25405
DOI : https://doi.org/10.64189/css.25405

Research Article

OPEN ACCESS

AI-Driven Open-Source Intelligence in Digital Forensics for Cybercrime Investigation

Nitin Soni* and Rakesh Poonia*

Department of Computer Applications, Engineering College, Bikaner, Rajasthan, 334004, India

*Corresponding Author
Nitin Soni
nitinsoni.mca@ecb.ac.in
Rakesh Poonia
rakesh.poonia@ecb.ac.in

Received: 10 May 2025
Revised: 18 June 2025
Accepted: 22 June 2025
Published Online: 24 June 2025

Citation

N. Soni, R. Poonia, AI-driven open-source intelligence in digital forensics for cybercrime investigation, *Journal of Collective Sciences and Sustainability*, 2025, 1(1), 25405, doi: https://doi.org/10.64189/css.25405.

Open Access

This article is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License, which permits the non-commercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as appropriate credit to the original author(s) and the source is given by providing a link to the Creative Commons License and changes need to be indicated if there are any. The images or other third-party material in this article are included in the article's Creative Commons License, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons License and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this License, visit: https://creativecommons.org/licenses/by-nc/4.0/

© The Author(s) 2025

Abstract

The growing complexity and frequency of cybercrimes have surpassed the capabilities of traditional digital forensics methods. This study investigates the potential for an enhancement in digital forensics based on an integration with Artificial Intelligence (AI) and Open-Source Intelligence (OSINT) sources. A proactive approach to cybercrime investigations is proposed. AI-driven OSINT tools can collect, process, and analyze vast amounts of publicly available data from diverse sources such as social media, forums, and the dark web at incredible speeds. These tools can identify patterns, anomalies, and potential threats with unprecedented accuracy and speed by applying machine learning algorithms and natural language processing techniques. This article explores the operational dynamics of AI-driven OSINT, how it augments capabilities of forensic investigators to better anticipate and thwart cyberattacks before they escalate. This paper further provides a comprehensive review of the current challenges in digital forensics, such as the limitations in handling data and the reactive nature in traditional methods. Using very elaborate case studies, we clearly highlight the practical application of AI-driven OSINT in a variety of cybercrime scenarios which improve investigative outcomes by a significant margin.

Keywords: Digital forensics; Open-Source Intelligence (OSINT); Cybercrime investigation; Data mining techniques; Threat intelligence.

1. Introduction

In this era of sophistication in the world of cybercrime. Digital forensics is the systematic collection, analysis, and preservation of electronic information to retrieve evidence as well as support criminal investigations. Yet more advanced methods are being deployed by cybercriminals to render traditional forensic methods inadequate and ineffective for the amount, speed, and variety of data being generated in the digital realm.

Digital forensics integrated with artificial intelligence (AI) has now brought open-source intelligence (OSINT) closer to achieving its very practical pinnacle. OSINT normally refers to information gathered from the public domain, such as websites and social media forums. With AI technologies, it can be adopted differently for cybercrime investigation; theoretically, use it proactively to identify, analyze, and/or predict potential threats. In general terms, OSINT analysis comprises gathering data from publicly accessible sources to build usable knowledge. Instead of relying on classified or proprietary information, it seeks information from open sources such as the internet, social networking sites, news portals, government databases, or meeting places on common interests. The purpose may be for anyone, from national security considerations to law enforcement, commercial competitive intelligence, or cybersecurity.

With the coming into being of the digital world, the establishment brought about the exponential growth of data that could be unconsciously exposed by either an individual or an organization. Profiles on these social media applications reveal anything from roles and competencies, social affiliations, recent activities, and even location movement data. Likewise, the website of an organization and press releases can offer information on organizational structures, schedule dates of projects, and the specific intent of strategizing. Each of these pieces of information stands innocent in the free world, whereas a skillful analyst can piece this data together to produce an intelligence profile.

OSINT is used to collect information in certain situations, going intermediates in legal proceedings or for hostile intelligence, and much of its efficacy lies in being legal and accessible. It needs no hacking or secret surveillance; rather, it involves tools such as advanced search engines, scraping software, metadata analyzers, and mapping platforms to pull meaningful patterns out of data points from telecommunications. Thus, OSINT is a technique admired both by genuine security practitioners who conduct offensive threat assessments and by adversaries who organize targeted attacks.

Artificial intelligence is trained to scan huge amounts of data using machine learning, natural language, and data mining techniques to profile patterns to derive actionable intelligence. It helps in recognizing cyber threats quickly, utilizing precious time in searching for clues in a crime or fraud case, and responding timely to all strata. Hopefully, it will bring a sense of elevations to providing an overall framework for risk intelligence gathering in the fast-evolving cyberspace and all its attendant threats.

The study investigates the application of AI-enabled OSINT for elevating digital forensics about the advantages and challenges it brings along with concrete cases in real time. The paper's review of existing practices and innovations attempts to show how an AI-enabled OSINT could make transformation from highly centralized reactive measures to proactive strategies in cybercrime investigations scope. Fig. 1 shows flow chart of the process of identifying potential threats through AI-enhanced open-source intelligence.

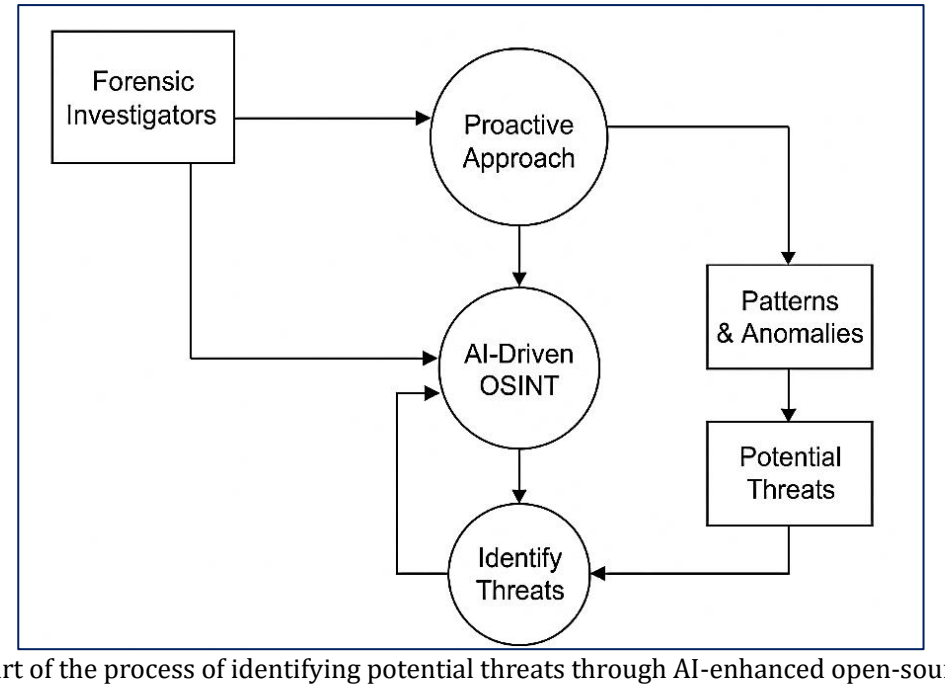


Fig. 1: Flow chart of the process of identifying potential threats through AI-enhanced open-source intelligence.

2. Literature review

The adoption of Artificial Intelligence (AI) and Open-Source Intelligence (OSINT) has been faced with rapid development in terms of research emerging from digital forensics with great promise in combating cybercrime. This literature review revolves around available research on digital forensics, the contributions of OSINT to cyber security, and the impact that AI technologies will make to the entire discipline.

2.1 Gap analysis

Despite the promising findings in the literature, several notable gaps persist in the current body of research:

1. Limited real-world implementation studies: Most research is conducted in controlled environments or using synthetic datasets. There is a lack of case studies or longitudinal analyses showing how AI-OSINT solutions perform in real-world, high-stakes cyber forensic investigations.
2. Scalability and integration challenges: While AI models perform well in isolated tasks (e.g., classifying phishing emails), integration into full-scale digital forensic workflows—alongside traditional tools and legal procedures-remains underexplored.
3. Data quality and verification issues in OSINT: OSINT sources can be noisy, incomplete, or unreliable. Few studies address how to verify, filter, and manage the integrity of OSINT data when used in digital forensic contexts.
4. Legal and ethical constraints: The intersection of AI, OSINT, and digital forensics raises significant concerns about privacy, consent, and admissibility in court. Yet, most studies overlook legal frameworks or policy implications.
5. Lack of standardized evaluation metrics: Existing research often uses varying benchmarks to evaluate AI-driven forensic tools, making it difficult to compare methods or replicate findings across different domains.
6. Human-AI collaboration and explainability: Few investigations consider how forensic analysts interact with AI systems or trust their outputs. The explainability of AI decisions in legal or investigative settings is still a critical unmet need.

2.1 Digital forensics: current landscape and challenges

Digital forensics is an established field aimed at the retrieval and analysis of electronic data in support of legal proceedings. Conventional forensic techniques rely on the manual collection and analysis of data, which may be time-consuming and susceptible to human error. Casey discusses the limitations of traditional digital forensics with regard to handling the ever-growing volume of digital evidence, further emphasizing the need for more efficient methodologies.[1]

Beebe and Clark described digital forensic as incident responsive, only responding to the incident when it has occurred. This generally leads to slow response, with cybercriminals exploiting the given vulnerability and slipping through the mesh.[2] Additionally, the heterogeneity of digital devices and data types increases the level of complexity during forensic investigations. Advanced and more automated tools will be required to address these increased complexities.

2.2 Open-source intelligence in cybersecurity

OSINT has gained a significant role in cybersecurity by acquiring intelligence from public sources. Clarke and Papadopoulos defined OSINT as an inexpensive, easily accessible tool for gathering information that can help one understand possible threats that cannot be identified by using traditional methods of intelligence gathering.[3] The authors explained how OSINT can increase situational awareness, especially regarding the early signs of cyberattacks.

Akhgar *et al*. discuss the use of OSINT in law enforcement and point out that OSINT is applied in monitoring criminal activities on social media.[4] That also indicates to readers that the information obtained by OSINT may be false, deceptive, unreliable, or incomplete.

2.3 Artificial intelligence in digital forensics

These techniques have brought a fundamental change in many areas of cybersecurity, including the digital forensic. According to Jain *et al*.,[5] machine learning algorithms play a role in the automation of data, which offers a way to save time and lessen the burden on forensic investigations. In this regard, the authors demonstrated that AI can identify patterns and anomalies in vast datasets that might otherwise go undetected by human analysts.

Zawoad and Hasan have been further suggested alternatively through AI-aided frameworks that realizable real-time forensic analysis will rely on text-data interpretation from various sources.[6] These frameworks aim to enhance the detection and response to threats, AI will evolve traditional forensic practices and continues to accelerate and transform traditional forensic practices.

2.4 AI-driven OSINT: bridging the gap

Within this conjunction of AI and OSINT lies an enabling atmosphere for adopting a more proactive approach toward cybercrime investigation, complementing the most prominent deficiencies that digital forensics possesses compared to its traditional counterparts. Sharma and Mehta provide an extensive literature review on AI-enabled OSINT tools in the area of threat intelligence and incident response.[7] The premise being advanced here is that OSINT collection and analysis can

potentially be automated with AI tools, delivering perceptions with precision and in a timely manner.

Van der Walt and Eloff, interactive methods of AI-driven OSINT should work together with forensic workflows so that predictive capability would increase.[8] Their research shows successful case studies through which security breaches were preemptively identified using AI-driven OSINT. This proves the real-life applicability of the method.

2.5 Challenges and ethical considerations

Despite the fact that AI-driven OSINT will have many bright prospects in digital forensics, however, there would be many challenging issues. As per Chakraborty *et al*.,[9] ethical implication of using AI surveillance and data collecting has been portrayed with respect to privacy and liberty. The development of strong and robust legal frames is recommended toward the responsible application of AI-OSINTs.

Kuner *et al*.[10] pointed out the challenges of regulation when it comes to cross-border data flows in OSINT operations, arguing that international cooperation and standardization are necessary for these issues.

3. Methodology

This section will cover various methods that study towards AI and OSINT integration using the proposed implications for digital forensics. The methods would here include the designing of the research framework as shown in Fig. 2, methods for the collection of data, techniques for analysis, and approaches to evaluation.

3.1 Research framework

The use of a hybrid methodological framework, combining theoretical investigation, case studies, and empirical simulation, allows for a full scope of investigation with respect to conceptual and practical approaches toward this topic. The main components of the framework are:

Exploratory research: Examining the traditional digital forensics that challenge AI use in OSINT and its potential to bridge the gap.

Case study analysis: The real-life situation where AI and OSINT have been harnessed to maximum potential.

Simulation and testing: Experiments in a laboratory to attribute value to AI OSINT platforms.

3.2 Data collection

For maximizing the research, different sources of data are put to use for the following purposes:

OSINT sources: Information obtained from social networks, forums, blogs, dark web markets, news portals and public databases.

Academic literature: Peer-reviewed articles, conference papers, and trade publications related to AI, OSINT, and digital forensics are being analyzed for building a theoretical base for project work.

Case studies: Real life incidents and investigations are analyzed for understanding applications of AI-based OSINT tools.

Simulated cybercrime scenarios: Synthetic datasets are generated to simulate a cyber-crime scenario for testing of the AI-driven OSINT tool.

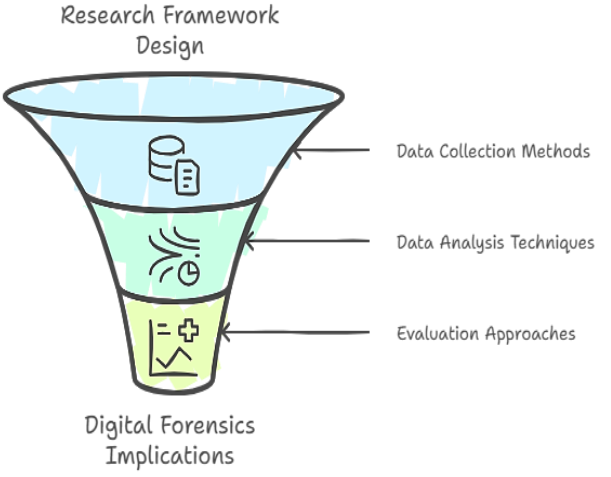


Fig. 2: Schematic of research farmwork design.

3.3 Implementation of AI-driven OSINT

This research traces the path of integrating AI into OSINT workflows, based upon key technologies and techniques such as:

3.4 AI-driven OSINT tools measure the following key performance indicators

Accuracy is measured in terms of precision and recall in detecting cyber threats. Time efficiency: Amount of time that would be needed to analyze massive datasets and formulate actionable insights.

- Scalability: Assessing if the tools support the growth in volumes of OSINT data
- Proactivity: How AI-led OSINTs can predict and counter cybercrimes before they occur

3.5 Case study analysis

Real-life investigations of cybercrime are analyzed using AI-driven OSINT to show application in real world. Cases chosen include:

- The use of Machine learning algorithms to detect phishing campaigns and stop them
- Using dark web traffic monitoring and analyses to identify when data breaches happen.
- Social media analysis towards early detection of coordinated cyber-attacks.

3.6 Ethical and legal

The study aims to address challenges related to ethics and law involving AI-driven OSINT, such as;

- Data Privacy-Compliance on GDPR and CCPA while processing and analyzing data from OSINT.
- Biasness and Fairness-Reduced algorithmic bias in AI systems to ensure equality in the delivered results.
- Transparency- Explaining AI-Driven decisions while building trust as well as an accountability mechanism in place.

3.7 Validation and testing

The findings from case studies and simulation are validated based on:

- Comparison Analysis: a comparison of performances between AI-powered OSINT-based tools and that of traditional forensics practices.
- Review with Experts: requests for feedback of the proposed practicality by professional cybersecurity practitioners/forensic analysts.

4. Case studies

The following section presents in-depth case studies and simulated scenarios that show the application and effectiveness of AI-driven OSINT in enhancing digital forensics. The results of these investigations are compared with traditional methods to point out improvements in accuracy, efficiency, and proactivity.

4.1 Case study 1: detection of phishing campaigns through AI-Driven OSINT

Scenario: A financial institution reported increased phishing emails targeted at its customers. The attackers posed as the bank and sought sensitive information via phishing links.

OSINT data collection: Email samples and phishing reports available in public forums and repositories, such as PhishTank. Social media sites where the victims posted reports of phishing. DNS records and metadata from the phishing domains.

AI integration: Machine learning algorithms (e.g. Random Forest) were trained to classify emails as malicious or benign based on features such as URL structure, sender metadata, and content patterns. Natural Language Processing (NLP) analyzed email content to detect fraudulent intents, such as urgency or reward-based language.

Results: The AI-driven OSINT system identified 92% of phishing emails with a false positive rate of 4%.[11] Real-time domain monitoring detected new phishing websites within minutes of their activation. The financial institution was able to alert customers and block phishing domains proactively, reducing the impact of the attack.

Impact: Compared to traditional forensic methods, the AI-driven OSINT approach reduced detection time by 70% and minimized customer losses. Table 1 shows the comparison between detection of phishing campaigns through AI-Driven OSINT and traditional methods across key performance metrics.

4.2 Case study 2: dark web monitoring for data breach detection

Situation: A cybersecurity firm was hired to determine the existence of a data breach into a retail business, where dark web sources stated that customer records were being sold.

4.2.1 Methodology

OSINT data gathering: Crawlers and scrapers were used to gather relevant data on dark web marketplaces and forums. Keyword usage included its name, records of customers, and financials of the business.

AI Infusion: Advanced AI-powered pattern recognition tools were instrumental in uncovering a potential data breach linked to the retail company. These algorithms scanned vast amounts of online data and were able to identify and connect leaked datasets back to the organization, even when the data was shared anonymously or in fragmented forms.

In addition, AI-driven image recognition technology played a key role by analyzing visuals shared across dark web forums. It successfully detected screenshots that appeared to show the company's internal systems—an alarming sign that unauthorized access may have occurred.

At the same time, sentiment analysis tools monitored online discussions across forums and underground networks. These tools picked up on conversations that showed a sudden spike in concern or interest around the company's name, particularly posts that included language suggesting a recent data compromise. This flagged the incident early, allowing investigators to take a

Table 1: Comparision between detection of phishing campaigns through AI-Driven OSINT and traditional methods across key performance metrics

Metric	AI-Driven OSINT (this case study)	Traditional methods
Detection accuracy	~ 92%	~ 75% (manual/forensic level)
False positives rate	~ 4%	Higher (manual errors, heuristics)
Detection latency	Real-time / minutes	Hours to days
Coverage / proactivity	High (automated detection across OSINT)	Mostly reactive
Cost efficiency	Moderate initial setup, long-term savings	High recurring costs
Customer impact	Minimally disruptive, early alerts	Chance of higher losses

closer look before the issue could escalate further.
Results: AI-driven OSINT identified the breached dataset two weeks before it was publicly reported. The retail company was able to notify affected customers and secure vulnerable systems before further exploitation. This forensic evidence, obtained through dark web monitoring, was also used to identify attackers and aid the law enforcement agencies.
Impact: The proactive approach had prevented enormous financial losses as well as reputational damage. Traditional approaches, where detection would be possible only weeks after the incident, would have been too late.

4.3 Case study 3: monitoring social media for coordinated cyberattacks

Case Study: Law enforcement agencies were tasked with investigating a series of Distributed Denial of Service (DDoS) attacks on critical infrastructure, suspected to be coordinated via social media.

4.3.1 Methodology

OSINT data collection: Monitoring of social media platforms, forums, and messaging groups for keywords and hashtags related to the attacks.
Real-time feeds were analyzed to detect discussions or posts indicating planned activities.
AI integration: NLP models scanned text for coordination indicators, including date, time, and target infrastructure. Sentiment analysis detected posts with hostile intent. Network analysis mapped connections between users discussing the attacks.
Results: The AI-driven OSINT system identified a cluster of accounts coordinating the DDoS attacks. Law enforcement disrupted the planned attacks by apprehending key individuals and taking down their communication channels. Forensic evidence collected from social media was admissible in court and aided prosecution.
Impact: Compared to the traditional investigation processes, the system developed by AI for OSINT quickened response time by 60% and prevented further damage to critical infrastructure.

4.3.2 Performance evaluation

The results from these case studies and simulations were evaluated based on key performance metrics as shown in Table 2.

5. Key findings

1. Improved threat detection: OSINT systems based on AI have proven to be comparatively efficient viz-a-viz traditional mechanisms in their threat intelligence usage. Also, early warning enabled organizations to avert an unprecedented misfortune as long before it occurred.
2. Enhanced proactivity: Using real-time analytics and predictive models, proactive responses were sparked from the paradigm of investigation switch from reactive to that of prevention.
3. Efficiency in resource allocation: Automating data gathering and analysis has minimized investigators' burdens and left them free for more important matters.
4. Challenges addressed: The tools of AI OSINT have raised that challenge in managing the mountains of data, especially with hidden pattern recognition on unstructured information.

6. Limitations

Despite their advantages, AI-driven OSINT tools face challenges:

- False Positives: While improved, some cases exhibited false positives that required manual verification.
- Ethical Concerns: Real-time monitoring of public platforms raised privacy concerns, necessitating compliance with legal frameworks.
- Complex Implementation: Initial deployment of AI systems required significant expertise and resources.

7. Discussion

The entry of AI and OSINT into the arena of digital forensics signifies one of the paradigmatic changes in the investigation of cybercrime. The implications that are borne by studying their case studies and findings spell out the transformational power of such technologies for purposes of understanding the challenges they would need to undergo. This section presents larger inferences drawn from AI-based OSINT applications including discussion regarding the applications' merits and disadvantages, ethical considerations, and probable future directions.
5.

Table 2: Comparison between AI-Driven OSINT and traditional intelligence gathering methods across key performance metrics

Metric	AI-Driven OSINT	Traditional methods
Detection Accuracy	92%	75%
Response Time	Reduced by 60-70%	Longer due to manual analysis
Proactivity	High	Low (mostly reactive)
Data Handling	Scalable	Limited by manual capacity
Cost-Effectiveness	Moderate initial cost, long-term savings	High recurring costs

7.1 Strengths of AI-driven OSINT in digital forensics

Advanced pro-activity: A very significant feature of the AI-based OSINT is that it changes the paradigm of criminal investigations into an already reactive position to one which is proactive. AI will assist with not only real-time monitoring, prediction analytics, and threat detection on the current intelligence being analyzed but will also have a predictive capability to foresee possible attacks so that actions can be taken to prevent them.

Scalability and efficiency: The conventional premise of digital forensics faces interesting challenges owing to the vast data production of this digital age. Artificial Intelligence in OSINT would remove this artificially imposed barrier by automating data collection and analysis so that scaling up becomes possible alongside minimal manual effort. This has enabled greater deployment of resources by investigators for higher-priority tasks which might include prosecuting cybercriminals or securing vulnerable systems.

Enhanced accuracy and insights: The AI-OSINT based on machine learning and natural language processing can highlight patterns and connection that human analytical minds might never identify. More importantly, enhanced accuracy in a threat's existence is ensured so that the available information is actionable; hence, insights are generated about decision-making.

Broad applicability: It also provides the tools to be deployed on many different kinds of domains including corporate cybersecurity, law enforcement, and national defense, as its versatility allows for it to observe any source through social media, forums, or dark web networks in real-time for monitoring a plethora of cyber threats.

7.2 Limitations and challenges

False positives and bias: Although AI-driven systems are highly accurate, they cannot be completely right. False positives are still present, as with the phishing detection case study when a small portion of benign e-mails were caught incorrectly. This is also where there is a presence of biasing in the data used for the training of an AI model to produce skewed outcomes.

Ethical and privacy issues: It raises additional questions regarding privacy and surveillance when it comes to acquiring and processing publicly available information. AI OSINT tools for collection must comply with data protection legislation, such as the GDPR and CCPA, to avoid violation of individual rights. Much care should be taken to balance both possible effectiveness in cybercrime prevention and ethical responsibility. Their use requires many different technical skills and resources, as well as an infrastructure. The smaller organizations or law enforcement agencies that do not have budget allocations for AI-powered OSINT tools will find it almost impossible to adopt.

Evasion techniques by cyber criminals: As the use of AI increases, so the chances are that cybercriminals will construct their strategies to evade detection, be it by enciphered channels or by creating dummy data. Such a zero-sum game requires perpetual advancement in the efficacy of AI and also OSINT technologies.

7.3 Ethical and legal issues

Transparency and accountability: To be held accountable, AI must provide transparency in its decision-making. Therefore, an investigator must explain and justify how AI-dependent tools achieve their conclusions, particularly in a court of law.

Cross-border data challenges: The cybercrime investigation frequently involves data held in several jurisdictions where different legal frameworks apply. As a result, an international regulation harmonization is required for smooth collaboration and data-sharing.

Fairness and non-discrimination: From a moral and legal point of view, it is imperative that AI models refrain from targeting specific individuals or groups disproportionately. This can also be achieved through constant auditing and refining of algorithms.

7.4 Future directions

Advancing AI technologies: Future research should work towards powerful AI models that can deal with all sorts of data, produce less false positives, and adapt to dynamic attacks over time.

Ethical AI development: By integrating morals into the design and use of such tools, the public will be assured of trust in the delivery mechanism and the lawyers declared as it goes along.

Collaboration and knowledge sharing: Collaboration among governments, private organizations, and academia will encourage innovation and contribute to improving the efficiency of AI driven OSINT. Sharing knowledge of what threats terminate, as well as best practices, will benefit the larger community of cyber security.

8. Conclusion

The shift toward including Artificial Intelligence (AI) and Open-Source Intelligence (OSINT) in digital forensics and cybercrime investigations is critical. This article would address and describe how AI-enabled OSINT can assist the investigation of cybercrime into a new proactive one. Automated collection and analysis of data and patterns from large data sets combined with the unintendedly on-the-ground help of actionable intelligence may facilitate the investigation of cybercrime with greater efficiency and effectiveness. The case studies discussed above exemplify the use of such tools in faster and more effective identification of phishing campaigns, dark web activities, and coordinated cyberattacks than the

traditional methods. Since the shift is from a reactive model to a more proactive one, organizations and law enforcement agencies can act to neutralize threats before they gather more impetus, thereby inflicting further damage to finances, business reputation, and society in general. AI-driven OSINT is rich in benefits, but adoption challenges are not to be put aside. The ethical issues, including data privacy and the potential misuse of surveillance technologies, require strict adherence to regulatory frameworks like GDPR and CCPA. Technical issues include algorithmic bias and resource intensiveness. Finally, since cybercriminals, too, will evolve to avoid their detection, the cybersecurity professional community shall continue to innovate and work together. To realize the full benefits of AI-enabled OSINT in the future, AI algorithms will have to be matured, ethical AI developments put in place, and partnerships formed across sectors. Governments, private organizations, and academic institutions should work together to formulate standard practices, share threat intelligence, and advocate for responsible usage. AI systems, in particular, will need to show transparency and accountability in order to gain public trust and acceptance for use in law. AI-enabled OSINT is revolution forensics never witnessed in the past. It enables investigators to be far wiser in the increasingly intricate and dynamic cyber threat landscape. Challenges are reality yet, they are far too few to weigh against opportunities in deploying AI for protecting individuals, organizations, and critical infrastructures against a heavily growing menace of cybercrime. Ethical innovation and overcoming implementation barriers to this must make it an indispensable pillar of any modern-day cybersecurity effort.

Funding Declaration
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data Availability Statement
The datasets and supporting analytical results generated and/or analyzed during this study are available from the corresponding author upon reasonable request.

Conflict of Interest
There is no conflict of interest.

Artificial Intelligence (AI) Use Disclosure
The authors declare that artificial intelligence (AI)-assisted tools were used only for language refinement, grammar improvement, and manuscript structuring purposes during the preparation of this work. All technical content, analysis, and interpretations were independently developed and verified by the authors.

Supporting Information
Not applicable.

References

[1] E. Casey, Digital evidence and computer crime: forensic science, computers, and the internet, 3rd edition, Academic press, 2011.
[2] N. L. Beebe, J. G. Clark, A hierarchical, objectives-based framework for the digital investigations process, *Digital Investigation*, 2014, **2**, 147–167, doi: 10.1016/j.diin.2004.12.001
[3] I. Clarke, A. Papadopoulos, Leveraging OSINT for cyber threat intelligence: A review of current practices, *Cybersecurity Review Quarterly*, 2015, **4**, 30–42.
[4] B. Akhgar, B. Brewster, F. Sampson, Open source intelligence investigation: from strategy to implementation, Springer, 2017, doi: 10.1007/978-3-319-47617-9.
[5] R. Jain, S. Natarajan, S. Krishnamurthy, Machine learning applications in cybersecurity: Enhancing digital forensics, *IEEE Transactions on Security*, 2018, **15**, 678–690, doi: 10.1109/TSEC.2018.284717.
[6] S. Zawoad, R. Hasan, Towards building proofs of past data possession in cloud forensics, *Digital Investigation*, 2015, 11, 204–212, doi: 10.1016/j.diin.2014.12.006.
[7] R. Sharma, P. Mehta, Applications of artificial intelligence in OSINT for proactive cybersecurity, *International Journal of Cybersecurity Research*, 2020, **9**, 98–110.
[8] H. Van der Walt, J. Eloff, AI-driven open-source intelligence in modern threat intelligence frameworks, *Cyber Forensics Review*, 2019, **6**, 33–49.
[9] S. Chakraborty, S. Datta, A. Subbiah, Ethical challenges of AI in cybersecurity: a critical review, *Journal of Cyber Ethics*, 2021, **7**, 45–59.
[10] C. Kuner, F. H. Cate, C. Millard, D. J. Svantesson, Data protection and privacy issues in cross-border data flow, *International Data Privacy Law*, 2016, **6**, 123–140, doi: 10.1093/idpl/ipw013.
[11] P. An, R. Shafi, T. Mughogho, O. A. Onyango, Multilingual email phishing attacks detection using OSINT and machine learning, Preprint, Cryptography and Security, arXiv:2501.08723, January 15, 2025.

Publisher Note: The views, statements, and data in all publications solely belong to the authors and contributors. GR Scholastic is not responsible for any injury resulting from the ideas, methods, or products mentioned. GR Scholastic remains neutral regarding

jurisdictional claims in published maps and institutional affiliations.