BULETIN

UiTM CAWANGAN NEGERI SEMBILAN
KAMPUS SEREMBAN

EDISI 10 2025

FPNS3

fpnuitmn9s3

https://encr.pw/FakultiPerakaunanS3

Data Analytics and Whistleblowing in Fraud Detection: An Academic Perspective

Raziah Bi Mohamed Sadique, Musliha Musman and Salwa Muda

Fraud represents a pervasive challenge across industries, with significant financial, reputational, and societal consequences. Traditional rule-based approaches to fraud detection have become inadequate in the face of evolving fraud strategies. Fraud has been a long-standing threat to economic stability and institutional integrity. According to the Association of Certified Fraud Examiners (ACFE), global organisations lose an estimated 5% of their revenue annually to fraud (ACFE, 2022). With the rapid digitalisation of financial transactions, e-commerce, and healthcare systems, fraud detection has become more complex, requiring sophisticated tools beyond conventional audit and rule-based methods. Data analytics has emerged as a transformative approach, offering the ability to detect hidden patterns, predict fraudulent activities, and prescribe interventions in real time.

Fraud prevention in organisations requires a holistic approach that integrates both technological tools and human mechanisms of accountability. While data analytics has become central in detecting anomalies and predicting fraudulent activity, whistleblowing provides a complementary avenue by enabling individuals with insider knowledge to disclose misconduct that may not be readily apparent in data. When combined, these approaches create a multi-layered framework that strengthens the resilience of organisations against fraud. Fraud detection research has traditionally relied on statistical anomaly detection (Bolton & Hand, 2002). Over the last two decades, machine learning (ML) has reshaped the landscape, enabling dynamic classification of fraudulent behaviour (Ngai et al., 2011). Contemporary studies emphasise integrating network analysis and graph-based methods to detect organised fraud rings (Pandit et al., 2007).

Recent advancements focus on deep learning models, outperforming conventional methods in high-dimensional and unstructured datasets (Zou et al., 2019). However, concerns remain regarding the black-box nature of such models, driving interest in explainable AI (XAI) to balance accuracy with interpretability (Adadi & Berrada, 2018). Furthermore, the adoption of big data platforms and real-time streaming analytics is highlighted in the literature as critical for timely fraud prevention. Data analytics for fraud detection can be conceptualised through four major categories: descriptive, diagnostic, predictive, and prescriptive analytics. Each type serves a different but complementary purpose in the fraud management lifecycle, from understanding historical patterns to recommending real-time interventions.

Descriptive analytics provides the foundation by examining historical data to identify unusual trends or anomalies. Its primary role is to answer, “What has happened?” by offering summaries of past events. In fraud detection, this may involve generating reports highlighting irregular claim frequencies, unexpected transaction amounts, or account activity patterns deviating from established baselines. For example, in the insurance sector, descriptive analytics can reveal excessive billing or repetitive claims filed under similar conditions, thereby flagging cases that warrant further investigation. Although descriptive analytics alone cannot determine causation or predict future fraud, it establishes critical baselines for comparison (Bolton & Hand, 2002).

Diagnostic analytics builds upon descriptive insights by addressing the question of “why did this happen?” This approach explores anomalies' underlying causes through statistical methods, segmentation, and clustering. For instance, a sudden spike in fraudulent credit card transactions may be explained by examining commonalities among compromised accounts, such as shared geolocations, merchant categories, or IP addresses. Diagnostic techniques help organisations to identify systemic vulnerabilities, such as weaknesses in verification procedures or collusion between actors in organised fraud rings. By uncovering these causal relationships, diagnostic analytics facilitates the design of more targeted fraud prevention strategies (Ngai et al., 2011).

Predictive analytics represents a more advanced application, leveraging machine learning and statistical modelling to estimate the probability that a transaction, claim, or account is fraudulent. In answering the question of "what could happen?" predictive models draw on historical fraud patterns to identify risk factors and generate fraud scores for new data instances. Common techniques include logistic regression, decision trees, random forests, support vector machines, and, more recently, deep learning architectures. For example, in the banking sector, predictive models can evaluate customer behaviour in real time, flagging transactions that deviate significantly from a cardholder's typical spending patterns. While predictive analytics greatly enhances the proactive detection of fraud, it also faces challenges, such as the problem of imbalanced datasets, where fraudulent cases are vastly outnumbered by legitimate transactions (Zou et al., 2019).

Finally, prescriptive analytics extends beyond prediction by recommending specific actions to minimise risk and prevent losses. It answers the question of "what should be done?" in response to suspicious activity. In practice, this may involve automatically blocking a high-risk transaction, escalating it to a human fraud analyst for review, or adjusting risk thresholds dynamically based on contextual data. Prescriptive models can incorporate decision optimisation techniques, business rules, and reinforcement learning algorithms to propose interventions that balance fraud prevention with customer experience. For instance, in e-commerce fraud detection, prescriptive analytics can prevent account takeovers by triggering multi-factor authentication when anomalies are detected. Prescriptive models are increasingly relevant as organisations seek to operationalise predictive insights into actionable fraud management strategies (Adadi & Berrada, 2018).

These four types of analytics form a continuum of analytical sophistication. Descriptive and diagnostic analytics provide retrospective and explanatory insights, while predictive and prescriptive analytics move toward proactive and preventive strategies. Integrating all four creates a holistic framework that allows organisations to understand past fraudulent behaviours and anticipate and act against emerging threats in real time. This layered approach has been increasingly emphasised in the academic literature on fraud detection (Ngai et al., 2011; Adadi & Berrada, 2018), underscoring the necessity of combining multiple analytical perspectives to stay ahead of evolving fraud tactics.

As outlined earlier, data analytics is a powerful mechanism for identifying fraudulent transactions and patterns that deviate from normal behaviour. Techniques such as anomaly detection, predictive modelling, and network analysis allow organisations to monitor large volumes of structured and unstructured data in real time (Bolton & Hand, 2002; Ngai et al., 2011). For example, in financial services, predictive analytics can detect unusual credit card spending patterns, while in healthcare, anomaly detection may reveal fraudulent billing practices. Despite its sophistication, data analytics is not infallible. Fraudsters continuously adapt their strategies, and limitations such as imbalanced data or system blind spots may lead to undetected cases or false positives (Zou et al., 2019).

Whistleblowing represents the human dimension of fraud prevention. Employees or stakeholders who witness unethical practices can report them through formal or confidential channels, often revealing information that data analytics cannot capture. For example, whistleblowers may disclose collusion, intent, or management override of controls, which are challenging to detect algorithmically (ACFE, 2022). Legal frameworks such as the Whistleblower Protection Act (WPA) 2010 in Malaysia or the Dodd-Frank Act in the United States encourage reporting by safeguarding whistleblowers from retaliation and, in some cases, offering financial incentives (Park & Blenkinsopp, 2009). However, the effectiveness of whistleblowing systems depends heavily on organisational culture, the availability of confidential reporting channels, and trust in the institution's ability to act on disclosures.

While data analytics and whistleblowing operate differently, their integration yields significant advantages in fraud prevention. Firstly, whistleblowing reports can be triangulated with analytics findings, strengthening the credibility of both sources. Secondly, whistleblowing disclosures can guide analytics teams toward high-risk areas of investigation, thereby enhancing resource allocation. Conversely, analytics can provide supporting evidence for whistleblower claims, enabling organisations to prioritise credible allegations and reduce malicious or unfounded reports. Thirdly, the joint use of these mechanisms fosters a culture of accountability: analytics signals that behaviour is being monitored objectively. At the same time, whistleblowing empowers employees to act ethically when they observe wrongdoing.

Despite the benefits, integrating data analytics and whistleblowing poses challenges. Analytics systems may generate false positives that burden whistleblowing channels, while over-reliance on whistleblowers risks selective reporting or fear-driven silence. Ethical and privacy concerns also arise when analytics systems track employee behaviour, which may discourage individuals from speaking out (Adadi & Berrada, 2018). Moreover, whistleblowing faces cultural and psychological barriers, including fear of retaliation, distrust of management, and potential stigmatisation of whistleblowers (Park & Blenkinsopp, 2009). Addressing these challenges requires building robust governance frameworks, ensuring transparency in analytics, and protecting whistleblowers through enforceable legal safeguards.

Fraud prevention is most effective when data analytics and whistleblowing are deployed as complementary tools. Analytics provides the computational power to process vast amounts of data, detecting irregularities and predicting fraud in real time, while whistleblowing adds a qualitative dimension by uncovering intent, collusion, and misconduct that analytics may miss. They create a hybrid model that strengthens technological and ethical safeguards against fraud. Future research and practice should focus on designing integrated frameworks that balance machine-driven detection with human-driven reporting, ensuring organisations remain adaptive, transparent, and resilient against evolving fraudulent threats.

References

Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access, 6*, 52138-52160.

Association of Certified Fraud Examiners (ACFE). (2022). *Report to the Nations: Global Study on Occupational Fraud and Abuse*. ACFE.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science, 17*(3), 235–255.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569.

Pandit, S., Chau, D. H., Wang, S., & Faloutsos, C. (2007). NetProbe: A fast and scalable system for fraud detection in online auction networks. *Proceedings of the 16th International Conference on World Wide Web*, 201-210.

Park, H., & Blenkinsopp, J. (2009). Whistleblowing as planned behavior: A survey of South Korean police officers. *Journal of Business Ethics, 85*(4), 545–556.

Transparency International. (2021). *Whistleblowing in Europe: Legal Protections for Whistleblowers*. Transparency International.

Zou, J., Zhang, J., & Jiang, P. (2019). Credit card fraud detection using autoencoder neural network. *arXiv preprint arXiv:1908.11553*.