

Big data and cloud computing in crime analysis

Group 5



November 24, 2023

w22058786

Christy Joseph

Word count: 1947

**Introduction**

In recent years, scholarly endeavors have delved into the intricate connections between law enforcement practices, data collection, and the transformative impact of big data technologies across various domains. Barnett-Ryan (2019) investigates how disparities among law enforcement agencies influence discretionary decisions to record crime data, drawing insights from national UCR Program data and incident data from agencies in the mid-South.

Big data analytics (BDA), characterized by its systematic approach to analyzing large volumes of data, takes center stage in the study by Feng et al. (2019). They apply BDA to criminal data, employing exploratory data analysis to visualize patterns and predict trends, showcasing the potential of advanced analytics in crime analysis.

As the landscape of software engineering undergoes significant shifts propelled by big data systems, Gurcan & Cagiltay ( 2019) aim to identify and map the competencies required for big data software engineering. Their work addresses the evolving knowledge domains and skill sets crucial for adapting educational programs to meet industrial needs and stay abreast of the latest trends.

The intersection of technology and crime analysis is further explored by Frith (2019), who utilizes latent class modeling to examine the offense location choices of serious acquisitive crime offenders. This approach, introduced in 2003, has gained popularity and has been employed in over 25 studies, demonstrating its relevance in understanding criminal behavior.

In the contemporary world, the convergence of big data analytics and cloud computing is a transformative force, reshaping approaches to complex challenges. This exploration delves into their intricate relationship, specifically within the realm of crime analysis and big data, with a focus on UK street crime data.

**Big Data Analytics and Cloud Computing Collaboration in criminal analysis**

Managing extensive datasets requires intensive computing and substantial resource allocation. The Europe–Brazil Collaboration of Big Data Scientific Research Through Cloud-Centric Applications (EUBra-BIGSEA) provides a comprehensive solution (Alic et al., 2019). This collaborative effort demonstrates how combining big data and cloud computing addresses challenges in scientific research applications.

Xu et al. (2020) showcase cloud computing's agility in responding to dynamic requirements in criminal behavior analysis. Their study utilizes robust data collection and cloud-based rapid response capabilities to explore criminal behavior characteristics, highlighting the potential of cloud computing in advancing crime analysis.

Cloud Data Mining and Privacy

Barua et al. (2021) introduce the concept of cloud data mining, shifting data mining and analytics using cloud resources. Zhang et al. (2023) navigate the intricate terrain of personal information security within the context of cloud computing, emphasizing the nuanced dimensions of privacy and improving criminal responsibility regarding citizens' information security.

Big Data Analytics Across Domains

Big data analytics (BDA) has been effectively applied in various domains, including crime data analysis. Feng et al. (2019) demonstrated the application of BDA to criminal data, conducting exploratory data analysis for visualization and trend prediction. Their work involved the use of state-of-the-art data mining and deep learning techniques, and they discovered interesting facts and patterns from criminal data in San Francisco, Chicago, and Philadelphia.

Similarly, Manengadan et al. (2021) utilized big data analytics and visualization techniques in the analysis of crime data across different parts of India. They applied BDA to criminal data for visualization and trend prediction, using the LSTM model for analysis.

These two studies exemplify the versatility of BDA in handling diverse datasets and its potential in providing valuable insights for various sectors. For instance, in the field of Intelligent Transportation Systems (ITS), BDA can be used to analyze data from various sources, apply different analytics approaches, and categorize applications. Similarly, in the power grid sector, BDA can help address challenges associated with integrating big data and microgrids.

In the manufacturing sector, BDA can be used to analyze non-linear time series data, as demonstrated by the use of the Prophet model algorithm. It can also help identify future directions in shaping manufacturing processes. In the realm of illegitimate information analysis, BDA can be used for preliminary data analysis and trend prediction.

**Cloud Computing for Crime Analysis**

The research conducted by Talukder et al. (2022) holds significance as it introduces a hybrid model that combines machine learning and deep learning to improve crime detection rates. This methodology is particularly pertinent in the realm of crime prediction, where conventional approaches may prove inadequate. The analysis of crime data in particular geographic regions is significantly enhanced by the pivotal involvement of machine learning algorithms. These algorithms are crucial for recognizing patterns and predicting upcoming trends in criminal activities. Furthermore, they offer valuable insights into the complexities of crime patterns, optimizing resource allocation, and devising efficient tactics to counter criminal activities.

In a distinct domain, Garg et al. (2020) delve into the security challenges inherent in cloud computing environments. As the use of cloud computing continues to grow, it has become a major focal point for potential cyber threats. The research emphasizes the essential requirement to create and enhance security methods to protect data and systems within the cloud. Security threats such as misconfiguration, unauthorized access, insecure interfaces, and account hijacking are highlighted as top concerns in cloud computing. Consequently, it is imperative for businesses to adopt a security-first mindset, ensuring consistent oversight and meticulous attention to detail in their strategies for cloud security.

Visualization Techniques in Crime Analytics

Feng et al. (2019) applied big data analytics (BDA) to criminal data, conducting exploratory data analysis for visualization and trend prediction. This study demonstrated the potential of BDA in identifying patterns, relations, and trends within a large volume of crime data. The researchers used state-of-the-art data mining and deep learning techniques to analyze criminal data from San Francisco, Chicago, and Philadelphia. The predictive results showed that the Prophet model and Keras stateful LSTM performed better than other neural network models, providing valuable insights for law enforcement organizations.

On the other hand, Manengadan et al. (2021) employed big data analytics and visualization techniques in crime data analysis in India. This study highlighted the importance of visualizing different patterns hidden in crime time series data. The researchers followed a series of operations including data collection, data pre-processing, visualization, and trends prediction, using the LSTM model.

In between these two studies, there is a clear progression in the field of big data analytics, crime prediction, and visual analytics. The work of Feng et al. (2019) laid the groundwork by demonstrating the potential of BDA in crime data analysis and prediction. Subsequently, Manengadan et al. (2021) built upon this foundation, applying similar techniques in a different context (India) and emphasizing the importance of visualization in understanding crime patterns. These studies collectively contribute to the field, showcasing applications in various domains and highlighting the potential of these techniques in aiding law enforcement efforts.

**Ethical and Legal Implications of Big Data and cloud computing**

The convergence of big data and cloud computing has resulted in substantial progress across diverse sectors, spanning healthcare to cybersecurity. Nevertheless, the adoption of these technologies introduces notable ethical and legal considerations.

In their work, Mokhtari et al. (2019) propose a layered architecture for future smart homes driven by big data, encompassing a smart home network layer and a cloud computing layer. While this innovative approach shows promise, it prompts concerns regarding data privacy and security. It is imperative to guarantee the preservation of individuals' privacy rights and the adequate protection of their data during collection, storage, and analysis. This involves the implementation of robust cybersecurity measures and adherence to data protection regulations.

Concurrently, Khanafseh et al. (2019) conduct an extensive survey on cloud forensics, exploring frameworks and solutions in digital forensics. This survey illuminates the legal challenges associated with cloud computing, encompassing issues such as data breaches, security violations, and privacy infringements. Given the dynamic nature of legal standards and regulations related to cloud computing, businesses must remain vigilant to avoid potential legal complications.

Lastly, Feng et al. (2019) apply big data analytics (BDA) to criminal data, employing exploratory data analysis for visualization and trend prediction. While their study unveils intriguing patterns in criminal data, it also underscores the ethical considerations tied to big data utilization. Companies must exercise mindfulness in their use of customers' personal data, respecting their privacy rights. Providing customers with access to their own data ensures they can modify or delete it as needed.

The promise of innovation and progress offered by big data and cloud computing must be navigated with a conscientious awareness of the ethical and legal ramifications. This involves upholding individuals' privacy rights, ensuring robust data security, and staying abreast of evolving legal standards and regulations.

**Addressing crime prediction**

The integration of machine learning techniques and interactive visualization systems has significantly advanced crime prediction and analysis.

Rajkumar et al. (2019) proposed a system capable of analyzing, detecting, and predicting crime probabilities in specific regions, supporting crime analytics with interactive visualizations that aid in crime prevention. This work emphasizes the importance of leveraging advanced technologies to enhance crime prediction and prevention.

Efficiently integrating machine learning techniques into interactive visualization systems is a key focus for Ali et al. (2019), who classified over 60 papers from various perspectives to enhance the synergy between human and computer capabilities. This research underscores the significance of integrating machine learning with interactive visualization to improve crime analysis and prediction.

These studies collectively contribute to the field of crime prediction and analysis, showcasing the potential of integrating machine learning techniques with interactive visualization systems to uncover hidden relationships within data and support crime prevention efforts. The advancements in this area have the potential to significantly impact criminal justice and law enforcement practices.

**Conclusion**

The fusion of big data analytics and crime analysis emerges as a potent tool for comprehending and anticipating criminal patterns. The methodical strategies employed in these investigations underscore the adaptability of big data technologies, underscoring their importance in preprocessing, visualization, and extracting actionable insights for crime prevention and control. The incorporation of open data, machine learning, and Bayesian modeling adds depth to the landscape of crime analysis, offering a comprehensive and multidimensional strategy for addressing intricate challenges in urban security. As progress continues, the synergy between data science and crime analysis becomes a fundamental element in constructing safer and more resilient communities.

The pivotal role of big data analytics in predicting and preventing crime lies in its ability to scrutinize vast datasets, revealing concealed patterns and correlations. This process entails analyzing diverse data types, including crime reports such as shootings, murders, and robberies, to identify trends and patterns in criminal behavior, ultimately aiding in the reduction of such offenses. Furthermore, big data analytics streamlines the identification of crime patterns, a task that is arduous and time-intensive for manual analysis by crime experts, thereby elevating the precision and effectiveness of crime detection and prevention.

Data analytics, encompassing big data, serves as a predictive tool for a spectrum of crimes, spanning financial offenses like money laundering, healthcare and insurance fraud, to insider trading. It proves influential in crime prevention, addressing scenarios from crowd management to averting road traffic accidents in diverse global regions. As more sophisticated data analytic techniques emerge, the scope for crime prediction and prevention continues to broaden.

In summary, the utilization of big data analytics in forecasting and preventing crime is an evolving domain with substantial potential for enhancing public safety. By harnessing the capabilities of data and technology, governments and law enforcement agencies can make informed, data-driven decisions to confront intricate challenges in urban security, ultimately fostering the development of safer and more resilient communities.

The realm of big data's role in crime prediction and prevention constitutes a multidisciplinary arena, integrating diverse technologies and methodologies. It is imperative to persist in exploring and advancing these approaches to continually enhance the efficacy of crime analysis, contributing to the innovation of solutions that bolster public safety.

References:

Barnett-Ryan, C.S. (2019) *Boundaries and policing:  space, jurisdictions, and roles in the collection of Official Crime Data* [Preprint]. doi:10.33915/etd.3865.

Feng, M. *et al.* (2019) ‘Big Data Analytics and mining for effective visualization and trends forecasting of Crime Data’, *IEEE Access*, 7, pp. 106111–106123. doi:10.1109/access.2019.2930410.

Gurcan, F. and Cagiltay, N.E. (2019) ‘Big Data Software Engineering: Analysis of knowledge domains and skill sets using LDA-based topic modeling’, *IEEE Access*, 7, pp. 82541–82552. doi:10.1109/access.2019.2924075.

Frith, M.J. (2019) ‘Modelling taste heterogeneity regarding offence location choices’, *Journal of Choice Modelling*, 33, p. 100187. doi:10.1016/j.jocm.2019.100187.

Alic, A.S. *et al.* (2019) ‘BIGSEA: A big data analytics platform for public transportation information’, *Future Generation Computer Systems*, 96, pp. 243–269. doi:10.1016/j.future.2019.02.011.

Syafalni, I. *et al.* (2020) ‘Cloud security implementation using homomorphic encryption’, *2020 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)* [Preprint]. doi:10.1109/comnetsat50391.2020.9328979.

Barua, H.B., Mondal, K.C. and Khatua, S. (2022) ‘Green Computing for Big Data and machine learning’, *5th Joint International Conference on Data Science &amp; Management of Data (9th ACM IKDD CODS and 27th COMAD)* [Preprint]. doi:10.1145/3493700.3493772.

Manengadan, M., Nandanan, S. and Subash, N. (2021) ‘Crime Data Analysis, visualization and prediction using LSTM’, *International Journal of Data Science and Analysis*, 7(3), p. 51. doi:10.11648/j.ijdsa.20210703.11.

Talukder, Md.A. (2023) *A dependable hybrid machine learning model for network intrusion detection* [Preprint]. doi:10.31224/2716.

Garg, D., Sidhu, J. and Rani, S. (2020) ‘A note on cloud computing security’, *International Journal of Ad Hoc and Ubiquitous Computing*, 33(3), p. 133. doi:10.1504/ijahuc.2020.10028277.

Mokhtari, G., Anvari-Moghaddam, A. and Zhang, Q. (2019) ‘A new layered architecture for future big data-driven Smart Homes’, *IEEE Access*, 7, pp. 19002–19012. doi:10.1109/access.2019.2896403.

Khanafseh, M., Qatawneh, M. and Almobaideen, W. (2019) ‘A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics’, *International Journal of Advanced Computer Science and Applications*, 10(8). doi:10.14569/ijacsa.2019.0100880.

S, R. *et al.* (2019) ‘Crime analysis and prediction using data mining techniques’, *Special Issue*, 5(Special Issue 1), pp. 602–607. doi:10.23883/ijrter.conf.20190322.078.yi0nm.

Ali, M. *et al.* (2019) ‘Clustering and classification for time series data in visual analytics: A survey’, *IEEE Access*, 7, pp. 181314–181338. doi:10.1109/access.2019.2958551.