AG Publishing House

Investigative Frontiers Integration of Science Transforming Criminal Investigation

Year: 2026

Mining for Clues: Big Data Analytics and the Transformation of Criminal Intelligence

Ms. Harsh Paliwal[1]

[1]*Assistant Professor Department of Computer Science Govt. Holkar Science College, Indore, Madhya Pradesh*

Abstract

Big data analytics is a game-changing technology in criminal intelligence as it helps law enforcement agencies to derive actionable insights from big and diverse data sets. This review highlights how integration of information from police records, surveillance systems, mobile devices, social media, financial transactions, geospatial databases, and open source intelligence are being used to improve criminal investigations using big data analytics. It provides an overview of essential analytical methods such as data mining, machine learning, text mining, link analysis, social network analysis and how they can be used in crime pattern analysis, predictive policing, organized crime detection and cybercrime investigations. The review also sheds light on the technical, ethical and legal issues related to data quality, privacy, algorithmic bias, governance, etc. with specific focus on the Indian context. Finally, it examines future trends like the use of artificial intelligence, real-time intelligence platforms, the cloud and edge computing, explainable AI, and cross-agency data sharing, which will influence intelligence-led policing in the future.

Keywords; Big Data Analytics; Criminal Intelligence; Predictive Policing; Artificial Intelligence; Intelligence-Led Policing

[1] ISBN No. - 978-93-7640-081-2

1 Introduction

Mining for Clues is a process that involves deriving meaningful patterns, relationships and actionable intelligence from large amounts of digital data for the purpose of supporting criminal investigations. Just like prospecting for precious metals in massive rock heaps, large data analysis helps investigators restore hidden evidence from various sources, including surveillance systems, social media, mobile devices, financial records and public documents. This data-driven approach has greatly improved law enforcement's capacity to detect criminal activities and identified organized crime networks and helped with intelligence-led policing.

Big Data are very large, complex datasets that are too difficult to deal with using traditional data management methods. Big Data Analytics relies on advanced computing techniques such as data mining, machine learning, and statistical analysis to gather, analyze and interpret this data to produce insights that can be applied to specific actions. In criminal justice, the analytical processes allow investigators to convert large amounts of disparate data into valuable intelligence and information that can be used for crime prevention, investigation, and strategic decision making.[2]

The term criminal intelligence has moved beyond the traditional investigative approach that relies largely on witness accounts, physical evidence and manual examination of records to technology-based intelligence systems. Along with the explosion of digital communication, internet services, surveillance technologies, cloud computing and connected devices, there has been an unparalleled amount of crime-related data generated. Thus, modern law enforcement agencies have increasingly turned to big data analytics to combine information from various sources to help them detect and report crimes more efficiently and to help them gather information to support their intelligence operations.[3]

The 5 Vs of big data analytics for criminal investigations include Volume (the vast amount of crime-related data, Velocity (the speed at which data is created and analyzed), Variety (incorporation of structured data and unstructured data from various sources), Veracity (the

[2] Y. Delgado, B. S. Price, P. J. Speaker, and S. L. Stoiloff, "Forensic intelligence: Data analytics as the bridge between forensic science and investigation," Forensic Sci. Int. Synerg., vol. 3, p. 100162, 2021, doi: https://doi.org/10.1016/j.fsisyn.2021.100162.

[3] T. Sholahudin, A. H. Yulianto, and Hartanto, "Transformation of Crime Combat in the Digital Era: From Conventional Criminal Law To Data-Based Predictive Systems," J. Indones. Law Policy Rev., vol. 7, no. 3, pp. 540–546, 2026, doi: https://doi.org/10.56371/jirpl.v7i3.708.

reliability and accuracy of the data), and Value (the ability to generate actionable intelligence to support timely and evidence-based investigative decisions).

2 Sources of Big Data and Analytical Techniques in Criminal Intelligence

Big data analytics can be effective for criminal intelligence only if a wide range of digital information is available, along with the necessary sophisticated analytical methods to derive value from it. Law enforcement authorities gather data from various, disparate sources that can yield a wealth of information for crime solving, criminal profiling and intelligence gathering. These datasets vary in format, size and complexity; thus, analytical methods are used to uncover underlying patterns, relationships, and trends that further informed investigative decisions.[4]

A. Major Data Sources

Information from many electronic and traditional sources are used in criminal intelligence. The most critical sources are:

1. **Police records:** Crime reports, arrest records, criminal histories, incident logs, and forensic databases.
2. **CCTV surveillance:** Video footage used for suspect identification, facial recognition, vehicle tracking, and event reconstruction.
3. **Mobile devices:** Call detail records, GPS locations, messages, application data, and digital evidence extracted from smartphones.
4. **Social media:** Public posts, images, videos, user interactions, and online communications useful for behavioural and threat analysis.
5. **Internet of Things (IoT):** Data generated from smart cameras, sensors, wearable devices, connected vehicles, and smart city infrastructure.
6. **Financial transactions:** Banking records, credit card transactions, cryptocurrency transfers, and suspicious financial activities related to fraud or money laundering.
7. **Open Source Intelligence (OSINT):** Publicly available information collected from websites, news portals, government records, blogs, and online forums.
8. **Geospatial data:** Geographic Information Systems (GIS), GPS coordinates, satellite imagery, and crime mapping data for hotspot analysis.

[4] A. S. M. Noor, S. S. Sanusi, and N. H. A. Rahim, "A Survey of Big Data and Data Mining Techniques for Crime Prevention," Compusoft, an Int. J. Adv. Comput. Technol., vol. 9, no. 11, 2020.

B. Structured and Unstructured Criminal Data

Both structured and unstructured data are used for criminal intelligence. Structured data are organized information stored in a pre-defined format that allows for efficient query and statistical analysis, like police records, criminal data, and transaction logs. Unstructured data are on the other hand, surveillance video, photos, e-mails, audio recordings, social media posts, and text documents that would need advanced technology, including natural language processing or computer vision, to glean useful intelligence. Combining both types of data offers a more holistic view of criminal activities.[5]

C. Core Analytical Methods

The principal analytical techniques used in criminal intelligence include:

1. **Data mining:** Discovers hidden patterns, associations, and anomalies from large crime datasets.
2. **Machine learning:** Predicts crime trends, classifies criminal behaviour, and improves investigative decision-making through adaptive algorithms.
3. **Text mining:** Extracts relevant information from reports, online communications, and social media content.
4. **Link analysis:** Identifies relationships among suspects, organizations, locations, and criminal events.
5. **Social network analysis:** Examines criminal networks by evaluating interactions and identifying influential individuals within organized groups.
6. **Visualization dashboards:** Present complex analytical results through interactive maps, graphs, and charts, enabling investigators to interpret crime patterns efficiently.

D. Role of Data Integration in Criminal Intelligence

Data integration is the process of joining data from a variety of data sources that are structurally different. Integrating these datasets with each other—such as police data and financial records, mobile data, geospatial data, and OSINT data—can help investigators make connections that may not be apparent from any individual data source. Integrated data provide a more complete

[5] D. Buil-gil, "The Structure of Unstructured Time and Crime: A Spare Time Model," Br. J. Criminol., vol. 66, pp. 1–22, 2026, doi: https://doi.org/10.1093/bjc/azaf035.

picture, better intelligence sharing between agencies, less investigative time, and better evidence-based decision-making for criminal prevention and investigations.[6]

3 Applications of Big Data Analytics in Criminal Intelligence

Big data analytics has revolutionized criminal intelligence, giving law enforcement agencies access to large and diverse sets of data to help them make informed and timely decisions. Analytical tools combine data from various digital sources, surveillance systems, financial transactions, and public records, uncovering their patterns, predicting crime, and maximizing investigation efforts. These have enhanced the role of criminal intelligence beyond reactive investigation to proactive crime prevention and strategic policing.[7]

1. **Crime Pattern and Hotspot Analysis:** The crime pattern analysis identifies the trends in crime history, spatial information and temporal information to find the hot spots and patterns of crime. Geographic Information Systems (GIS) and spatial analytics help investigators identify crime hotspots, identify seasonal or temporal trends and patterns, and assign police resources more efficiently. These analyses help guide targeted policing and prevention efforts in the community in areas at high risk for crime.
2. **Predictive Policing and Crime Forecasting:** Predictive policing is a technique that uses machine learning and statistical analysis of crime data to forecast the probability of crime occurring in the future. Predictive models examine factors like crime type, location, time, and offender activity to help police predict where and when crime is likely to occur, and allocate resources accordingly. These systems do increase operational efficiency, but they don't take the place of human judgment in making predictions.
3. **Criminal Network and Organized Crime Detection:** Big data analytics helps identify criminal organizations by examining the communications records, financial transactions, social media interactions, and data from mobile devices. Link analysis and social network analysis can be used to expose relationships between suspects, to determine the role of particular individuals within criminal networks, and to expose hidden criminal structures. These techniques are especially useful in studying organized crime, drug trafficking, transnational criminal networks and human trafficking.

---

[6] F. Ekundayo, "Big data and machine learning in digital forensics: Predictive technology for proactive crime prevention," World J. Adv. Res. Rev., vol. 24, no. 02, pp. 2692–2709, 2024, doi: https://doi.org/10.30574/wjarr.2024.24.2.3659.

[7] A. Jamarani, S. Haddadi, R. Sarvizadeh, M. Haghi Kashani, M. Akbari, and S. Moradi, Big data and predictive analytics: A systematic review of applications, vol. 57, no. 176. Springer Netherlands, 2024. doi: 10.1007/s10462-024-10811-5.

4. **Financial Fraud, Cybercrime, and Terrorism Intelligence:** The financial sector and law enforcement utilize big data analytics to identify fraudulent transactions, money laundering, identity theft, cyberattacks and terrorist financing. By analyzing banking transactions, cryptocurrency transfers, network traffic, and digital communications in real-time, suspicious activities can be quickly identified, providing a timely opportunity for investigations and minimizing financial and national security threats.
5. **Decision Support for Investigators and Law Enforcement Agencies:** Big data analytics can improve the decision making process by connecting data from various sources into dashboards and intelligence platforms for interaction. These systems enable investigators to have full situational awareness, prioritize investigative leads, help evidence correlate and enhance inter-agency information sharing. This therefore facilitates quicker investigations, optimisation of resources, and better operational and strategic decision-making.[8]

4 Challenges, Ethical Issues, and Legal Considerations

By leveraging big data analysis in criminal intelligence, law enforcement agencies have become more efficient, able to process vast amounts of information and data. But there are also crucial technical, ethical and legal challenges to implementing it. As AI, digital surveillance, and criminal databases are increasingly adopted across India, it is essential to strike a balance that ensures the safety of the public without compromising their rights. It is crucial for big data-driven intelligence systems to be both reliable and legally compliant, while at the same time remaining transparent.[9]

A. Challenges

The challenge of criminal intelligence is that it involves maintaining quality and consistency of data from various sources. Data from police files, CCTV, mobile devices, financial records and social media are not always available in the same format, complete, or accurate. Analytical results may not be reliable if there are missing, duplicated, or outdated records, and may result in the incorrect intelligence. In addition, the inability to provide information sharing and coordinated investigations efficiently due to lack of interoperability between different databases

[8] M. Thompson, "Big Data and its Application in Predictive Policing and Crime Prevention," Am. J. Big Data, vol. 03, no. 04, pp. 11–15, 2022, doi: 10.71465/ajbd722.

[9] C. Kerdvibulvech, "Big data and AI-driven evidence analysis: a global perspective on citation trends, accessibility, and future research in legal applications," J. Big Data, vol. 11, no. 180, 2024, doi: https://doi.org/10.1186/s40537-024-01046-w.

across law enforcement agencies and states. Standardized data formats and development of technologies are therefore key to successful data integration and analysis.[10]

B. Ethical Issues

The vast amount of personal data collected and processed is a key issue of ethics and morality, with particular attention to privacy, surveillance, and equity. The use of technologies like facial recognition, location tracking, and social media monitoring can lead to constant monitoring of people, which raises concerns about the potential for over-surveillance and misuse of personal information. Furthermore, AI analytical tools can generate skewed results when faced with incomplete or skewed data sets, leading to discriminatory policing and unfair profiling. Thus, criminal intelligence systems need to be designed in a transparent, explainable, regularly tested against algorithms, and supervised by humans to maintain the objectivity, accountability and ethics of analytical decisions.[11]

C. Legal Considerations

The growing legal and regulatory landscape in India for digital evidence and personal data must be taken into account when implementing big data analytics in criminal investigations. The information collected, processed, stored and shared by investigative agencies must comply with the provisions of the applicable data protection laws and the provisions of criminal procedure. To ensure admissibility and reliability of digital evidence, there is a need for effective data governance that includes secure data storage, controlled access, audit trail, data integrity, and inter-agency accountability. The legal infrastructure has to be robust enough to allow the use of big data analytics in a lawful manner, and to protect the public's trust that with the use of technology, investigation of crimes can be conducted without infringing on the rights and principles of human beings.[12]

5 Emerging Trends and Future Directions

Digital technologies are rapidly evolving and continually changing the nature of criminal intelligence. Advances in artificial intelligence (AI), cloud computing, and real-time data

[10] A. T. T. Wong, "Opportunities and Challenges of Big Data Analytics in Crime Investigation," Int. Ann. Criminol., vol. 62, no. 3–4, pp. 570–584, 2024, doi: DOI: 10.1017/cri.2025.3.

[11] S. Holloway, "Investigating the Ethical Implications of Big Data Analytics in Information Systems Management," Preprint, pp. 0–14, 2025, doi: 10.20944/preprints202501 .0293.v1.

[12] P. Singh, "Artificial intelligence, the cogency of current legal framework and legal challenges," Int. J. Adv. Acad. Stud., vol. 6, no. 8, pp. 44–48, 2024, doi: https://doi.org/10.33545/27068919.2024.v6.i8a.1249.

processing are now helping law enforcement agencies to more readily recognize, analyse, and respond to criminal activity. The challenges of the future will witness further advancements by the further integration, intelligence and collaboration of criminal intelligence systems, which will support evidence-based decision making, enhance the effectiveness of operations and public safety.[13]

1. **Integration of Artificial Intelligence with Big Data Analytics:** AI is increasingly being used along with big data analytics to automate the analysis of large and complex criminal data sets. Machine learning, deep learning and computer vision algorithms can detect crime patterns, classify criminal activities, identify faces and objects in surveillance footage and flag anomalies that might be suspicious behaviour. AI-powered tools, along with the use of big data, help create more accurate and timely intelligence, which helps in anticipating criminal actions and making decisions during investigations.
2. **Real-Time Intelligence Systems:** Criminal Intelligence is becoming real-time, and information from CCTV networks, mobile devices, emergency response and social media can be processed in real time. Real-time intelligence systems can be used to track and manage live incidents, quickly detect new threats, and provide instant operational action coordination to law enforcement agencies. This capability helps to increase situational awareness and increases the efficiency of investigations where time matters.
3. **Cloud Computing and Edge Analytics:** Cloud computing offers scalable infrastructure to store, process and share vast amounts of criminal information amongst various agencies. Edge analytics complements this by analyzing data at or close to the source, like from surveillance cameras or IoT devices, which eliminates latency issues and helps with quicker threat detection. Cloud and edge computing together creates more efficient computing, and ensures secure and timely criminal intelligence.[14]
4. **Explainable AI (XAI) for Criminal Intelligence:** With the growing role of AI in crime investigation, Explainable Artificial Intelligence (XAI) is turning into a crucial research area. XAI is designed to ensure that AI predictions and recommendations are easily understood and transparent, enabling investigators to understand the analytical output and the logic

[13] J. Marin, G. Guerreros, and D. Calderon-vilca, "Using Big Data Analytics to Identify Trends and Group Crimes through Clustering," Int. J. Comput., vol. 23, no. 2, 2024, doi: 10.47839/ijc.23.3.3658.

[14] T. A. Hakami, Y. M. Alginahi, and O. Sabri, "Exploring the Evolution of Big Data Technologies: A Systematic Literature Review of Trends, Challenges, and Future Directions," Futur. Internet, vol. 17, no. 427, pp. 1–29, 2025, doi: https://doi.org/10.3390/fi17090427.

behind automated decisions. Fostering explainability fosters trust, accountability, and legally defensible intelligence practices, while boosting investigations using AI.

5. **Cross-Agency Data Sharing and Smart Policing Initiatives:** Police departments, forensic labs, financial institutions, and cybersecurity firms will all need to have the ability to share information securely to provide criminal intelligence in the future. The ability to access and use shared intelligence in real time through integrated information platforms and smart policing efforts allows for coordinated investigations to be performed by authorized agencies. These partnerships help ensure that crime is detected more quickly, that there is better inter-agency working and that more effective action is taken on more demanding and transnational crime situations.

6 Conclusion

Big data analytics has revolutionized the field of criminal intelligence by providing an effective way to collect, integrate and analyse huge amounts of unstructured, complex data from various digital sources. The use of advanced analytical tools such as machine learning, data mining, network analysis and others has enhanced the identification of crime patterns, predictive policing, organised crime investigations, and the use of intelligence in decision making. With the increasing use of data-driven technologies, however, comes challenges around data quality, interoperability, privacy, algorithmic bias and legal compliance – especially in India's evolving digital governance framework. Fostering public trust and responsible technology use requires tackling these challenges through strong data governance, clear analytical models, and suitable regulatory protections. In the future, the use of AI, real-time analytics, cloud and edge computing, explainable AI, and collaborative data-sharing platforms will further improve the effectiveness of criminal intelligence. These changes will facilitate more proactive, accurate and evidence-based policing and efficient and accountable criminal justice systems.

7 Reference

[1] Y. Delgado, B. S. Price, P. J. Speaker, and S. L. Stoiloff, “Forensic intelligence: Data analytics as the bridge between forensic science and investigation,” Forensic Sci. Int. Synerg., vol. 3, p. 100162, 2021, doi: https://doi.org/10.1016/j.fsisyn.2021.100162.

[2] T. Sholahudin, A. H. Yulianto, and Hartanto, “Transformation of Crime Combat in the Digital Era: From Conventional Criminal Law To Data-Based Predictive Systems,” J. Indones. Law Policy Rev., vol. 7, no. 3, pp. 540–546, 2026, doi: https://doi.org/10.56371/jirpl.v7i3.708.

[3] S. M. Noor, S. S. Sanusi, and N. H. A. Rahim, “A Survey of Big Data and Data Mining Techniques for Crime Prevention,” Compusoft, an Int. J. Adv. Comput. Technol., vol. 9, no. 11, 2020.

[4] Buil-gil, “The Structure of Unstructured Time and Crime: A Spare Time Model,” Br. J. Criminol., vol. 66, pp. 1–22, 2026, doi: https://doi.org/10.1093/bjc/azaf035.

[5] Ekundayo, “Big data and machine learning in digital forensics: Predictive technology for proactive crime prevention,” World J. Adv. Res. Rev., vol. 24, no. 02, pp. 2692–2709, 2024, doi: https://doi.org/10.30574/wjarr.2024.24.2.3659.

[6] Jamarani, S. Haddadi, R. Sarvizadeh, M. Haghi Kashani, M. Akbari, and S. Moradi, Big data and predictive analytics: A systematic review of applications, vol. 57, no. 176. Springer Netherlands, 2024. doi: 10.1007/s10462-024-10811-5.

[7] M. Thompson, “Big Data and its Application in Predictive Policing and Crime Prevention,” Am. J. Big Data, vol. 03, no. 04, pp. 11–15, 2022, doi: 10.71465/ajbd722.

[8] Kerdvibulvech, “Big data and AI-driven evidence analysis: a global perspective on citation trends, accessibility, and future research in legal applications,” J. Big Data, vol. 11, no. 180, 2024, doi: https://doi.org/10.1186/s40537-024-01046-w.

[9] T. T. Wong, “Opportunities and Challenges of Big Data Analytics in Crime Investigation,” Int. Ann. Criminol., vol. 62, no. 3–4, pp. 570–584, 2024, doi: DOI: 10.1017/cri.2025.3.

[10] S. Holloway, “Investigating the Ethical Implications of Big Data Analytics in Information Systems Management,” Preprint, pp. 0–14, 2025, doi: 10.20944/preprints202501 .0293.v1.

[11] P. Singh, “Artificial intelligence, the cogency of current legal framework and legal challenges,” Int. J. Adv. Acad. Stud., vol. 6, no. 8, pp. 44–48, 2024, doi: https://doi.org/10.33545/27068919.2024.v6.i8a.1249.

[12] J. Marin, G. Guerreros, and D. Calderon-vilca, “Using Big Data Analytics to Identify Trends and Group Crimes through Clustering,” Int. J. Comput., vol. 23, no. 2, 2024, doi: 10.47839/ijc.23.3.3658.

[13] T. A. Hakami, Y. M. Alginahi, and O. Sabri, “Exploring the Evolution of Big Data Technologies: A Systematic Literature Review of Trends, Challenges, and Future Directions,” Futur. Internet, vol. 17, no. 427, pp. 1–29, 2025, doi: https://doi.org/10.3390/fi17090427.