Issues in Information Systems
Volume 25, Issue 4, pp. 91-105, 2024

DOI: https://doi.org/10.48009/4_iis_2024_107

Conceptualising the use of detective analytics underpinned by Actor-network theory

Nontobeko Mlambo, *Cape Peninsula University of Technology (SA), Mlambononto@gmail.com*
Tiko Iyamu, *Cape Peninsula University of Technology (SA), Iyamut@cput.ac.za*

Abstract

Despite several mitigating measures, crime continues to disrupt and destabilise processes and activities in the financial sector. Detective analytics is increasingly explored as an additional mitigative solution by many financial institutions, to respond to the growing crime activities creatively and innovatively. This study aimed to examine how detective analytics can be used to follow the actors of crime activities. Actor-network theory (ANT) is employed as a lens to gain a deeper understanding of how activities can be traced, and tracked, to mitigate financial crime in institutions. The interpretive approach was applied. The findings revealed Seamless integration of incidents, Cybersecurity detection, In-house fraud detection, External infiltrate detection, and Image-matching data into one cohesive system. The study highlights the need for gaining a deeper understanding of networks of actors, following the actors, and passage points within an organisation. The findings have significant implications for improving the efficiency and effectiveness of detective analytics, from both technical and non-technical perspectives.

Keywords: actor-network theory; detective analytics; conceptualisation; it solutions; financial crime

Introduction

Financial institutions play a very vital role in the economy of any country. Financial institutions include banking agencies that assist individuals and organisations with carrying out transactions at both national and international levels (Ericson, 2021). The transactions include exchanging of forex and assets, from small to large volumes (Sunio & Mendejar, 2022). Some of the transactions have severe implications and consequences for the actors or the representing agents involved. For example, when a transaction goes wrong on a large scale, an entire organisation can be declared liquidated, which affects the livelihoods of the employees and others connected with the organisation. It is therefore critical, to always guide against the transactions by being precautionary with the enabling facets, primarily, which are people, data and technology.

Financial institutions rely on data for the processing of millions of transactions daily (Hasan & Rizvi, 2022). The data is enabled and supported using information technology (IT) solutions (Bataev, 2018). Furthermore, the manipulation, use and management of the data and IT solutions are carried out by people (Sahar, Safie & Bakar, 2019). Thus, financial institutions continue to build the security and protection of their assets and finances around these three facets. According to Li et al. (2020), financial institutions analyse data, to gain a better understanding and make better financial decisions and help prevent processing of suspicious transactions. Despite the preventative, detective, precautionary and security measures, processes and transactions are often in danger because of fraudulent activities, from unprecedented

circumstances (Yamen et al., 2019). Some of the activities are from internal and external entities and agents including humans' actions, consciously or unconsciously.

In the last ten years, South Africa has been one of the most hit countries in the world by financial crime (Kempen, 2020). Achim, Borlea and Văidean (2021) argue that financial crime is double in low-income countries than it is in high-income countries. This could be attributed to the sophistication of preventative, detective, and other security measures in high-income countries, using IT solutions (Hope, 2020). Some financial crimes are detected by financial institutions (Gombiro, Jantjies & Mavetera, 2015). There are loopholes in the current methods and approaches, hence, the rate of financial crime in South Africa is increasing. Thus, a different mechanism is required, to advance protection and security against financial crime in the country. This should allow and enable early detection of the crime before and as it happens, using the most appropriate mechanism such as detective analytics.

Detective analytics is in the family of data analytics, which includes diagnostics, descriptive, predictive, and prescriptive (Vanani & Shaabani, 2021). Data analytics are widely used to combat financial crimes and the most used analytics are predictive, prescriptive, and detective analytics (Menezes et al., 2019). Although there is closeness and a bit of overlap among the analytics tools (Lee, Cheang & Moslehpour, 2022), detective analytics uniquely focuses on identifying a problem in data, as and when it occurs (Menezes et al., 2019; Poornima & Pushpalatha, 2020). In its advancement, detective analytics focuses on performing the diagnostics on big data and small data (normal), uncovers and rectifies infeasible events and occurrences (Empl & Pernul, 2023; Aliguliyev, Imamverdiyev & Abdullayeva, 2016). The few organisations that are using detective analytics do so because it is considered advanced analytics (Al-Banna et al., 2023; Menezes et al., 2022).

However, there remain two fundamental issues. Firstly, not many financial institutions use and know how to fully utilize the capabilities of detective analytics (Liu, Shin, & Burns, 2021). Secondly, despite its advancement, challenges persist. Thus, this study sets out to conceptualise how a sociotechnical theory, actor-network theory (ANT) can be complementarily applied with detective analytics, to trace, track, and prevent financial crime in a financial institution.

This paper is organised into six main sections. The first section introduces the study, respectively. A review of the literature focusing on the core aspects of the study is presented in the second section. In the third section, the theory, ANT that underpins the study is discussed. The methodology applied in the study is covered in the fourth section. The analysis and discussion are presented in the fifth section. A conclusion is drawn in the final section.

Literature review

This section presents the literature reviewed. It focuses on the core aspects of the study, which are financial crime in institutions and detective analytics.

Financial crime in institutions

Most financial institutions rely on data, and the growth of data is drastic throughout the whole world (Bataev, 2018). Hasan, Popp and Oláh (2020) state that hundreds of millions of financial transactions occur in financial institutions each day and all these transactions lead to data creation. In this age of innovation and machine learning, data is seen as one of the most vital contributors in decision-making for most financial institutions. Consequently, financial institutions have been targets for financial crimes both internally and externally (Yamen et al., 2019). Internally by individuals who have access to transaction data

and externally by individuals or organisations that target specific individuals' information to commit financial crimes. Financial institutions have seen a high rise in financial crimes over the past ten years which negatively impacts the development and reliability of information systems (Hope, 2020). Achim, Borlea and Văidean (2021) argue that financial crime is double in low-income countries than it is in high-income countries. South Africa has been one of the leading countries exposed to financial crime (Kempen, 2020).

Financial crime is a widespread problem and has been reported to be very aggressive in African countries due to the high rate of poverty. The economic development minister in South Africa has claimed that over 76000 jobs are lost every year due to financial crime (Hope, 2020). The South African government has tried their best to implement strategies to combat crime in general and these strategies also include the regulation of laws relating to financial crime (De Koker, 2007; Kshetri, 2019). Macdonald (2019) states that financial crime activities such as money laundering have been considered the new way of making a living for most South Africans and a very profitable business to most. According to Van Niekerk (2017), most South African financial institutions have experienced a much higher rate of financial crimes due to the high demand for online transactions. Notwithstanding that most institutions have implemented technological enhancements to combat financial crime, Coetzee (2018) argues that technology is the main driver of financial crime.

Detective analytics

The use of data analytics has grown exponentially in the financial sector (Cockcroft & Russell, 2018). This can be attributed to its strengths of accurate reporting, cost reduction, enhanced decision making and operational benefits (Alsghaier et al., 2017; Kumar et al., 2020; Lazarova-Molnar, Mohamed & Al-Jaroodi, 2018; Ifenthaler, 2017; Wang &Hajli, 2017). Data analytics in the financial sector creates opportunities to advance financial management for both customers and organisations (Giebe, Hammerström & Zwerenz, 2019; Nobanee, 2021). Andriosopoulos et al. (2019) state that most financial problems that exist can be solved by examining the available data, which can be done using data analytics. However, some researchers argue that the advancement of data analytics in the financial sector has not been thoroughly explored (López-Robles et al., 2019; Samuel, 2017; Sun, Shi & Zhang, 2019). The most explored data analytics methods in the financial sector are descriptive analytics, diagnostic analytics, predictive analytics and prescriptive analytics. However, detective analytics has little to no research conducted in finance literature.

Detective analytics focuses on the analytics (or analysis) of data, like other tools such as descriptive analytics, diagnostic analytics, predictive analytics, and prescriptive analytics. Descriptive analytics is used to understand what had occurred in the past using historical data (Janakiraman & Ayyanathan, 2021). While diagnostic analytics focuses on historical data, to gain a deeper understanding of the reason behind certain outcomes (Balali et al., 2020), hence it is mostly used to build insights into why certain events occurred in the way they do (Deshpande, Sharma & Peddoju, 2019). Predictive analytics is used to determine patterns and themes to understand what could happen in the near future (Jeble et al., 2018; Selvan & Balasundaram, 2021). From an organisation's perspective, De Jesus Liriano (2019) states that prescriptive is to forecast a problem or a solution.

For many years, financial institutions have been using data analytics to derive patterns that lead to financial criminal activities (Andriosopoulos et al., 2019; Derindere Köseoğlu, Ead & Abbassy, 2022; Ravi & Kamaruddin, 2017). Fosso Wamba (2017) states that data analytics help to collect relevant data, to access and integrate the data in providing reports of deeper insights into business operations and productions. Thus, like other sectors, the use of data analytics has enhanced and enabled the financial sector in making better decisions (Ranjan & Jeyanthi, 2021). Increasingly, many organisations can use data analytics, to explore

and visualize data to a simple representation that can be easily understood by both users and managers (Khedr, Kholeif & Saad, 2017).

Despite the benefits that data analytics offers organisations, the financial sector continues to experience an increase in financial crimes (Holzenthal, 2017; Yeoh, 2019). Detective analytics is used to diagnose and detect a problem immediately as and when the problem occurs (Vanani & Majidian, 2021). However, not many financial institutions use and know how to fully utilize the capabilities of detective analytics (Liu, Shin, & Burns, 2021). Therefore, detective analytics should be critically explored in the financial sector to help combat crime activities within the institutions.

Among other things, detective analytics is used by organisations, to detect fraudulent activities (Abdallah, Maarof & Zainal, 2016). To detect means to discover and identify a problem before it occurs. The use of detective analytics is not only advantageous for future purposes but could also be used to detect traces and track incidents using historical data (Sun, Huang & Gong, 2011). Menezes et al. (2019) describe detective analytics as the combination of predictive analytics and prescriptive analytics in the sense that it forecasts and recommends solutions to problems as and when they occur. Thornton et al. (2013) state that fraud detection is used mostly to detect unknowns and known unknowns. Verma, Taneja & Arora (2017) emphasise the need for financial institutions to adopt effective fraud detection techniques such as detective analytics to reduce the number of fraud instances. The use of detective analytics is a needed mechanism for financial institutions due to most processes being data-driven (West & Battacharya, 2016).

Underpinning theory

This study is underpinned by a sociotechnical theory, actor-network theory (ANT). The theory is selected to underpin the study based on three main reasons. Firstly, the nature of the study requires a sociotechnical view because, from technology alone, the challenges remain with the phenomenon. Secondly, in financial fraudulent activities, negotiations occur between humans, technologies, or humans and technology actors. One of the main focuses of ANT is understanding negotiation shifts among actors, consciously or unconsciously (Callon, 1986). Thirdly, the mantra 'follow the actors' of the theory helps to connect (or link) non-humans (activities) with humans through rules and networks including the tools used.

The complementarity of ANT and detective analytics bridges any possible gap, either in the analysis of the data or interpretation of the findings. Iyamu (2021) provides a comprehensive justification and offers a guide for complementarily employing theories.

Actor-Network theory

The ANT is a sociotechnical theory that is used by researchers to explain the relationship between humans and non-human objects (Couldry, 2008). Sage, Dainty and Brookes (2011) further state that ANT is mostly focused on the formation of networks, the relationship between actors, and shifting negotiation within the actor-network. This helps to understand how human and non-human actors are involved in an activity or incident (Gao, 2005). According to Walsham (1997), an actor-network is formed immediately when the actors have aligned interests. Actor-networks are formed consciously or unconsciously, based on an allied interest (Latour, 1996). In summation, the theory focuses on how networks are built, maintained, and what makes the network dissolve (Michael, 2017; Shim & Shin, 2016).

Applying ANT allows the researcher to follow the actors in their heterogeneous networks. This is because the theory offers methodological steps in the activities, actions and interactions between actors in a network

(Heeks & Stanforth, 2015; Callon, 1986). According to Iyamu (2021, p. 73), "ANT provides a platform which allows for the analysis of both human and non-human interaction in a network. This means that ANT is a resource for understanding the actions of humans". Lefkowitz (2022) draws on ANT, to trace information pathways that enable human to access actions and connect with needed resources. Kumar and Tissenbaum (2022) employ ANT to provide an underutilized post humanist lens to understand the creation of collaborative connections between action-based interaction.

Another strength of ANT that is critically useful in this study is the concept of translation. The translation in ANT is the process of creating a relationship with things, which did not exist, previously (Lezaun, 2017). Translation occurs when the human actors' interests are aligned with their actor-network (Walsham, 1997). The use of ANT has gained popularity in areas of IS research, in areas such as the adoption of technology, examination of healthcare systems, and assessment of IT solutions that support and enable engineering, finance, and education activities. Also, ANT is increasingly applied to gain a deeper understanding of processes and innovation of technology (Shim & Shin, 2016).

Methodological approach

In this research, assumptions were made, which are aligned with existing philosophies, ontology and epistemology. This is not new, studies are consistently based on assumptions and guide inquiries (Endjala, 2022), that certain realities exist (Neuhaus, 2017) and knowledge can be gained (Hájek & Hartmann, 2010; Titchen & Ajjawi, 2010).

In ontology, there are many realities to the existence of artefacts (Walliman, 2017), such as events and technology (Poli & Seibt, 2010). The Events and realities of this study are the existence of financial institutions, financial crimes, and detective analytics. Ontologically, detective analytics is understood and viewed from different perspectives. For example, detective analytics was used with the Internet of Things (IoT) to generate new insights (Empl & Pernul, 2023). Another reality is that detective analytics has been used to obtain accurate predictions by organisations (Menezes et al., 2019). Also, there are various ways or approaches to the implementation or adoption of detective analytics. This includes the use of frameworks, policies, and models (Broeders et al., 2017; McKee, 2017; Pramanik, Lau, & Chowdhury, 2016). Some of the approaches have been employed by organisations across the world.

Based on the ontological assumption, a subjective stance is taken in this research, which allows us to employ our creative reasoning and interpretations (Coats, 1983), to conclude this research. After all, there is no universal 'fit' in providing the solution, in the use of detective analytics. Thus, subjectively, the researcher can induce from data, how to develop an instrumentation and apply detective analytics to mitigate financial. From the epistemology perspective, subjectivism is the stance for this research. primarily, this is because it allows different interpretations, which enables learning and gaining knowledge from various standpoints (Tolmen, 2020; Titchen & Ajjawi, 2010; Walsham, 2006).

Data collection

Existing materials (documents) were gathered using the document analysis technique. The technique allows the rationalisation of materials from the heap available in the forms of books, newspaper articles, peer-reviewed articles, and organisational reports (Morgan, 2022). The data was collected using a set of criteria that included areas of focus, publication timeframe, and credible sources. The areas of focus were crime in

financial institutions, detective analytics, and ANT, which are the core aspects of the study. The timeframe was vita, thus, papers published within ten years were considered, to gain insights into critical aspects such as the historical background and meanings associated with the phenomenon over time (Iyamu, Nehemia-Maletzky & Shaanika, 2016). Based on the newness of the approach, detective analytics only a small sample of the most appropriate and relevant literature could be gathered. This is not new as it has been experienced and argued in many IS studies Nyikana & Iyamu, 2023; Brereton et al., 2007; Glass, Ramesh & Vessey, 2004).

Materials published in Journal outlets, books, conference proceedings and the internet between 2013 and 2023 were gathered. A total of 255 papers were collected from database sources such as Ebscohost, IEEE, AIS, and Emerald. The sources were important because they instilled credibility and reliability in the data (Nyikana & Iyamu, 2023). Based on the focus and objective of the study, only 77 papers were relevant and used for the study.

Data analysis and discussion

As presented in the section that follows including Table 1. ANT is used to gain an understanding of how networks of actors (humans and non-humans) can be linked together in a crime-related event. This is primarily because ANT proposes and allows actors to be followed, to establish their roles in the processes and activities in finance transactions within an organisation. Table 1 reveals how ANT helps to gain a deeper understanding of the relationship that exists between the actors in the process of executing finance transactions. This includes committing a financial crime or attempting to mitigate the financial crime.

Table 1: ANT as a Lens

ANT Tenet	ANT Translative view	Factor
Actor-network	Detective analytics integrates multiple operations, scales, scenarios, and layers (Al-Banna et al., 2023). The multiplexity is made up of actor-networks, of humans and non-humans. they are interwoven, which means that they cannot be separated in their diagnostics. The actor-networks imbibe leverages automation of processes based on centralised data, to detect crime patterns across enterprise-wide.	Seamlessly integrates incident
Follow the actors	Detective analytics enacts operations for detecting incidents of compromise in real-time and offline. Detective analytics generates new insights as non-human actors transform. From a cybersecurity perspective, some non-human actors commonly transform are signatures, processes, and rules (Empl & Pernul, 2023). The operations link various compromises to an incident by following the actors. This enhances the power of connecting disparate data across enterprise-wide.	Cybersecurity detection
Obligatory passage points	This obligatory passage point infuses tacit knowledge into members of an actor-network, which helps to maintain the translation of fraud-related actions and gain an understanding of the traces. Walton (2013) argues that the OPP facilitates and filters the appropriateness of action that is congruent with the agreed superordinate goals. The OPP is the result of "translations", in which the actors have no choice but to accept the dedicates (Callon, 1986). It is thus, an essential glue that brings together various links.	In-house fraud detection

	OPP brings a different dimension that supports the unfolding of participatory including an understanding of actors' roles and identities through recognition. The translation of obligated processes and rules helps, to follow the actors (Minniti & Magaudda, 2024). This is a crucial dynamic in the use of detective analytics for the diagnosis of events, to indose consistency towards increased accuracy.	
Blackbox	Following the actors can lead to opening a black box, from which new insights are gained from the translations of the links and interactions between human and non-human actors. Silvis and Alexander (2014) suggest that following the actors over time and across a multitude is an important means of analysis, to gain explicit insights. Opening the black boxes and examining the ontology of the actor-networks that led to their construction (Latour, 2005).	External infiltrate detection
Actor-network	Detective analytics expands the accuracy capability of IT. According to Menezes et al. (2022), detective analytics induces a level of preciseness in its operations on veracity, volume, variety, and velocity of data. Advances the analytics to detect inconsistencies including image recognition in big data, from feasible to its smallness.	Image-matching data into one cohesive system

From ANT, a social context perspective, five factors were found to be crucial points in following the actors, to mitigate financial crime in an organisation. The factors are (1) Seamless integration of incidents, (2) Cybersecurity detection, (3) In-house fraud detection, (4) External infiltrate detection, and (5) Image-matching data into one cohesive system.

Correspondingly, some activities and actions involved unregulated and unprecedented movements (Riddel & Hales, 2018). Consequently, organisations are increasingly employing detective analytics to manage and promote their business efficacy (Boodhun & Jayabalan, 2018). Islam et al. (2021) however, suggest that it is challenging to identify some hidden characters that manifest in many environments. Thus, the analysis of fraudulent or suspected incidents should not follow a fixed process (Silvis & Alexander, 2014). In our attempt to gain a deeper understanding of how to employ detective analytics in the qualitative world for analysis purposes, we focus on the notion of 'actor-network', 'follow the actors', 'obligatory passage point' (OPP), and black box from ANT perspective.

Relationships between actors, humans and non-humans are informed by processes of association and translation that can be, according to Michael (2017, p. 41), "material as well as social, physical as well as semiotic". ANT's mantra is "to follow the actors" (Latour, 2005, p. 12) that are not exclusively human but non-human parts of interactions within networks. Stalph (2019) argues that actor-networks need to be unfolded and the inherent black boxes offer insights into their ontologies and allow detailed accounts of these inner workings. The OPP characterises the dynamics convergence of the processes of network constitution and highlights crucial participatory roles and identities of various actors (Minniti & Magaudda, 2024).

Detective analytics focuses on performing the diagnostics on big data and small data (normal), uncovers and rectifies infeasible events and occurrences (Empl & Pernul, 2023; Aliguliyev, Imamverdiyev & Abdullayeva, 2016). From this standpoint, OPP, in a detective analytics operation, helps to gain insights about actors' roles in activity by recognising their identities, how they transformed, and consolidating their alignments. Also, ANT proposes a relational ontology, to gain a deeper understanding of networks and

existing syntax as enactments of associations between actors, human and nonhuman (Stalph, 2019). The syntax Is discovered as we follow the actors (Silvis & Alexander, 2014). Complementarily, using detective analytics, explicitly, ensures the timeliness, consistency, and integration of big data, in recognising activities and traces of events in an environment (Iyamu, 2022; Menezes et al., 2022). In detective analytics, constraints are reduced, and the diagnosis eliminates and rectifies inappropriate values.

Across the world, governments of countries are trying various approaches to combat financial crimes in financial institutions. Yet, the situation has not eased, instead, it has increased. Hope (2020) cites evidence of a financial crime and argues that until corruption channels such as embezzlement, theft, bribes, kickbacks, money laundering, and illicit financial flow are thoroughly investigated financial crime will continue to increase. The approach, "follow the actor" is consistently useful, as it spears the traces of the minds, processes, and occurrences, towards a fundamentally constructive decision. Among other things, this provides nuance and an in-depth assessment of the interrelatedness that exists between human actors and nonhuman actants along with their translation and participatory power. In 2021, during the lockdown caused by Covid-19, which resulted in more reliance on online transactions, financial crime in South Africa increased by 15.1% (Ferreira & Koko, 2022).

The perpetrators of financial crimes in organisations are either internal or external personnel. From the internal perspective, the crimes are usually intended or unconscious (human error) by employees who have access to internal procedures and data, while the external factors include fraudsters, phishing and money laundering (Nakajima, 2007). The increase in financial crime is due to the emerging technologies that institutions adopt to enhance processes (West & Battacharya, 2016). Thus, there is a need to explore how the use of detective analytics as a mechanism can be used to detect financial crime.

Conclusion

This study highlights the critical challenges faced by organisations in mitigating financial crime due to the constrain of following the actors. The findings reveal that Seamless integration of incidents, Cybersecurity detection, In-house fraud detection, External infiltrate detection, and Image-matching data into one cohesive system are major barriers to effectively mitigating financial crime in organisations. An understanding of these factors has the potential to address these challenges. However, the implementation of detective analytics would require significant efforts in terms of understanding the implications from both technical and non-technical perspectives. However, the study also has some limitations, such as the focus on a non-empirical or case study approach. Future research should aim to validate the findings in organisational settings and explore the feasibility and impact of implementing detective analytics in a financial institution.

References

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, 90-113.

Achim, M. V., Borlea, S. N., & Văidean, V. L. (2021). Does technology matter for combating economic and financial crime? A panel data study. *Technological and economic development of economy*, 27(1), 223-261.

Al-Banna, A., Menezes, B. C., Yaqot, M., & Kelly, J. D. (2023). Decision regression for modelling of supply chain resilience in interdependent networks: LNG case. In *Computer Aided Chemical Engineering* (Vol. 52, pp. 1113-1118). Elsevier.

Aliguliyev, R., Imamverdiyev, Y., & Abdullayeva, F. (2016). The investigation of opportunities of big data analytics as analytics-as-a-service in cloud computing for oil and gas industry. *Problems of information technology*, 7(1), 9-22.

Alsghaier, H., Akour, M., Shehabat, I., & Aldiabat, S. (2017). The importance of big data analytics in business: a case study. *American Journal of Software Engineering and Applications*, 6(4), 111-115.

Andriosopoulos, D., Doumpos, M., Pardalos, P. M., & Zopounidis, C. (2019). Computational approaches and data analytics in financial services: A literature review. *Journal of the Operational Research Society*, 70(10), 1581-1599.

Balali, F., Nouri, J., Nasiri, A., & Zhao, T. (2020). *Data Intensive Industrial Asset Management*. Cham: Springer International Publishing.

Bataev, A. V. (2018, September). Evaluation of Using Big Data Technologies in Russian Financial Institutions. In 2018 *IEEE International Conference" Quality Management, Transport and Information Security, Information Technologies*"(IT&QM&IS) (pp. 573-577). IEEE.

Boodhun, N., & Jayabalan, M. (2018). Risk prediction in life insurance industry using supervised learning algorithms. *Complex & Intelligent Systems*, 4(2), 145-154.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of systems and software*, 80(4), 571-583.

Broeders, D., Schrijvers, E., van der Sloot, B., Van Brakel, R., de Hoog, J., & Ballin, E. H. (2017). Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data. *Computer Law & Security Review*, 33(3), 309-323.

Callon, M. (1986). The sociology of an actor-network: The case of the electric vehicle. In *Mapping the dynamics of science and technology: Sociology of science in the real world* (pp. 19-34). London: Palgrave Macmillan UK.

Coats, A. W. (1983). The revival of subjectivism in economics. In *Beyond Positive Economics? Proceedings of Section F (Economics) of the British Association for the Advancement of Science York 1981* (pp. 87-103). London: Palgrave Macmillan UK.

Cockcroft, S., & Russell, M. (2018). Big data opportunities for accounting and finance practice and research. *Australian Accounting Review*, 28(3), 323-333.

Coetzee, J. (2018). Strategic implications of Fintech on South African retail banks. *South African Journal of Economic and Management Sciences*, 21(1), 1-11.

Couldry, N. (2008). Actor network theory and media: Do they connect and on what terms?.

De Jesus Liriano EDD, R. (2019). Improving the Learning Process in the Higher Education Through the Use of a Predictive Tool (Dashboard). *FDLA Journal*, 4(1), 7.

De Koker, L. (2007). Financial crime in south africa. *Economic affairs*, 27(1), 34-38.

Derindere Köseoğlu, S., Ead, W. M., & Abbassy, M. M. (2022). Basics of Financial Data Analytics. In *Financial Data Analytics: Theory and Application* (pp. 23-57). Cham: Springer International Publishing.

Deshpande, P. S., Sharma, S. C., & Peddoju, S. K. (2019). *Security and Data Storage Aspect in Cloud Computing* (Vol. 52). Singapore: Springer.

Empl, P., & Pernul, G. (2023). Digital-twin-based security analytics for the Internet of things. *Information*, 14(2), 95-215.

Endjala, T. (2022). *An Employee Assistance Programme (EAP) to support midwives affected by maternal deaths and stillbirths in Khomas region, Namibia* (Doctoral dissertation, University of Namibia).

Ericson, J. (2021). Communication Breakdown: Identifying weaknesses and improvement possibilities in the cooperation between law enforcement and financial institutions regarding romance fraud.

Ferreira, E., Koko, K., 2022. Latest crime statistics: Murder, kidnapping and commercial crimes increase. Available; https://mg.co.za/news/2022-02-18-latest-crime-statistics-murder-kidnapping-and-commercial-crimes-increase/

Fosso Wamba, P. S. (2017). Big data analytics and business process innovation. *Business Process Management Journal*, 23(3), 470-476.

Gao, P. (2005). Using actor-network theory to analyse strategy formulation. *Information Systems Journal*, 15(3), 255-275.

Giebe, C., Hammerström, L., & Zwerenz, D. (2019). Big data & analytics as a sustainable customer loyalty instrument in banking and finance.

Glass, R. L., Ramesh, V., & Vessey, I. (2004). An analysis of research in computing disciplines. *Communications of the ACM*, 47(6), 89-94.

Gombiro, C., Jantjies, M., & Mavetera, N. (2015). A conceptual framework for detecting financial crime in mobile money transactions. *Journal of Governance and Regulation*, 4(4), 727-734.

Hájek, A., & Hartmann, S. (2010). Bayesian epistemology.

Hasan, I., & Rizvi, S. A. M. (2022). AI-driven fraud detection and mitigation in e-commerce transactions. *In Proceedings of Data Analytics and Management: ICDAM 2021, Volume 1* (pp. 403-414). Springer Singapore.

Hasan, M. M., Popp, J., & Oláh, J. (2020). Current landscape and influence of big data on finance. *Journal of Big Data*, 7(1), 21.

Heeks, R., & Stanforth, C. (2015). Technological change in developing countries: opening the black box of process using actor–network theory. *Development Studies Research*, 2(1), 33-50.

Holzenthal, F. (2017). Five trends shaping the fight against financial crime. *Computer Fraud & Security*, 2017(3), 5-9.

Hope, Sr, K. R. (2020). Channels of corruption in Africa: analytical review of trends in financial crimes. *Journal of Financial Crime*, 27(1), 294-306.

Ifenthaler, D., 2017. Designing effective digital learning environments: Toward learning analytics design. *Technology, Knowledge and Learning*, 22, 401-404.

Islam, M. R., Liu, S., Biddle, R., Razzak, I., Wang, X., Tilocca, P., & Xu, G. (2021). Discovering dynamic adverse behavior of policyholders in the life insurance industry. *Technological Forecasting and Social Change*, 163, 120486.

Iyamu, T. (2022). *Advancing big data analytics for healthcare service delivery*. London: Routledge.

Iyamu, T. (2021). *Applying theories for information systems research*. London: Routledge.

Iyamu, T., Nehemia-Maletzky, M., & Shaanika, I. (2016). The overlapping nature of business analysis and business architecture: What we need to know. *Electronic Journal of Information Systems Evaluation*, 19(3), 169-179.

Janakiraman, S., & Ayyanathan, N. (2021). *Big Data Framework for Indian Green Coffee Export Demand Modeling and Descriptive Analysis using Nosql-MONGODB* (No. 6919). EasyChair.

Jeble, S., Dubey, R., Childe, S. J., Papadopoulos, T., Roubaud, D., & Prakash, A. (2018). Impact of big data and predictive analytics capability on supply chain sustainability. *The International Journal of Logistics Management*, 29(2), 513-538.

Kempen, A. (2020). The world of private investigators in South Africa. *Servamus Community-based Safety and Security Magazine*, 113(11), 34-37.

Khedr, A., Kholeif, S., & Saad, F. (2017). An integrated business intelligence framework for healthcare analytics. *International Journal*, 7(5).

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81.

Kumar, V., & Tissenbaum, M. (2022). Supporting collaborative classroom networks through technology: An actor network theory approach to understanding social behaviours and design. *British Journal of Educational Technology*, 53(6), 1549-1570.

Kumar, Y., Sood, K., Kaul, S., & Vasuja, R. (2020). Big data analytics and its benefits in healthcare. *Big data analytics in healthcare*, 3-21.

Latour, B. (1996). On actor-network theory: A few clarifications. *Soziale welt*, 369-381.

Latour, B. (2005). An introduction to actor-network-theory. *Reassembling the social*.

Lazarova-Molnar, S., Mohamed, N., & Al-Jaroodi, J. (2018, October). Collaborative data analytics for industry 4.0: challenges, opportunities and models. In *2018 sixth international conference on enterprise systems (ES)* (pp. 100-107). IEEE.

Lefkowitz, D. (2022). Black boxes and information pathways: An actor-network theory approach to breast cancer survivorship care. *Social Science & Medicine*, 307, 115184.

Lee, C.S., Cheang, P.Y.S. and Moslehpour, M., 2022. Predictive analytics in business analytics: decision tree. *Advances in Decision Sciences*, 26(1), pp.1-29.

Lezaun, J. (2017). Actor-network theory.

Li, J., Li, J., Zhu, X., Yao, Y., & Casu, B. (2020). Risk spillovers between FinTech and traditional financial institutions: Evidence from the US. *International Review of Financial Analysis*, 71, 101544.

Liu, X., Shin, H., & Burns, A. C. (2021). Examining the impact of luxury brand's social media marketing on customer engagement: Using big data analytics and natural language processing. *Journal of Business research*, 125, 815-826.

López-Robles, J. R., Rodríguez-Salvador, M., Gamboa-Rosales, N. K., Ramirez-Rosales, S., & Cobo, M. J. (2019). The last five years of Big Data Research in Economics, Econometrics and Finance: Identification and conceptual analysis. *Procedia computer science*, 162, 729-736.

Macdonald, D. (2019). Barriers to reconstruction and development: A brief view of corruption and economic crime in Southern Africa. In *Structural Adjustment, Reconstruction and Development in Africa* (pp. 172-178). Routledge.

McKee, H. (2017). An Instructor Learning Analytics Implementation Model. *Online Learning*, 21(3), 87-102.

Menezes, B. C., Kelly, J. D., Leal, A. G., & Le Roux, G. C. (2019). Predictive, prescriptive and detective analytics for smart manufacturing in the information age. *IFAC-PapersOnLine*, 52(1), 568-573.

Menezes, B., Yaqot, M., Hassaan, S., Franzoi, R., AlQashouti, N., & Al-Banna, A. (2022, October). Digital Transformation in the Era of Industry 4.0 and Society 5.0: A perspective. In *2022 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA)* (pp. 1-6). IEEE.

Michael, M. (2017). Actor-network theory: Trial, trails and translations. London: Sage publications.

Minniti, S., & Magaudda, P. (2024). The 'obligatory passage point'in knowledge co-production: Italy's participatory environmental monitoring platform. *Science as Culture*, 1-18.

Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*, 27(1), 64-77.

Nakajima, C. (2007). Issues in fighting financial crime. *Economic Affairs*, 27(1), 2-5.

Neuhaus, F. (2017, September). On the Definition of 'Ontology'. In JOWO.

Nobanee, H. (2021). A bibliometric review of big data in finance. *Big Data*, 9(2), pp.73-78.

Nyikana, W., & Iyamu, T. (2023). A formulaic approach for selecting big data analytics tools for organizational purposes. In *Handbook of research on driving socioeconomic development with big data* (pp. 224-242). IGI Global.

Poli, R., & Seibt, J. (Eds.). (2010). *Theory and applications of ontology: Philosophical perspectives*. New York: Springer.

Poornima, S., & Pushpalatha, M. (2020). A survey on various applications of prescriptive analytics. *International Journal of Intelligent Networks*, 1, 76-84.

Pramanik, M. I., Lau, R. Y., & Chowdhury, M. K. H. (2016). Automatic crime detector: A framework for criminal pattern detection in big data era.

Raeesi Vanani, I. and Majidian, S. (2021). Prescriptive analytics in internet of things with concentration on deep learning. *Introduction to Internet of Things in Management Science and Operations Research: Implemented Studies*, pp.31-54.

Ranjan, J., & Jeyanthi, M. (2021). Big Data Analytics in the Healthcare Industry. In *Global Business Leadership Development for the Fourth Industrial Revolution* (pp. 134-154). IGI Global.

Ravi, V., & Kamaruddin, S. (2017). Big data analytics enabled smart financial services: opportunities and challenges. In *Big Data Analytics: 5th International Conference, BDA 2017, Hyderabad, India, December 12-15, 2017, Proceedings 5* (pp. 15-39). Springer International Publishing.

Sage, D., Dainty, A., & Brookes, N. (2011). How actor-network theories can help in understanding project complexities. *International Journal of Managing Projects in Business*, 4(2), 274-293.

Shahar, S. M., Mohd Satar, N., & Abu Bakar, K. A. (2019). The challenges in managing information technology shared services operations. *International Journal of Recent Technology and Engineering (IJRTE)*, 8, 322-328.

Samuel, J. (2017). Information token driven machine learning for electronic markets: Performance effects in behavioral financial big data analytics. *JISTEM-Journal of Information Systems and Technology Management*, 14, 371-383.

Selvan, C., & Balasundaram, S. R. (2021). Data analysis in context-based statistical modeling in predictive analytics. In *Handbook of Research on Engineering, Business, and Healthcare Applications of Data Science and Analytics* (pp. 96-114). IGI Global.

Shim, Y., & Shin, D. H. (2016). Analyzing China's fintech industry from the perspective of actor–network theory. *Telecommunications Policy*, 40(2-3), 168-181.

Silvis, E., & M. Alexander, P. (2014). A study using a graphical syntax for actor-network theory. *Information Technology & People*, 27(2), 110-128.

Stalph, F. (2019). Hybrids, materiality, and black boxes: Concepts of actor-network theory in data journalism research. *Sociology Compass*, 13(11), e12738.

Sun, S., Huang, D., & Gong, Y. (2011). Gross error detection and data reconciliation using historical data. *Procedia Engineering*, 15, 55-59.

Sun, Y., Shi, Y., & Zhang, Z. (2019). Finance big data: Management, analysis, and applications. *International Journal of Electronic Commerce*, 23(1), 9-11.

Sunio, V., & Mendejar, J. (2022). Financing low-carbon transport transition in the Philippines: Mapping financing sources, gaps and directionality of innovation. *Transportation Research Interdisciplinary Perspectives*, 14, 100590.

Sutherland, E. (2017). Governance of cybersecurity-the case of South Africa. *The African Journal of Information and Communication*, 20, 83-112.

Thornton, D., Mueller, R. M., Schoutsen, P., & Van Hillegersberg, J. (2013). Predicting healthcare fraud in medicaid: a multidimensional data model and analysis techniques for fraud detection. *Procedia technology*, 9, 1252-1264.

Titchen, A., & Ajjawi, R. (2010). Writing contemporary ontological and epistemological questions about practice. In *Researching Practice* (pp. 45-55). Brill.

Tolmen, R. (2020). *Understanding the influence of technological innovation within the insurance industry in KwaZulu-Natal*. The IIE.

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication*, 20, 113-132.

Vanani, I. R., & Shaabani, A. (2021). Digital Transformation: Utilization of Analytics and Machine Learning in Smart Manufacturing. In *Artificial Intelligence, Machine Learning, and Data Science Technologies* (pp. 269-281). CRC Press.

Verma, A., Taneja, A., & Arora, A. (2017, August). Fraud detection and frequent pattern matching in insurance claims using data mining techniques. In *2017 tenth international conference on contemporary computing (IC3)* (pp. 1-7). IEEE.

Walliman, N. (2017). Research theory. In *Research methods: the basics* (pp. 16-30). Routledge.

Walsham, G. (1997, May). Actor-network theory and IS research: current status and future prospects. In *Information Systems and Qualitative Research: Proceedings of the IFIP TC8 WG 8.2 International Conference on Information Systems and Qualitative Research, 31st May–3rd June 1997, Philadelphia, Pennsylvania, USA* (pp. 466-480). Boston, MA: Springer US.

Walsham, G. (2006). Doing interpretive research. *European journal of information systems*, 15(3), 320-330.

Walton, J. (2013, September). The obligatory passage point: abstracting the meaning in tacit knowledge. In *Proceedings of the 14th European Conference on Knowledge Management* (Vol. 2, pp. 769-775). Academic Conferences and Publishing International Limited.

Wang, Y., & Hajli, N. (2017). Exploring the path to big data analytics success in healthcare. *Journal of Business Research*, 70, 287-299.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. *Computers & security*, 57, 47-66.

Yamen, A., Al Qudah, A., Badawi, A., & Bani-Mustafa, A. (2019). The impact of national culture on financial crime. *Journal of Money Laundering Control*, 22(2), 373-387.

Yeoh, P. (2019). Artificial intelligence: accelerator or panacea for financial crime?. *Journal of Financial Crime*, 26(2), 634-646.