

The use of detective analytics for mitigating financial crimes: A South African perspective

Nontobeko Mlambo , Tiko Iyamu 

Department of Information Technology, Cape Peninsula University of Technology, Cape Town, South Africa

ABSTRACT

South African organisations are increasingly exploring the use of detective analytics in mitigating financial crimes. However, many organisations are struggling with how to employ the tool in detecting and preventing financial crimes. This study aimed to conceptualise how detective analytics can be used to mitigate financial crimes in organisations. Qualitative data were gathered from different sources, from peer-reviewed to grey literature. Actor-network theory (ANT) was employed as a lens, through its mantra ‘follow the actors’, to gain insights on how activities can be identified, traced, and tracked, in mitigating 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 obligatory passage points within an organisation. The findings have significant implications for improving the efficiency and effectiveness of the use of detective analytics, from both technical and non-technical perspectives.

Keywords Actor-network theory, Detective analytics, Financial crime

Categories • Information systems ~ Cross-computing tools and techniques, Design

Email

Nontobeko Mlambo – mlambononto@gmail.com

Tiko Iyamu – iyamut@cput.ac.za (CORRESPONDING)

Article history

Received: 30 May 2024

Accepted: 4 October 2024

Online: 2 July 2025

1 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 (Cole, 2023). The transactions include the 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

Mlambo, N., and Iyamu, T. (2025). The use of detective analytics for mitigating financial crimes: A South African perspective. *South African Computer Journal* 37(1), 45–62. <https://doi.org/10.18489/sacj.v37i1.18697>

Copyright © the author(s); published under a [Creative Commons NonCommercial 4.0 License](https://creativecommons.org/licenses/by-nc/4.0/) 
SACJ is a publication of [SAICSIT](https://www.saicsit.org/). ISSN 1015-7999 (print) ISSN 2313-7835 (online)

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 (Andrade-Rojas et al., 2024). Thus, financial institutions continue to build the security and protection of their assets and finances around these three facets. Financial institutions analyse data, to gain a better understanding and make better financial decisions and help prevent processing of suspicious transactions (Li et al., 2020). 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). It is argued that financial crime is double in low-income countries than it is in high-income countries (Achim et al., 2021). This could be attributed to the sophistication of preventative, detective, and other security measures in high-income countries, using IT solutions. Some financial crimes are detected by financial institutions (Gombiro et al., 2015). However, there are loopholes in the current methods and approaches, hence, the rate of financial crime in South Africa is increasing (Macdonald, 2019). 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 classified in the group 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 et al., 2022), detective analytics uniquely focuses on identifying a problem in data, as and when it occurs (Poornima & Pushpalatha, 2020). In its advancement, detective analytics focuses on performing diagnostics on big data and small data (normal), uncovers and rectifies infeasible events including occurrences (Aliguliyev et al., 2016; Empl & Pernul, 2023). 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 or know how to fully utilise the capabilities of detective analytics (Liu et al., 2021). Secondly, despite its advancement, challenges persist. Thus, the research objective is to gain a deeper understanding on how detective analytics can be applied to mitigate financial crimes in organisations. This prompts the research question, which is: *How can detective analytics be employed for mitigating financial crimes in organisations?* Actor-network theory (ANT) was employed as a lens, to examine human and non-human roles in applying detective analytics, to trace, track, and prevent financial crime in financial organisations.

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

2 PROBLEMATISING THE STUDY

Like many organisations, financial institutions depend on data for their strategic and operational activities. Unfortunately, the data includes processes which are continually infiltrated or manipulated, consciously by actors in criminal activities, and unconsciously by human errors (Akinbowale et al., 2020). Some of these crimes are so severe that the organisation is affected and may shut down, which inevitably has an impact on the livelihood of employees. Thus, institutions are constantly exploring and employing tools and approaches to mitigate financial crimes, which is prohibitive to business continuity. Thus, IT solutions are increasingly relied upon for remedy.

Despite the IT security solutions and preventative tools such as the Financial Intelligence Centre Act (FICA), 2001 (Republic of South Africa [RSA], 2001); Banks Act, 1990 (RSA, 1990); and Inspection of Financial Institutions Act, 1998 (RSA, 1998) that have been deployed in layers, for mitigation purposes, financial crimes are on the increase in South Africa (Chitimira & Ncube, 2021; Sutherland, 2017). Economic crime remains significantly higher than the global average rate of 49% (Thomson, 2024; White, 2018). Consequently, many institutions continue to lose income to criminal activities, which affects their sustainability and competitiveness. Another negative effect is that the affected institutions suffer reputation damage, which takes considerable time to recover from (Kshetri, 2019). These highlighted problems derail economic development and growth and affect individuals' job security in the country. Thus, it is critical to find a fresh and more sophisticated solution to mitigating financial crimes for South African institutions.

3 LITERATURE REVIEW

3.1 Financial crime in institutions

Most financial institutions rely on data, and the growth of data is drastic throughout the whole world (Bataev, 2018). Hundreds of millions of financial transactions occur in financial institutions each day and all these transactions lead to data creation (Hasan & Rizvi, 2022). 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). Financial crime is double in low-income countries compared with high-income countries (Achim et al., 2021). 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). Activities of financial crime seem to be increasing in South Africa. In recent years many financial institutions in South Africa have experienced an increased rate of financial crimes due to the high demand for online transactions (van Niekerk, 2017). Notwithstanding the mitigating approaches implemented by some institutions, technological enhancements are used to commit many financial crimes (Coetzee, 2018).

3.2 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. Data analytics in the financial sector creates opportunities to advance financial management for both customers and organisations (Giebe et al., 2019; Nobanee, 2021). With advances in solutions, most financial problems that exist can be solved by examining the available data, which can be done using data analytics (Andriosopoulos et al., 2019). However, some researchers argue that the advancement of data analytics in the financial sector has not been thoroughly explored (López-Robles et al., 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 has occurred in the past using historical data (Janakiraman & Ayyanathan, 2022). While diagnostic analytics focuses on historical data, to gain a deeper understanding of the reason behind certain outcomes (Balali et al., 2020), hence it was mostly used to build insights into why certain events occurred in the way they do (Deshpande et al., 2019). Predictive analytics is used to determine patterns and themes to understand what could happen in the future (Jeble et al., 2018; Selvan & Balasundaram, 2021). From an organisation's perspective, to predict is to forecast a problem or a solution (De Jesús Liriano & Sevillano, 2019).

For many years, financial institutions have been using data analytics to derive patterns that lead to financial criminal activities (Andriosopoulos et al., 2019; Köseoğlu et al., 2022).

Data analytics help to collect relevant data, and to access and integrate the data in providing reports of deeper insights into business operations and productions (Fosso Wamba, 2017). Thus, like other sectors, the use of data analytics has enhanced and enabled the financial sector to make better decisions (Ranjan & Jeyanthi, 2020). Increasingly, many organisations can use data analytics, to explore and visualise data to a simple representation that can be easily understood by both users and managers (Hoang & Bui, 2023).

Despite the benefits that data analytics offers organisations, the financial sector continues to experience an increase in financial crimes (Holzenthall, 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 or know how to fully utilise the capabilities of detective analytics (Liu et al., 2021). Therefore, detective analytics should be critically explored in the financial sector to help combat criminal activities within the institutions.

Among other things, detective analytics is used by organisations, to detect fraudulent activities (Abdallah et al., 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 et al., 2011). Detective analytics is often described 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 (Menezes et al., 2019). Fraud detection is used mostly to detect unknowns and known unknowns (Thornton et al., 2013). This makes detective analytics critical for organisations. Corroboratively, there seems to be an emphasis on 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 & Bhattacharya, 2016).

4 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. A comprehensive justification and a guide for complementarily employing theories have been provided in the literature (Iyamu, 2021).

The ANT is a sociotechnical theory that is used by researchers to explain the relationship

between humans and non-human objects (Iyamu, 2024). There are further explanations on how and why ANT mostly focuses on the formation of networks, the relationship between actors, and shifting negotiation within the actor-network (Sage et al., 2011). This helps to understand how human and non-human actors are involved in an activity or incident (Gao, 2005). An actor-network is formed immediately when the actors have aligned interests (Walsham, 1997), and the actor-networks are formed consciously or unconsciously, based on common understanding (Latour, 1996). In summation, the theory focuses on how networks are built and maintained including 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 (Callon, 1986; Heeks & Stanforth, 2015). “ANT provides a platform which allows for the analysis of both human and non-human interaction in a network” (Iyamu, 2021, p. 73). This means that ANT is a resource for understanding the actions of humans. Congruently, a researcher can draw on ANT to trace information pathways that enable humans to access actions and connect with needed resources (Lefkowitz, 2022). Thus, ANT was employed to provide an underutilised post-humanist lens to understand the creation of collaborative connections between action-based interactions (Kumar & Tissenbaum, 2022).

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).

5 METHODOLOGICAL APPROACH

Based on the focus of the study, the qualitative method was employed. This is because the qualitative method allows an in-depth understanding of the phenomenon being studied (Morgan, 2022). Such understanding is achieved because it allows subjective reasoning and views of the data (Akyildiz & Ahmed, 2021). Additionally, a qualitative method is described as a method that enables an understanding of the factors influencing human behaviours and attitudes in a setting (Iyamu, 2024).

This allows the many realities about human behaviour including events and technology to be explored. 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, some of which have been applied by organisations across the world (Broeders et al., 2017).

Existing materials (documents) were gathered using the document analysis technique. The technique allows the rationalisation of available literature, in the forms of books, newspaper articles, peer-reviewed articles, and technical reports (Morgan, 2022). The data were collected using a set of criteria, to ensure appropriateness. As shown in Table 1, the criteria consist of three groupings:

- i. areas of focus,
- ii. publication dates, and
- iii. credible sources.

Each of the groups was further categorised. The areas of focus include crime in financial institutions, detective analytics and ANT, which are the core aspects of the study. The publication dates were vital, to imbibe context and relevance. Thus, articles 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 et al., 2016). For credibility purposes, the concentration was on peer-reviewed articles. Based on the newness of detective analytics, we could only gather a small-sized collection of literature that was most appropriate and relevant to the study. This type of circumstance is not new as it has been experienced and argued in many IS studies (Nyikana & Iyamu, 2023).

Materials published in journals, books, conference proceedings and the internet between 2013 and 2023 were gathered. A total of 255 articles were collected from databases such as Ebscohost, IEEE, AIS, and Emerald. The databases were used as sources because they host many computing articles and instil 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. Table 1 presents a sample of the papers.

Guided by the objective of the study, which was to gain an understanding of how detective analytics can be applied to mitigate financial crimes in organisations, the data were processed, and meanings were associated in the context of the study. ANT was employed as a lens in the analysis of the data, to gain deeper insights into mitigating financial crimes in organisations. The analysis focuses on three fundamental areas:

- i. to advance an understanding of evidence in the literature on how humans interact with systems and processes that are obligatory to commit financial crimes;
- ii. by following the actors, to gain insights on how actor-networks are formed, consciously or unintended, that lead to financial crimes; and
- iii. a better understanding of actors' relationships and how they interact in committing financial crimes in organisations.

Table 1: Data classification

Focus	Source	Type
Crime in financial institutions	The impact of national culture on financial crime	(Yamen et al., 2019) Journal
	Channels of corruption in Africa: analytical review of trends in financial crimes	(Hope, 2020) Journal
	Does technology matter for combating economic and financial crime? A panel data study	(Achim et al., 2021) Journal
	The world of private investigators in South Africa	(Kempen, 2020) Journal
	Financial crime in South Africa	(De Koker, 2007) Journal
Detective analytics	Digital Transformation: Utilization of Analytics and Machine Learning in Smart Manufacturing	(Vanani & Shaabani, 2021) Book chapter
	Fraud detection system: A survey	(Abdallah et al., 2016) Journal
	Gross error detection and data reconciliation using historical data	(Sun et al., 2011) Journal
	Predictive, prescriptive, and detective analytics for smart manufacturing in the information age	(Menezes et al., 2019) Journal
	Intelligent financial fraud detection: a comprehensive review	(West & Bhattacharya, 2016) Journal
Actor-network theory	Actor-network theory: Trial, trails, and translations	(Kumar & Tissenbaum, 2022) Book chapter
	How actor-network theories can help in understanding project complexities	(Sage et al., 2011) Journal
	Using actor-network theory to analyse strategy formulation	(Gao, 2005) Journal
	Actor-network theory and IS research: current status and future prospects	(Walsham, 1997) Conference proceedings
	On actor-network theory: A few clarifications	(Latour, 1996) Journal
	Applying theories for information systems research	(Iyamu, 2021) Book chapter

6 DATA ANALYSIS

As presented in the section that follows including Table 2 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 2 reveals how ANT helps to gain a deeper understanding of the relationship that exists between the actors in the process of executing financial transactions. This includes committing a financial crime or attempting to mitigate the financial crime. In Table 3, the implications of the factors are explained. This includes how activities of financial transactions are connected and lead to crime.

From ANT, a social context perspective, five factors were found to be crucial points in

Table 2: Findings from the analysis

ANT Tenet	ANT Translative view	Factor
Actor-network	Detective analytics integrates multiple operations, scales, scenarios, and layers (Al-Banna et al., 2023). The multiplexity consists of actor-networks, of humans and non-humans. Both humans and non-humans are interwoven, which means that they cannot be separated. For example, humans and non-humans play roles for a financial transaction to occur. The actor-networks leverage automation of processes based on centralised data, to detect crime patterns across enterprise-wide.	Seamlessly integrates incident
Follow the actors	Detective analytics enacts real-time and offline operations, in detecting compromising incidents. Also, 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 to connect disparate data across an enterprise.	Cybersecurity detection
Obligatory passage points	The concept of obligatory passage point (OPP) infuses tacit knowledge into members of a unit (an actor-network), to maintain a common translation of fraud-related actions and gain a better understanding. OPP is used to facilitate and filter the appropriateness of action that is congruent with the agreed 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 mitigating financial crimes. Thus, OPP brings a different dimension that reveals the roles and identities including recognition of the actors. The translation of obligated processes and rules are required, in following the actors (Latour, 1996). This is a crucial dynamic in the use of detective analytics for the diagnosis of evens, to induce consistency and accuracy.	In-house fraud detection
Black box	By following the actors, it can lead to opening a black box, to gain new insights. Transaction of the new insights leads to discovering of the links and interactions between human and non-human actors, in a financial transaction. Following the actors over time and across a multitude is an important means of analysis, to gain insights. Also, opening the black boxes and examining the ontology of the actor-networks can lead to the construction of new dynamics.	External infiltrate detection
Actor-network	Detective analytics expands the accuracy capability of IT solutions. Detective analytics induces a level of preciseness in its operations on veracity, volume, variety, and velocity of data (Menezes et al., 2022). It advances detective analytics to detect inconsistencies including image recognition in big data and small data.	Image-matching data into one cohesive system

following the actors to mitigate financial crime in an organisation. The factors are:

- i. Seamless integration of incidents,
- ii. Cybersecurity detection,
- iii. In-house fraud detection,
- iv. External infiltrate detection, and
- v. Image-matching data into one cohesive system.

The discussion that follows should be read with Tables 2 and 3, to gain a better understanding.

Table 3: Implication of the study

Factor	Technical	Non-technical
Seamlessly integrates incident	It enables the automation of processes and resolves fragmentations. Also, it enables the synchronisation of processes in following the actors. By doing so, it removes manual monitoring and reactive response to fraudulent incidents.	Distinction of actors' roles and defining the communication channel within the structure of the environment. Incident management must be enabled using automated processes, to actively remediate reported incidents.
In-house fraud detection	It must promulgate a policy that allows connectivity to enable and support the centralisation of systems and processes. Thus, the detective approach can enable enterprise-wide and connect processes and databases.	Employees and relevant authorities must understand how to follow the actors. Thus, operations and investigations of fraudulent transactions and activities can be fortified. Requirements must be defined and used to follow.
Cybersecurity detection	Cyber activities involve nodes and networks of actors. Thus, it requires an understanding of the fundamentals of detecting and responding to cybersecurity incidents by following the actors.	Employees and relevant authorities must understand how to link activities and associated events. Therefore, documentation and reporting of cybersecurity incidents require a special approach for communicating security breaches.
External infiltrate detection	Employs tools for tracing external links that explore internal leaks. Response time finds millions of link connections per second and minute.	Social engineering attacks are human interactions used to manipulate security procedures. A process must be developed to mitigate this activity.
Image-matching data into one cohesive system	Following the actors early enough helps to detect when an actor transforms or impersonates himself or herself. Cohesiveness increases accuracy through its integrated approach to fraud prevention.	It requires the configuration of rules and intents within an organisation. Fraud categorisation-based rules help to ease processing and anomaly detection.

7 DISCUSSION OF THE FINDINGS

The factors revealed from the analysis: Seamless integration of incidents, Cybersecurity detection, In-house fraud detection, External infiltrate detection, and Image-matching data into one cohesive system are interrelated in committing or detecting financial crimes in organisations. Seamless integration refers to the smooth and efficient connection between processes and computer technology such as detective analytics. Seamless integration of technology has been demonstrated to eliminate insertion and mismatch of incidents, from internal and external intrusion to image matching. Cybersecurity detection is an aspect of IT solutions focusing on activities including images in cyberspace. The solution is intended to detect and recognise fraudulent activities as they occur within an organisation (Abdallah et al., 2016). Financial cybercrime could be orchestrated from in-house or externally. In-house fraud detection discovers and identifies fraudulent financial activities within an organisation. The detection system is used to follow and trace actors' financial activities as they try to enter an organisation's space and commit a crime.

Correspondingly, some activities and actions involved unregulated and unprecedented movements. Consequently, organisations are increasingly employing detective analytics to manage and promote their business efficacy (Iyamu, 2022). However, 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. 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 “material as well as social, physical as well as semiotic” (Michael, 2017, p. 41). ANT’s mantra is “to follow the actors” (Boodhun & Jayabalan, 2018, p. 12) that are not exclusively human but non-human parts of interactions within networks. 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 dynamic 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 (Aliguliyev et al., 2016; Empl & Pernul, 2023). 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 non-human.

The syntax is discovered as we follow the actors. Complementarily, using detective analytics, explicitly, ensures the timeliness, consistency, and integration of big data, in recognising activities and traces of events in an environment (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. Revealed in the literature, there is evidence of financial crimes and it is argued 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 (Hope, 2020). 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 non-human 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%.

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. The increase in financial crime is due to the emerging technologies that institutions adopt to enhance processes (West & Bhattacharya, 2016). Thus, there is a need to explore how the use of detective analytics as a mechanism can be used to detect financial crime.

8 IMPLICATION OF THE STUDY

The factors that manifest from using ANT to examine the use of detective analytics are Seamless integration of incidents, In-house fraud detection, Cybersecurity detection; External infiltrate detection; and Image-matching data into one cohesive system. Each of the factors has both technical and non-technical implications, as tabulated in Table 3. Fundamentally, the implication can provide guidelines on how humans interpret and apply rules in carrying out financial transactions in an organisation. This includes how detective analytics integrate with other tools or systems, to mitigate financial crime.

9 CONTRIBUTION OF THE STUDY

This study is intended to serve as a comprehensive work and extend detective analytics for mitigating financial crimes, in the literature. This study focuses on articles published between 2013 and 2023. In lieu of the other studies on detective analytics available thus far in the literature, this study makes the following three main contributions:

- i. It adds to the literature on detective analytics by providing a nuanced perspective on mitigating financial crimes, from both business and IT perspectives.
- ii. It demonstrates the advancement of ANT, in gaining a better understanding of complex organisational phenomena.
- iii. It reveals the need for a continual comprehensive investigation of advances in detecting and mitigating financial crimes in organisations. It thus suggests that organisations need to focus on advancing detection capability.

10 CONCLUSION

This study highlights the critical challenges faced by organisations in mitigating financial crime due to the constraint 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. Nonetheless, 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. <https://doi.org/10.1016/j.jnca.2016.04.007>
- 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. <https://doi.org/10.3846/tede.2021.13977>
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime*, 27(3), 945–958. <https://doi.org/10.1108/jfc-03-2020-0037>
- Akyildiz, S. T., & Ahmed, K. H. (2021). An overview of qualitative research and focus group discussion. *International Journal of Academic Research in Education*, 7(1), 1–15. <https://doi.org/10.17985/ijare.866762>
- Al-Banna, A., Menezes, B. C., Yaqot, M., & Kelly, J. D. (2023). Decision regression for modeling of supply chain resilience in interdependent networks: LNG case. In *33rd European symposium on computer aided process engineering* (pp. 1113–1118). Elsevier. <https://doi.org/10.1016/b978-0-443-15274-0.50178-5>
- Aliguliyev, R., Imamverdiyev, Y., & Abdullayeva, F. (2016). The investigation of the opportunities of big data analytics as analytics-as-a-service in cloud computing for oil and gas industry. *Problems of Information Technology*, 07(1), 9–22. <https://doi.org/10.25045/jpit.v07.i1.02>
- Andrade-Rojas, M. G., Saldanha, T. J. V., Kathuria, A., Khuntia, J., & Boh, W. (2024). How information technology overcomes deficiencies for innovation in small and medium-sized enterprises: Closed innovation vs. open innovation. *Information Systems Research*. <https://doi.org/10.1287/ISRE.2021.0096>
- 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. <https://doi.org/10.1080/01605682.2019.1595193>
- Balali, F., Nouri, J., Nasiri, A., & Zhao, T. (2020). Data analytics. In *Data intensive industrial asset management* (pp. 105–113). Springer International Publishing. https://doi.org/10.1007/978-3-030-35930-0_7
- Bataev, A. V. (2018). Evaluation of using big data technologies in Russian financial institutions. *Proceedings of the 2018 International Conference “Quality Management, Transport and Information Security, Information Technologies”*, 573–577. <https://doi.org/10.1109/ITMQIS.2018.8524938>
- Boodhun, N., & Jayabalan, M. (2018). Risk prediction in life insurance industry using supervised learning algorithms. *Complex & Intelligent Systems*, 4(2), 145–154. <https://doi.org/10.1007/s40747-018-0072-1>

- Broeders, D., Schrijvers, E., van der Sloot, B., van Brakel, R., de Hoog, J., & Hirsch Ballin, E. (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. <http://doi.org/10.1016/j.clsr.2017.03.002>
- Callon, M. (1986). The sociology of an actor-network: The case of the electric vehicle. In *Mapping the dynamics of science and technology* (pp. 19–34). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-07408-2_2
- Chitimira, H., & Ncube, P. (2021). The regulation and use of artificial intelligence and 5G technology to combat cybercrime and financial crime in South African banks. *Potchefstroom Electronic Law Journal*, 24, 1–33. <https://doi.org/10.17159/1727-3781/2021/v24i0a10742>
- Cockcroft, S., & Russell, M. (2018). Big data opportunities for accounting and finance practice and research. *Australian Accounting Review*, 28(3), 323–333. <https://doi.org/10.1111/auar.12218>
- Coetzee, J. (2018). Strategic implications of Fintech on South African retail banks. *South African Journal of Economic and Management Sciences*, 21(1). <https://doi.org/10.4102/sajems.v21i1.2455>
- Cole, T. (2023). How are financial institutions enabling online fraud? A developmental online financial fraud policy review. *Journal of Financial Crime*, 30(6), 1458–1473. <https://doi.org/10.1108/JFC-10-2022-0261>
- De Jesús Liriano, R., & Sevillano, M. C. (2019). Improving the learning process in the higher education through the use of a predictive tool (dashboard). *Distance Learning*, 16(1), 33–40. <https://eric.ed.gov/?id=EJ1299603>
- De Koker, L. (2007). Financial crime in South Africa. *Economic Affairs*, 27(1), 34–38. <https://doi.org/10.1111/j.1468-0270.2007.00707.x>
- Deshpande, P. S., Sharma, S. C., & Peddoju, S. K. (2019). *Security and data storage aspect in cloud computing*. Springer Singapore. <https://doi.org/10.1007/978-981-13-6089-3>
- Empl, P., & Pernul, G. (2023). Digital-twin-based security analytics for the internet of things. *Information*, 14(2), 95. <https://doi.org/10.3390/info14020095>
- Fosso Wamba, S. (2017). Big data analytics and business process innovation. *Business Process Management Journal*, 23(3), 470–476. <https://doi.org/10.1108/bpmj-02-2017-0046>
- Gao, P. (2005). Using actor-network theory to analyse strategy formulation. *Information Systems Journal*, 15(3), 255–275. <https://doi.org/10.1111/j.1365-2575.2005.00197.x>
- Giebe, C., Hammerström, L., & Zwerenz, D. (2019). Big data & analytics as a sustainable customer loyalty instrument in banking and finance. *Financial Markets, Institutions and Risks*, 3(4), 74–88. [https://doi.org/10.21272/fmir.3\(4\).74-88.2019](https://doi.org/10.21272/fmir.3(4).74-88.2019)
- 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. https://doi.org/10.22495/jgr_v4_i4_c6_p8

- Hasan, I., & Rizvi, S. (2022). AI-driven fraud detection and mitigation in e-commerce transactions. *Lecture Notes on Data Engineering and Communications Technologies*, 90, 403–414. https://doi.org/10.1007/978-981-16-6289-8_34
- 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. <https://doi.org/10.1080/21665095.2015.1026610>
- Hoang, T. G., & Bui, M. L. (2023). Business intelligence and analytic (BIA) stage-of-practice in micro-, small- and medium-sized enterprises (MSMEs). *Journal of Enterprise Information Management*, 36(4), 1080–1104. <https://doi.org/10.1108/jeim-01-2022-0037>
- Holzenthal, F. (2017). Five trends shaping the fight against financial crime. *Computer Fraud & Security*, 2017(3), 5–9. [https://doi.org/10.1016/s1361-3723\(17\)30022-2](https://doi.org/10.1016/s1361-3723(17)30022-2)
- Hope, K. R. (2020). Channels of corruption in Africa: Analytical review of trends in financial crimes. *Journal of Financial Crime*, 27(1), 294–306. <https://doi.org/10.1108/jfc-05-2019-0053>
- Iyamu, T. (2024). *The application of sociotechnical theories in information systems research*. London: Cambridge Scholar Press.
- Iyamu, T. (2021). *Applying theories for information systems research*. Routledge. <https://doi.org/10.4324/9781003184119>
- Iyamu, T. (2022). *Advancing big data analytics for healthcare service delivery*. Routledge. <https://doi.org/10.4324/9781003251064>
- 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. <https://academic-publishing.org/index.php/ejise/article/view/159>
- Janakiraman, S., & Ayyanathan, N. (2022). Design and development of big data framework using NoSQL–MongoDB and descriptive analytics of Indian green coffee export demand modeling. In *Disruptive technologies for big data and cloud applications* (pp. 777–785). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-2177-3_72
- 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. <https://doi.org/10.1108/ijlm-05-2017-0134>
- Kempen, A. (2020). The world of private investigators in South Africa. *Servamus Community-based Safety and Security Magazine*, 11(113), 34–37. <https://hdl.handle.net/10520/ejc-servamus-v113-n11-a12>
- Köseoglu, S. D., Ead, W. M., & Abbassy, M. M. (2022). Basics of financial data analytics. In *Financial data analytics* (pp. 23–57). Springer International Publishing. https://doi.org/10.1007/978-3-030-83799-0_2
- Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77–81. <https://doi.org/10.1080/1097198x.2019.1603527>

- 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. <https://doi.org/10.1111/bjet.13274>
- Latour, B. (1996). On actor-network theory: A few clarifications. *Soziale Welt*, 47, 369–381. <https://www.jstor.org/stable/40878163>
- Lee, C. S., Cheang, P. Y. S., & Moslehpour, M. (2022). Predictive analytics in business analytics: Decision tree. *Advances in Decision Sciences*, 26, 1–29. <https://doi.org/10.47654/V26Y2022I1P1-30>
- Lefkowitz, D. (2022). Black boxes and information pathways: An actor-network theory approach to breast cancer survivorship care. *Social Science & Medicine*, 307, 115184. <https://doi.org/10.1016/j.socscimed.2022.115184>
- Lezaun, J. (2017). Actor-network theory. In *Social theory now*. The University of Chicago Press.
- Li, J., Li, J., Zhu, X., Yao, Y., & Casu, B. (2020). Risk spillovers between FinTech and traditional financial institutions: Evidence from the U.S. *International Review of Financial Analysis*, 71, 101544. <https://doi.org/10.1016/J.IRFA.2020.101544>
- 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. <https://doi.org/10.1016/j.jbusres.2019.04.042>
- 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. <https://doi.org/10.1016/j.procs.2019.12.044>
- 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. <https://doi.org/10.4324/9780429401749-15>
- Menezes, B., 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. <https://doi.org/10.1016/j.ifacol.2019.06.123>
- Menezes, B., Yaqot, M., Hassaan, S., Franzoi, R., AlQashouti, N., & Al-Banna, A. (2022). Digital transformation in the era of Industry 4.0 and Society 5.0: A perspective. *2022 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, 1–6. <https://doi.org/10.1109/esmarta56775.2022.9935399>
- Michael, M. (2017). *Actor-network theory: Trials, trails and translations*. SAGE Publications Ltd. <https://doi.org/10.4135/9781473983045>
- Minniti, S., & Magaudda, P. (2024). The 'obligatory passage point' in knowledge co-production: Italy's participatory environmental monitoring platform. *Science as Culture*, 34(1), 13–30. <https://doi.org/10.1080/09505431.2024.2317236>

- Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*. <https://doi.org/10.46743/2160-3715/2022.5044>
- Nobanee, H. (2021). A bibliometric review of big data in finance. *Big Data*, 9(2), 73–78. <http://s://doi.org/10.1089/big.2021.29044.edi>
- 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. <https://doi.org/10.4018/978-1-6684-5959-1.ch010>
- Poornima, S., & Pushpalatha, M. (2020). A survey on various applications of prescriptive analytics. *International Journal of Intelligent Networks*, 1, 76–84. <https://doi.org/10.1016/j.ijin.2020.07.001>
- Ranjan, J., & Jeyanthi, M. P. (2020). Big data analytics in the healthcare industry. In *Global business leadership development for the fourth industrial revolution* (pp. 134–154). IGI Global. <https://doi.org/10.4018/978-1-7998-4861-5.ch006>
- Republic of South Africa. (1990). *Banks Act (previously known as deposit-taking institutions Act) 94 of 1990* [Retrieved June 13, 2025]. <https://www.gov.za/documents/deposit-taking-institutions-act-6-mar-2015-1030>
- Republic of South Africa. (1998). *Inspection of financial institutions Act 80 of 1998* [Retrieved June 13, 2025]. <https://www.gov.za/documents/inspection-financial-institutions-act>
- Republic of South Africa. (2001). *Financial intelligence centre Act 38 of 2001* [Retrieved June 13, 2025]. <https://www.gov.za/documents/financial-intelligence-centre-act>
- 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. <https://doi.org/10.1108/175383711111120243>
- 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. <https://doi.org/10.4018/978-1-7998-3053-5.ch006>
- 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. <https://doi.org/10.1016/j.telpol.2015.11.005>
- Sun, S., Huang, D., & Gong, Y. (2011). Gross error detection and data reconciliation using historical data. *Procedia Engineering*, 15, 55–59. <https://doi.org/10.1016/j.proeng.2011.08.012>
- 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. <https://doi.org/10.1016/J.TRIP.2022.100590>
- Sutherland, E. (2017). Governance of cybersecurity – The case of South Africa. *The African Journal of Information and Communication (AJIC)*, (20), 83–112. <https://doi.org/10.23962/10539/23574>

- Thomson, D. (2024). Navigating the new era of financial resilience: Preparing for Dora [Retrieved 4 August 2024]. <https://www.bizcommunity.com/article/navigating-the-new-era-of-financial-resilience-preparing-for-dora-903064a>
- Thornton, D., Mueller, R. M., Schoutsen, P., & van Hillegersberg, J. (2013). Predicting health-care fraud in Medicaid: A multidimensional data model and analysis techniques for fraud detection. *Procedia Technology*, 9, 1252–1264. <https://doi.org/10.1016/j.protcy.2013.12.140>
- van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, (20). <https://doi.org/10.23962/10539/23573>
- Vanani, I. R., & Majidian, S. (2021). Prescriptive analytics in internet of things with concentration on deep learning. In *Introduction to internet of things in management science and operations research* (pp. 31–54). Springer International Publishing. https://doi.org/10.1007/978-3-030-74644-5_2
- Vanani, I. R., & Shaabani, A. (2021). Digital transformation. In *Artificial intelligence, machine learning, and data science technologies* (pp. 269–281). CRC Press. <https://doi.org/10.1201/9781003153405-14>
- Walsham, G. (1997). Actor-network theory and IS research: Current status and future prospects. In *Information systems and qualitative research* (pp. 466–480). Springer US. https://doi.org/10.1007/978-0-387-35309-8_23
- West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, 47–66. <https://doi.org/10.1016/j.cose.2015.09.005>
- White, T. (2018). Reported economic crime in South Africa hits record levels; cost and accountability concerns rising [Retrieved June 2022]. <https://pricewaterhousecoopers-pwc.africa-newsroom.com/press/reported-economic-crime-in-south-africa-hits-record-levels-cost-and-accountability-concerns-rising?lang=en>
- 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. <https://doi.org/10.1108/jmlc-01-2018-0004>
- Yeoh, P. (2019). Artificial intelligence: Accelerator or panacea for financial crime? *Journal of Financial Crime*, 26(2), 634–646. <https://doi.org/10.1108/jfc-08-2018-0077>