Leveraging AI to address SIM swap fraud during 2G/3G shutdown

Marvel Mandaza

Supervisor: Professor Patrick Ndayizigamiye

A research project submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2024

DECLARATION

I, Marvel Mandaza, declare that this research report is my own, unaided work. It is being submitted in partial fulfilment of the requirements for the degree of Master of Management in Digital Business at Wits Business School, University of the Witwatersrand, Johannesburg.

I further declare that:

- This report has not been submitted previously for any degree or examination at any other university or institution.
- All sources used have been acknowledged through appropriate referencing, and no part of this report has been plagiarised.
- I have adhered to the ethical research guidelines as stipulated by Wits Business School.

Signed: Marvel Mandaza

……

Date: ……

ACKNOWLEDGEMENTS

Firstly, my deepest appreciation goes to my family. Their patience and understanding have been invaluable as I balanced my commitments across academics, work, and personal life.

I am also deeply grateful to my employer, whose generosity and flexibility have made it possible for me to dedicate the necessary time and resources to this research.

Lastly, I would like to recognise and thank my academic supervisor, Professor Patrick Ndayizigamiye. His expertise, insightful guidance, and constructive feedback were instrumental in shaping this research.

ABSTRACT

This research explores the potential of artificial intelligence (AI) as a safeguard against SIM (subscriber identity module) swap fraud in the evolving landscape of the global 2G/3G network shutdown. As the telecommunications industry transitions to more advanced 4G and 5G networks, phasing out of older 2G/3G infrastructure could inadvertently create new vulnerabilities that fraudsters may exploit. SIM swap fraud, where attackers gain unauthorised control of a victim's mobile number, is particularly concerning during this period, as it enables interception of sensitive communications like one-time passwords, which can compromise financial accounts and personal information. Thus, this study assessed AI's capacity to address these emerging risks. Using a systematic literature review grounded in the PRISMA framework, this research offers a comprehensive evaluation of the current knowledge base.

Through bibliometric analysis, this work identifies key trends, influential publications, and leading researchers focused on AI-driven fraud prevention in telecommunications. This analytical approach yields a data-driven perspective on the field, highlighting influential areas and collaborative networks that shape the ongoing discourse around fraud mitigation amid network transitions. The findings indicate notable gaps in the existing literature and highlights high-impact studies, establishing a solid foundation for further research.

In addition, a thematic analysis delves into recurring patterns across the reviewed literature, identifying significant themes such as AI's role in anomaly detection, the prevention of social engineering attacks, and predictive analytics. This method categorises new fraud tactics arising during the 2G/3G shutdown, along with the specific security vulnerabilities that emerge in this transition phase. By examining these themes, the study illustrates AI's potential to identify fraudulent activities in real time and strengthen security within customer service contexts, where social engineering remains a critical threat.

Ultimately, this research contributes actionable insights for AI-driven security measures in the telecommunications sector. The findings aim to inform telecom operators, financial institutions, and policymakers in crafting effective strategies to combat fraud, acknowledging the complex challenges that arise from decommissioning legacy networks.

*Keywords**:** Artificial Intelligence, SIM Swap Fraud, 2G/3G Shutdown*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

- AI: Artificial Intelligence
- SIM: Subscriber Identity Module
- PRISMA: Preferred Reporting Items for Systematic Reviews and Meta-Analyses

CHAPTER 1. INTRODUCTION

1.1 Statement of purpose

This research examines the potential of artificial intelligence (AI) to mitigate SIM (subscriber identity module) swap fraud, particularly within the context of the 2G/3G network shutdown. The phasing out of these legacy networks appears to have increased vulnerabilities, providing an opportunity for fraudsters to exploit weaknesses in the transitional period. In response, this study employs a systematic literature review to analyse how these vulnerabilities are being targeted and to assess AI's effectiveness as a countermeasure.

Adhering to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Page *et al*., 2020) ensured a rigorous and transparent search strategy that minimised bias and strengthened the reliability of findings. By focusing on AI's potential to tackle SIM swap fraud in the wake of 2G/3G decommissioning, the review aims to provide a comprehensive overview of relevant studies, offering both breadth and depth on this issue.

This research addresses the heightened concern regarding increased criminal activity associated with the legacy network phase-out. Fraudsters may exploit these newly exposed vulnerabilities, often targeting populations that remain reliant on 2G/3G devices and SIM cards. AI, with its advanced capabilities in pattern recognition and anomaly detection, emerges as a promising tool for countering such sophisticated threats.

Findings from this study offer insights specific to the South African telecommunications sector, where the interplay between technological advancement and evolving criminal tactics requires continuous adaptation. By identifying and evaluating AI-based strategies, this research seeks to guide the

development of targeted interventions and policies aimed at reducing SIM swap fraud. Furthermore, the study aligns with the South African government's investment in AI for crime prevention, as outlined in the National AI Strategy (Department of Communications and Digital Technologies, 2023), highlighting AI's strategic role in safeguarding digital infrastructures against fraud.

1.2 Background of the study

South Africa's mobile telecommunications landscape is undergoing a transformative shift with the planned shutdown of 2G and 3G networks (GSMA, 2023). While this migration to 4G and 5G networks offers the promise of faster speeds and enhanced connectivity, it simultaneously introduces security risks, most notably an apparent rise in SIM swap fraud (iiDENTIFii, 2024).

SIM swap fraud, a prevalent cybercrime in South Africa (Cooper, 2024), involves fraudsters impersonating legitimate users to persuade mobile network operators to transfer the victim's phone number to a SIM card under their control. Once they gain control of the number, these perpetrators can intercept one-time passwords and access other sensitive data, facilitating unauthorised transactions and enabling identity theft.

South Africa's susceptibility to SIM swap fraud can be attributed to several factors. With a high mobile phone penetration rate, the country presents a large target pool for potential fraud (World Bank, 2024). Additionally, recent parliamentary hearings have highlighted shortcomings in identity verification processes at mobile network operators, raising concerns about the ease with which criminals can obtain fraudulent documentation to carry out SIM swaps (Parliamentary Monitoring Group, 2023).

Despite efforts by mobile network operators to implement anti-fraud measures, such as biometric authentication and awareness campaigns (MTN Group, 2022;

Vodacom Group, 2022), the complexity of migrating millions of users from legacy networks presents fresh vulnerabilities. This transition phase, marked by potential customer service delays and operational challenges, could be exploited by fraudsters, leveraging any confusion to deceive both users and mobile network staff.

The escalating sophistication of AI-powered tools also intensifies the risk (Whitman & Mattord, 2023). Deepfake technologies now enable fraudsters to convincingly mimic voices to deceive customer service representatives, while AI-driven phishing techniques can manipulate users into divulging sensitive information.

This convergence of factors, the network shutdown, existing security gaps, and the evolution of cybercrime tactics, emphasises the need for a proactive and robust response to protect users and financial systems. Given AI's potential to detect and prevent fraud, this research investigates how AI might be effectively harnessed to mitigate the expected rise in SIM swap fraud during this critical transition period.

1.3 Research problem

The rapid shift from 2G and 3G networks to more advanced 4G and 5G technologies brings a mix of both promising opportunities and complex challenges. While these modern networks offer notable improvements, including enhanced security, higher data transfer rates, and reduced latency, they also usher in a period of increased vulnerability during the transition (African Wireless Communications, 2024). Among these emerging threats, SIM swap fraud stands out as a growing concern, a cybercrime tactic where fraudsters assume control of a victim’s mobile number to intercept calls and messages, especially those used for two-factor authentication, enabling access to the victim’s financial and personal information (SABRIC, 2022). With the increasing sophistication of SIM

swap tactics, coupled with the reliance on mobile phones for banking and authentication, the urgency to address this threat through innovative approaches, such as AI, becomes ever more pressing.

The core of the research problem lies in the new vulnerabilities exposed by the global shutdown of 2G and 3G networks, a move aimed at promoting the uptake of more efficient 4G and 5G services. These legacy networks remain widely used, especially in developing regions with high mobile penetration but where smartphone usage is less prevalent (SABRIC, 2022). During the transition phase, as devices and infrastructure undergo upgrades, an environment ripe for exploitation by fraudsters is inadvertently created.

The risks associated with the 2G/3G shutdown are amplified by the rapid rise in mobile banking, a sector that has grown significantly worldwide. Mobile banking's convenience has driven a surge in adoption, a trend further accelerated by the COVID-19 pandemic, which heightened reliance on digital services (SABRIC, 2022). As more individuals engage in financial transactions on mobile devices, SIM swap fraud becomes an increasingly lucrative target for cybercriminals.

Historically, before the emergence of AI, various control measures were implemented to combat SIM swap fraud. These included enhanced customer verification procedures, account alerts, restrictions on remote SIM swap requests, educational campaigns, network security measures, partnerships with financial institutions, and regulatory compliance frameworks. Although effective in bolstering verification, raising awareness, and improving technical security, these strategies often focus on procedural and technical aspects rather than leveraging predictive or dynamic technologies like AI (Murugalakshmi & Robin, 2023).

AI now offers promising possibilities for combating SIM swap fraud through advanced analytics, machine learning, and pattern recognition (Nguyen *et al*., 2022). By processing vast datasets, AI systems can identify irregularities and

suspicious patterns indicative of a SIM swap attempt. However, despite AI's potential, its application in the context of network transitions and the specific vulnerabilities of the 2G/3G shutdown remains underexplored. This research thus seeks to bridge this gap, examining how AI can be effectively applied to address the unique challenges that arise during these critical network transitions.

The research problem addresses knowledge gaps across three primary areas, namely:

1. Identification of new vulnerabilities: This dimension investigates which SIM swap vulnerabilities emerged because of the 2G/3G network shutdown.
2. Identification of evolving trends: This dimension explores how SIM swap fraudsters adapted their tactics to exploit opportunities presented by network migration.
3. Implementation of suitable threat countermeasures: This dimension examines how AI technologies could offer effective countermeasures for mitigating SIM swap vulnerabilities.

This research seeks to address these critical gaps by utilising AI to develop robust strategies for countering SIM swap fraud during network transition. The aim is to strengthen the security of mobile banking and financial services in South Africa, protecting users against the heightened risks associated with this period of technological change. Through AI-driven insights, this study aspires to contribute to a safer digital environment by mitigating vulnerabilities that fraudsters could exploit amidst the shift from legacy to advanced network systems.

1.4 Research objectives

Given the identified research problem and its three dimensions, this study aimed to achieve the following objectives:

1. To outline the research landscape and identify critical trends and gaps in the literature related to the application of AI to address SIM swap fraud during the 2G/3G network shutdown.
2. To investigate how advancements in mobile technology, specifically the shutdown of 2G and 3G networks in favour of 4G and 5G, created new vulnerabilities for SIM swap attacks.
3. To understand the evolving tactics and techniques employed by fraudsters in response to these technological changes.
4. To evaluate the application of AI as a potential solution for addressing SIM swap fraud.

In achieving these objectives, this research aims to contribute meaningfully to the growing body of knowledge on employing AI to mitigate SIM swap fraud risks amid the 2G/3G network shutdown. By focusing on AI-driven approaches within this specific transitional context, the study not only addresses immediate security concerns but also provides insights that may inform future strategies for fraud prevention as telecommunications networks continue to evolve.

1.5 Rationale

The growing sophistication of SIM swap fraud, fuelled by advancements in AI-driven tools like deepfakes and increasingly refined social engineering tactics (Whitman & Mattord, 2023), draw attention to the need for a proactive and innovative response to this evolving threat (iiDENTIFii, 2024). With high global mobile phone penetration and an ever-increasing dependence on mobile banking services, conditions are ripe for such fraudulent activities to proliferate. The impending shutdown of 2G and 3G networks has further exacerbated these challenges, creating new vulnerabilities as mobile networks transition to 4G and 5G technologies (African Wireless Communications, 2024).

While AI presents promising avenues for detecting and preventing fraud, its specific application to counter SIM swap fraud in the context of widespread network transitions remains largely under-explored. To address this gap, this study undertook a systematic literature review, providing several critical insights and benefits that aim to advance understanding in this area. Key highlights of the review are:

- Comprehensive overview: This systematic literature review collated and synthesised existing research on AI applications in fraud detection, both on a global scale and within similar network transition contexts. This broad yet focused overview enabled a deeper understanding of the current state of knowledge, illuminating potential methodologies while also identifying areas ripe for further investigation.
- Identification of best practices: By analysing successful AI implementations in fraud prevention across various scenarios, the review identified best practices and common pitfalls. These insights were instrumental in shaping contextually relevant solutions, helping to adapt proven strategies to the specific challenges posed by SIM swap fraud in South Africa.
- Gap analysis: The review conducted a targeted gap analysis, pinpointing specific areas where research remains limited. Notably, it revealed a lack of studies on AI applications specifically designed to address the unique security risks associated with network shutdowns. This analysis provides a foundation for future research efforts.
- Evidence-based recommendations: Based on the review's findings, evidence-based recommendations were developed for key stakeholders, including mobile network operators, financial institutions, and policymakers. These recommendations aim to guide the creation of effective, context-sensitive strategies to mitigate SIM swap fraud risks

during the transitional period, ensuring a proactive approach to safeguarding users.

Through this systematic literature review, the research sought to establish a robust foundation for the development of AI-powered solutions tailored to the specific challenges presented by network transitions. The insights gained not only enhance consumer protection efforts but also offer valuable guidance for telecommunications markets facing similar transitions globally. By focusing on the nuanced vulnerabilities that arise during such technological shifts, this study contributes meaningfully to the broader discourse on safeguarding digital infrastructure and stresses the critical role of AI in advancing security within the telecommunications sector.

1.6 Delimitations of the study

This research, while aiming to provide meaningful insights into the use of AI in combating SIM swap fraud during the 2G/3G network shutdown, recognises certain delimitations that may influence the scope and generalisability of its findings. For instance, the focus on specific geographic and technological contexts may limit the applicability of the results to regions or markets with dissimilar conditions. Furthermore, the study's reliance on existing literature, rather than empirical testing of AI models, constrains its conclusions to theoretical implications, which may not fully capture the complexities encountered in practical applications. By acknowledging these delimitations, the research points out the need for further empirical studies to validate and expand upon its findings, ultimately strengthening the foundations for AI-driven fraud prevention strategies in dynamic network environments. The main delimitations identified for this study were:

- Technological focus: This research was specifically concentrated on AI-driven solutions for detecting and preventing SIM swap fraud. While

acknowledging that other technological approaches may exist, these alternatives were beyond the scope of this study and, consequently, were not explored in depth.

- Timeframe: The study focused on the current state of SIM swap fraud and the application of AI within the context of the ongoing 2G/3G network shutdowns. Although the findings may offer insights with future relevance, the study did not aim to predict long-term trends or technological advancements beyond this transitional period.
- Research design: The research employed a systematic literature review, providing a rigorous and comprehensive overview of existing studies. However, it is important to note that this methodology may not fully capture the intricacies and challenges encountered in real-world applications of AI for fraud prevention, which could limit the practical applicability of some findings.

By acknowledging these delimitations, the study sought to provide a transparent and grounded assessment of its scope and potential impact. Although tailored to the context of the 2G/3G network shutdowns, the findings offer a foundational basis for future research and the formulation of targeted solutions to combat SIM swap fraud within an evolving technological landscape. Recognising these boundaries enabled the research to maintain a focused and manageable scope, allowing for an in-depth exploration of AI's potential in addressing the specific vulnerabilities that arise from network transitions. This approach not only enhances the clarity of the study's contributions but also reinforces its relevance as a stepping stone for further empirical investigations and practical applications in this area.

1.7 Definition of terms

To ensure clarity and precision, this section defines key terms and concepts central to this research. Establishing these definitions provides a shared

understanding of the terminology used throughout the dissertation, facilitating consistent interpretation, and helping readers navigate the specialised language associated with SIM swap fraud, AI applications, and network transitions. By clearly delineating these terms, this section aims to reduce ambiguity and enhance the coherence of the study. The key definitions for this research are as follows:

- Artificial intelligence (AI): A broad field concerned with the theory and development of computer systems capable of performing tasks that traditionally require human intelligence, such as visual perception, speech recognition, decision-making, and language translation (Russell & Norvig, 2021). Within the scope of this study, AI specifically refers to machine learning algorithms and techniques applied for fraud detection and prevention.
- SIM swap fraud: A type of identity theft in which a fraudster deceives a mobile network operator into transferring a victim's phone number to a SIM card controlled by the fraudster. This enables the interception of SMS messages containing one-time passwords or other sensitive data, potentially compromising bank accounts, social media profiles, and various online services (Cooper, 2024).
- Mobile network operator: An entity that provides wireless communication services to mobile phone users. In South Africa, major mobile network operators include Vodacom, MTN, Cell C, and Telkom (Independent Communications Authority of South Africa, 2023).
- Two-factor authentication: A security protocol that requires two separate credentials to verify a user's identity, typically combining something the user knows, for example, a password, with something the user has, for example, a one-time password sent to a mobile device. While two-factor

authentication adds an additional layer of security, it remains vulnerable to compromise through SIM swap fraud (Grassi & Fenton, 2017).

- Machine learning: A branch of AI focused on developing algorithms capable of learning patterns and making predictions or decisions from data without explicit programming. In fraud detection, machine learning algorithms are used to analyse large datasets, identifying anomalies and patterns that may indicate fraudulent activity (Bhattacharyya *et al*., 2011)

These definitions serve as a foundational reference throughout the study, helping to ensure a clear and cohesive understanding of the specialised terms within the context of AI-driven fraud prevention.

1.8 Assumptions and limitations

This research, while striving to offer valuable insights into the application of AI for combating SIM swap fraud during the 2G/3G network shutdown, operated under specific assumptions and acknowledged certain limitations. These factors may influence the scope and generalisability of its findings.

1.8.1 Assumptions

- Implementation challenges: This study primarily examined the technical feasibility of AI-based solutions, assuming these could be implemented within existing telecommunication infrastructures and regulatory frameworks. However, practical implementation may face challenges related to cost, technical integration, and regulatory compliance, which were outside the study's focus.
- Ethical considerations: It was assumed that AI deployment for SIM swap fraud prevention would adhere to ethical standards, avoiding unintended consequences like discrimination or privacy infringement. However, the

ethical landscape of AI is complex, and responsible implementation requires careful, context-sensitive evaluation.

- Human factor: Although AI can automate many aspects of fraud detection, this study assumed that human expertise would remain integral in interpreting AI outputs, making final decisions, and adapting to evolving fraud patterns. Therefore, the effectiveness of AI solutions may be contingent upon the availability of skilled personnel and the success of human-AI collaboration.

1.8.2 Limitations

- Limited scope of the literature: Due to the rapidly advancing nature of AI research and the specific context of SIM swap fraud, the systematic literature review may not encompass all relevant studies, potentially limiting the breadth of insights.
- Publication bias: The literature review may be subject to publication bias, as studies reporting positive or statistically significant results are often prioritised for publication. This bias could result in an overestimation of AI's effectiveness in combating SIM swap fraud.
- Heterogeneity of studies: The studies included in this review vary in methodologies, AI techniques, data sources, and evaluation metrics. This heterogeneity poses challenges to synthesising findings and drawing conclusive statements about AI's overall efficacy in this context.
- Rapidly evolving landscape: Given the continuous evolution of AI technologies and fraud tactics, the findings of this research may have limited longevity. As new technologies and adaptive fraud methods emerge, the applicability of this study's conclusions may diminish over time.

By acknowledging these assumptions and limitations, this study aimed to offer a transparent and realistic assessment of its findings and implications. Moreover, these limitations provide a roadmap for future research, suggesting directions for addressing current gaps and expanding our understanding of AI's role in mitigating SIM swap fraud in an ever-changing digital landscape.

CHAPTER 2. PRELIMINARY LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

The global telecommunications landscape is experiencing a significant shift as 2G and 3G networks are gradually phased out in favour of more advanced 4G and 5G technologies (GSMA, 2023). This transition promises faster data speeds and improved connectivity, yet it also introduces new security vulnerabilities that cybercriminals, particularly those engaged in SIM swap fraud, may exploit (Kim *et al*., 2022).

This comprehensive literature review critically analyses existing research on SIM swap fraud, examining the role of AI in detecting and preventing fraud, and addressing the specific challenges and opportunities presented by the 2G/3G network shutdown. Through a synthesis of current knowledge, this review aims to inform the development of more robust strategies for countering SIM swap fraud in an increasingly intricate technological environment.

2.2 Background

The global transition from 2G/3G to 4G/5G networks represents a pivotal advancement in mobile communication technologies, spurred by increasing demands for faster data speeds, seamless connectivity, and support for advanced applications (Agrawal *et al*., 2015; Akhtar, 2009). While 4G networks already provide substantial improvements over previous generations, the emerging 5G technology offers even greater data rates, improved spectrum efficiency, and enhanced support for pervasive computing (Sule & Joshi, 2014). This shift entails not only architectural changes but also the adoption of new

standards and the development of innovative devices and applications (Akhtar, 2009).

However, this evolution also brings considerable security challenges. Although 5G is designed to incorporate advanced security features, the reliance on 4G core networks during this transition period exposes significant vulnerabilities (Lasierra *et al*., 2023; Holtrup *et al*., 2021). In certain regions, these risks are further amplified by outdated devices, financial constraints, and limited awareness of cybersecurity practices (Asmare & Ayalew, 2023).

The migration to 4G/5G necessitates a revaluation of SIM card security and identity management protocols. Existing SIM security measures, particularly those based on PIN-based access control, exhibit vulnerabilities that could facilitate various forms of cyberattacks (Zhao *et al*., 2021). Furthermore, the adoption of embedded Universal Integrated Circuit Cards (eUICCs) in 5G and Internet of Things (IoT) devices introduces additional complexities, underscoring the need for more robust security frameworks to protect both users and service providers (Chitroub *et al*., 2018).

Among the cybersecurity threats exacerbated by this transition, SIM swap fraud stands out. This method, increasingly prevalent, involves fraudsters exploiting weaknesses in mobile provider verification processes to gain control of a victim's phone number (Cooper, 2024; iiDENTIFii, 2024). By circumventing two-factor authentication protocols, attackers gain access to sensitive information, posing serious risks to victims. The growing incidence of SIM swap fraud highlights the urgent need for innovative countermeasures.

As the shift to 4G/5G networks advances, it is essential to address the security challenges that accompany this technological transformation. This involves developing robust authentication protocols, implementing granular access controls, and enhancing security measures for eUICCs. Additionally, promoting cybersecurity awareness and educating users on potential risks remain crucial to

mitigating SIM swap fraud and other emerging threats within this new digital landscape.

2.3 Offender opportunities presented by 2G/3G shutdown

The transition from 2G/3G to 4G/5G networks has presented cybercriminals with new opportunities to exploit emerging vulnerabilities, particularly through SIM swap fraud. This discussion explores the motivations driving fraudsters to target these weaknesses, with an emphasis on both technical and socio-economic factors.

2.3.1 Economic incentives

Economic gain remains the primary driver behind most cybercrime, and SIM swap fraud is no exception. Fraudsters are drawn to SIM swap attacks due to the significant financial rewards, as intercepting two-factor authentication codes enables access to bank accounts, cryptocurrency wallets, and other financial services (Hallman, n.d.). The 2G/3G shutdown exacerbates these vulnerabilities by creating transitional gaps that fraudsters can exploit, taking advantage of the confusion and reduced security vigilance that often accompanies major technological changes (African Wireless Communications, 2024).

2.3.2 Exploitation of technological vulnerabilities

The shutdown of 2G and 3G networks is more than a technical upgrade; it is a complex migration involving millions of users and various stages of system interoperability. Temporary vulnerabilities, such as initial compatibility issues between older and newer systems, create entry points for fraudsters (GSMA, 2021). Additionally, users relying on legacy devices may lack updated security features, increasing their susceptibility to SIM swap attacks during this period (SABRIC, 2022).

2.3.3 Social engineering opportunities

Network shutdowns often require extensive customer communication, providing opportunities for social engineering. Fraudsters can impersonate customer service representatives, using phishing messages and fake calls to deceive users into revealing personal information (Hadnagy, 2018). This period of technological transition, marked by increased user uncertainty, allows fraudsters to exploit the need for guidance and trick users into giving up sensitive information.

2.3.4 Regulatory and compliance loopholes

Regulatory frameworks governing telecommunications often lag technological advancements, and this gap may widen during the 2G/3G to 4G/5G transition. Existing regulations mandating robust authentication and SIM registration processes may not be fully updated to address new risks posed by emerging mobile technologies (Kibuuka, 2024). In regions with limited regulatory enforcement, fraudsters may exploit these compliance gaps, taking advantage of the reduced likelihood of detection and prosecution.

2.3.5 Accessibility of tools and techniques

The tools and techniques required to carry out SIM swap fraud are increasingly accessible on dark web forums, where resources such as hacking tools, stolen personal data, and detailed attack guides are readily available (Wanyonyi & Bird, 2021). This ease of access lowers the entry barriers for cybercriminals. During the 2G/3G shutdown, when security measures may be temporarily relaxed, the accessibility of these tools further enables fraudsters to take advantage of transitional vulnerabilities.

2.3.6 Disruption of established security practices

The migration to 4G and 5G networks disrupts established security routines for both users and network operators. Users accustomed to certain security protocols may struggle to adapt to new security requirements, increasing their vulnerability to attacks (Hadnagy, 2018). Similarly, network operators focused on upgrading infrastructure may divert resources from ongoing security measures, inadvertently providing fraudsters with opportunities to perpetrate SIM swap fraud.

2.3.7 Exploiting user behaviour and awareness

User behaviour and awareness significantly impact the success of SIM swap fraud. Many users remain unaware of the security risks associated with network shutdowns, failing to take precautions like updating contact information or enabling additional security measures (SABRIC, 2022). Fraudsters exploit this lack of awareness, particularly during periods of transition, when educational campaigns may not reach all users in time.

2.3.8 Targeting high-value individuals

During 2G/3G shutdown, fraudsters may specifically target high-value individuals, such as business executives, politicians, and celebrities, who are more likely to use mobile banking and other sensitive services linked to their phone numbers. The financial and reputational damage that can be inflicted on these individuals is significant, making them attractive targets for SIM swap fraud (Bhavana et al., 2024).

High-value targets are often more vulnerable during periods of technological transition due to the complexity of their mobile setups and the higher stakes involved. Fraudsters can use advanced techniques and dedicate more resources

to compromising these targets, knowing that the potential rewards are substantial.

2.3.9 Opportunistic exploitation of large-scale events

2G/3G shutdown tends to be a large-scale event that affects millions of users simultaneously. Fraudsters are adept at exploiting such events to maximise their impact. The widespread nature of the network transition means that fraudsters can cast a wide net, targeting numerous users with the expectation that even a small success rate will yield significant rewards (Wanyonyi & Bird, 2021).

Opportunistic exploitation during such events is not uncommon in the cybercriminal world. Fraudsters take advantage of the confusion and lack of preparedness that often accompany large-scale technological changes. 2G/3G shutdown is no different, providing a fertile ground for fraudsters to perpetrate SIM swap fraud on a large scale.

2.3.10 Leveraging AI and automation

Cybercriminals are increasingly using AI to enhance their capabilities, automating phishing messages, social engineering attacks, and data analysis to identify potential targets (Mattord & Whitman, 2023). During the 2G/3G shutdown, AI-driven attacks become even more potent, allowing fraudsters to exploit transitional data and opportunities with greater efficiency. The use of AI not only accelerates the speed and scale of attacks but also complicates detection and prevention efforts.

Understanding these motivations and factors is essential for developing effective countermeasures to protect users against SIM swap fraud during this critical period. By recognising the multifaceted drivers behind these fraud attempts, stakeholders, including mobile network operators, financial institutions, and

regulatory bodies, can implement targeted strategies to strengthen security. Potential measures include enhancing authentication protocols, promoting user awareness, updating regulatory frameworks, and employing AI in fraud detection and prevention. As the telecommunications landscape continues to evolve, a proactive, adaptive approach to cybersecurity is crucial in staying ahead of fraudsters. The first proposition put forward for this research was, therefore:

Proposition 1

2G/3G shutdown will lead to an increase in SIM swap fraud due to a larger pool of potentially motivated offenders.

2.4 Increased user vulnerability

The transition from 2G/3G to 4G/5G networks is expected to heighten user vulnerability to SIM swap fraud, driven by a combination of technical, social, and regulatory factors. Understanding these vulnerabilities is crucial to evaluating and implementing effective countermeasures that can safeguard users during this period of network migration.

2.4.1 Technological transition and new vulnerabilities

The migration to 4G/5G entails substantial changes in both network infrastructure and user devices, which can introduce temporary security gaps. For example, as older devices that only support 2G/3G networks become obsolete, users are forced to upgrade to newer devices (GSMA, 2021). This transition period creates an environment ripe for exploitation, as fraudsters may leverage outdated security practices and technical vulnerabilities associated with new systems to conduct SIM swap fraud.

2.4.2 Increased user confusion and lack of awareness

As network operators inform users about the necessity to upgrade devices and SIM cards, fraudsters may exploit the heightened communication through social engineering tactics. With users receiving SMSs, emails, and calls regarding the transition, fraudsters can impersonate network representatives, tricking users into disclosing personal information or clicking on malicious links (Hadnagy, 2018). During periods of technological change, the general confusion and lack of awareness around new processes make users particularly susceptible to these deceptive tactics.

2.4.3 Legacy devices and inadequate security

Many users still rely on legacy devices compatible only with 2G/3G networks, which often lack advanced security features, such as biometric authentication or secure boot processes (SABRIC, 2022). As users gradually transition to newer, more secure devices, there is a vulnerable window during which they continue using outdated devices. Fraudsters can exploit this period, targeting users who have yet to fully transition to the security advantages of newer technology.

2.4.4 Regulatory gaps and compliance challenges

The regulatory frameworks governing telecommunications frequently lag rapid technological advancements. As the transition to 4G/5G unfolds, regulatory measures mandating robust user authentication and secure SIM registration processes may not yet be fully enforced or updated to address the new risks (Kibuuka, 2024). This regulatory lag provides a critical window for fraudsters, who may take advantage of compliance gaps to perpetrate SIM swap fraud with a reduced likelihood of detection or prosecution.

2.4.5 Demographic factors

Certain demographic groups may be more susceptible to SIM swap fraud during the 2G/3G shutdown. For instance, older adults who may be less familiar with new technologies could find the transition more challenging and may be more vulnerable to social engineering attacks or unaware of necessary security practices on new devices (Mattord & Whitman, 2023). Similarly, individuals with lower digital literacy levels may struggle to comprehend the implications of the network shutdown and the steps required to protect themselves (Jain & Gupta, 2021).

By considering these factors, stakeholders, including network operators, regulatory bodies, and consumer advocacy groups, can take a proactive approach to address increased user vulnerabilities during the network transition. Efforts to enhance communication clarity, bolster regulatory compliance, and target educational campaigns at high-risk groups may collectively contribute to reducing the risks associated with SIM swap fraud in this evolving technological landscape. The second proposition for the research was, therefore:

Proposition 2

2G/3G shutdown will lead to an increase in SIM swap fraud due to a larger pool of suitable targets.

2.5 The role of AI in addressing SIM swap fraud

AI has emerged as a promising tool for tackling SIM swap fraud (Murugalakshmi *et al.*, 2023). By analysing patterns and trends in fraud activity, AI allows organisations to adopt a more proactive approach to threat detection and prevention. AI-driven solutions can help identify suspicious behaviour, flag potential instances of fraud in real time, and offer robust defences against

emerging cybercrime tactics (Ganesan *et al*., 2020), especially in the context of network shutdowns (Haidine *et al*., 2016).AI's role in fraud prevention also extends to other areas, such as enhancing contact centre security where both familiar and novel threats challenge traditional measures (Cordoso, 2021). This section explores various AI applications in SIM swap fraud detection and prevention.

2.5.1 AI in fraud detection and prevention

Machine learning, a subset of AI, has become a key player in combating SIM swap fraud. By processing vast amounts of data, machine learning algorithms can identify patterns and anomalies that may signal fraudulent activities (Bhattacharyya *et al*., 2011). These algorithms continuously learn and adapt, improving their precision in detecting new and evolving fraud tactics over time.

AI techniques such as anomaly detection can uncover atypical patterns of behaviour, while behavioural biometrics analyse user interactions to verify authenticity (Ali *et al*., 2024). Natural language processing can interpret text-based communications for indicators of fraud (Ngai *et al*., 2010), and graph analysis reveals hidden connections between entities involved in fraudulent schemes (Cheng *et al*., 2020). Together, these AI techniques form a multi-faceted approach to fraud detection that is both comprehensive and adaptable to dynamic fraud scenarios.

2.5.2 Pattern recognition and anomaly detection

AI excels at recognising patterns and detecting anomalies in large datasets. Through machine learning, AI systems can establish baselines of normal user behaviour, such as the frequency of SIM card changes, geographical locations, and transaction histories, allowing them to detect deviations that may suggest fraud (Nguyen *et al*., 2022). For instance, if a SIM swap request originates from

an unusual location or if the request frequency surpasses normal thresholds, AI can flag the activity as suspicious, enabling network operators to investigate before approving the swap.

Behavioural biometrics add another layer of security by analysing unique user traits like typing speed, swipe patterns, and interactions with mobile applications. These traits are difficult for fraudsters to replicate accurately, allowing AI systems to trigger additional authentication steps or alerts when discrepancies are detected (Hadnagy, 2018). This technique reinforces security even when social engineering tactics have compromised traditional verification methods.

2.5.3 Fraud detection models

Advanced machine learning techniques can enhance existing fraud detection models. Supervised learning algorithms, trained on datasets containing both legitimate and fraudulent SIM swap cases, enable models to distinguish between the two by evaluating features such as transaction patterns, device information, and network activity (Goodfellow, Bengio, & Courville, 2016). Meanwhile, unsupervised learning algorithms can identify new fraud patterns not included in training data, offering a dynamic and adaptable defence mechanism against evolving fraud techniques (Celebi & Aydin, 2016).

Continuous updates to these fraud detection models ensure that AI systems stay abreast of fraud tactics, providing network operators with a resilient strategy for identifying and preventing SIM swap attacks.

2.5.4 Natural language processing for social engineering detection

Social engineering, commonly employed in SIM swap fraud, often involves fraudsters manipulating customer service representatives. Natural language processing can analyse the language and tone used in customer interactions to

detect potential fraud attempts, identifying red flags such as urgency, inconsistencies, and unusual requests in real time (Jurafsky & Martin, 2000). By integrating natural language processing with call centre operations, network operators can support customer service representatives by alerting them to potential fraud attempts, enhancing their ability to recognise and thwart social engineering tactics.

2.5.5 Predictive analytics

AI-powered predictive analytics uses historical data to anticipate potential fraud attempts. By examining past patterns, AI systems can identify users at higher risk of being targeted, based on factors like behaviour and transaction history (Becker *et al*., 2011). For instance, users who frequently travel internationally or conduct high-value transactions may be more attractive targets for fraudsters. Predictive analytics enables proactive interventions, such as additional authentication steps and heightened monitoring, helping to prevent fraud before it occurs (Parmar & Patel, 2017).

2.5.6 Challenges in implementing AI for addressing SIM swap fraud

Implementing AI systems to counter SIM swap fraud presents several challenges:

- Data privacy and security: Effective AI models require extensive user data, raising privacy concerns. Ensuring compliance with data protection regulations, like the General Data Protection Regulation (GDPR), requires robust data encryption, access controls, and anonymisation techniques (Voigt & Von dem Bussche, 2017).
- Algorithmic bias: AI models are susceptible to biases in training data, which can lead to unfair outcomes. For instance, certain demographic groups might be disproportionately flagged as suspicious, leading to false positives and negative user experiences (Barocas, Hardt, & Narayanan,

2023). Addressing these biases involves careful data selection, regular model auditing, and the implementation of fairness-aware algorithms.

- Adversarial attacks: Fraudsters can employ adversarial attacks to manipulate AI systems, feeding them carefully crafted inputs that deceive the model into making incorrect decisions (Goodfellow *et al*., 2016). Developing AI models resilient to these attacks is essential to maintaining robust fraud detection capabilities.
- Integration with existing infrastructure: Integrating AI with current network and security systems can be complex and resource-intensive, requiring significant investment in both technology and skilled personnel (Nguyen *et al*., 2022).
- Building user trust: Users may be wary of AI monitoring their activities. Building transparency around AI's role, data security, and benefits for fraud prevention is essential to fostering trust and ensuring successful adoption (Hadnagy, 2018).

In conclusion, while AI holds significant promise in addressing SIM swap fraud, implementing effective AI systems necessitates overcoming these challenges. By addressing issues around data privacy, algorithmic bias, adversarial attacks, infrastructure integration, and user trust, network operators can maximise AI's potential to protect users from emerging fraud risks and contribute to a more secure digital landscape. The third proposition for this research was, therefore:

Proposition 3

Implementing AI as a capable guardian will reduce the overall rate of successful SIM swap fraud attempts.

2.5.7 Research gaps and future directions

While research on AI applications in fraud detection is expanding, a significant gap remains concerning the specific challenges and opportunities associated with the 2G/3G network shutdown within South Africa's unique socio-technical context. Further research is essential to:

- Identify and analyse emerging SIM swap fraud tactics: As the transition to 4G/5G unfolds, understanding the specific SIM swap fraud tactics likely to emerge is critical. Given South Africa's unique socio-technical dynamics, this analysis should consider regional factors that may shape fraud tactics, including economic conditions, digital literacy levels, and telecommunications infrastructure.
- Develop and evaluate tailored AI models: To effectively combat SIM swap fraud during this transition, AI models must be adapted to South Africa's telecommunications landscape and the specific characteristics of the evolving threat landscape. Research should focus on creating models that are responsive to regional challenges, such as varied device adoption rates, specific fraud patterns, and network operator practices.
- Investigate ethical and privacy implications: Ensuring that AI-driven fraud detection is deployed responsibly involves examining the ethical and privacy implications of these technologies. This includes assessing how AI may affect vulnerable populations, such as low-income users or those with limited digital literacy and implementing safeguards to protect these groups from disproportionate impact.

By addressing these areas, future research can contribute to the responsible and effective deployment of AI for fraud prevention in South Africa, ultimately strengthening both user security and trust in digital services amidst the network transition.

2.6 Analytical framework

2.6.1 Theoretical framework

While numerous theoretical frameworks could be applied to the study of SIM swap fraud, this research adopts the Routine Activity Theory (RAT) as its primary lens due to its strong alignment with the research objectives. Originally developed in criminology by Cohen and Felson in 1979 (Figure 1), the RAT posits that crime is likely to occur when three elements intersect: a motivated offender, a suitable target, and the absence of a capable guardian. This framework's emphasis on situational factors, rather than focusing solely on offender characteristics, makes it particularly well-suited for examining how the 2G/3G network shutdown, a significant situational shift, may create new opportunities for SIM swap fraud. By focusing on the situational changes brought about by this technological transition, the RAT provides a practical framework for understanding and anticipating the risks associated with emerging vulnerabilities.

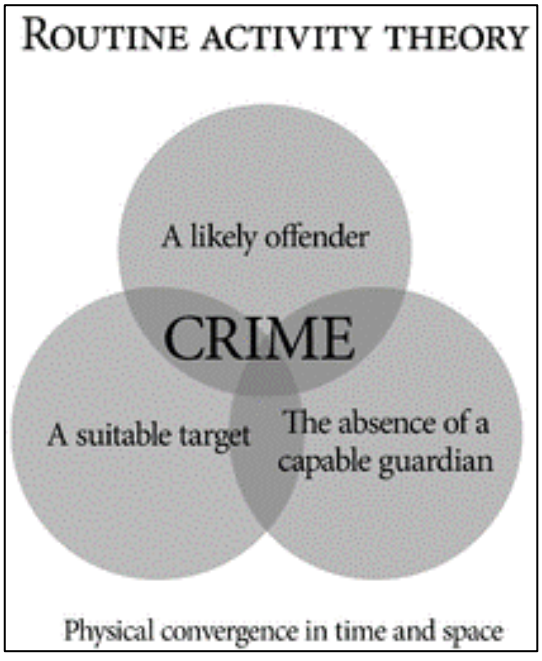


Figure 1: A graphical model of the Routine Activity Theory

In the context of SIM swap fraud, the RAT offers a structured lens through which to examine the interplay of key factors that contribute to this crime. Here, the motivated offender is the individual or group equipped with the knowledge, skills, and intent to commit SIM swap fraud. The suitable target comprises mobile phone users who may be particularly vulnerable due to factors such as limited awareness, reliance on outdated devices, or insufficient security practices.

The 2G/3G shutdown is anticipated to expand the pool of suitable targets, as users are forced onto potentially less secure networks or face confusion during the transition – conditions ripe for exploitation by fraudsters. The transition may also increase offenders' motivation, as they perceive new vulnerabilities and opportunities within this period of technological change.

While theories like the Social Learning Theory and the General Deterrence Theory could provide valuable insights into SIM swap fraud, the RAT's focus on situational dynamics and applicability to technological shifts make it especially relevant here.

By adopting the RAT, this research aims to systematically examine how the 2G/3G shutdown may intensify conditions conducive to SIM swap fraud. Additionally, it explores how AI can act as a capable guardian by disrupting the convergence of motivated offender, suitable target, and inadequate guardianship. Ultimately, this understanding is intended to guide the development of evidence-based prevention strategies aligned with the RAT's practical applications for crime reduction.

2.6.2 Conceptual framework

This study builds a conceptual framework rooted in the RAT to analyse SIM swap fraud risks specific to the 2G/3G shutdown in South Africa. While it acknowledges the theory's core components, that is, motivated offender, suitable target, and

lack of capable guardianship, the framework also integrates contextual technological and social factors unique to this scenario. The key components of the conceptual framework, illustrated in Figure 2, are as follows:

- Motivated offender: Beyond conventional motives like financial gain and identity theft, the 2G/3G shutdown may introduce new incentives for fraudsters, including user confusion during the migration and security gaps in unfamiliar networks or devices. Understanding these motivations and offender profiles is crucial for creating targeted interventions that address these evolving risks.
- Suitable target: Factors at the individual level, such as lack of awareness, poor security practices, and limited digital literacy, heighten user vulnerability. The 2G/3G shutdown introduces new vulnerabilities, such as forced migration to new networks and the potential for misinformation to fuel social engineering attacks. Recognising these specific risk factors enables more focused user education initiatives and awareness campaigns.
- Lack of capable guardianship: This component spans both technological and social domains. Technologically, it involves assessing the robustness of current security measures, identifying gaps in network infrastructure, and exploring the role of AI-powered solutions in fraud detection and prevention. Socially, it includes evaluating the impact of awareness campaigns, law enforcement responses, and community-based efforts to counter SIM swap fraud. The 2G/3G shutdown adds complexity, necessitating an evaluation of stakeholder preparedness and the availability of support services for victims.

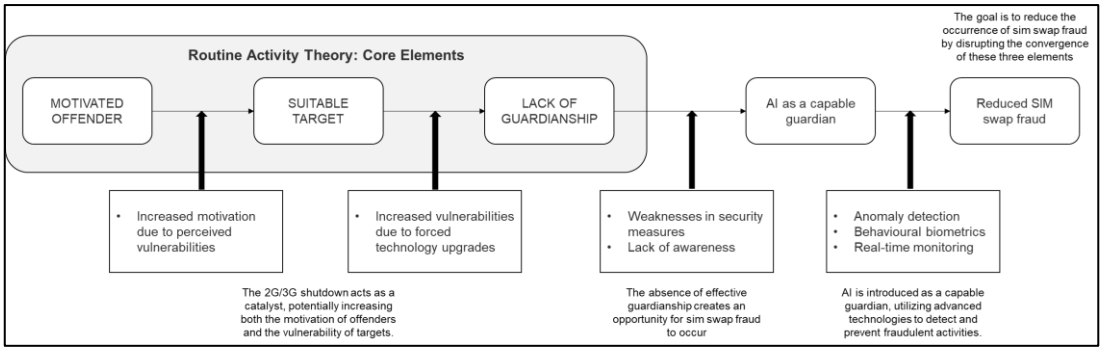


Figure 2: Conceptual framework (based on the RAT)

By broadening RAT's scope to incorporate these contextual factors, this framework provides a comprehensive approach to understanding and addressing SIM swap fraud during this transitional period.

From these core concepts, the research dimensions are defined as:

1. Research dimension 1: Motivated offender
    - Profiling: Identify characteristics of typical SIM swap fraud perpetrators.
    - Evolving tactics: Analyse how fraudsters adapt their techniques in response to the 2G/3G shutdown and new security measures.
2. Research dimension 2: Suitable target
    - Vulnerability assessment: Identify factors that increase user vulnerability.
    - Impact analysis: Assess the financial and psychological impact of SIM swap fraud on victims.
3. Research dimension 3: Lack of capable guardianship
    - Current measures: Evaluate the effectiveness of existing security measures.
    - AI as a guardian: Investigate how AI can enhance detection and prevention.

The conceptual framework also acknowledges the broader environmental factors influencing the occurrence and impact of SIM swap fraud. Socioeconomic elements, such as income inequality and unemployment, may contribute to the prevalence of fraud by creating conditions that drive individuals towards cybercriminal activities or make certain populations more vulnerable. The regulatory environment, particularly the efficacy of laws and enforcement mechanisms in deterring crime, plays a crucial role in shaping fraud dynamics. Furthermore, the rapid advancement of technology, with the rollout of 5G and the adoption of eSIM technologies, presents both new challenges and opportunities for fraudsters and the entities working to prevent such attacks.

By encompassing these multifaceted dimensions, this refined conceptual framework provides a more granular and context-sensitive understanding of SIM swap fraud amid the 2G/3G network shutdown. It serves as a structured roadmap for a comprehensive research agenda, guiding inquiries into the motivations and tactics of offenders, the vulnerabilities of potential targets, the effectiveness of current and prospective safeguards, and the broader socio-technical landscape in which this crime unfolds.

Ultimately, the framework aims to facilitate the development of targeted and effective prevention strategies that address the unique impact of SIM swap fraud in markets like South Africa. This approach supports the design of interventions that are both empirically grounded and responsive to the complex factors shaping fraud within this transitional period.

2.7 Conclusion

The transition from 2G and 3G networks to 4G and 5G in South Africa marks a pivotal moment in addressing the threat of SIM swap fraud. While AI presents a powerful tool to counter this evolving risk, its effective deployment hinges on a nuanced understanding of the unique socio-technical context and associated

challenges. By adopting a conceptual framework rooted in the RAT, this research aimed to explore and test propositions regarding the factors driving SIM swap fraud within the transitional landscape:

1. **Proposition 1**

   2G/3G shutdown will lead to an increase in SIM swap fraud due to a larger pool of potentially motivated offenders.

2. **Proposition 2**

   2G/3G shutdown will lead to an increase in SIM swap fraud due to a larger pool of suitable targets.

3. **Proposition 3**

   Implementing AI as a capable guardian will reduce the overall rate of successful SIM swap fraud attempts.

The framework's integration of technological, social, and economic dimensions enables a comprehensive analysis of how AI can serve as a capable guardian in preventing fraud. Ultimately, this study seeks to inform the development of contextually relevant, evidence-based strategies to mitigate SIM swap fraud and bolster security within the dynamic South African telecommunications environment.

The primary aim of this preliminary literature review was to establish a comprehensive overview of the research landscape related to AI-driven fraud prevention, with a specific focus on SIM swap fraud.

CHAPTER 3. RESEARCH METHODOLOGY

This research adopted the RAT as its primary theoretical framework to analyse the dynamics underpinning SIM swap fraud and to evaluate the potential of AI as a strategic response to this issue. The RAT's emphasis on situational factors provides a robust foundation for understanding how the 2G/3G network shutdown might create new opportunities for SIM swap fraud, thereby guiding the investigation into AI's role in fraud prevention.

To objectively identify relevant existing literature for further analyses a systematic literature review was conducted following the PRISMA guidelines. This methodological approach ensured a rigorous and transparent process for synthesising existing research, identifying critical knowledge gaps, and gathering evidence-based insights on the effectiveness of AI in countering SIM swap fraud amid technological transitions. The PRISMA framework facilitated a structured review, enhancing the credibility and reliability of findings by systematically capturing relevant studies and filtering out biases. The data included in the systematic review was subsequently interrogated, via bibliometric and thematic analyses, to further outline the nuances in the literature and enable a structured and objective synthesis of observations and recommendations.

By combining a solid theoretical foundation with a comprehensive literature review and supporting, bibliometric and thematic, analyses, this research aimed to provide a nuanced understanding of SIM swap fraud. Additionally, the research sought to contribute to the development of effective AI-driven solutions designed to protect individuals and organisations in an increasingly digital and connected landscape.

3.1 Research paradigm

This study was grounded in the interpretivist research paradigm, which asserts that reality is socially constructed and subjective, shaped by individual experiences and contextual influences. Interpretivism prioritises understanding the meanings that people assign to their experiences, making it particularly appropriate for research that seeks to explore complex human behaviours and socio-technical phenomena. Unlike positivism, which emphasises objective measurement and generalisability through quantitative methods, interpretivism values depth, reflexivity, and contextual insight (Merriam & Tisdell, 2015).

In line with this paradigm, the study employed a qualitative systematic literature review to explore the evolving dynamics of SIM swap fraud, particularly within the transitional context of the 2G/3G network shutdown. This approach involved synthesising qualitative studies to uncover patterns, narratives, and themes that offer a contextualised understanding of the phenomenon (Lincoln, 1985). It also recognised the researcher's interpretive role in the process, acknowledging that meaning is co-constructed through engagement with data.

A key strength of interpretivism lies in its emphasis on reflexivity, which requires researchers to critically reflect on their own assumptions and potential biases. This was essential in ensuring transparency and credibility throughout the analytical process. By interpreting findings in relation to broader theoretical and contextual frameworks, the study aimed to generate insights that go beyond surface-level observations (Creswell & Poth, 2016).

3.1.1 Rationale

A qualitative systematic literature review was chosen due to the emerging and underdeveloped nature of this research domain, especially in the South African context. A purely quantitative approach would have failed to capture the nuanced

interrelations between fraud behaviours, user vulnerabilities, and systemic gaps. Qualitative synthesis, by contrast, allowed the study to examine how contextual conditions, such as regulatory fragmentation or digital illiteracy, exacerbate susceptibility during periods of technological transition (Van Looy, 2021).

Furthermore, the exploratory orientation of interpretivism was particularly relevant to this study, given the evolving nature of both SIM swap fraud and AI-based prevention tools (William, 2024). This methodological stance enabled the inclusion of diverse perspectives from academic, policy, and industry literature, enriching the research with insights grounded in real-world complexity. Importantly, this approach supported the investigation of not only what is happening, but why it is happening, and how contextual forces shape these dynamics (Lawler & Waldner, 2023).

3.1.2 Implications

Using an interpretivist lens provided a rich, context-sensitive understanding of how fraudsters exploit transitional vulnerabilities in mobile network infrastructure, and how AI might be deployed to counteract these threats (Merriam & Tisdell, 2015). The approach also facilitated an exploration of the subjective experiences of those impacted by SIM swap fraud, including both users and system implementers, which is crucial for the development of user-centred, socially responsive AI interventions (Guba & Lincoln, 1994).

Additionally, interpretivism supports methodological flexibility, making it well-suited for examining emerging digital threats through qualitative synthesis. The inclusion of multiple data sources and viewpoints contributed to a more holistic and grounded perspective on the phenomenon (Creswell & Poth, 2016). Reflexivity played a vital role here, ensuring that the research process remained ethically aware and transparent, especially in addressing sensitive issues such as fraud and data protection (Mason, 2005).

Finally, the paradigm enabled the development of theory-informed, actionable insights. By grounding the findings in lived experiences and situated realities, the study was able to propose AI-based strategies that are both conceptually robust and practically feasible (Strauss & Corbin, 1998). This reinforces the importance of interpretivism not only for understanding social phenomena, but also for designing context-appropriate interventions in rapidly changing digital environments.

3.2 Research approach

This research adopted a mixed methods qualitative process which blended three different approaches to enable the objective identification of literature, qualitative validation of included sources and synthesis of insights and recommendations gleaned therefrom. This high-level research approach is illustrated in Figure 3.

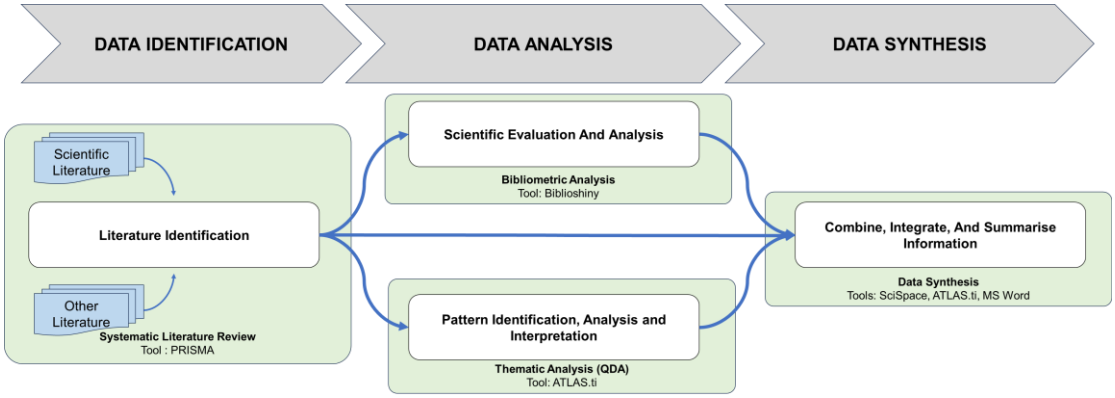


Figure 3: High-level research approach

3.3 Research design

This research adopted a qualitative approach, employing a systematic literature review as the primary method to identify existing literature to investigate the role

of AI in addressing SIM swap fraud trends during the 2G/3G shutdown in South Africa. The subsequent bibliometric and thematic analysis improved the rigour of the results compared to what a systematic review would have produced in isolation.

The integration of bibliometric and thematic analyses offers a structured, multi-dimensional perspective on SIM swap fraud and AI's role in its prevention thus ensuring dual-pronged analytical rigour.

The bibliometric analysis identifies key terms, publications, and trends, creating a map of core research areas and informing the direction of the thematic analysis. This initial framework guides the thematic analysis, ensuring that emerging themes are rooted in established academic discourse.

This analytical interdependence, as illustrated in Figure 4, highlights under-researched areas and informs a structured thematic analysis that delves into the more nuanced aspects of SIM swap fraud, such as the influence of network shutdowns on fraud risks in underserved regions. By aligning both methods, the research bridges theoretical perspectives with practical insights, resulting in a layered, in-depth understanding of the subject.

It was, therefore, necessary to conduct both the systematic literature review and bibliometric analysis, allowing the two approaches to complement each other by addressing areas that neither could cover individually.

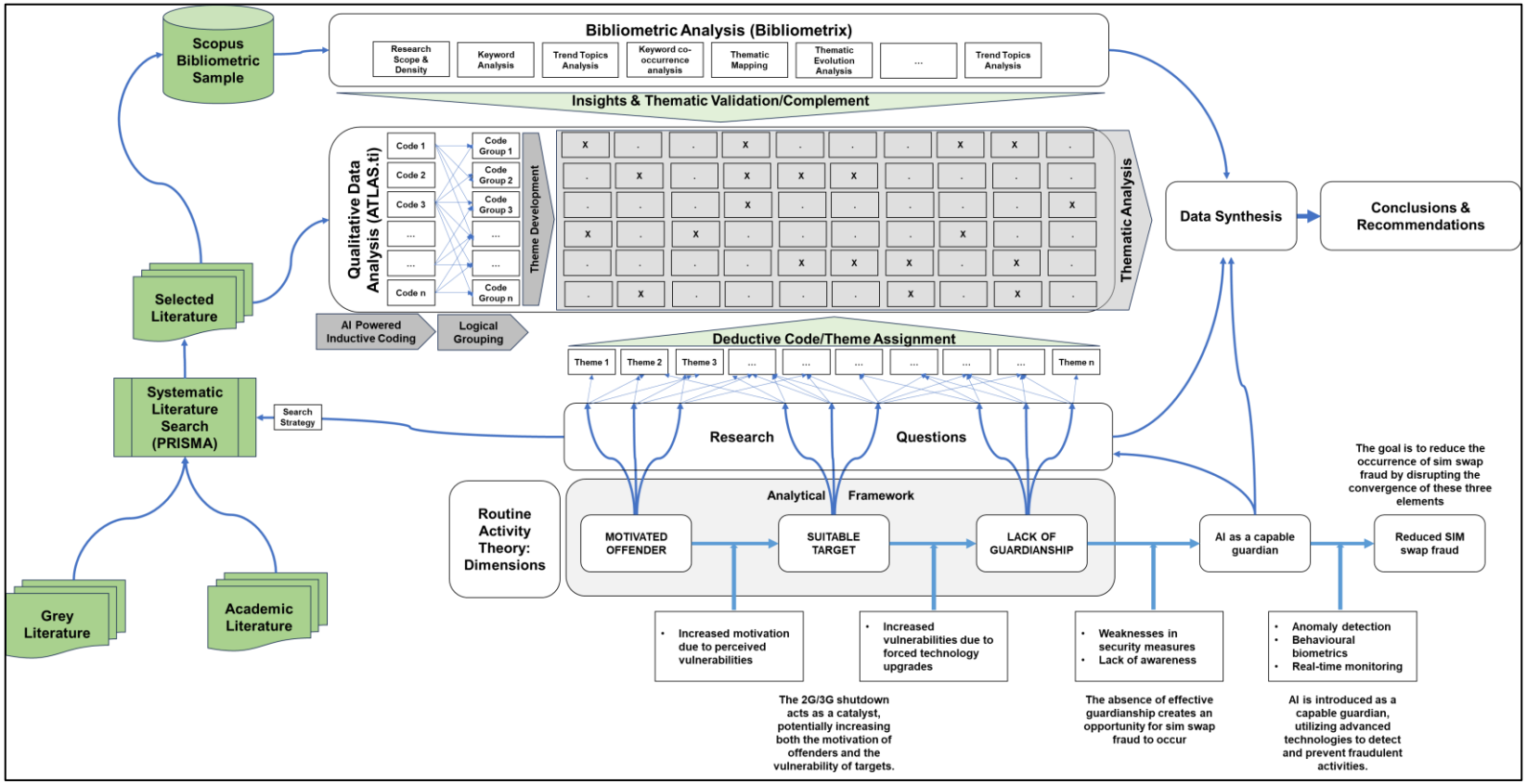


Figure 4: Research analytical flow and coupling

3.3.1 Systematic literature review overview

The systematic literature review was conducted following the PRISMA methodology, adapted from Page *et al*. (2021), as illustrated in Figure 5.

The PRISMA guidelines provide a structured framework for identifying and selecting relevant studies through a rigorous screening process, ensuring that only studies meeting pre-defined inclusion criteria are included in the analysis. This systematic approach was instrumental in identifying effective AI techniques for detecting and preventing SIM swap fraud, as well as in uncovering key challenges and limitations that must be addressed within this domain.

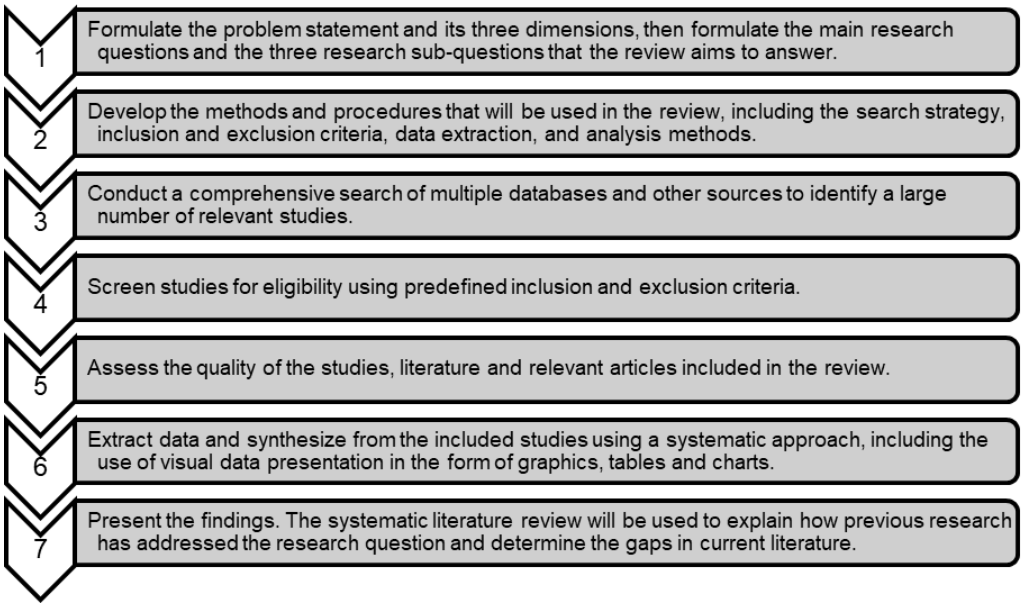


Figure 5: Systematic literature review process

A qualitative approach was particularly well-suited to this research, as it facilitates the integration of diverse data types and perspectives, yielding a more comprehensive and nuanced understanding of the research problem. By leveraging the strengths of a qualitative systematic literature review, this research generated findings that are both relevant and actionable, offering a foundation for developing AI-based solutions aimed

at combating SIM swap fraud amidst the network transition. This approach enabled the study to capture the complexity of the socio-technical landscape in which SIM swap fraud occurs, providing insights that are both contextually relevant and practically applicable.

3.3.2 Bibliometric analysis overview

To address the first research objective, “to outline the research landscape and identify critical trends and gaps in the literature related to the application of AI to address SIM swap fraud during the 2G/3G network shutdown”, a bibliometric analysis was undertaken.

The bibliometric analysis provided critical insights into the research landscape surrounding SIM swap fraud, AI-driven fraud detection, and telecommunication network transitions. It mapped current trends, identified influential contributions, and highlighted gaps, forming a comprehensive overview of the research in this field.

The analysis first revealed publication trends over time, showing how interest in these topics has evolved, with a noticeable increase in publication volume in recent years. This rise suggests a growing maturity and relevance of these research areas. Key authors and foundational works were also identified, spotlighting researchers and studies that have shaped the field. Highly cited works marked seminal contributions, influencing subsequent methodologies and focus areas.

A geographic analysis of institutional and regional contributions illustrated which countries and institutions are at the forefront of research efforts. Certain regions and institutions demonstrated higher research output, likely due to regional investments in telecommunications or an emphasis on fraud prevention technology. Collaboration patterns among authors indicated networks of frequent collaboration, reflecting research hubs and potential avenues for future international partnerships.

Through keyword analysis and thematic clustering, the bibliometric analysis highlighted dominant themes and emerging areas of interest. This analysis identified specific topics driving research while revealing areas that remain underexplored, providing a roadmap for future research. Gaps in the literature were identified by examining citation patterns and thematic clusters, focusing attention on essential areas that could advance knowledge in SIM swap fraud prevention during network transitions.

Together, these findings offer a detailed map of the research landscape, summarising influential contributions, collaboration networks, and emerging research needs. This analysis supports the qualitative data interpretation by contextualising the evolution and strategic advancements in leveraging AI to counter SIM swap fraud during the 2G/3G network transition.

1. Data collection and scope

   The bibliometric analysis mapped and assessed the literature on SIM swap fraud and AI-driven fraud detection, especially as they pertain to network shutdowns. Data was extracted only from the subset of included sources that were available on Scopus (n=71). The bibliometric metadata was retrieved in BibTeX format for uniformity, allowing the extraction of relevant bibliographic fields like authorship, publication year, keywords, abstracts, and citation data.

2. Data processing and analytical tools

   Using Bibliometrix, an R-based software, a range of tools explored citation patterns, collaboration networks, keyword trends, and thematic developments. Initial data review identified missing metadata fields, such as science categories and keywords plus, which were acknowledged as potential limitations for thematic mapping.

3. Analysis techniques

Quantitative and network-based analyses provided insights into research trends, impactful publications, and collaboration networks:

- Annual scientific production: Publication trends by year highlighted growth phases and shifts in research focus, tracing the field's development from foundational studies to recent surges.
- Citation and source impact analysis: Authors and sources were evaluated using h-index, g-index, and m-index metrics, identifying the most impactful publications, journals, and authors.
- Keyword and thematic analysis: Frequency counts and co-occurrence networks for keywords outlined prevalent research themes, with thematic mapping categorising keywords by influence and network connections.
- Geographical and collaboration analysis: Mapped scientific production by country to show regional contributions and collaboration networks, identifying the USA, China, and India as leading contributors.
- Co-citation network analysis: Identified seminal works and influential authors using metrics like betweenness, closeness, and PageRank centrality, mapping key thematic groups.
- Trend analysis and thematic evolution: Temporal keyword analysis revealed shifts in research focus, tracing thematic evolution towards areas like 5G security and AI-driven fraud prevention.
- Data visualisation: The visualisation tools in Bibliometrix aided in interpreting complex data. Visualisations generated were:
    - Time series and bar charts for annual publication trends.
    - Thematic maps and clustering graphs for keyword relationships.
    - Country maps for regional research outputs.
    - Co-citation and collaboration networks for connectivity and influence.

This bibliometric methodology offers a systematic, data-driven understanding of AI, telecommunications, and fraud detection research. By mapping publications, collaboration networks, and trends, the analysis establishes a foundation that highlights research gaps and guides future studies in AI-driven network security and fraud prevention.

4. Limitations of Bibliometric analysis

Despite the comprehensive extent of the bibliometric dataset, some missing metadata fields might influence thematic analyses. Limiting the study to Scopus could introduce disciplinary bias, although Scopus's breadth justified its selection.

Furthermore, while bibliometric indicators such as citation counts provide valuable metadata, they do not always reflect the quality or practical relevance of research. Additionally, the review is susceptible to language bias, as English-language publications dominate academic databases, potentially overlooking important findings published in other languages. The focus on peer-reviewed literature may also omit industry reports or unpublished case studies that are equally relevant.

3.3.3 Thematic analysis and narrative synthesis overview

This study used a thematic analysis approach to systematically explore the factors influencing SIM swap fraud during the 2G/3G network shutdown. The analysis was conducted using ATLAS.ti software, which facilitated efficient data processing, coding, and categorisation of the literature. The following outlines the step-by-step methodology:

1. Data collection and processing

The initial phase involved compiling a broad selection of academic and non-academic literature through the PRISMA methodology, ensuring a comprehensive perspective on SIM swap fraud. Using ATLAS.ti, the selected documents

underwent AI-assisted coding, allowing for the identification of recurring themes and patterns across the dataset. This systematic organisation of data was aligned with the analytical framework of the RAT.

2. Inductive coding

The first step in the analysis used an inductive coding process:

- Initial code generation: The AI coding tool in ATLAS.ti generated around 5,000 initial codes, facilitating the organic emergence of themes without pre-set categories.
- Code filtering and refinement: Each code was evaluated for relevance to the research objectives, reducing the code set to approximately 1,500 and then further to 600 focused codes. These refined codes provided key insights related to the study's objectives.

3. Deductive categorisation

To introduce a theory-driven structure, the final set of 600 codes was deductively categorised into three primary dimensions in line with the RAT:

- Motivated offender: Codes here related to themes such as offender profiling and adaptive tactics, offering insights into the behaviours and motivations of SIM swap fraud perpetrators.
- Suitable target: This dimension encompassed factors increasing user vulnerability, including demographic susceptibilities, misinformation, and susceptibility to social engineering.
- Lack of capable guardianship: Codes in this category assessed current security measures and AI’s potential role in fraud prevention, highlighting technological and regulatory challenges in preventing SIM swap fraud.

4. Data visualisation in ATLAS.ti

The data visualisation tools in ATLAS.ti, including code co-occurrence maps and network views, helped identify relationships and intersections among codes. These visuals enabled the strategic selection of the most relevant insights, supporting a comprehensive examination of the interconnected themes.

5. Theory-driven analysis with the RAT

To reinforce alignment with the RAT, the deductive categorisation phase organised codes within three dimensions:

- Motivated offender focused on profiling and adaptive behaviours of SIM swap fraudsters.
- Suitable target analysed user vulnerability factors, which were intensified by the 2G/3G network shutdown.
- Lack of capable guardianship assessed the effectiveness of existing security protocols and the role of AI-driven solutions.

This theory-driven structure allowed emergent insights to be seamlessly integrated with pre-defined dimensions, adding coherence and depth to the thematic analysis.

6. Result synthesis

The combined inductive and deductive approach provided a comprehensive synthesis of insights within each dimension. The findings present a nuanced understanding of SIM swap fraud, pinpointing areas where AI-driven interventions can address the unique challenges associated with the 2G/3G network transition.

In summary, this approach employed AI-assisted coding, iterative refinement, and theory-driven categorisation within the RAT, establishing a rigorous foundation for analysis and recommendations. This methodology was crucial for managing a large

dataset, ensuring a thorough and relevant synthesis of the literature that informs effective AI solutions to mitigate SIM swap fraud.

3.4 Interpretation and discussion

In the interpretation and discussion phase, findings from the systematic review were synthesised to develop a comprehensive view of the existing evidence. The narrative synthesis served as the foundation for integrating results across studies, offering a cohesive presentation of insights into how AI can address SIM swap fraud, particularly in the context of the 2G/3G network shutdown. By weaving together individual findings, this synthesis provided a robust perspective on the current research landscape and highlighted the key patterns, challenges, and opportunities within the field.

A critical component of the discussion involved acknowledging the limitations inherent in both the included studies and the review process itself. Potential biases, such as publication bias and language restrictions, were addressed, as well as gaps in the existing literature, including limited research from certain geographical regions and underexplored aspects of AI applications for telecom fraud prevention. By openly recognising these limitations, the synthesis highlighted areas where the evidence base may be less comprehensive, ensuring a balanced interpretation of the findings.

The study explored the practical implications of its findings for policymakers, industry practitioners, and researchers. Practical implications:

- For policymakers: The synthesis pointed out the importance of adaptive regulatory frameworks to effectively manage AI-driven fraud prevention tools as they evolve. This regulatory adaptability is essential for ensuring robust, flexible protection in response to rapidly advancing fraud tactics.
- For industry practitioners: Insights were provided on the potential for integrating AI into mobile security systems to mitigate fraud risks during network transitions.

Practitioners were encouraged to adopt AI applications that focus on predictive analytics, real-time monitoring, and enhanced verification processes.

- For researchers: The discussion identified key areas for future research, especially the need for studies examining AI's effectiveness in varied socio-economic and technological contexts. Research in regions heavily impacted by network upgrades, where SIM swap fraud may pose unique challenges, was deemed particularly valuable.

The conclusions presented a concise summary of the main findings and their significance. The review reinforced AI's potential as a powerful tool in combating SIM swap fraud during network transitions, while also emphasising the need for continued research to keep pace with evolving security threats in telecommunications. These conclusions affirmed the relevance of the evidence gathered, providing a solid foundation for further advancements and strategic development in AI-driven telecom security.

3.5 Limitations and challenges of the study

While the study provides a comprehensive examination of AI's role in combating SIM swap fraud during the 2G/3G network shutdown, several limitations and challenges could impact the findings.

3.5.1 Limitations of the systematic literature review

A notable limitation is publication bias. Although the PRISMA guidelines are designed to minimise bias, studies with positive or significant outcomes are often more likely to be published, which can lead to an overestimation of AI's effectiveness in fraud prevention. Additionally, heterogeneity among the studies poses challenges, as the included studies varied widely in methodology, sample size, context, and definitions of SIM swap fraud. This variability complicates the synthesis and comparison of findings, potentially affecting the coherence of the conclusions. Furthermore, the review may

have faced a limited scope if certain relevant grey literature sources, such as unpublished reports and conference abstracts, were difficult to locate or assess.

3.5.2 Limitations of the thematic analysis

Thematic analysis, used for synthesising qualitative data, presents issues of subjectivity, as the interpretation can be influenced by the researcher's perspectives and biases. This may introduce unintended bias, potentially affecting the reliability of the analysis. Furthermore, thematic analysis's in-depth, context-specific focus can result in limited generalisability, as findings derived from specific cases may not apply to broader or different contexts.

3.5.3 Other challenges

The rapidly evolving landscape of SIM swap fraud and AI technologies introduces additional challenges, potentially reducing the long-term applicability of the findings as fraud tactics and prevention tools evolve. Ethical considerations are also critical, particularly concerning privacy, data security, and potential biases within AI algorithms, all of which require careful consideration to ensure the responsible deployment of AI in fraud prevention.

3.5.4 Mitigation strategies

To address publication bias, the literature search included grey literature and unpublished studies. For subjectivity in thematic analysis, automated deductive coding was used to ensure a structured coding framework, improving inter-rater reliability. Given the rapidly evolving landscape of fraud and AI, this research recommends ongoing study and monitoring to adapt prevention strategies to emerging threats. Ethical considerations were addressed through engagement with relevant literature on the ethical implications of AI in fraud detection, ensuring transparency, accountability, and adherence to ethical standards in AI-based solutions.

By acknowledging the limitations and implementing mitigation strategies, this study aimed to provide reliable insights into SIM swap fraud and contribute to the development of effective, ethically grounded prevention strategies.

While the research findings confirm AI's potential in detecting SIM swap fraud, a critical review reveals notable blind spots. Many studies emphasise technical performance metrics (e.g. accuracy, precision) but give little attention to ethical or practical implementation challenges, such as the availability of training data, resource constraints, or user trust. Moreover, most empirical evidence stems from developed markets, limiting the transferability of findings to South Africa's context. This imbalance in the literature not only narrows the scope of AI solutions proposed but also risks exacerbating digital inequalities if applied uncritically.

3.6 Data collection methods, population, and sample

3.6.1 Data collection method

The method applied in the identification and collection of relevant literature follows the PRISMA guidelines. The method is covered in detail in the section on data collection for the systematic review (page 61).

3.6.2 Population

In this study, "population" refers to the body of literature systematically searched, screened, and analysed to address the research objectives. For this study on SIM swap fraud during the 2G/3G network shutdown, the population encompassed a broad range of published and grey literature relevant to the topic.

The primary focus was on published research studies, including peer-reviewed articles, research reports, and dissertations directly related to SIM swap fraud. These sources covered various aspects of SIM swap fraud, such as trends, tactics, impacts, and the

specific influence of 2G/3G network shutdowns. Additionally, studies exploring AI technologies for detecting and preventing SIM swap fraud were considered essential. Theoretical frameworks, such as the RAT, were also included, as they provide structured insights into the mechanisms behind SIM swap fraud.

Grey literature formed another crucial part of the population, encompassing government reports, white papers, industry publications, and conference proceedings. Although these sources are not peer-reviewed, they often offer valuable insights into SIM swap fraud, particularly from practical or policy perspectives, contributing to a comprehensive view of the issue.

The population was not limited to studies that explicitly mentioned all key terms, such as SIM swap fraud, 2G/3G shutdown, and AI, in their titles or abstracts. Instead, the search strategy was designed to capture relevant studies, even those using alternative terminology, ensuring that pertinent literature was not overlooked due to variations in phrasing.

To refine the study population and maintain quality, inclusion and exclusion criteria were applied rigorously. Only relevant, high-quality studies were included in the final review, with a search timeframe from 2010 to 2024. This timeframe was selected to incorporate recent and up-to-date research while allowing a historical perspective on the evolution of SIM swap fraud controls alongside mobile technology advancements. Studies dating back to 2010 provided valuable context for comparing early SIM swap prevention measures with those developed in response to more recent mobile network advancements.

Defining the population in this way enabled the systematic review to identify and analyse pertinent literature on SIM swap fraud within the context of the 2G/3G shutdown, supporting the study’s aim of providing a comprehensive and current understanding of the issues and potential solutions surrounding SIM swap fraud.

3.6.3 Sample and sampling method

In this study, the sample consisted of the specific studies selected for inclusion, while the sampling method describes the systematic process used to identify and select these studies.

The sampling method was structured to ensure alignment with the research objectives, focusing on key themes such as SIM swap fraud trends, the impact of 2G/3G network shutdowns on these trends, and the application of AI in fraud detection and prevention. Guided by the PRISMA framework, this process upheld principles of transparency, reproducibility, and methodological rigour.

The final sample included studies that met all inclusion criteria, excluding those that did not align with the study's focus. These studies were systematically identified through the defined search strategy, first screened by titles and abstracts, and subsequently evaluated in full text for eligibility.

The sample size was not predetermined but defined by the number of relevant studies identified through the search process, aiming to encompass all eligible studies rather than meet a specific numerical target.

Unlike traditional sampling methods in primary research, the PRISMA approach employs a systematic and comprehensive search and screening process to capture all relevant studies within a defined population. This method ensured that the sample was representative of the available evidence, minimising selection bias. Additionally, the approach facilitated the identification of gaps in the literature, pointing to areas for future research.

3.7 Research instruments

In a systematic literature review, "research instruments" differ from conventional data collection tools, such as interviews or surveys. Instead, this study utilised the following primary instruments:

- Appendix A - PRISMA 2020 checklist: This checklist ensured adherence to PRISMA guidelines, supporting a transparent, structured, and systematic review process.
- PRISMA 2020 Flow diagram (Figure 6): This diagram tracked the selection process, including searches across databases, registers, and other sources, providing a visual summary of study selection and screening.
- Search strategy (p. 61): Outlining specific keywords, search terms, and combinations, the search strategy was essential in defining the initial pool of potential studies and maintaining consistency across databases.
- Inclusion and exclusion criteria (p. 63): These pre-defined criteria helped filter out irrelevant or low-quality studies, ensuring the final sample was both relevant to the research objectives and methodologically sound.
- Appendix C - Data extraction form (Figure 40): A standardised form was used for consistent and objective data extraction from each included study, enabling structured and comparable data analysis.
- Appendix C - Quality assessment tool (Figure 41): This checklist assessed the quality and depth of each study, ensuring only robust research contributed to the findings.

These instruments facilitated a structured, transparent, and reproducible approach, minimising bias, enhancing reliability, and reinforcing the overall rigour of the research.

3.8 Data analysis strategies and interpretation

The data analysis for this research employed qualitative techniques to thoroughly address the research objectives following a structured and transparent approach.

3.8.1 Quality assessment

Quality assessment of the included studies adhered to PRISMA standards, covering essential elements such as title, abstract, methods, results, and narrative discussion. Sci-Space facilitated both qualitative and quantitative rankings of each study, providing a nuanced understanding of quality and relevance. The research supervisor independently reviewed the extracted data, and any discrepancies were resolved through discussion, ensuring consistency in the assessment. Quality assessment findings were integrated into the data synthesis and interpretation phases, helping to highlight any biases or limitations within the available evidence.

3.8.2 Data extraction

A standardised data extraction form was developed to capture all relevant information from the studies meeting inclusion criteria. This form was pilot-tested on a subset of studies to ensure clarity and comprehensiveness, allowing for effective data extraction. The Sci-Space semantic literature review tool was employed to minimise bias and enhance precision during the final data extraction phase. The extraction was optimised to target information directly relevant to the research objectives, with all extracted data rigorously reviewed for accuracy and reliability.

3.8.3 Ensuring Trustworthiness and Quality

In line with the interpretivist paradigm underpinning this research, quality assurance was approached through the lens of trustworthiness, which comprises credibility, dependability, confirmability, and transferability (Lincoln & Guba, 1985).

- Credibility was enhanced through prolonged engagement with diverse data sources and by employing a dual-approach methodology — bibliometric analysis and thematic synthesis. This method triangulation allowed cross-validation of patterns and ensured analytical rigour.
- Dependability was supported by detailed documentation of the analytical procedures, including coding steps in ATLAS.ti, PRISMA-based selection criteria, and iterative refinement of themes. These steps ensured that the research process could be traced and audited.
- Confirmability was established through reflexive practices, where the researcher acknowledged potential biases and consciously bracketed prior assumptions during thematic analysis.
- Transferability was addressed by providing thick descriptions of the South African telecom context, the 2G/3G shutdown, and SIM swap fraud phenomena. This allows future researchers to determine applicability to similar digital environments undergoing technological transitions.

3.9 Ethical considerations

While systematic literature reviews do not involve direct interaction with human subjects, ethical adherence was essential to ensure research integrity and trustworthiness.

- Transparency and rigour: The study adhered to the PRISMA guidelines (Page *et al*., 2021), ensuring transparency and reproducibility. The approach included

clearly defined research objectives, search strategy, and inclusion/exclusion criteria, with any protocol deviations fully documented.

- Objectivity and bias minimisation: Objectivity was maintained through efforts to avoid selective reporting, transparently state potential conflicts of interest, and ensure that personal opinions did not unduly influence the review process (Chigbu *et al*., 2023).
- Fair representation of evidence: Studies with both positive and negative findings were incorporated, providing a balanced perspective on the literature (Uttley *et al*., 2023). Limitations within the included studies were acknowledged.
- Intellectual property and attribution: All included studies were properly cited, following strict anti-plagiarism protocols, and ensuring due recognition of scholars' contributions (Hosseini *et al*., 2023).
- Societal impact: Consideration was given to ensure the AI solutions proposed did not unfairly impact specific groups (Khogali & Mekid, 2023), promoting social equity in fraud prevention.
- Responsible AI principles: Ethical standards for AI deployment, including transparency, explainability, fairness, and respect for human rights, were observed to prevent misuse and unintended harm (Jobin *et al*., 2019).

By addressing these ethical considerations, the review was conducted responsibly and contributed to advancing knowledge on SIM swap fraud, supporting the development of effective, equitable AI-based solutions.

CHAPTER 4. SYSTEMATIC LITERATURE REVIEW

4.1 PRISMA framework

The PRISMA framework (Page *et al*., 2021), as illustrated in Figure 6, provided a structured, transparent, and reproducible approach to conducting the systematic literature review.

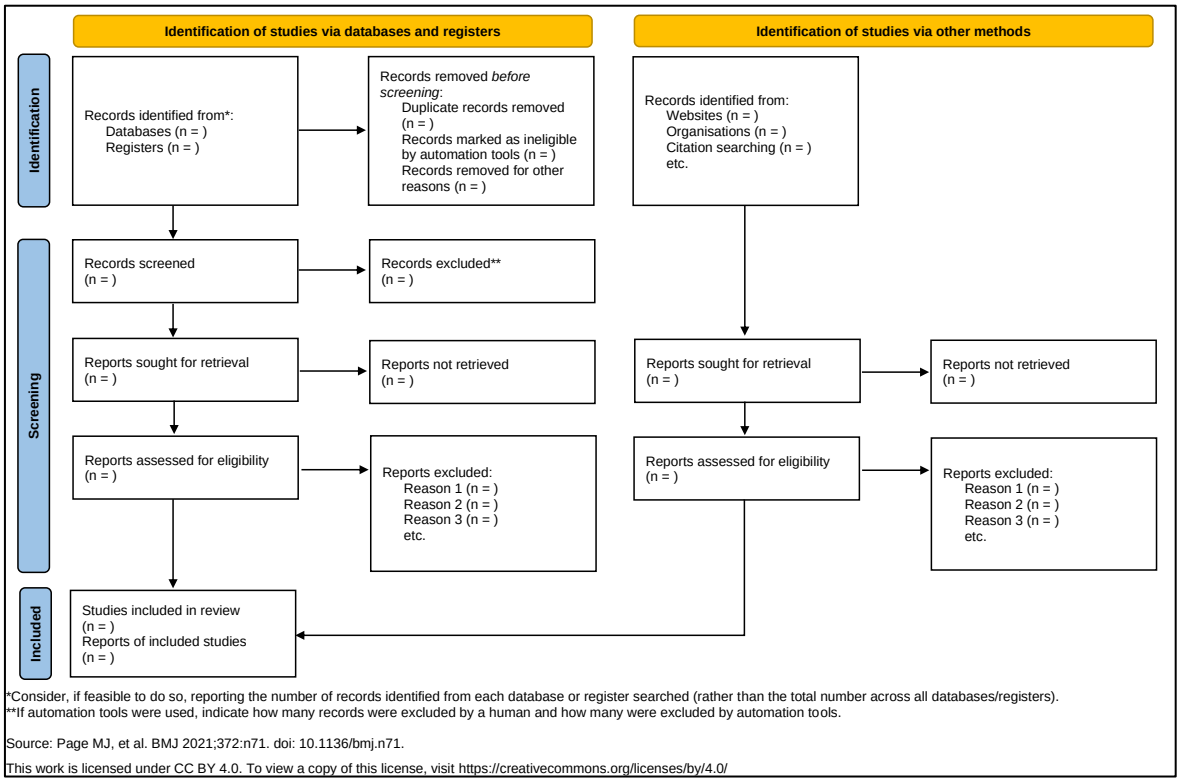


Figure 6: PRISMA 2020 flow diagram for new systematic reviews which included searches of databases, registers, and other sources

The PRISMA checklist offered a structured framework guiding each step of the review process:

1. Identification: In this initial step, a comprehensive search strategy was developed to locate relevant studies across a range of sources, including

academic databases, grey literature, and relevant websites. Carefully selected search terms covered a broad spectrum of topics related to AI, SIM swap fraud, fraud detection, and the 2G/3G network shutdown. This strategy ensured a thorough and aligned search with the study's central themes.

2. Screening: The identified studies were then evaluated based on pre-defined eligibility criteria, focusing on relevance to the research objectives, study design, methodological quality, and publication date. By applying these criteria, the screening stage ensured that only studies of sufficient quality and relevance advanced to the next stage of the review.
3. Eligibility: In this phase, full-text assessments were conducted on studies that met the screening criteria, allowing for a deeper evaluation of their content and methodological rigour. Exclusion reasons were documented at this stage, ensuring transparency in the selection process and a final study sample that aligned closely with the research objectives.
4. Inclusion: Studies that passed the eligibility phase were included in the final review, and key data was extracted from each study. This data encompassed study design, sample size, AI techniques employed, evaluation metrics, and main findings. Systematic data extraction laid a solid foundation for synthesising the literature in a structured and coherent manner.
5. Synthesis: The final stage involved a narrative synthesis of the extracted data, summarising individual study findings while identifying patterns, trends, and gaps across the literature. This narrative synthesis enabled a holistic interpretation, allowing for a cohesive presentation of insights that informed the study's overall conclusions.

By following these structured steps, the PRISMA checklist ensured a rigorous, transparent, and comprehensive review process. This approach facilitated a thorough understanding of the existing literature on AI applications in SIM swap fraud prevention, particularly within the context of the 2G/3G network shutdown.

4.2 Rationale for the PRISMA research design

The PRISMA research design was chosen for its alignment with the study's objectives and its well-established suitability for conducting systematic literature reviews. This design facilitated a structured and rigorous approach to identifying and analysing literature relevant to AI and SIM swap fraud in the context of the 2G/3G network shutdown, ensuring the research objectives were thoroughly addressed and supported by a comprehensive knowledge base.

The systematic literature review approach enabled a focused yet expansive exploration of pertinent studies. Using PRISMA's structured review process, the study ensured that relevant literature was comprehensively identified and analysed, providing a robust foundation for addressing the research objectives.

PRISMA also enhanced the rigour and transparency of the research process. Its step-by-step guidelines enabled a clear, reproducible approach to study selection, data extraction, and synthesis, bolstering the credibility and validity of the findings. By documenting each stage in detail, PRISMA supported replicability and verification, contributing to the study's reliability.

Furthermore, narrative synthesis, integral to this systematic review, allowed for a detailed consolidation of findings across studies. This approach enabled the research to present a cohesive summary of patterns, trends, and gaps in the literature, essential for forming a well-rounded perspective on AI applications in SIM swap fraud prevention. Additionally, by identifying key gaps and limitations in existing literature, the study highlights areas for further exploration, offering a foundation for future advancements in the field.

4.3 Advantages of the design

The PRISMA framework provided several significant advantages that strengthened the study:

- Comprehensive review: The PRISMA framework enabled a thorough review of existing literature, minimising biases, and increasing reliability. Through structured study selection, data extraction, and synthesis, PRISMA facilitated an inclusive review, allowing for a robust understanding of key themes in AI applications for SIM swap fraud prevention.
- Evidence-based recommendations: The design supported the development of actionable recommendations for stakeholders, including policymakers, practitioners, and researchers. By synthesising findings from multiple studies, the research provides practical, evidence-based insights to guide stakeholders in combating SIM swap fraud, particularly during the 2G/3G network shutdown.

4.4 Disadvantages of the design

While effective, the chosen research design also presented limitations:

- Publication bias: Systematic reviews are susceptible to publication bias, as studies with positive or significant results are more likely to be published. This bias may limit comprehensiveness, potentially underrepresenting studies with null or negative outcomes in the analysed literature.
- Resource-intensive process: The systematic review process was time-consuming and labour-intensive. Meticulously identifying, screening, and synthesising studies, alongside detailed documentation to ensure transparency and adherence to PRISMA, demanded significant resources.

Despite these limitations, the systematic literature review was ultimately deemed the most appropriate approach for this research. Its strengths, ensuring reliability,

transparency, and actionable recommendations, outweighed its limitations, contributing to the study's credibility and practical relevance in understanding AI's potential for addressing SIM swap fraud during the 2G/3G network transition.

4.5 Procedure for data collection

The data collection process centred on retrieving and synthesising information from existing literature.

4.5.1 Search strategy

The literature search spanned six major databases, Google Scholar, IEEE Xplore, ProQuest Telecommunications, ScienceDirect, Scopus, and the Scopus AI Semantic Search Engine, selected to cover both scholarly and industry-specific research on telecommunications, cybersecurity, and AI applications.

The search utilised a range of keywords and Boolean operators to locate studies covering primary areas of SIM swap fraud, the 2G/3G shutdown, and AI. Each search term was derived from key topics in the research objectives and categorised into primary, secondary, and tertiary terms. Examples of primary terms included "SIM swap fraud," "AI in fraud prevention," and "2G network shutdown," while secondary and tertiary terms included "social engineering in fraud," "multi-factor authentication," and "telecom regulations." The multi-layered use of Boolean operators ensured flexibility in broadening or narrowing results across databases, maximising relevant article retrieval.

To manage relevance and prevent information overload, each search was limited to the first 200 results or 10 pages per term, as results in most databases are ranked by relevance. Table 1 lists the search terms used, while Table 2 outlines additional semantic search terms queried in Scopus AI. The semantic search process was further refined through:

- Open-ended queries (for example, “How is AI improving fraud detection in telecom?”)
- Conversational phrases (for example, “ways to prevent SIM swap attacks”)
- Broader exploratory keywords (for example, “network transitions and fraud risks”)

Furthermore, Scopus AI’s concept map visually displayed thematic linkages, enabling cross-validation of themes identified through bibliometric and qualitative analysis. Citation chaining (or snowballing) was then applied, adding 31 relevant articles cited by shortlisted studies.

Table 1: List of search terms used

Category	Primary Search Terms
SIM Swap Fraud	"SIM swap fraud" OR "SIM swapping" OR "SIM swap attacks" OR "SIM hijacking" OR "mobile phone fraud" ("SIM swap" OR "SIM hijacking") AND ("fraud prevention" OR "cybersecurity") ("SIM swap fraud" AND "cybersecurity vulnerabilities") OR ("mobile network vulnerabilities" AND "SIM hijacking")
Artificial Intelligence in Fraud Prevention	("Artificial intelligence" OR "AI") AND ("fraud prevention" OR "fraud detection") ("Machine learning" OR "deep learning") AND ("fraud detection" OR "cybersecurity") ("AI-powered security" AND "fraud prevention") OR ("AI applications" AND "telecom security")
2G/3G Network Shutdown	("2G network shutdown" OR "3G network shutdown") AND ("fraud" OR "telecom security") ("network migration" AND "4G" OR "5G") OR ("legacy network phase-out" AND "SIM swap fraud") ("2G shutdown" OR "3G shutdown") AND ("AI" OR "cybersecurity vulnerabilities")
Fraud Techniques and Vulnerabilities	("Social engineering" AND "SIM swap fraud") OR ("fraud techniques" AND "cybersecurity") ("Cybersecurity vulnerabilities" AND "SIM swapping") OR ("mobile network vulnerabilities" AND "fraud prevention") "Deepfakes" AND ("fraud prevention" OR "cybersecurity")
Digital Technologies for Addressing Fraud	("Biometric authentication" AND "SIM swap") OR ("multi-factor authentication" AND "fraud prevention") ("Blockchain-based identity verification" OR "encryption in mobile networks") AND ("fraud" OR "AI") ("Digital technologies" AND "telecom security") OR ("fraud detection" AND "biometric authentication")
Regulatory and Policy Frameworks	("Telecom regulations" AND "fraud prevention") OR ("financial security regulations" AND "AI") ("Data privacy laws" AND "SIM registration") OR ("regulatory frameworks" AND "network shutdown") ("Telecom policy" OR "financial security") AND ("fraud" OR "network transition")
Case Studies and Implementation Examples	("Case studies" AND "SIM swap fraud") OR ("lessons" AND "network transitions") ("AI implementation" AND "telecom security") OR ("success stories" AND "fraud prevention") ("Case examples" AND "SIM hijacking") AND ("network security" OR "AI")
Technological Advancements and Trends	("Innovations" AND "mobile security") OR ("trends" AND "AI for cybersecurity") ("Future of mobile networks" AND "fraud prevention") OR ("emerging threats" AND "mobile banking") ("Technological advancements" AND "SIM swap") AND ("AI" OR "fraud")
Geographical and Contextual Factors	("Fraud trends" AND "regions") OR ("telecom security" AND "developing countries") ("Impact of network shutdowns" AND "globally") OR ("comparative studies" AND "network transitions") ("Regional fraud" AND "network security") OR ("network shutdown" AND "global impact")

Table 2: Semantic search terms

Category	Semantic Search Terms
SIM Swap Fraud and Cybersecurity Concerns	How SIM swap fraud is affecting mobile security Key vulnerabilities exploited in SIM swapping attacks Role of social engineering in SIM hijacking and fraud Impact of SIM swap fraud on personal data and account security Common techniques used in SIM swap attacks and their countermeasures
AI and Machine Learning in Fraud Detection	How AI is being used to detect and prevent fraud in telecom Machine learning models for identifying fraud in mobile networks Application of deep learning for preventing SIM hijacking Artificial intelligence-driven solutions for telecom security Leveraging AI to safeguard against SIM swap and other mobile fraud
2G/3G Network Shutdown and Security Implications	How shutting down 2G/3G networks affects mobile security Migration from 2G/3G to 4G/5G and its impact on fraud risks Security challenges in transitioning legacy networks to modern standards Risks and benefits of phasing out old mobile networks Influence of network upgrades on telecom security and fraud prevention
Fraud Prevention Technologies and Methods	Role of biometric authentication in preventing SIM swap fraud How blockchain technology can enhance identity verification in telecom Multi-factor authentication as a tool against mobile fraud Encryption methods used to secure mobile networks from fraud Comparing digital technologies for fraud prevention in telecom
Regulatory Frameworks and Policies in Telecom Security	Impact of telecom regulations on preventing SIM swap fraud How data privacy laws influence SIM registration and fraud prevention Regulatory policies addressing network shutdowns and fraud risks Financial regulations focused on preventing telecom fraud Legal approaches to combating SIM hijacking in mobile networks
Technological Advancements and Emerging Trends	Emerging trends in AI for mobile network security Future developments in mobile networks and their security implications How mobile security technologies are evolving with new threats Innovations in fraud detection for telecom networks The future of telecom security amid evolving fraud techniques
Global Perspectives and Regional Factors in Telecom Fraud	How telecom fraud varies across different regions Security challenges in telecom for developing countries Global impact of network shutdowns on mobile fraud Regional trends in mobile fraud and telecom security Comparative perspectives on network transition and fraud risks

4.5.2 Inclusion and exclusion criteria

The inclusion and exclusion criteria were applied initially to titles and abstracts (or full texts where no abstract was available) to exclude irrelevant studies early in the process.

- Inclusion criteria:
    - Articles published between 2010 and 2024 (backward citation chaining included earlier pivotal studies)
    - Studies on SIM swap fraud, 2G/3G shutdown, or AI applications in fraud detection
    - Peer-reviewed studies or high-quality grey literature

    - Studies in English only.
- Exclusion criteria:
    - Non-English studies
    - Studies outside the search window unless captured through citation chaining.

The initial search yielded 3,280 articles. After removing duplicates, 2,970 unique articles remained. Title and abstract screening excluded 2,160 records unrelated to the study's focus, such as articles not addressing SIM swap fraud, network transitions, or AI in fraud prevention. The remaining 810 articles underwent full-text assessment against inclusion and exclusion criteria, with 620 excluded primarily due to publication date, peer-reviewed status, language, or relevance.

The final selection of 190 studies comprised:

- Google Scholar: 47
- IEEE Xplore: 7
- ProQuest Telecommunications: 20
- ScienceDirect: 2
- Scopus (including Scopus AI Semantic Search): 40
- Snowballing (backward citation tracing): 31
- Grey literature: 43.

These selected articles supported a comprehensive review of AI applications in SIM swap fraud prevention amid network transitions.

4.5.3 Literature search limitations and mitigation measures

Despite the thorough search process, several limitations emerged:

- Database and source bias: Relying on specific databases may have led to an emphasis on studies accessible within these platforms, potentially overlooking

region-specific journals. Including grey literature and using citation chaining helped mitigate this limitation.

- Language restriction: Restricting to English-language articles might exclude valuable non-English research, particularly relevant in regions with distinct mobile fraud dynamics. However, prioritising studies with global or cross-regional analyses partially addressed this.
- Date range limitation: The focus on 2010–2024 could risk excluding foundational studies. Backward citation chaining allowed the inclusion of pivotal studies predating this range, ensuring a comprehensive perspective.
- Keyword sensitivity in semantic search: Variability in terminology across disciplines may have led to missed studies. Broader semantic search terms helped capture conceptually related literature that may not have been identified through standard keywords.
- Search result limitation: Restricting to 200 results per search term may have excluded relevant but lower-ranked studies. However, this limit was considered reasonable, given that highly relevant articles typically rank early in search results.

Overall, this structured approach ensured a relevant and comprehensive selection of studies, minimising bias and reflecting a balanced view of the literature on AI-driven fraud prevention in telecommunications during network transitions. Figure 7 illustrates the PRISMA flow diagram output for this rigorous systematic literature search.

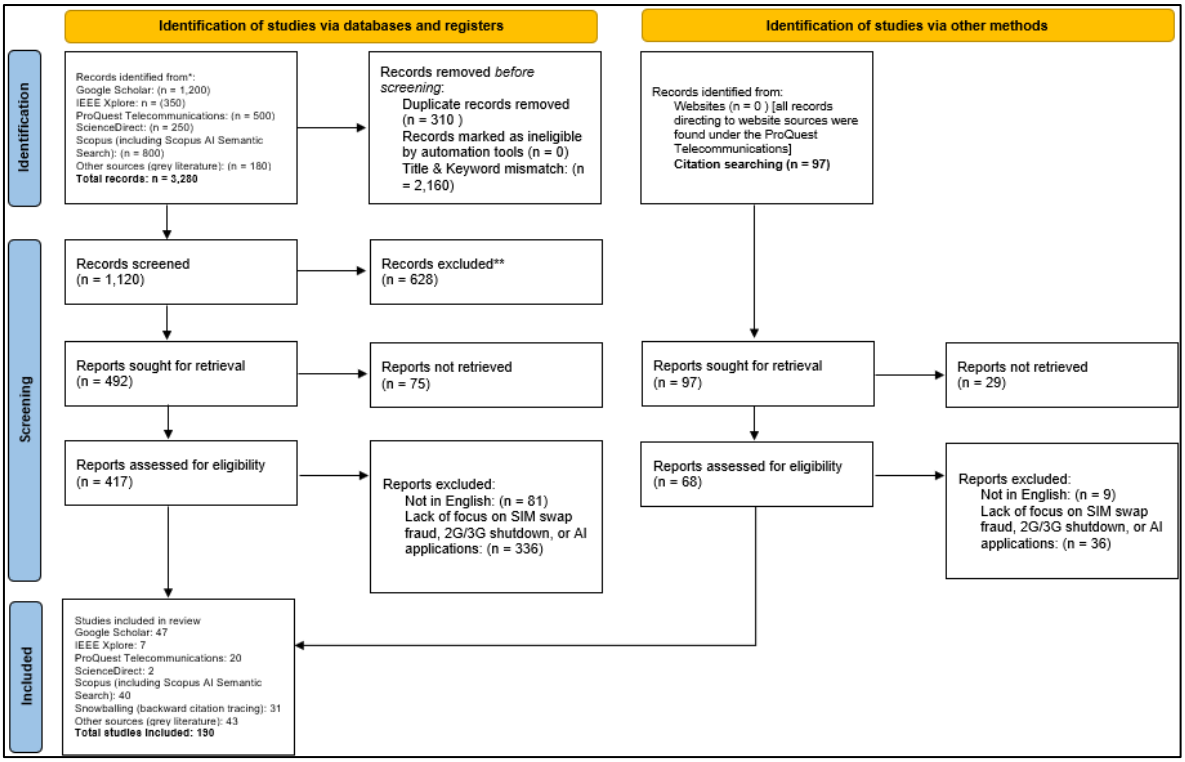


Figure 7: PRISMA flow diagram output for the systematic literature search

CHAPTER 5. BIBLIOMETRIC ANALYSIS FINDINGS AND DISCUSSION

5.1 Introduction

This chapter provides a systematic bibliometric analysis of the research surrounding AI applications for SIM swap fraud detection, particularly in the context of network shutdowns. Utilising Bibliometrix software, the analysis highlights key publication trends, influential contributors, thematic development, and collaborative networks within the field. This data-driven approach offers an organised perspective on the evolving academic landscape, enabling an assessment of existing research contributions and the identification of gaps for further exploration.

5.2 Data import

The data was imported from Scopus in BibTeX format into Bibliometrix, and the completeness of the metadata was assessed and reported as shown in Table 3. Key fields such as abstract, affiliation, author, document type, journal, language, publication year, title, and total citations had zero missing entries, ensuring high data integrity for core analyses. Minor missing entries in the cited references and DOI fields (1.41% and 7.04%, respectively) were unlikely to impact the analysis. However, substantial missing data in the keywords and corresponding author fields (21.13% and 35.21%, respectively) limited some aspects of keyword and author collaboration analysis. Keywords plus (ID) was selected as the primary thematic analysis unit to mitigate these issues.

In summary, the overall imported dataset, with the main information shown in Figure 8, had excellent coverage in the most critical fields, ensuring the integrity of the bibliometric analysis. Some minor gaps in keywords and corresponding I author information may have limited certain analyses, but the dataset remains

highly usable for the core bibliometric insights. Special attention was therefore given to thematic and author collaboration analyses to account for missing data in those fields.

Table 3: Missing data analysis

Metadata	Description	Missing Counts	Missing %	Status
AB	Abstract	0	0.00	Excellent
C1	Affiliation	0	0.00	Excellent
AU	Author	0	0.00	Excellent
DT	Document Type	0	0.00	Excellent
SO	Journal	0	0.00	Excellent
LA	Language	0	0.00	Excellent
PY	Publication Year	0	0.00	Excellent
TI	Title	0	0.00	Excellent
TC	Total Citation	0	0.00	Excellent
CR	Cited References	1	1.41	Good
DI	DOI	5	7.04	Good
ID	Keywords Plus	10	14.08	Acceptable
DE	Keywords	15	21.13	Poor
RP	Corresponding Author	25	35.21	Poor
WC	Science Categories	71	100.00	Completely missing

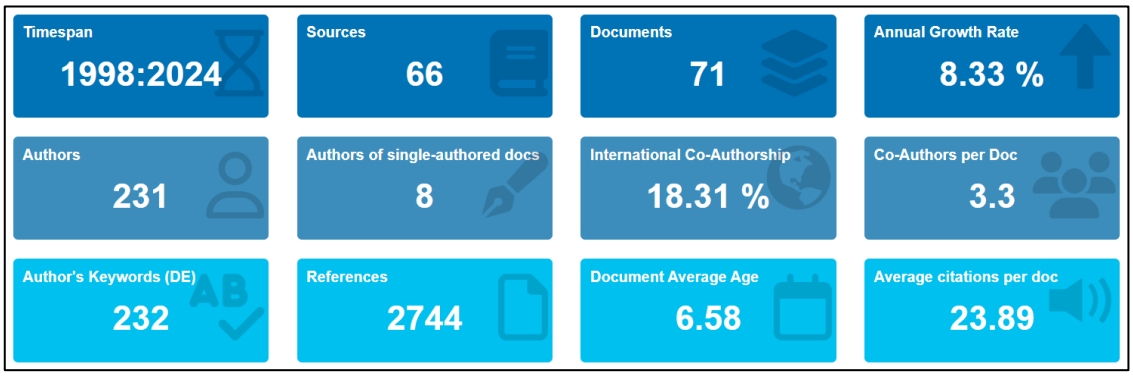


Figure 8: Dataset - main information summary

Due to the challenges associated with the author keywords (DE), this analysis elected to use keywords plus (ID) as the primary unit for thematic analysis. The Three field plot in Figure 9 shows the linkage between the flawed author

keywords (DE), the keywords plus (ID), and the spatial distribution by country (AU_CO).

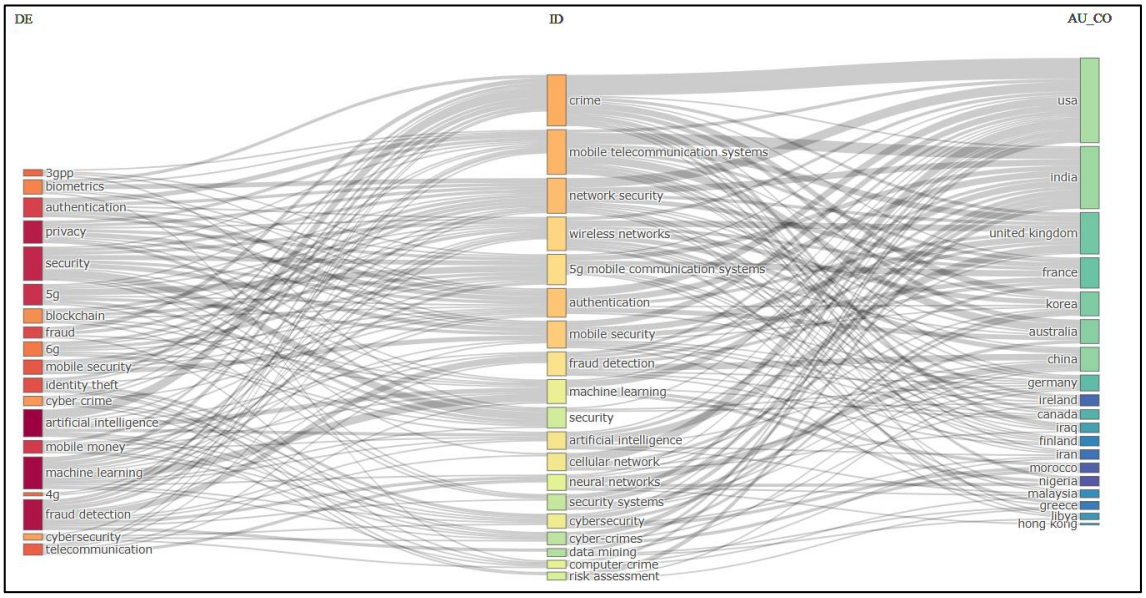


Figure 9: Three field plot

5.3 Annual scientific production

The annual scientific production (Figure 10) reveals three distinct phases:

- 1998-2007: Minimal research output, indicating an early, nascent stage for SIM swap fraud and AI-driven fraud detection.
- 2008-2019: A gradual increase in interest, reflecting foundational work in fraud detection and telecommunications security.
- 2020-present: A significant surge in publications aligns with digital transformation due to the COVID-19 pandemic, highlighting increasing interest in mobile security, fraud detection, and AI.

The recent spike in publications, particularly in 2023 and 2024, spotlights a critical shift in research interest, with mobile network security, 5G transitions, and AI-based fraud detection gaining prominence.

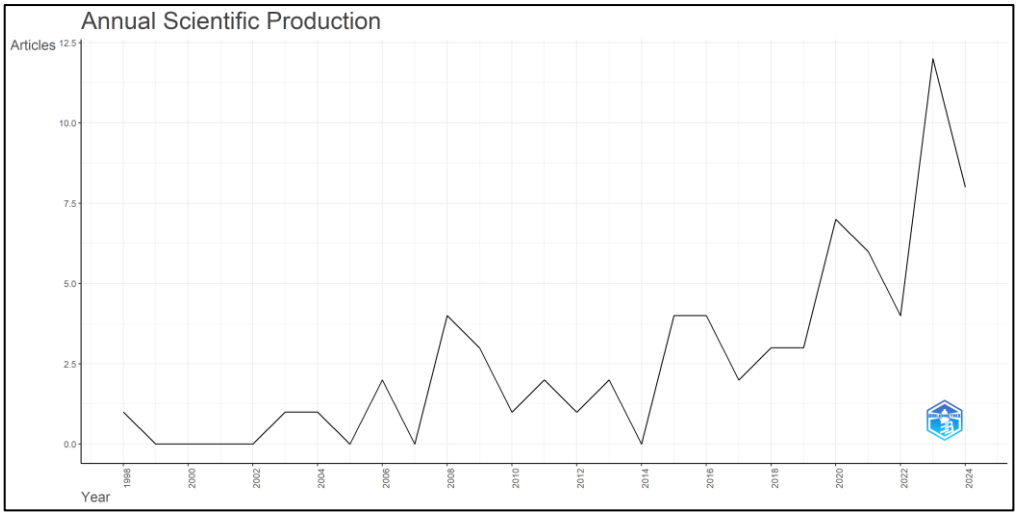


Figure 10: Annual scientific production

Notably, the only significant cross-country collaboration in the data was between China and the USA. Furthermore, the scientific production data indicates a high concentration of research activity in technologically advanced nations, such as the USA, India, and China (Figure 11). These countries are driving research in areas related to AI, telecommunications, and cybersecurity. However, there is also significant participation from other countries across Europe, Asia, and Africa, suggesting that the topic is of global interest, with various regions contributing to advancements in the field. This diversity of contributions reflects the widespread relevance of the research topic across different contexts and regions.

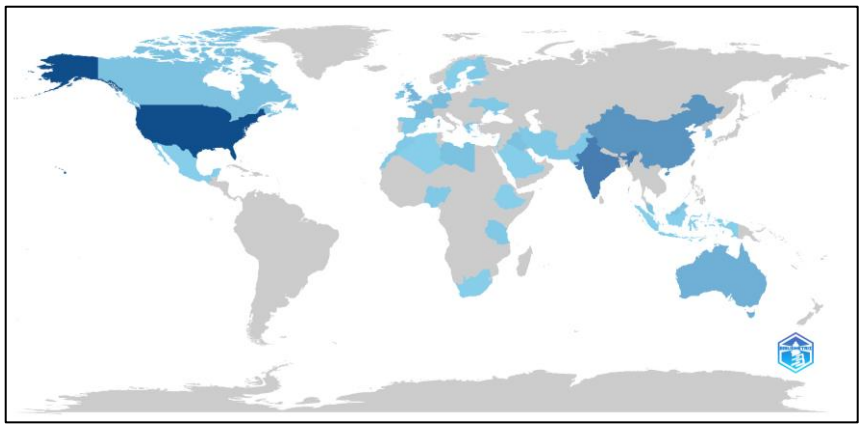


Figure 11: Countries' scientific production

5.4 Authorship and Influence Patterns

5.4.1 Source impact and productivity

The table in Appendix D presents an overview of the source impact and productivity. Several sources, such as IEEE Access and Lecture Notes in Computer Science, demonstrate high productivity and citation impact, with IEEE Access showing considerable recent contributions. High-impact conferences like ACM and IEEE/ACIS also emerge as influential sources. However, many sources remain niche with limited citation counts, suggesting potential areas for increased research visibility.

5.4.2 Author impact and productivity

The table in Appendix E shows the report on author impact and productivity. Authors such as Lu and Aderounmu show higher productivity and citation impact, while the broader field remains populated by researchers with single publications. Recent contributions indicate growing interest, although the field still lacks a large cohort of highly influential authors, reflecting an emergent research area.

In summary, the data reveals that most authors have made limited but growing contributions to the field, with only a few emerging as major influencers based on their citation impact and number of publications. The relatively low h-index and g-index across most authors suggest that the research area is still developing, with many authors contributing to an emerging body of knowledge. However, recent growth in publication numbers and citation counts, particularly from 2020 onwards, highlights that the field is gaining momentum, with key authors beginning to make significant impacts in AI-based fraud detection and network security research.

5.4.3 Co-citation network analysis

The co-citation network analysis (Figure 12) highlights six clusters representing thematic similarities among authors. Key influencers include Fawcett (1997) and Bagga (2020), who bridge thematic groups, while clusters suggest focal points around historical AI and fraud detection research. The analysis identifies foundational and emerging research themes, guiding the exploration of seminal and recent works.

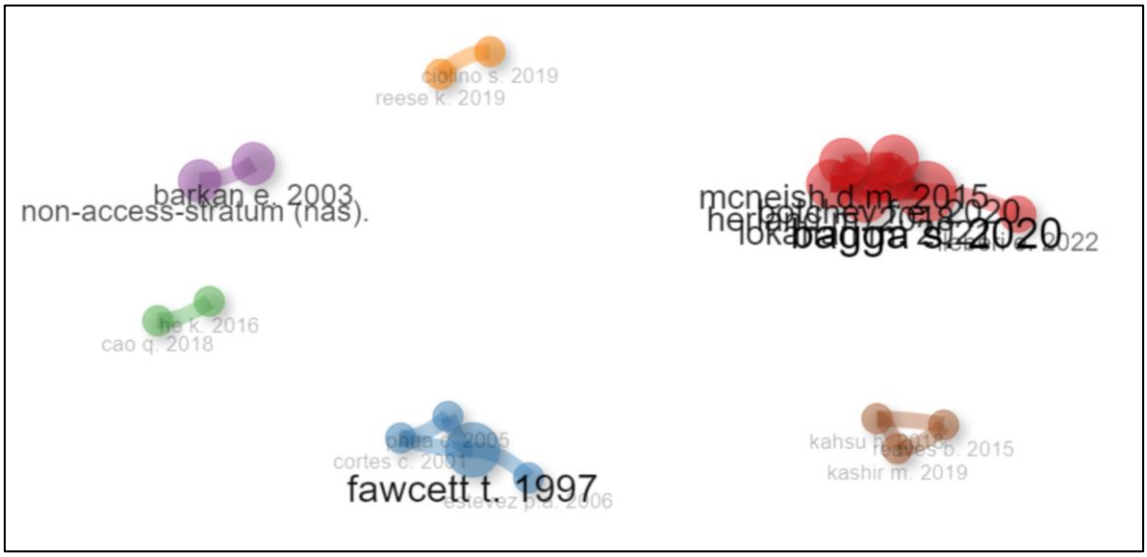


Figure 12: Co-citation network diagram

The co-citation network analysis highlights the key authors contributing to the field, with a few, such as Fawcett T. 1997 and Bagga S. 2020, emerging as central figures in connecting different parts of the network and having high influence. The clustering indicates that there are thematic subgroups within the literature, with each cluster focusing on specific aspects of AI, fraud detection, or telecommunications. Understanding the position and influence of these authors can guide further exploration of seminal works and emerging research areas.

5.5 Emerging Research Themes and Directions

5.5.1 Keyword analysis

The keywords plus word cloud (Figure 13) shows primary themes like crime, network security, and mobile telecommunications, underscoring the critical role of AI in addressing digital fraud. Emerging technologies, including machine learning and 5G, feature prominently, indicating a growing reliance on AI and mobile security in telecommunications.

Figure 13: Keywords plus - word cloud

The keyword frequency analysis highlights several core research areas within the broader field of fraud detection, AI, and telecommunications security. Crime prevention, network security, and authentication emerge as dominant concerns, with a strong focus on leveraging AI technologies to address these challenges. The terms also point out the critical importance of securing mobile telecommunications systems, as these networks are central to both modern communications and the economy. The research landscape is therefore focused on balancing technological advancement with robust security measures, particularly in the context of rapidly evolving mobile and digital ecosystems.

5.5.2 Trend topics analysis

Trends from 2007 to 2024 (Figure 14) highlight an evolution from traditional fraud detection to mobile security and AI-driven solutions. Research focus shifted from early fraud detection to mobile telecommunications, 5G, and AI-based fraud detection, with a recent emphasis on cybersecurity and risk assessment.

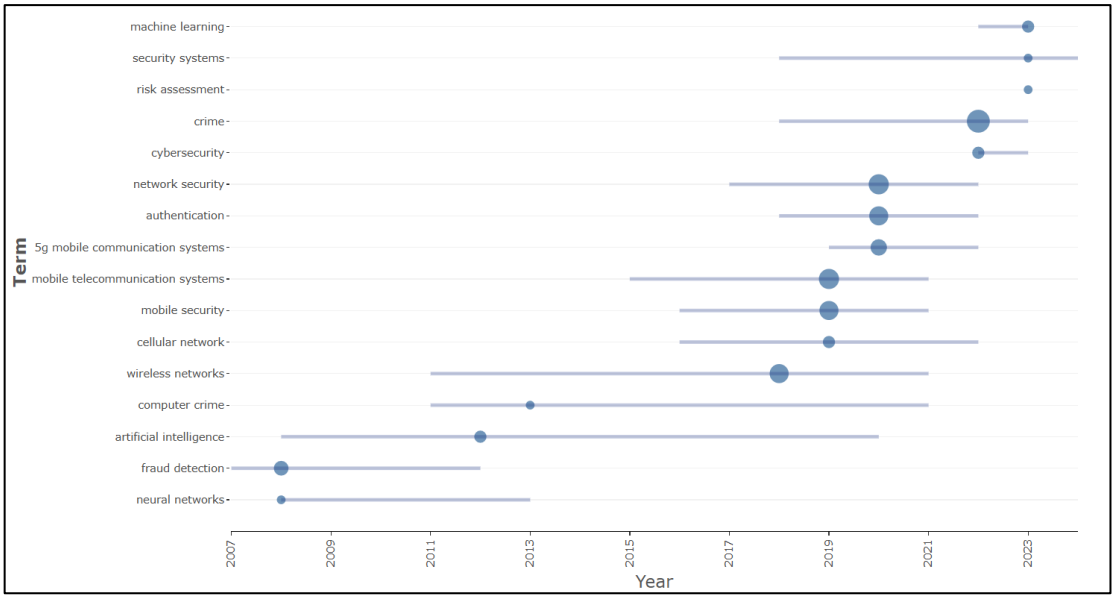


Figure 14: Trend topics plot

The timeline data shows a clear progression from early concerns about fraud detection and neural networks to a broader focus on mobile telecommunications and security systems in recent years. As telecommunications systems evolve, as is the case with the rise of 5G, the research focus has shifted towards securing these infrastructures through cybersecurity, machine learning, and risk assessment. The increasing prevalence of crime and cyberattacks has further driven research toward more advanced authentication methods and robust security systems, making these topics central to current and future research efforts.

5.5.3 Keywords plus co-occurrence analysis

The keywords plus co-occurrence network analysis (Figure 15) reveals interconnected research themes across crime, telecommunication security, and AI techniques. High betweenness centrality for terms like crime and network security illustrates their centrality in linking topics, while clusters indicate thematic cohesion around mobile communications, fraud detection, and emerging technologies.

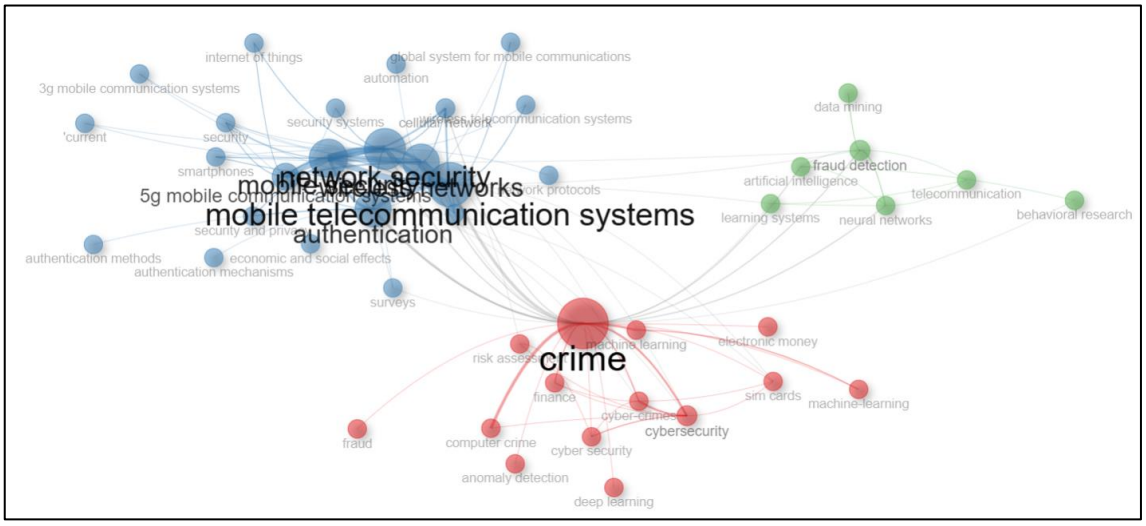


Figure 15: Keywords plus co-occurrence network

The network analysis demonstrates that research on crime, cybersecurity, and fraud detection is highly interconnected with the telecommunications sector, particularly as mobile networks become more prevalent and complex. The application of AI technologies, including machine learning and neural networks, plays a critical role in addressing these challenges, as reflected in the central positions of these terms. Securing mobile and network infrastructures while combating cybercrime remains a major focus, with authentication and security systems emerging as essential components of this research domain.

5.5.4 Thematic mapping

The thematic mapping (Figure 16) highlights clusters centred on fraud detection, crime prevention, and mobile network security. Each cluster reflects specialised research areas, such as crime analysis, telecommunications security, and advanced AI-based fraud detection. Emerging AI technologies are instrumental in these clusters, with applications spanning fraud prevention and mobile infrastructure security.

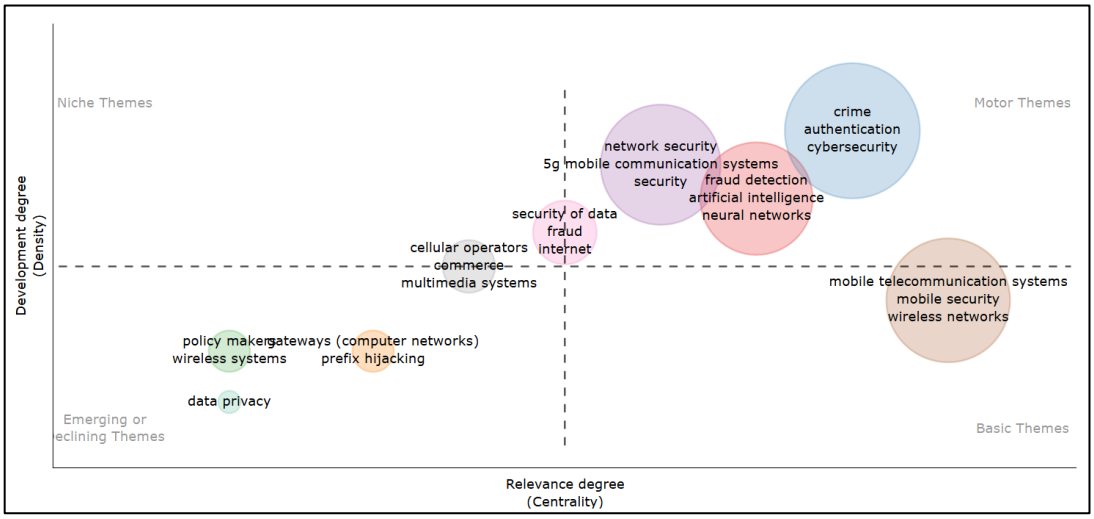


Figure 16: Thematic mapping

1. Fraud detection cluster (Cluster 1):
    - Fraud detection is a prominent theme, with high betweenness centrality (1063.09), indicating it plays a crucial role in connecting other terms related to fraud prevention. It is associated with subfields like artificial intelligence (524.07), neural networks (558.80), and data mining (687.42), which are instrumental in advancing fraud detection techniques.
    - The presence of telecommunication and telecom frauds in this cluster suggests that much of the research is focused on fraud prevention within the telecommunications sector, where advanced AI-driven techniques are being applied.

- Terms such as smart cards, fraudsters, and machine learning techniques emphasise the practical application of AI to identify and mitigate fraudulent activity.
- Deep learning and behavioural research are also featured, highlighting the use of advanced models and the study of human behaviour in identifying fraud.

2. Crime cluster (Cluster 2):
    - Crime has the highest betweenness (6726.97) and PageRank (0.037), making it the most central node in the network. This signifies its critical role in connecting other themes, particularly those related to cybersecurity and risk assessment.
    - The presence of authentication (1638.05) and cybersecurity (240.34) highlights the importance of securing systems to prevent crime, especially in digital environments. Cybercrimes and computer crimes are also key topics in this cluster, reflecting concerns over digital threats.
    - Risk assessment, cyberattacks, and cyberspaces are other important terms, emphasising the need to evaluate and mitigate risks in increasingly interconnected digital systems. This shows how research in this area is focused on understanding the broader impacts of cybercrime and identifying potential vulnerabilities in systems.
3. Network Security Cluster (Cluster 4):
    - Network security and mobile telecommunication systems are pivotal to this cluster, with high betweenness centrality (3389.43 and 2384.16, respectively). These terms represent core areas of concern in the telecommunications field, especially with the rollout of 5G mobile communication systems (1772.38) and the growing demand for mobile security (1984.29).
    - This cluster also contains terms like security systems, internet of things, and blockchain, indicating that research is addressing emerging technologies and their associated security challenges. Authentication

methods, multi-factor authentication, and privacy are other significant topics, reflecting ongoing efforts to secure networks and protect user data.

- The appearance of queueing networks and security features suggests a technical focus on optimizing network performance while ensuring robust security measures.

4. Mobile Telecommunications Cluster (Cluster 6):
    - Terms such as wireless networks (2360.42), cellular network (521.51), and global system for mobile communications indicate the cluster's strong focus on mobile communications infrastructure. Smartphones and mobile network operators reflect the importance of securing mobile devices and services.
    - Denial-of-service attacks, fraud prevention, and security vulnerabilities are key concerns in this cluster, emphasizing the need for robust defense against common threats to mobile systems.
    - 3G and 5G mobile communication systems indicate that the research is evolving alongside technological advancements, focusing on both legacy and next-generation systems.
5. Data Privacy and Security of Data Cluster (Cluster 7):
    - Security of data (874.93) and fraud (200.94) are central terms, highlighting concerns about protecting sensitive information in digital environments. Data privacy (227.29) also appears, showing that protecting user privacy is a key focus area.
    - Internet, websites, and cellular operators reflect the role of data security in both internet and mobile communications. Commerce and multimedia systems are also linked, indicating the research is addressing the intersection of security, e-commerce, and multimedia data exchange.

This thematic mapping emphasises the critical role of fraud detection, crime prevention, and network security within the broader research landscape. The integration of advanced technologies, such as AI, neural networks, and

blockchain, into security systems is evident, particularly in the telecommunications sector. The clusters also reflect a strong focus on mitigating security risks in mobile communications, with particular attention paid to authentication, data privacy, and protecting mobile networks from emerging threats. As new technologies like 5G and IoT become more widespread, the need for secure, robust systems is a central theme in ongoing research efforts.

5.5.5 Thematic evolution analysis

The thematic evolution (Figure 17) demonstrates a progression from early crime and fraud classification (1998–2011) to mobile security and 5G (2012–2018). Recent focus on cybersecurity and authentication (2019–2021) reflects concerns over digital crime, evolving toward broader cybercrime and network security themes (2022–2024). This evolution draws attention to the research field's adaptation to technological shifts and security challenges.

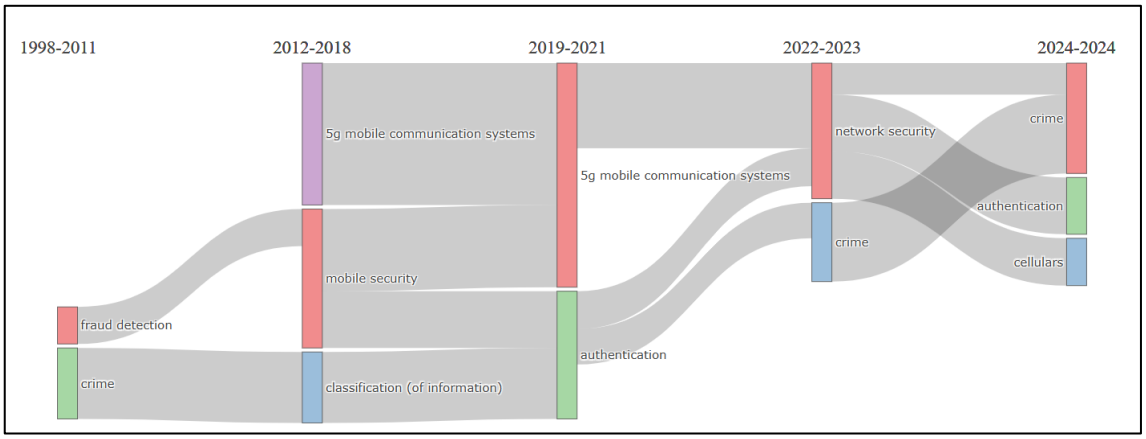


Figure 17: Thematic evolution

1. Crime and fraud detection (1998–2011):
    - In the earliest phase (1998–2011), crime and fraud detection were central themes, associated with terms like classification (of information) and wireless networks. This suggests early research was focused on classifying crime-related data and understanding how information systems could be vulnerable to fraud.

- The evolution from fraud detection to mobile security and wireless networks reflects the increasing relevance of securing mobile systems as mobile devices became more widespread during the 2000s.

2. Mobile and 5G systems (2012–2018):
    - In the 2012–2018 period, there is a notable shift towards mobile telecommunication systems and 5G mobile communication systems, indicating a growing research interest in securing mobile infrastructures. This period marks the beginning of significant technological advancements, particularly the development and testing of 5G networks, which necessitated new security protocols.
    - Mobile security and network security began to emerge more prominently, alongside wireless networks, showing that securing the mobile communication space was becoming a key concern.
3. Authentication and network security (2019–2021):
    - In the 2019–2021 period, authentication and network security became more important. This shift corresponds to the widespread rollout of 5G and the growing importance of protecting user identities and ensuring secure access to mobile and wireless networks.
    - The link between mobile security and authentication stresses the need to secure individual devices and ensure that only authorised users can access sensitive mobile networks, which becomes especially critical with the proliferation of mobile services and e-commerce.
4. Crime and cybersecurity (2022–2024):
    - In the most recent phase (2022–2024), the term crime continues to be a major research focus, evolving from concerns about mobile security to a broader emphasis on cybercrime and fraud prevention. This reflects the growing sophistication of cyberattacks, particularly as mobile networks expand globally.
    - Network security continues to be crucial, especially as it relates to the ongoing evolution of mobile telecommunication systems. The focus on cellular and mobile infrastructure highlights the persistent concern over

securing mobile networks in the face of emerging technologies and cyberthreats.

The main thematic transition highlights evident in the analyses are:

- Fraud detection in earlier phases has morphed into concerns over mobile security, network security, and ultimately, the intersection of crime and cybersecurity. This reflects the broadening of research from traditional fraud detection to the security of complex, large-scale mobile systems.
- Authentication has become a critical theme over time, particularly from 2019 onward, as it relates to both network security and crime prevention. This reflects the increasing reliance on multi-factor authentication and identity verification in securing systems.
- The themes of mobile telecommunications systems and 5G mobile communications remain consistent over time, indicating that securing these networks is a long-term challenge.

The stability column indicates how stable each theme has been over time. The relatively low stability scores suggest that many of these themes are evolving rapidly in response to technological changes and emerging threats. This is particularly true for topics like crime, mobile security, and network security, where new vulnerabilities and challenges are constantly arising.

The thematic evolution therefore shows a clear progression from early concerns about crime and fraud detection toward more complex and interconnected topics, such as mobile security, authentication, and network security. As telecommunications technologies like 5G have become more prevalent, the focus has shifted to securing these infrastructures, with authentication and crime prevention playing central roles. This evolution shows the dynamic nature of the field, where technological advancements continually introduce new security challenges, necessitating ongoing research and adaptation.

5.6 Conclusion

From foundational work on crime and fraud detection, research has evolved to focus on securing 5G networks, integrating AI, and addressing rising cyber threats, indicating a highly adaptive and responsive research landscape.

Fraud detection, crime prevention, and network security remain central themes, with AI applications playing a crucial role. The field increasingly addresses data privacy, authentication, and the protection of mobile infrastructure.

The analysis highlights the critical role of AI technologies like machine learning and neural networks in advancing fraud detection and cybersecurity within telecommunications.

The research is globally distributed, with significant contributions from the USA, India, China, and Europe, highlighting the global relevance of telecommunications security and AI-driven fraud prevention.

Ongoing challenges, such as evolving cyber threats and the transition to 5G, present research opportunities in data privacy, authentication, and AI solutions for emerging security issues.

The analysis highlights interconnected themes across fraud detection, AI, and cybersecurity, suggesting an ongoing emphasis on AI-driven solutions for mobile telecommunications security.

Overall, the bibliometric analysis reveals a fast-evolving research landscape increasingly focused on AI's role in telecom security, but still lacking in regional specificity and targeted exploration of SIM swap fraud. These findings underscore the need for studies like this one, which address these gaps within a localised and applied context. Table 4 is a summary of the key Bibliometric insights:

Table 4: Summary of key Bibliometric insights

Research Growth and Influence	• Strong upward trend in publication volume since 2018, particularly post-COVID. • Top contributing countries: USA, China, and India; limited presence from Africa. • Most cited articles focused on anomaly detection and telecom fraud.
Author and Network Dynamics	• Author collaborations are regionalised with little cross-border interaction. • Core contributors are clustered around a few telecom and AI-focused journals.
Thematic Patterns	• High-frequency keywords: “machine learning”, “fraud detection”, “5G security”. • Emerging themes: integration of AI in telecom security and social engineering defences. • Gaps in literature related to developing economies and SIM swap-specific models.
Implications for This Study	• Confirms AI’s relevance to SIM swap fraud prevention. • Suggests a global knowledge gap in addressing transitional fraud in Africa. • Highlights the need for context-specific AI solutions as addressed in this report.

CHAPTER 6. SYSTEMATIC REVIEW FINDINGS AND DISCUSSION

6.1 Introduction

Having established the dominant research themes, author networks, and evolving topical foci through bibliometric analysis, Chapter 6 now transitions into a thematic synthesis. This chapter applies an interpretive lens to explore how fraud risks and AI interventions are framed in the literature, drawing from the subset of studies identified in the PRISMA review. These insights provide deeper context to the patterns observed in Chapter 5 and explore how theoretical and practical concerns about SIM swap fraud unfold in practice.

This chapter presents the findings from a nuanced thematic analysis of selected literature, carried out using the ATLAS.ti platform. Drawing on insights gleaned from the earlier bibliometric analysis, this thematic approach is designed to identify and explore core themes within the research landscape. Each thematic dimension is systematically examined using analytical units sourced from both scholarly and non-academic materials, reflecting the final coding outcomes. The findings are critically analysed, aiming for a synthesis that offers both depth and clarity on the subject.

6.2 Motivated offender dimension

6.2.1 Offender profiling

This section considers the characteristics of SIM swap fraud perpetrators through the motivated offender lens, specifically addressing: What defines SIM swap fraud perpetrators?

Predominantly, the motivation for SIM swap fraud is financial, as suggested by Abuhamoud, Alsadi, and Ali (2024), and further echoed by Harinath (2023).

These studies reveal how perpetrators manipulate mobile networks to access bank accounts, conduct unauthorised transactions, or steal cryptocurrency (Kim & Kwon, 2022; Hallman, n.d.). The potential for significant financial gain, coupled with the low risk of immediate detection, renders this crime particularly attractive.

While profit appears to be the primary incentive, other motives, such as identity theft or personal vendettas, are also documented. Holtrup *et al*. (2021) observe that some attackers seek maliciously to disrupt communications, while Faircloth *et al*. (2022) discuss cases driven by personal grievances or a desire for notoriety. The allure of quick financial rewards adds layers of psychological complexity to offender profiling in SIM swap fraud. Additionally, the shift to 4G and 5G networks in developing regions presents new opportunities for exploitation, as security measures often lag in these areas (Asmare & Ayalew, 2023; Bello *et al*., 2023).

A key tactic employed by perpetrators is sophisticated social engineering, often involving telecom insiders to transfer phone numbers to fraudulent SIM cards (FCC, 2023). Techniques like smishing (SMS phishing) and vishing (voice phishing) enable fraudsters to gather critical information, such as verification codes (Koul *et al.*, 2020). Alarmingly, recent studies also highlight cases of physical coercion, where perpetrators use threats to compel victims into giving access to financial applications (SABRIC, 2022). These behaviours collectively reflect a high degree of adaptability among SIM swap perpetrators, who demonstrate a readiness to employ deception, manipulation, and even intimidation.

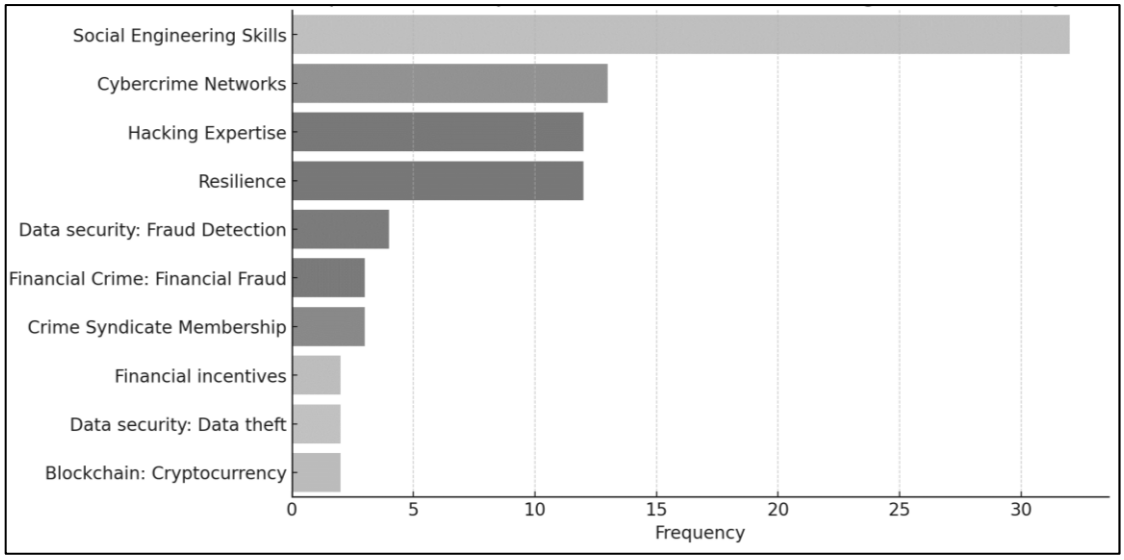


Figure 18: Offender profiling - Most prominent codes

Figure 18 highlights dominant themes in offender profiling, notably social engineering skills, cybercrime networks, hacking expertise, and resilience. These code groupings encompass both technical abilities and psychological strategies.

1. Social engineering skills

   Social engineering emerges as a prevalent theme, identified in 32 instances within the dataset. Fraudsters exploit human vulnerabilities, commonly manipulating customer service representatives to gain unauthorised SIM access. Tambunan *et al*. (2021) suggest that the susceptibility of customer service agents remains a weak point, inadvertently aiding fraudsters. This aligns with the RAT, emphasising how psychological tactics are used to overcome inadequate guardianship. Addressing this vulnerability by reinforcing staff training and security awareness is critical.

2. Cybercrime networks

   The dataset also reveals cybercrime networks, referenced 13 times, indicating that organised crime groups are often behind SIM swap fraud. These syndicates leverage shared resources, insider information, and operational coordination to carry out complex attacks (Tambunan *et al*., 2021; Rana &

Baria, 2015). The involvement of such criminal organisations points to the structured nature of SIM swap fraud, signalling a need for inter-organisational collaboration and rigorous internal control.

3. Hacking expertise

   Hacking expertise is referenced in 12 instances, underscoring the technical prowess of SIM swap perpetrators. Offenders employ advanced hacking tools, including keyloggers and encryption bypass methods (Becker *et al*., 2011; Rana & Baria, 2015). This technical skill set allows them to exploit security vulnerabilities, further emphasising the necessity for sophisticated cybersecurity frameworks.

4. Resilience

   This theme, found in 12 instances, highlights the financial motivations driving SIM swap fraud, with offenders relentlessly targeting mobile banking systems to divert funds (Nama & Obaid, 2024).

The analysis portrays a comprehensive profile of SIM swap offenders as highly adaptable, technically skilled individuals operating within organised networks, motivated primarily by financial incentives. These individuals exhibit resilience and strategically employ social engineering to exploit human vulnerabilities, while cybercrime networks and technical sophistication enhance their ability to bypass defences. The RAT's motivated offender dimension provides a framework for understanding these perpetrators as highly capable adversaries.

6.2.2 SIM swap fraud tactics

This section delves into the specific tactics and techniques employed in SIM swap fraud, addressing the question: What tactics or techniques are deployed in SIM swap fraud cases?

SIM swap fraud is characterised by various deceptive strategies aimed at seizing control of a victim's mobile number. Fraudsters often start by acquiring sensitive personal data via social engineering tactics such as phishing and vishing, thereby creating a convincing victim profile (Jordaan & Von Solms, 2011). Equipped with this information, perpetrators initiate a SIM swap request, exploiting mobile providers' procedures to take over the victim's phone number (Marakalala, 2023). Such fraudulent activities point out the need for stronger security protocols within telecoms (FCC, 2023).

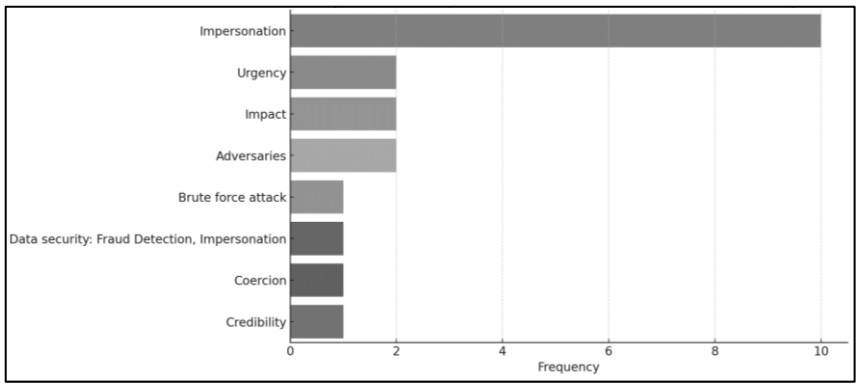


Figure 19: Fraud tactics - Most prominent codes

Figure 19 illustrates that impersonation emerges as the most prominent theme, followed by urgency, brute force attacks, coercion, and related tactics.

1. Impersonation

   Impersonation, which is referenced 10 times, involves fraudsters assuming the identities of legitimate customers. Impersonation techniques include SMS, email, and social media impersonations, where fraudsters present themselves convincingly as account holders (FCC, 2023). This tactic aligns with the RAT by exploiting procedural weaknesses in identity verification (Kim *et al*., 2022; Urbas & Kone, 200t).

2. Urgency

The creation of urgency is another technique used, albeit less frequently, where perpetrators create a sense of immediacy to pressure customer service representatives into bypassing standard checks (BEREC Europa, 2023). This emotional manipulation reflects offenders' strategic use of situational weaknesses, aligning with the RAT's motivated offender concept.

3. Brute force attack

   A brute force attack refers to a hacking method that involves systematically trying every possible combination of characters or numbers to gain unauthorised access to a system or account. Although less common, this attack method highlights the technical expertise of some offenders. Notable cases like the T-Mobile data breach demonstrate how such attacks facilitate large-scale fraud (Faircloth *et al*., 2022).

4. Coercion

   Coercion, although rare, involves threats or intimidation to compel insiders into cooperating with fraudsters. Natarajan and Ashara (2024) report cases of coercion that highlight a darker side to SIM swap fraud, aligning with the RAT's broader view of offender manipulation.

Figure 20 and Figure 21 are the Scopus AI semantic search concept maps on topics about SIM swap fraud tactics. The additional concepts, beyond those illustrated by the thematic analysis, suggest avenues for deeper future exploration.

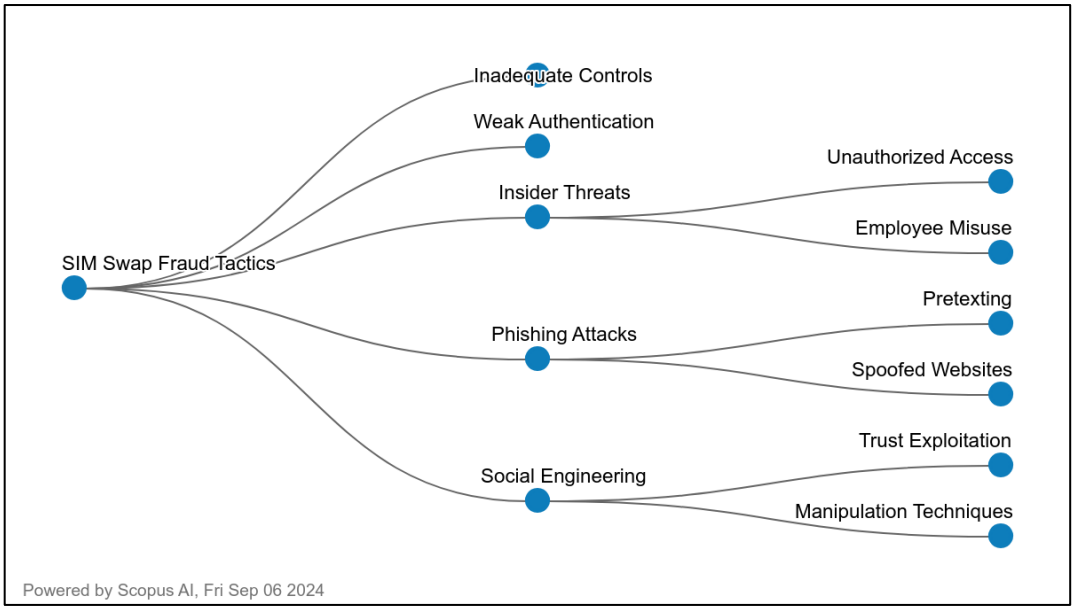


Figure 20: SIM swap fraud tactics concept map

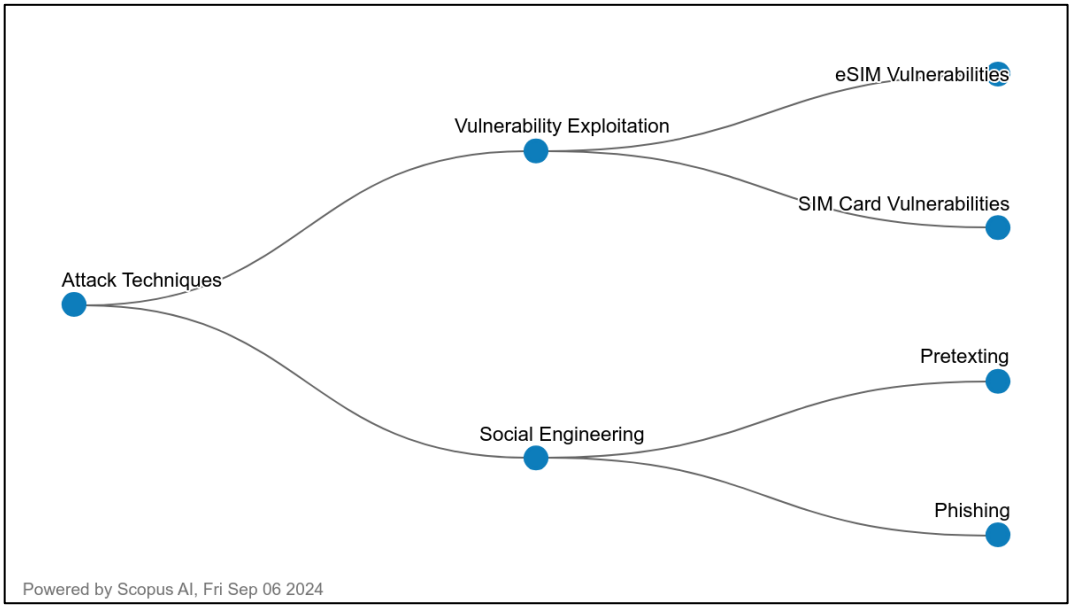


Figure 21: Attack vector concept map

The analysis shows a multifaceted approach by offenders who are adept at navigating social and technical systems. The RAT's motivated offender dimension offers valuable insights into the strategies used by these individuals. The themes and concepts identified in this section reinforce the importance of a

layered defence strategy that addresses both technical and human vulnerabilities.

6.2.3 Evolving tactics

As legacy networks are phased out, perpetrators increasingly exploit vulnerabilities in emerging 4G and 5G technologies. Behrad *et al*. (2020) note issues such as the international mobile subscriber identity (IMSI) disclosure, enabling attackers to conduct “man-in-the-middle” attacks. These evolving tactics illustrate how offenders adapt to exploit gaps associated with technological transitions, including software-defined networking and network function virtualisation vulnerabilities in 5G networks (Chitre & Sriramulu, 2022).

An initial analysis of the dataset, as shown in Figure 21, reveals themes illustrating how fraudsters adapt to technological and security shifts:

- Deepfake (3 mentions) – indicates the use of synthetic media for identity impersonation.
- Technological transition (1 mention) – highlights rapid adjustments in response to evolving technology.
- Ineffective systems (1 mention) – points to gaps in current security measures that fail to address emerging tactics.
- Corporate espionage (1 mention) – points to the penetration of corporate environments to access sensitive data.

Figure 21 displays these evolving tactics, with deepfake emerging as a significant theme, suggesting that fraudsters are increasingly using synthetic media as part of their strategies.

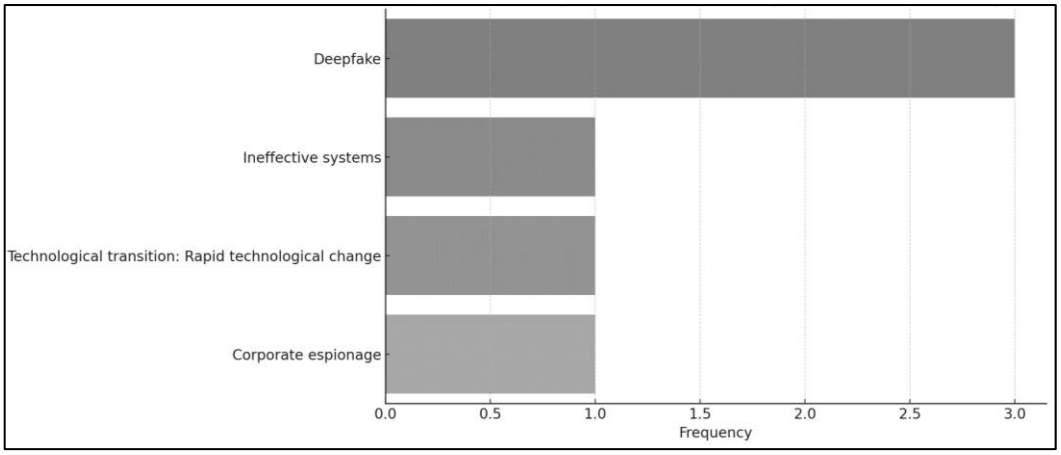


Figure 22: Evolving tactics - Most prominent codes

1. Deepfake

   The deepfake theme reflects a sophisticated adaptation in response to the 2G/3G shutdown, with fraudsters employing synthetic media to impersonate legitimate users or alter information. This tactic allows offenders to bypass traditional verification systems that rely on biometrics or voice recognition. Kotak *et al*. (2023) note that “fraudsters use deepfake techniques to fool biometric recognition with manipulated prints and anomalies,” and the accessibility of such tools has made synthetic impersonation more feasible. This theme highlights a technologically advanced form of fraud that can circumvent emerging security protocols.

2. Ineffective systems

   The exploitation of ineffective systems theme brings to light notable limitations within existing security frameworks, particularly their inability to counter increasingly sophisticated fraud tactics, such as the use of deepfakes. Notably, during the transition from 2G to 3G networks, certain security gaps have remained unaddressed, providing new avenues for fraudsters to exploit. A recent survey report revealed that 54.90% of respondents in the telecommunications security field believed that current security measures were insufficient to counter new SIM swap fraud techniques (GSMA, 2024). This finding suggests a critical need for vigilance in adapting security

measures, as fraudsters continue to exploit outdated or suboptimal protocols, particularly amidst technological shifts.

The theme captures several instances where systemic weaknesses or protocol gaps surface, demonstrating how offenders are quick to identify and exploit these vulnerabilities. For instance, Behrad, Bertin, and Crespi (2020) illustrate how fraudsters leverage rogue eNodeBs to redirect mobile traffic, exposing encryption and authentication flaws. Similarly, Jover (2019) describes cases where attackers manipulate legacy protocols to initiate SIM swaps, taking advantage of outdated security practices that persist despite advancements.

In the context of the RAT's concept of the motivated offender, ineffective systems represent the very vulnerabilities that drive offenders' actions, showing how these individuals or groups capitalise on lapses in network security updates. This theme clarifies an ongoing imperative: continuously evaluating and enhancing systems, as fraudsters frequently adapt to and exploit weak points left by outdated or insufficiently robust measures. Such insights highlight the dynamic and responsive nature of cybersecurity, where proactive adjustment remains essential in staying ahead of adaptive criminal tactics.

3. Corporate espionage

The corporate espionage theme reveals a more indirect, yet highly strategic, adaptation tactic where fraudsters penetrate corporate environments to access sensitive data, which is then leveraged to facilitate SIM swap fraud. With the recent shift towards remote work, digital data exchange has increased significantly, inadvertently broadening the entry points available to fraudsters. Kotak *et al*. (2023) highlight that "home offices provide ample opportunity for fraudsters to engage in corporate espionage," enabling them to obtain data critical for executing high-level SIM swaps. This theme thus

captures instances of unauthorised data acquisition, underscoring the organised and often coordinated nature of these fraud efforts.

Direct exploitation of telecom and banking systems also plays a significant role in SIM swap fraud. As Kibuuka (2024) explains, attackers deploy methods like SIM jacker and wireless internet browser attacks to compromise SIM cards, intercept SMS-based authentication codes, and bypass conventional security measures. Such tactics reveal the sophisticated means by which fraudsters circumvent standard protections, pointing to an urgent need for strengthened, cross-organisational security protocols.

In terms of theoretical framing, corporate espionage aligns well with the RAT's motivated offender concept, illustrating how fraudsters infiltrate corporate networks to bypass individual security barriers. This adaptation points out the importance of robust data security within corporate environments, particularly as these settings become increasingly attractive targets for highly motivated offenders. It further suggests that as fraud tactics evolve, a more comprehensive, inter-organisational approach to security – one that spans corporate, telecom, and financial domains – may be necessary to effectively counteract these increasingly sophisticated threats.

4. Technological transition

The technological transition theme explores how fraudsters continuously evolve their methods to circumvent advancements in security protocols, particularly those introduced during the 2G/3G network shutdown. As mobile networks migrate towards more secure systems, it appears that fraudsters are persistently recalibrating their tactics to maintain their effectiveness. This adaptation process highlights offenders' active engagement in not only learning about emerging security measures but also identifying potential vulnerabilities that may arise as networks advance.

This theme reflects resilience and adaptability among offenders, who seem willing to invest time and resources into refining their techniques. Such

adjustments suggest that while enhanced security protocols undoubtedly raise barriers, they also prompt offenders to innovate, potentially creating new, unforeseen vulnerabilities. These findings highlight the importance of not only implementing robust security measures but also maintaining an agile approach to threat management, recognising that any new technology shift may introduce fresh challenges in fraud prevention.

The transition to 4G and 5G has created opportunities for fraudsters to exploit. Kim and Kwon (2022) note that the shift has increased authentication complexity, which attackers exploit. Behrad *et al*. (2018) further discuss how attackers leverage IMSI disclosure vulnerabilities to obtain critical user information for SIM swaps.

The theme of technological transition reinforces the RAT's emphasis on the persistence and adaptability of motivated offenders, as fraudsters innovate to find alternative routes when vulnerabilities are eliminated.

This analysis makes clear the impressive adaptability displayed by fraudsters in response to advancing technologies and heightened security protocols. The deepfake theme, for instance, highlights a particularly advanced tactic, where synthetic media is deployed to bypass modern verification systems, presenting considerable detection challenges. Meanwhile, the ineffective systems theme draws attention to the limitations in existing security protocols, especially those exposed during the 2G/3G phase-out, revealing areas where current defences may lack robustness. Similarly, corporate espionage illustrates the organised, methodical nature of some fraud operations, where perpetrators infiltrate corporate environments to obtain valuable data, which is then leveraged in sophisticated fraud schemes. The technological transition theme points to a broader trend: as network infrastructure becomes more secure, fraudsters are observed adapting their techniques, reflecting an ongoing cycle of innovation and response.

Collectively, these themes illustrate the sophisticated and flexible strategies used by motivated offenders. When viewed through the lens of the RAT, these themes highlight the persistence and resourcefulness of offenders, as they continually devise new methods to circumvent emerging barriers. Tactics like deepfakes and corporate espionage demonstrate the high level of sophistication at play, while ineffective systems and technological transitions expose security gaps that fraudsters are quick to exploit. This evolving interplay between offensive and defensive tactics signals the need for continued vigilance and iterative improvements in security protocols, enabling organisations to anticipate and effectively counteract these adaptive fraud tactics.

The semantic search concept map for evolving attack vectors, shown in Figure 23, visualises the most prevalent areas covered in the sampled academic literature. These concepts are aligned with the view in the broader thematic analysis which suggests adequate research coverage.

The ongoing evolution of SIM swap fraud tactics highlights the pressing need for enhanced security within the telecom and financial sectors. Measures to counteract these threats include reducing social engineering risks, strengthening network defences, and improving authentication processes. As noted by the South African Banking Risk Information Centre (SABRIC) (SABRIC, 2022), smishing and phishing remain common, yet preventable, techniques; thus, awareness campaigns and targeted training could substantially mitigate these risks.

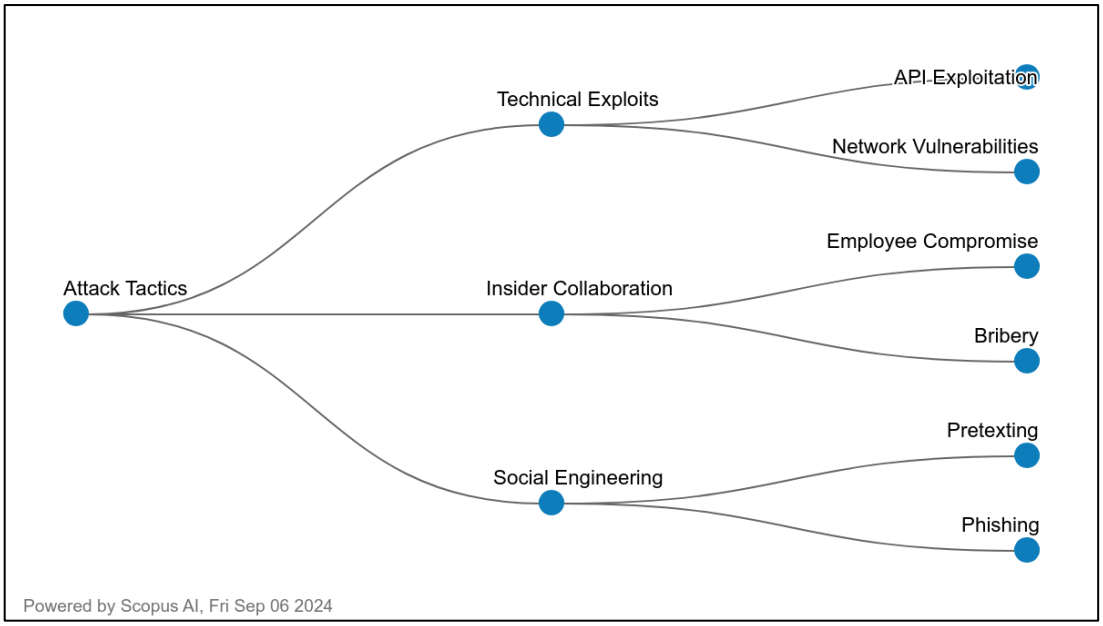


Figure 23: Evolving attack vectors concept map

Advanced verification methods, such as biometric authentication and multi-factor identity checks, also offer promising defences against SIM swap fraud. Jordaan and Von Solms (2011) advocate for biometric solutions, positing that linking biometric data to SIM registrations could add a valuable layer of security. Moreover, collaboration among telecom operators, financial institutions, and regulatory bodies is essential in developing unified and robust countermeasures.

Telecom operators and regulatory bodies have responded to evolving threats with adaptive security measures. The Federal Communications Commission (2023), for example, spotlights the value of flexible authentication processes, including AI-based behavioural analysis, enhanced customer authentication, and mandatory multi-factor authentication for high-risk transactions. Nevertheless, as Nicholls, Kuppa, and Le-Khac (2021) cautioned, fraudsters continue to innovate, employing deepfake technology and other advanced tactics to deceive even AI-driven detection systems.

Machine learning and advanced analytics play a pivotal role in fraud detection by identifying suspicious patterns in real time, as highlighted by Bello *et al*. (2023). However, fraudsters are also developing techniques to evade detection, including

methods that mimic legitimate behaviours to bypass machine learning algorithms (Kim *et al*., 2022).

In response to these challenges, regulatory bodies are updating policies to mitigate risk. The Commission for Communications Regulation (2024), for example, has issued guidelines aimed at reducing vulnerabilities associated with the 2G/3G phase-out, recommending standardised SIM swap procedures and enhanced cross-sector collaboration. Yet, as Kazembe (2023) points out, significant gaps remain, particularly in regions with limited infrastructure and regulatory oversight.

In conclusion, the evolving strategies employed by SIM swap fraudsters illustrate a sophisticated response to both the 2G/3G shutdown and new security measures. The RAT's motivated offender framework provides valuable insights into these strategies, highlighting offenders' persistence in surmounting modern defences. These findings emphasise the necessity for advanced, multi-layered protections that address both technical and social vulnerabilities, thus strengthening resilience against these complex and ever-evolving fraud tactics.

6.3 Suitable target dimension

6.3.1 Vulnerability factors

This section explores the factors that heighten user vulnerability to SIM swap fraud, focusing on the question: What factors increase user vulnerability to SIM swap fraud? Analysis of the data reveals key themes that shed light on the specific vulnerabilities commonly exploited by fraudsters. Four main themes – confidentiality, vulnerabilities, data accessibility, and knowledge gap – emerge, each highlighting a particular aspect of how both user and system weaknesses contribute to susceptibility to fraud.

Figure 24 illustrates the most frequently mentioned factors contributing to user vulnerability, with confidentiality and vulnerabilities emerging as dominant

themes. This finding suggests that issues related to data protection and security weaknesses are especially prevalent. The coding analysis identifies several key insights into these vulnerabilities, highlighting confidentiality, telecommunications system vulnerabilities (under code “vulnerabilities”), data accessibility, and knowledge gap as essential factors.

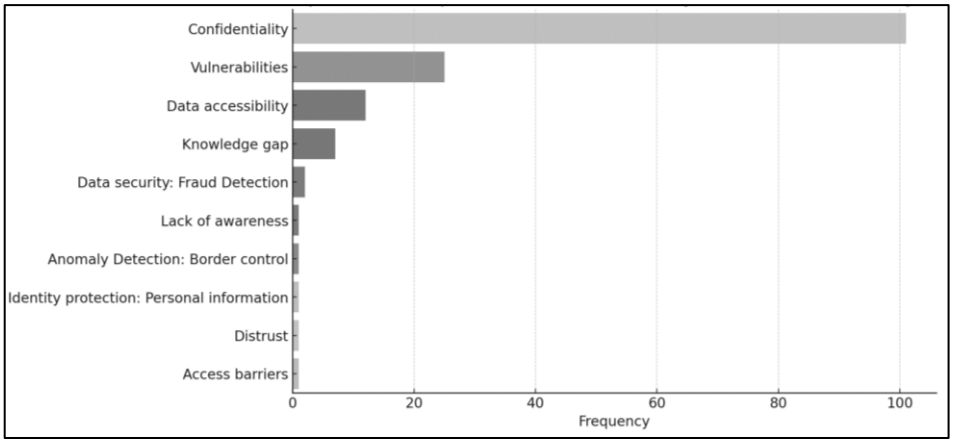


Figure 24: Target vulnerability - Most prominent codes

1. Confidentiality

   Confidentiality appears as the most frequently mentioned theme, with 101 instances, underscoring the critical importance of data privacy and secure storage practices. Vulnerabilities arise when sensitive data, such as personal identifiers and financial information, are inadequately protected, rendering Users prime targets for fraud. For instance, a report noted that “five million dataset records of applicants contained sensitive personal information, heightening risks when such data is not masked or securely stored (Sanni *et al.*, 2023). The emphasis on data masking as a necessary safeguard is also evident: “Data Masking and Vectorization are essential to maintain confidentiality and protect against unauthorized access” (Siriwardhana, 2021).

   This theme is based on a code group clusters codes with references to secure data handling, data masking, and unauthorised access prevention. Within the

RAT, confidentiality aligns with the suitable target concept, indicating that insufficient data protection increases user vulnerability to motivated offenders. Ensuring robust privacy safeguards is vital, as inadequate protection of personal data makes users more susceptible to fraud.

2. Telecommunications system vulnerabilities (“vulnerabilities” code)

   The vulnerabilities code, cited 25 times, highlights structural weaknesses in telecommunications systems and user practices that increase susceptibility to fraud. Common vulnerabilities include outdated security protocols, weak identity verification methods, and inadequate cybersecurity measures. Salaudeen *et al*. (2022) note that “security weaknesses in verification processes allow fraudsters to bypass safeguards and gain unauthorized access to user accounts.”

   Weak authentication practices represent a major vulnerability. Many mobile network operators rely on less secure methods, such as call log verification, which attackers can exploit (Lee *et al*., 2020). Additionally, unencrypted communication channels between devices and SIM cards pose significant risks, allowing attackers to intercept authentication requests and circumvent multi-factor authentication (Zhao *et al*., 2021; Tambunan, Suryadi, & Hamid, 2021). Vulnerabilities like weak passwords further exacerbate risk, offering accessible entry points for fraudsters (Ettiane, Elkouch, & Chaoub, 2016; Kashir & Bashir, 2019).

   This theme encompasses technical and procedural weaknesses, demonstrating how a broad spectrum of security gaps can increase users’ vulnerability to SIM swap fraud. In RAT terms, vulnerabilities represent the intersection of a suitable target and a motivated offender, suggesting that addressing these specific weaknesses can help organisations protect users from fraud more effectively.

3. Data accessibility

Data accessibility, with 12 mentions, emphasises the risks posed by unauthorised access to user information. Fraudsters exploit accessible data, using it to impersonate or authenticate as the target user. One study explains that “the high accessibility of sensitive data, including phone numbers and financial details, enables fraudsters to initiate SIM swaps with ease” (Koul *et al*., 2020).

Weak data-sharing protocols or widely accessible information can make users more vulnerable. For instance, unencrypted communication channels provide avenues for unauthorised interception of sensitive information (Zhao *et al*., 2021). Within the RAT framework, data accessibility aligns with the suitable target concept, illustrating that reducing data accessibility and enforcing strict data-sharing protocols can mitigate user vulnerability to SIM swap fraud.

4. Knowledge gap

The knowledge gap theme, cited in seven instances, points to a lack of user awareness about security practices and fraud risks (Tambunan *et al*., 2021; Lee *et al*., 2020). Many users are unfamiliar with SIM swap fraud tactics and the importance of securing their mobile and financial accounts. A report noted that “a significant knowledge gap among users regarding SIM swap fraud makes them less vigilant and therefore more vulnerable to these types of attacks” (Sanni *et al*., 2023).

This theme highlights the importance of user awareness, education on security risks, and proactive security practices. When users lack awareness, they are more likely to comply with fraudulent requests, such as revealing one-time passwords or verification codes (Lin *et al*., 2023; Harinath, 2023). Educating users about fraud risks could substantially reduce vulnerability, as informed users are more inclined to adopt protective measures. According to the RAT, the knowledge gap exemplifies a suitable target, as uninformed users are easier to exploit. Therefore, increasing awareness can reduce user attractiveness as targets and help prevent SIM swap fraud.

This thematic analysis identifies critical factors that elevate user vulnerability to SIM swap fraud, encompassing gaps in confidentiality, telecommunications system vulnerabilities, data accessibility, and user knowledge gaps. Each theme demonstrates how both technical and behavioural elements contribute to user susceptibility.

Figure 25 shows the semantic search concept map, highlighting technical risks that co-occur with these vulnerabilities, which collectively increase users' exposure to fraud.

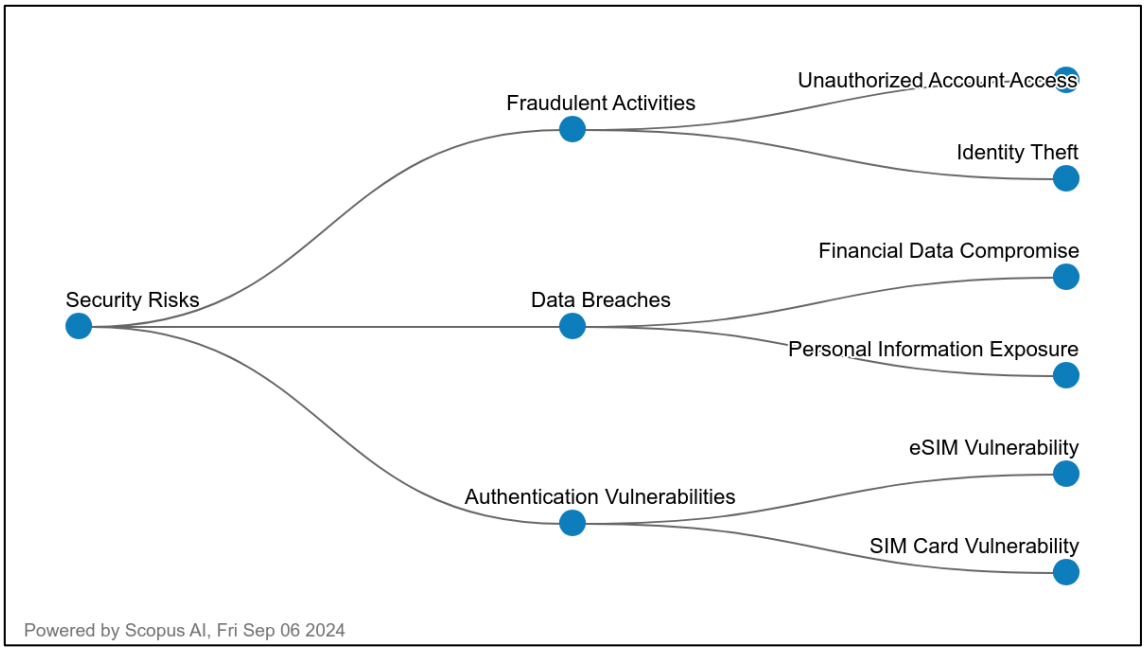


Figure 25: Technical vulnerability factor concept map

From a RAT perspective, these themes collectively construct a multi-dimensional profile of vulnerability under the suitable target framework. Confidentiality and data accessibility reveal how data security deficiencies make users attractive targets, while vulnerabilities expose system weaknesses that fraudsters can exploit. The knowledge gap highlights the critical role of user education in reducing risk, as informed users are less likely to fall victim to fraud.

In conclusion, factors like weak passwords, susceptibility to social engineering, inadequate authentication mechanisms, and general unawareness converge to

heighten user vulnerability to SIM swap fraud. Addressing these vulnerabilities requires a multi-layered approach, incorporating stronger authentication methods, continuous public education on security practices, and stricter regulatory measures to enforce higher security standards in mobile networks. Together, these measures can decrease user attractiveness as targets and bolster resilience against SIM swap fraud.

6.3.2 Misinformation and social engineering

The limited research specifically addressing misinformation related to the 2G/3G shutdown has left a notable gap, one that fraudsters have actively exploited. As older mobile network generations are phased out, the lack of clear communication has fostered an environment ripe for deceptive practices, particularly in relation to SIM swap fraud. This gap in reliable information has allowed misinformation to become a potent tool for cybercriminals.

Fraudsters have taken advantage of confusion surrounding the 2G/3G shutdown to commit financial and identity-based crimes. According to LexisNexis Risk Solutions (2024), misinformation about the network shutdown has driven a surge in fraudulent activities, as cybercriminals spread false narratives that create panic among users. This environment of uncertainty enables fraudsters to manipulate victims, often by creating a sense of urgency around account security. Through this tactic, they coerce individuals into disclosing sensitive information or authorising SIM swaps under the guise of ensuring network compatibility.

Assolini (2019) highlights how misinformation surrounding the 2G/3G shutdown has triggered waves of SIM swap attacks in regions such as Africa, Turkey, and the UAE. In these cases, fraudsters contact mobile carriers, impersonating legitimate users and requesting a SIM swap under the pretext of network transition requirements. Leveraging these narratives, fraudsters often succeed in transferring victims' phone numbers to SIM cards under their control. This access allows them to bypass two-factor authentication, granting entry to financial and

online accounts and often resulting in substantial financial losses and identity theft for the victims.

Social engineering is integral to exploiting misinformation about the network shutdown (Hallman, n.d.). Rosa (2024) explains how fraudsters craft plausible stories, such as the need to prevent service disruptions due to network upgrades. These narratives are designed to prompt victims to act quickly and without verifying the information. By preying on users' fears of service loss, fraudsters can manipulate individuals into sharing sensitive information or authorising SIM swaps, illustrating the potent combination of misinformation and social engineering (Ali *et al*., 2024).

The broader implications of misinformation in enabling mobile number hijacking are outlined by ICASA (2016), which describes how misinformation-driven narratives can facilitate large-scale fraud schemes. The interconnected nature of digital fraud tactics, particularly when social engineering and misinformation converge, demonstrates the necessity for robust countermeasures to protect users.

Further illustrating this threat, the SABRIC (SABRIC, 2022) describes how cybercriminals use tactics such as phishing, vishing, and pretexting to conduct digital banking fraud. Fraudsters often impersonate network or banking representatives, claiming urgent updates are necessary due to the 2G/3G shutdown. Victims are tricked into sharing critical account details, either by clicking on links to fake websites or providing verification codes directly over the phone.

To combat misinformation-based SIM swap fraud, emerging technologies like machine learning and AI show significant promise. Nicholls, Kuppa, and Le-Khac (2021) discuss how AI-driven approaches can enhance the detection and mitigation of social engineering risks. By analysing patterns in fraudulent communication and suspicious account activity, machine learning models could improve the security of financial and telecommunications platforms. Such models

can flag unusual behaviours, such as sudden SIM swap requests associated with misinformation campaigns, thereby helping prevent fraud before it occurs.

The spread of misinformation around the 2G/3G network shutdown has had serious consequences for digital security, as fraudsters leverage user confusion to perpetrate SIM swap attacks and other forms of cybercrime. The combination of misinformation and social engineering has proven highly effective, capitalising on user fears of service disruption, and targeting weaknesses in authentication processes within mobile network providers. Addressing this issue calls for a multi-faceted approach: public education initiatives to dispel misinformation, enhanced authentication methods to reduce fraud vulnerability, and the deployment of AI-based systems capable of detecting and mitigating fraudulent activity. Together, these strategies could strengthen resilience against misinformation-driven fraud in an era of rapid technological transition.

6.3.3 Social interventions

This section explores community and social initiatives aimed at preventing SIM swap fraud, focusing on the question: Are there community-driven or social efforts to reduce SIM swap fraud? While most studies reviewed examine the mechanics and impacts of SIM swap fraud rather than specific community-based initiatives, they draw attention to the importance of enhancing authentication processes and raising consumer awareness. For instance, the FCC mandated mobile network operators to implement stronger authentication measures and provide timely notifications for SIM swap requests, reflecting a regulatory approach to consumer protection (FCC, 2023).

The SABRIC similarly highlights the importance of public education on mobile fraud, suggesting that community engagement can be instrumental in reducing SIM swap risks (Marakalala, 2023). Although these measures are not explicitly labelled as "community initiatives," they collectively contribute to a broad-based approach to enhancing consumer protection.

Figure 26 reveals four primary themes within social interventions: Regulation, data security and fraud detection, consumer protection and awareness, and financial technology and crime prevention. Together, these themes represent distinct but interconnected strategies for preventing SIM swap fraud:

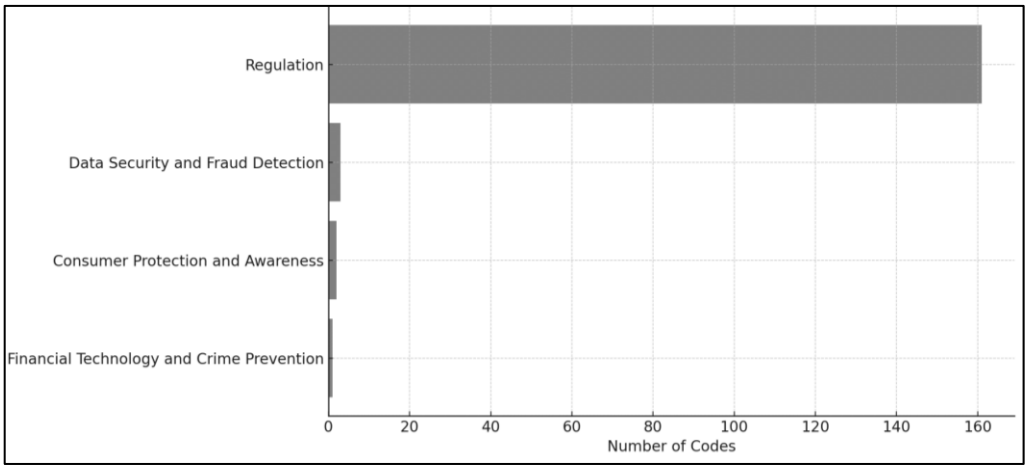


Figure 26: Social interventions – themes

1. Regulation

   Regulation stands out as the most prominent theme, highlighting the essential role of regulatory bodies in combating SIM swap fraud through legal frameworks and cross-sector collaboration. Several sources emphasise regulatory challenges, such as the “unclear and inconsistent regulation concerning the management of consumer data,” which can create gaps in fraud prevention (FCC, 2023). Kim *et al*. (2022) stress the need for cross-sector cooperation, arguing that “Regulators, whether public (e.g., ministries) or private (e.g., telecommunications organisations), must collaborate to secure user data.” This call for cooperation among regulatory and industry stakeholders reflects an understanding that effective fraud prevention demands a multifaceted approach.

   The emphasis on regulation aligns with the literature suggesting that a robust regulatory environment is critical for reducing digital fraud risks (Kumar, 2024; Lee *et al*., 2018; Tambunan, 2022). From the perspective of the RAT, effective

regulation modifies offender behaviour by increasing the risks and reducing the rewards associated with SIM swap fraud.

2. Data security and fraud detection

   The theme of data security and fraud detection highlights technological solutions, such as AI and machine learning, which monitor and detect fraudulent activity. This theme is closely linked to regulation, as regulatory guidelines often govern technological solutions. For example, a study by Saadia *et al*. (2024) highlights that the use of automated voice recognition is one of the most controversial areas in fraud detection as the need for data processing consent is a heavily regulated data protection aspect. The GSMA (2024) further points to the need for clear mandates in data processing and tracking, with telecommunications security respondents noting that ambiguity in data processing and consent guidelines concerning passive fraud detection hampers the technology's effectiveness.

   Overall, this theme highlights the role of secure, AI-driven data practices in detecting and preventing fraud. The RAT supports this emphasis by suggesting that enhanced data security and fraud detection can decrease target suitability, thereby deterring offenders. By identifying specific fraud risks, technological solutions contribute to the broader goal of reducing fraud.

3. Consumer protection and awareness

   Consumer protection and awareness highlights efforts to empower users through education and community-centred initiatives aimed at increasing public understanding of SIM swap fraud. This theme encompasses both institutional protections for consumer data and awareness campaigns that educate users on potential fraud risks. For instance, one source points out the need for "consumer-centred protection policies" to help smaller carriers adapt to emerging threats (FCC, 2023). The FCC also emphasises the importance of education through "Local Number Portability rules that safeguard user identity, which are essential for maintaining trust in mobile services."

The RAT suggests that increasing consumer awareness and resilience makes them less suitable targets for fraud. Public education initiatives, therefore, equip consumers with the knowledge to recognise suspicious behaviour, reducing their vulnerability to attacks. Research similarly supports the role of public awareness as a critical component of fraud prevention (Kim *et al*., 2022; Lee *et al.*, 2020; Zaeifi *et al*., 2024).

4. Financial technology and crime prevention

   Although less frequently discussed, financial technology and crime prevention focuses on the role of financial institutions in implementing anti-fraud measures. This theme stresses the importance of security features within financial technology platforms. One source noted that “Banks are increasingly called upon to act as gatekeepers against fraud, focusing on protecting digital assets through secure identification protocols” (Dayyabu *et al*., 2023). This aligns with broader trends in financial technology, where institutions are seen as central actors in fraud prevention.

   In the context of the RAT, financial institutions enable broader social intervention by providing structural support that protects individuals who might otherwise be susceptible to fraud. As an example, financial institutions tend to include recent SIM swap checks before approving suspicious transactions on the customer’s profile (SABRIC, 2024). This theme suggests that while the role of financial institutions is crucial, it is also part of a larger, interconnected system involving regulatory frameworks and consumer awareness efforts.

This analysis highlights four key areas that contribute to social interventions against SIM swap fraud: Regulation, data security and fraud detection, Consumer protection and awareness, and financial technology and crime prevention. Each theme addresses an essential component of the fraud prevention ecosystem, illustrating the varied roles that different stakeholders play in mitigating SIM swap risks.

Regulation and data security, and fraud detection stand out as the most prominent themes, reflecting a reliance on structural and technological measures to create a secure environment. Consumer protection and awareness emphasises individual agency and the role of community education in reducing fraud vulnerability. Financial technology and crime prevention emphasises the responsibility of financial institutions in safeguarding digital assets and detecting suspicious activity.

This analysis further suggests that coordinated efforts across these dimensions are crucial for building a robust defence against SIM swap fraud. Regulatory measures, advanced data security practices, consumer education, and financial institution involvement all play vital roles in reducing target suitability for fraud. Moving forward, future research should focus on assessing the practical impact of these initiatives on fraud rates to better understand how these efforts translate into tangible outcomes for individuals and communities.

6.3.4 Prevalence of SIM swap fraud

SIM swap fraud has emerged as a major challenge in the digital landscape, particularly exacerbated by vulnerabilities inherent in mobile telecommunications and the gradual phasing out of older network technologies like 2G and 3G. The reported rates of SIM swap fraud reveal a worrying trend across various regions, both in terms of the frequency of attacks and the associated financial losses.

This section examines reported rates and estimates of SIM swap fraud, addressing the question: What are the reported rates or estimates of SIM swap fraud?

The most frequent codes indicate emerging themes around legal action, financial impact, regulatory compliance, and cybercrime and security.

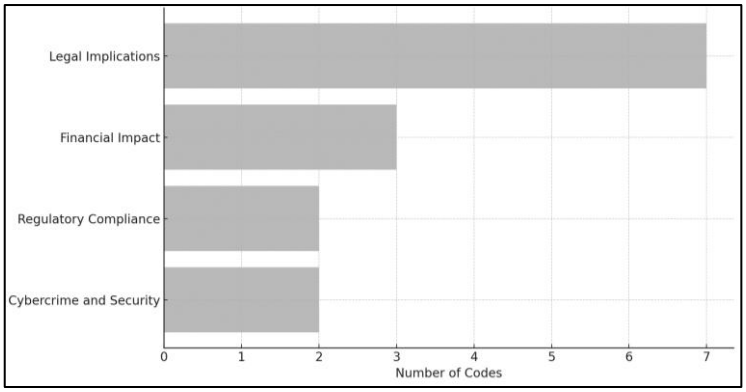


Figure 27: Prevalence of SIM swap fraud - themes

Figure 27 highlights the distribution of primary themes in the data:

- Legal implications: This theme, the most prevalent, encompasses regulatory, prosecutorial, and legal frameworks addressing SIM swap fraud.
- Financial impact: Focused on the monetary damage SIM swap fraud inflicts, including loss of assets and economic implications for organisations and individuals.
- Regulatory compliance: Reflects the role of laws and regulatory standards designed to counter SIM swap fraud and enhance cybersecurity.
- Cybercrime and security: Captures the classification of SIM swap fraud within broader cybercrime categories, emphasising data breaches and digital theft.

Each key theme is elaborated on below:

1. Legal implications

The legal implication theme represents the prosecutorial, legislative, and enforcement responses to SIM swap fraud, highlighting the global push to classify and prosecute such incidents within cybercrime and fraud statutes. As the most prevalent theme, legal implications outline the varied ways jurisdictions have responded to the rise in SIM swap fraud.

The data indicates that many countries have adapted their legal frameworks to combat SIM swap fraud by criminalising unauthorised access and hacking activities. For example, under India's Information Technology Act, Sections 66 and 66(c) provide a foundation for prosecuting unauthorised access (Telecom Regulatory Authority of India, 2023). SIM swap fraud often involves digital identity theft, and by classifying it under cybercrime and hacking laws, jurisdictions aim to deter such incidents through criminal sanctions.

Legal frameworks can be understood as formal guardianship measures, a core tenet of the RAT, to systematically reduce target suitability to SIM swap fraud As legislative bodies continue to respond to the rise of SIM swap fraud, they aim to increase the cost of such criminal activities and deter potential offenders through stricter penalties. However, the varying effectiveness of these laws highlights the ongoing challenges of prosecuting digital crimes, which often transcend geographical boundaries.

2. Financial impact

The financial impact theme captures the economic repercussions associated with SIM swap fraud. These impacts range from direct financial losses, such as cryptocurrency theft, to indirect costs, including reputational damage and the expenses tied to heightened security measures.

The data indicates the extensive financial losses suffered by both individuals and institutions. Cryptocurrency accounts have proven particularly vulnerable, with millions of dollars in digital assets lost to unauthorised transactions following SIM swaps. The direct financial losses are often accompanied by a loss of trust, as customers may question the security measures employed by companies unable to prevent such fraud.

The RAT considers the financial assets affected by SIM swap fraud as suitable targets due to their high value and relatively weak protections in some digital ecosystems. The financial incentives for criminals increase as digital transactions

proliferate, making monetary and reputational loss a defining characteristic of SIM swap fraud's impact.

3. Regulatory compliance

The theme of regulatory compliance reflects the obligations imposed on telecommunications providers, digital platforms, and other stakeholders to mitigate the risks associated with SIM swap fraud. This includes legal standards and industry guidelines that mandate improved authentication and identity verification measures.

The data highlight the critical role of regulatory standards in preventing SIM swap fraud. By mandating stricter verification processes, regulators aim to create a deterrent against unauthorised SIM swaps (Telecom Regulatory Authority of India, 2023; Electronic Communications Committee, 2018). Many telecommunication companies are now required to adopt multi-factor authentication or additional security layers, making it more challenging for criminals to initiate fraudulent SIM swaps (Rwanda Utilities Regulatory Authority, 2024).

According to the RAT, regulations serve as a form of external vulnerability control by compelling companies to enhance their security measures. By making targets less suitable through compliance requirements, regulatory bodies seek to reduce SIM swap fraud incidents. However, the variability in regulatory adherence across jurisdictions indicates that some targets may remain vulnerable, underscoring the limitations of current compliance standards.

4. Cybercrime and security

The cybercrime and security theme classifies SIM swap fraud as a type of cybercrime, exploring how attackers exploit technological vulnerabilities and weak security measures to execute fraud. This theme also addresses the broader cybersecurity risks associated with SIM swaps, such as data breaches and unauthorised access.

The data illustrates how SIM swap fraud exploits weaknesses within telecommunications and digital identity verification systems. Criminals often target these systems due to their role as gateways to digital assets and sensitive information (FCC, 2022). SIM swaps enable attackers to bypass traditional security measures, leveraging mobile devices as an entry point to account credentials and financial information.

The RAT suggests that system vulnerability control, such as robust security protocols, facilitates criminal acts like SIM swap fraud. The lack of adequate cybersecurity measures in some digital platforms and telecommunication companies increases the suitability of these systems as targets. Thus, enhancing security protocols could reduce the feasibility of SIM swap attacks, aligning with theoretical perspectives that emphasise prevention through stronger digital vulnerability controls.

The prevalence of SIM swap fraud has been documented in multiple studies, indicating its significant impact across the globe. The Federal Bureau of Investigation (FBI) reported 1,611 cases of SIM swapping in the USA in 2021, amounting to losses of approximately $6.8 million, highlighting the increasing frequency and financial severity of such frauds (Kim *et al*., 2022). Similarly, significant cases have been recorded in other countries, including a high-profile incident in Canada where a group of teenagers was arrested for stealing $36 million in virtual assets through SIM swap schemes, further showcasing the widespread nature of this fraud (Kim *et al*., 2022).

In South Korea, there have been over 40 reported cases of SIM swap fraud under investigation since early 2022, reflecting a recent surge in fraudulent activity (Kim *et al*., 2022). Additionally, research conducted in China revealed that over 256,000 instances of phone fraud occurred in 2020, leading to losses of approximately $18.6 billion, while Korea reported losses of $0.6 billion from scam calls, illustrating the substantial financial impact in Asia (Oh *et al*., 2023).

India has witnessed numerous cases of SIM swap fraud, often resulting in significant financial losses for individuals and businesses. For instance, an 18-year-old was accused of orchestrating SIM swaps to steal $23.8 million, and a businessman in Mumbai lost Rs.18.6 million (Harinath, 2023). This trend is consistent with widespread incidents across the country involving major telecom operators like Airtel, Vodafone, and BSNL, which have been repeatedly targeted (Bhavana, Miriam, & Robin, 2024).

In Africa, SIM swap fraud remains a persistent issue, with documented cases leading to substantial losses for telecommunications operators and governments. For example, in Zimbabwe, a study found a mean prevalence rate of 2.34 for SIM swap fraud, underscoring its impact on the electronic banking sector (Manhide & Nkomo, 2023). South Africa has also experienced significant cases of SIM swap fraud, with the SABRIC reporting 4,508 incidents in 2021. However, a marked decline to 71 cases in 2022 was observed, suggesting some progress in fraud prevention measures (SABRIC, 2022).

The transition away from 2G and 3G networks has had an impact on the prevalence of SIM swap fraud. As noted by Jackson (2020), studies conducted by Princeton University demonstrated the vulnerability of carriers such as Verizon, AT&T, and T-Mobile, where all 30 test cases of SIM swap attempts were successful. This indicates that as networks transition, such vulnerabilities have become more apparent and are frequently exploited by fraudsters.

The reported rates of SIM swap fraud have also been affected by inadequate network security practices. In Australia, the Australian Communications and Media Authority (ACMA, 2022) highlighted a substantial increase in phone and text scams, including SIM swap fraud, with a 63% rise in scam reports over the 12 months leading up to September 2021. The financial losses reported during this period rose by 77%, underscoring the economic impact of these scams. However, the integration of AI solutions has shown promise in reducing fraud, as the GSMA (2024) reported a 40-45% decline in SIM swap cases following the deployment of AI-based detection methods.

Significant financial losses associated with SIM swap fraud have also been documented through various legal cases. In Tanzania, for instance, a plaintiff reported losing Tshs 28,462,078 due to an illegal SIM swap, reflecting the direct financial harm suffered by victims and the legal complexities surrounding such cases (Assey v. Vodacom Tanzania, 2023). In Nigeria, Omotubora (2020) described SIM swap fraud as an increasingly common method used to bypass SMS-based one-time passwords (OTPs), with rates expected to have surpassed those of ATM fraud by 2020.

Furthermore, the 2023 Identity Fraud Study by Javelin Strategy reported a 6% increase in identity fraud incidents in the USA compared to 2022, reinforcing the notion that this form of cybercrime continues to pose a serious threat to financial security (Buzzard, 2023).

The reported rates and estimates of SIM swap fraud highlight a global challenge, with significant financial losses and widespread prevalence across regions. The transition from 2G/3G networks has, in some cases, exacerbated these issues, as fraudsters exploit emerging vulnerabilities. While efforts to curb SIM swap fraud, such as the integration of AI-based solutions, have shown promise, the continued rise in reported cases indicates that robust, multi-faceted approaches are necessary to mitigate this evolving threat.

The thematic analysis of SIM swap fraud impacts reveals four primary areas of concern: legal implications, financial impact, regulatory compliance, and cybercrime and security. Each theme illustrates the multifaceted challenges posed by SIM swap fraud, which is not only a criminal offence but also a significant economic, regulatory, and security issue. Legal frameworks aim to address the criminal aspects, while financial and reputational losses highlight the need for greater preventive measures. Regulatory compliance serves as a mandated form of guardianship, pushing companies to implement protective protocols, and cybersecurity measures aimed to counteract technical vulnerabilities.

The RAT's focus on the dynamics of a suitable target offers a theoretical lens to understand SIM swap fraud's persistence in the digital age. Strengthening legal frameworks, enhancing compliance standards, and adopting robust cybersecurity protocols could collectively reduce SIM swap incidents by reducing target vulnerability. This thematic analysis emphasises that effective responses to SIM swap fraud require an integrated approach involving legal, regulatory, financial, and technological measures, bridging gaps across these domains to create a safer digital ecosystem.

6.4 Lack of capable guardianship dimension

6.4.1 Current fraud measures

SIM swap fraud has grown into a significant threat in today's digital ecosystem, capitalising on weaknesses within mobile telecommunications and identity verification processes. This section examines the measures currently in place to counter SIM swap fraud, guided by the question: What are the existing security strategies to prevent SIM swap fraud? Efforts to address SIM swap fraud generally focus on enhancing identity verification and deploying advanced technologies to safeguard user data and prevent unauthorised access.

One promising solution is the BIO-Swap system, which employs biometric data to verify subscriber identities during SIM swap requests, thus acting as a trusted intermediary for mobile network operators (Jordaan & Von Solms, 2011). Increasingly, mobile networks are encouraged to implement robust data security strategies to reduce identity theft risks (iiDENTIFii, 2024). Other methods, such as real-time monitoring for suspicious activity and device legitimacy verification, are also being used to bolster consumer security (FCC, 2023).

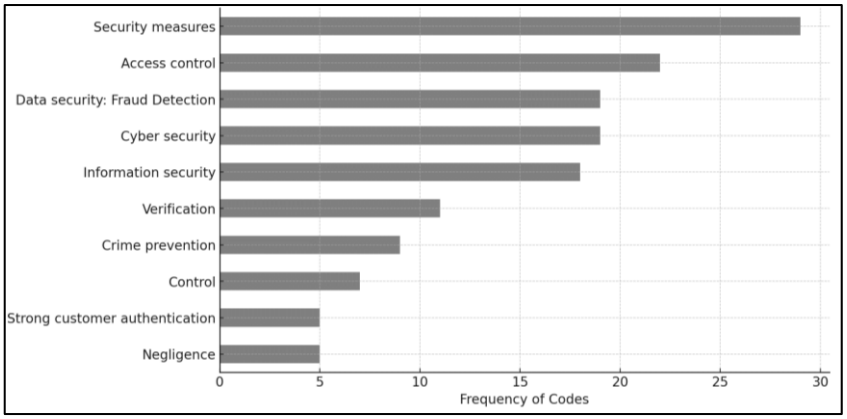


Figure 28: Current fraud measures – Most prominent codes

Key themes constructed from the codes under fraud prevention measures, as illustrated in Figure 28, are access control, and data security. All the interventions under these themes play a vital role in creating a layered security approach against SIM swap fraud. Upon review, the most prolific coding term “security measures” proved to be an all-encompassing term for all the measures discussed tin the literature and is therefore excluded in the below discussion to maintain an acceptable level of thematic exclusivity.

1. Access control

    Access control encompasses mechanisms such as multi-factor authentication and stringent identity verification protocols. These controls limit unauthorised access to sensitive services by ensuring that only verified users can initiate SIM swaps. For instance, Ekeh *et al*. (2022) suggest implementing multi-step verification or locking SIM cards to prevent unauthorised activations. By creating additional layers of security, access control measures make it more difficult for fraudsters to target users, establishing significant barriers to unauthorised activity.

    The Scopus semantic search concept map on authentication processes, shown in Figure 29, highlights that access control processes are among the most prolific yet have faced challenges against persistent attackers. While

effective, these measures must evolve continuously to withstand increasingly sophisticated fraud tactics.

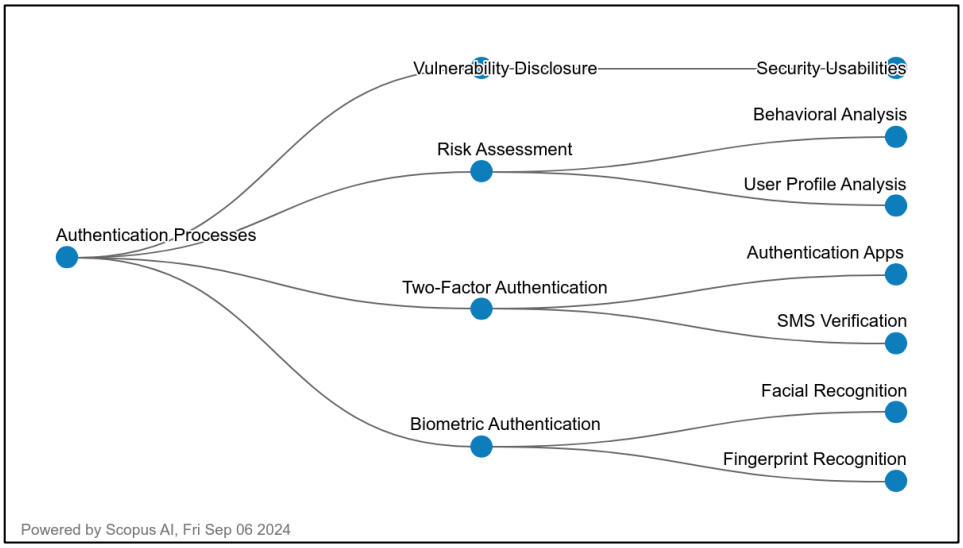


Figure 29: Authentication processes concept map

The access control measures most referenced in the literature include:

- Multi-factor authentication: Widely adopted to combat SIM swap fraud, MFA requires multiple verification steps, reducing the success rate of fraud attempts (Lee *et al*., 2021). However, social engineering tactics still present a vulnerability, as fraudsters may manipulate victims or service providers into revealing secondary authentication information (SABRIC, 2022).
- Biometric verification: Biometric systems provide enhanced security, relying on unique physical attributes that are difficult to replicate (Sood *et al*., 2023). Although generally effective, biometric systems are not immune to sophisticated attacks, underscoring the importance of secure biometric storage and verification processes (Toorani & Beheshti, 2008).
- AI and machine learning: AI-driven fraud detection systems are particularly adaptive to emerging fraud tactics. Al-Humaigani *et al*. (2009) show that AI can rapidly identify and respond to new fraud

strategies. However, maintaining these systems requires significant data and computational resources, which may be challenging for smaller operators (Masrub & Alahemar, 2020).

2. Data security

Data security focuses on protecting user data from unauthorised access and ensuring data integrity through measures like encryption, fraud monitoring, and secure storage. Sanni *et al*. (2023) note that "To protect against SIM swap fraud, emphasis is placed on data encryption and monitoring of data access," which aligns with Jordaan & Von Solm's (2011) advocacy for fraud detection algorithms to flag unusual account access patterns. In RAT terms, data security measures decreased target suitability by protecting information that could otherwise be exploited in SIM swap schemes.

Data security measures most referenced in the literature include:

- Network-based security solutions: Some network providers require SIM registration and verification, involving background checks before issuing new SIM cards. While such protocols are critical for fraud deterrence (Masrub & Alahemar, 2020), they may also delay legitimate transactions and can be vulnerable to exploitation by well-organised fraudsters.
- Machine learning for real-time detection: Algorithms that detect and block suspicious activities in real time have proven effective in identifying fraud patterns associated with SIM swaps (Al-Humaigani *et al*., 2009). However, false positives remain a challenge, as they can disrupt services for genuine customers.
- Blockchain technology: An emerging solution, blockchain, is being explored for its potential to secure identity management and SIM-related transactions. Its decentralised, tamper-proof nature makes it appealing for anti-fraud measures (Krishnan *et al*., 2024), although

high costs and technical demands may limit its accessibility for some network providers.

The literature on SIM swap fraud prevention stresses the importance of a multi-layered approach. Combining access control and data security protocols creates a comprehensive defence against unauthorised access. Studies suggest that measures such as two-factor authentication, data encryption, and cyberthreat monitoring are particularly effective in deterring fraudsters. This analysis aligns with the RAT, which suggests that effective guardianship reduces opportunities for crime by establishing multiple protective layers.

In summary, by reinforcing protections against unauthorised access and improving data security, telecommunications companies can better safeguard users from SIM swap fraud and contribute to a safer digital environment. These findings suggest that successful fraud prevention depends on the integration of various technical solutions including rigorous verification protocols and enhanced user awareness of their application.

6.4.2 Preparedness for 2G/3G shutdown

As telecommunications networks advance from 2G and 3G to newer technologies, the need for robust fraud prevention strategies has intensified, particularly concerning SIM swap fraud. This section examines stakeholders' readiness to address these security challenges, guided by the question: What is the level of preparedness among stakeholders in combating SIM swap fraud following the 2G/3G shutdown? The RAT, especially the lack of capable guardianship dimension, provides a useful lens for assessing stakeholder efforts in user protection post-shutdown.

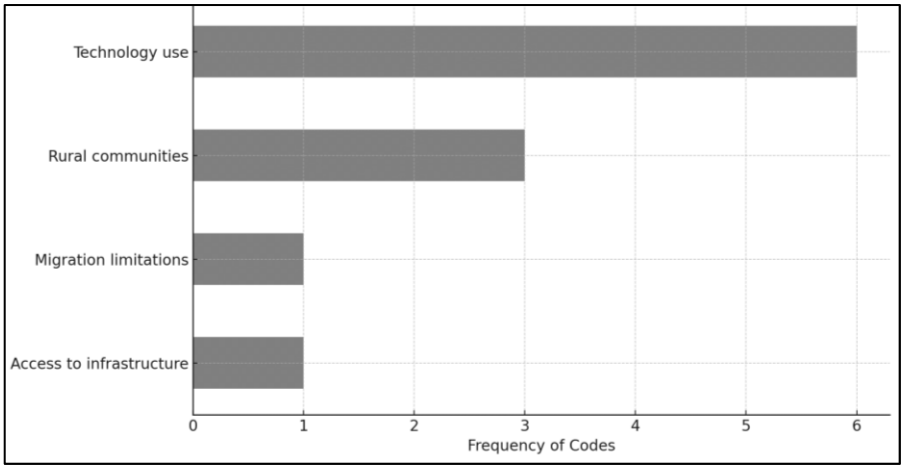


Figure 30: Preparedness for 2G/3G shutdown - top themes

This analysis highlights critical areas where stakeholders encounter both challenges and opportunities. Key themes, illustrated in Figure 30, include technology use, rural communities, migration limitations, and access to infrastructure.

1. Technology use

   The technology use theme, with six mentions, reflects stakeholders' adoption of advanced security technologies to counteract SIM swap fraud. This theme highlights the preparedness of stakeholders to leverage new technologies to replace the security functions previously offered by legacy networks (National Identity Management Commission, 2021). However, access to these technologies is not uniform across different environments, which may leave certain groups more vulnerable than others. Through the RAT lens, these disparities in technology access compromise effective guardianship, as users in some areas may lack adequate protection against SIM swap fraud. The concept map related to technology transition implications is shown in Figure 31.

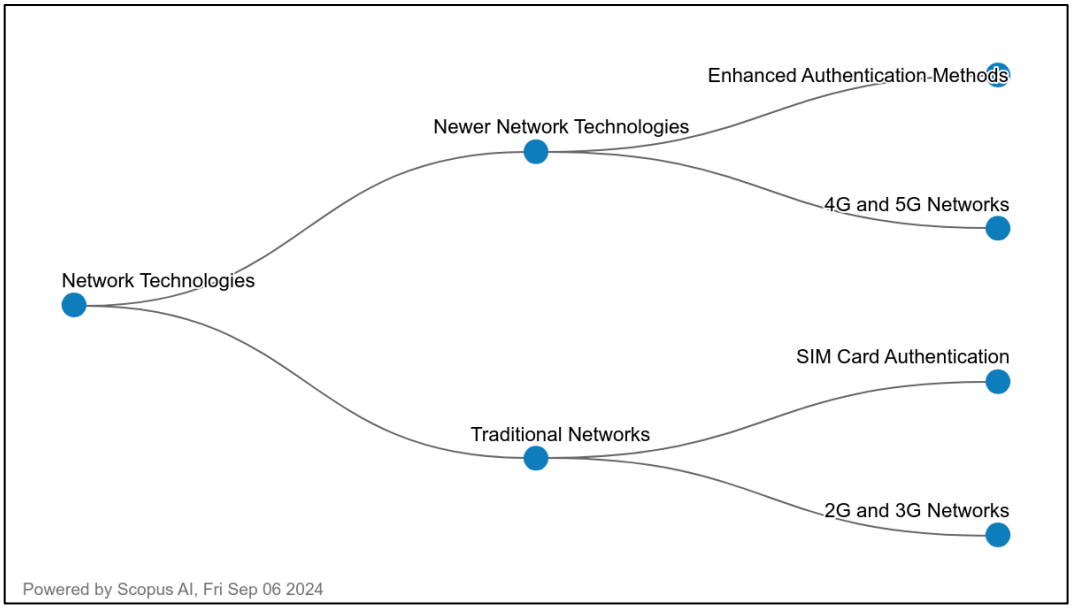


Figure 31: Network technology contrast concept map

2. Rural communities

   The rural communities theme, coded three times, highlights specific challenges in implementing fraud prevention in isolated regions. Rural communities often lack immediate access to advanced technologies, making them particularly vulnerable during and after network transitions (BEREC Europa, 2023). This theme suggests a gap in preparedness, as stakeholders may not allocate resources evenly, leading to weaker defences in rural areas. The RAT's notion of lack of capable guardianship is evident here – reliance on outdated security measures in these regions increases their exposure to fraud risks.

3. Migration limitations

   Migration limitations, noted once in the data, address the constraints associated with transitioning from 2G/3G to newer network technologies. Although mentioned infrequently, this theme is significant, as delays in migration can create temporary security gaps. A staggered approach to network upgrades can leave certain users exposed without continuous fraud

protection (BEREC Europa, 2023). This aligns with the RAT, as partial migration leads to periods where guardianship is incomplete, thereby increasing susceptibility to SIM swap fraud.

4. Access to infrastructure

   Access to infrastructure, also mentioned once, highlights the critical role of robust physical and digital infrastructure in implementing new security measures. Effective fraud prevention depends on consistent access to advanced technologies across regions. Although infrequently mentioned, this theme underscores the foundational importance of infrastructure in enabling stakeholder preparedness. Inadequate infrastructure, according to the RAT, weakens capable guardianship, making it difficult to protect users effectively.

The themes identified reveal various aspects of stakeholder preparedness and the associated challenges in achieving effective guardianship. Technology use emerges as a primary focus, highlighting stakeholders' reliance on advanced security measures like multi-factor authentication and biometric verification to address the vulnerabilities that legacy networks left exposed (Lee *et al*., 2023). However, access to these technologies is inconsistent, with rural communities facing significant gaps in fraud prevention infrastructure (Al-Humaigani *et al*., 2009). The concept map linked to 2G/3G phase-out challenges is shown in Figure 32.

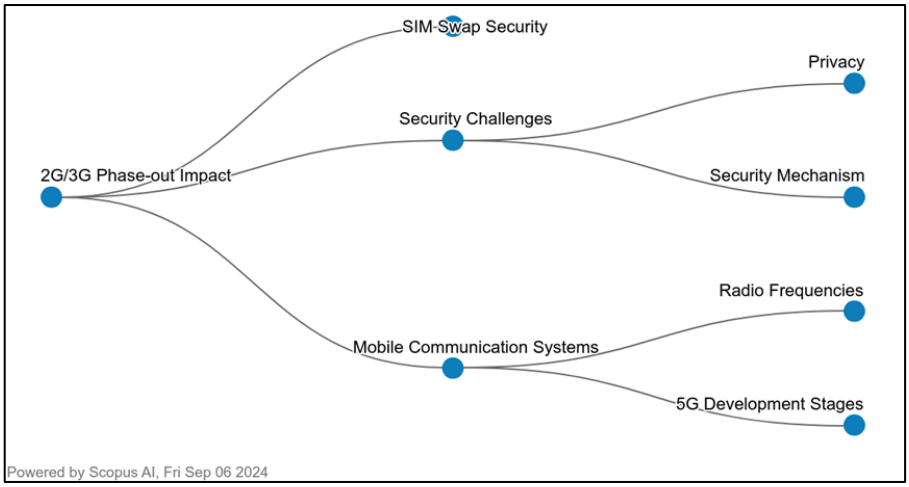


Figure 32: 2G/3G phase-out challenges contrast concept map

Migration limitations and access to infrastructure also represent systemic barriers to comprehensive preparedness. Delays in migration from 2G/3G can create temporary gaps in fraud defences, while limited infrastructure restricts the consistent application of security measures across regions. From the RAT's perspective, guardianship is compromised in areas without robust technological support, leaving users more exposed to fraud. These areas include:

- Strategic initiatives to enhance preparedness

  In response to these challenges, telecommunication companies, financial institutions, and regulatory bodies have implemented multi-layered security strategies. Telecom operators, for instance, have upgraded their security infrastructure with multi-factor authentication, biometric verification, and real-time monitoring systems, which are critical in detecting fraudulent SIM swap attempts (Lee *et al*., 2023). Collaborative frameworks between telecom providers and law enforcement enable rapid information exchange and quicker responses to fraud, bolstering security (Toorani & Beheshti, 2008).

  Regulatory bodies also play a vital role by enforcing stricter identity verification standards. In regions with high incidences of SIM swap fraud, governments have mandated reporting and collaboration with cybersecurity experts to enhance detection efforts (Masrub & Alahemar, 2020). Additionally,

cybersecurity task forces are being established to anticipate emerging fraud tactics, providing another layer of protection post-2G/3G shutdown (Al-Humaigani *et al*., 2009). Financial institutions, too, have strengthened security through AI-driven solutions that monitor transaction patterns and flag anomalies indicative of SIM swap fraud (Ammayappan, 2013).

- Persistent challenges and opportunities for improvement

Despite these advancements, stakeholders still face challenges due to rapid technological change and inconsistent regulatory practices across regions. Kumar (2024) noted that consistent cross-border collaboration and policy enforcement are crucial, particularly in regions with less regulated telecommunication infrastructures. Misalignment across sectors further emphasises the need for enhanced coordination and adaptability to evolving fraud tactics.

Noteworthy progress has been made in reducing SIM swap fraud incidents. In South Africa, for example, reported cases dropped from 4,508 in 2021 to just 71 in 2022, reflecting the effectiveness of current measures (SABRIC, 2022). Nonetheless, thousands of cases persist across the globe each year, underscoring the continued vulnerability within mobile banking and the need for sustained vigilance (iiDENTIFii, 2024). The success of biometric SIM registration in countries like Kenya and Russia, suggests that similar strategies could strengthen defences on a global scale (iiDENTIFii, 2024).

The analysis highlights the importance of a comprehensive and inclusive approach to mitigating SIM swap fraud in the post-2G/3G shutdown context. Effective guardianship necessitates not only the deployment of advanced security measures but also their equitable distribution across different regions and demographics. Addressing the unique vulnerabilities of rural communities and ensuring infrastructure and migration strategies align with fraud prevention goals are essential for a resilient defence framework.

Informed by the RAT, this analysis reinforces the need for technology-driven, inclusive guardianship to protect all users effectively. By balancing technological access, geographic inclusivity, and infrastructural support, stakeholders can create a cohesive approach to fraud prevention, ensuring robust protections remain accessible to all user segments in the post-shutdown landscape.

6.4.3 AI in fraud detection

This section examines the integration of AI in detecting and preventing fraud, addressing the question: How is AI currently employed to enhance fraud detection? The introduction of AI has significantly bolstered the fraud detection capabilities of financial institutions, enabling them to analyse vast amounts of transactional data in real time. Leveraging machine learning algorithms and advanced analytics, AI systems can rapidly identify anomalies and detect patterns indicative of fraud with remarkable accuracy and efficiency (Natarajan & Ashara, 2024; Sood *et al*., 2023; Sharma, 2024). For instance, AI tools can flag unusual account activities and identify irregular transaction behaviours, enhancing both the speed and precision of fraud detection processes (Malhotra *et al*., 2023). Moreover, AI-driven tools have demonstrated substantial success in filtering out fraudulent phone calls, effectively distinguishing malicious activity from legitimate interactions (Malhotra *et al*., 2023). Overall, AI augments traditional fraud detection methods by automating routine tasks and supporting human analysts, thereby fortifying organisational defences against fraud (Adekunle & Jaiyeola, 2024).

The literature identifies several core themes, as shown in Figure 33, which include technological advancements, machine learning applications, data security, and automation. Each of these themes offers insights into how AI is shaping more resilient fraud prevention frameworks.

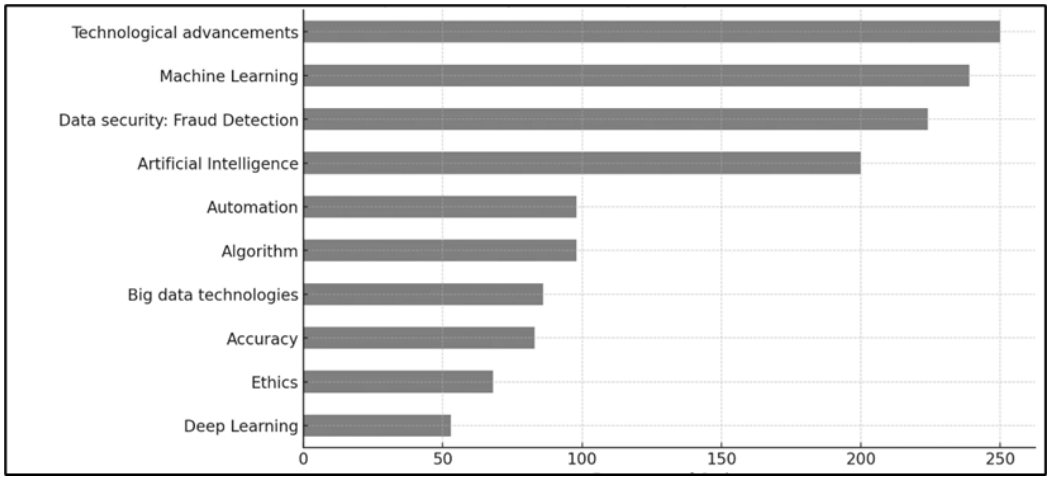


Figure 33: AI in fraud detection - Most prominent codes

These themes are further illustrated in Figure 34, generated through a Scopus AI semantic search on AI applications in fraud prevention. The concept map highlights prevalent technologies and specific use cases within the field.

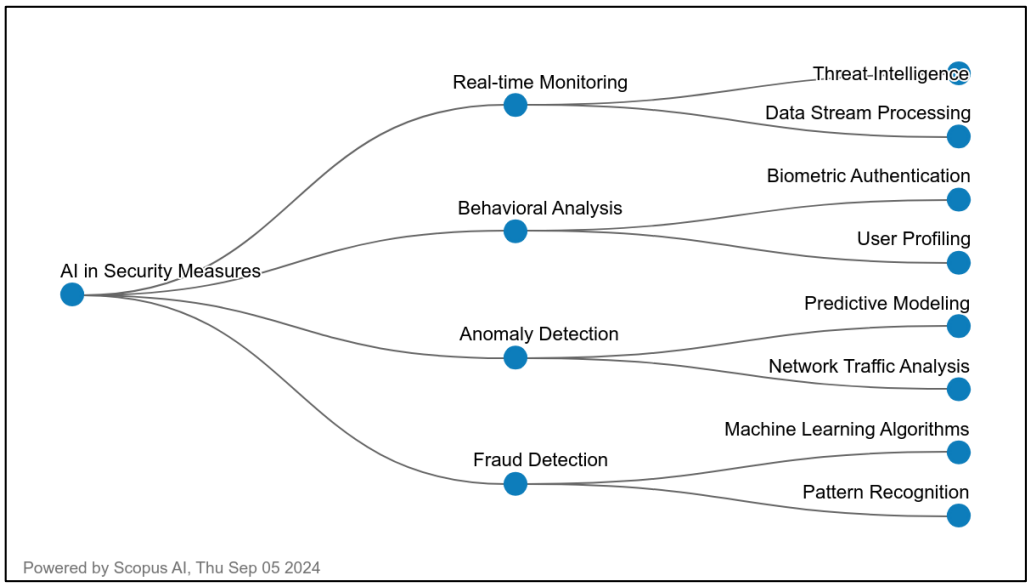


Figure 34: AI in security measures concept map

1. Technological advancements

   Technological advancements emerged as the most frequently cited theme, reflecting the ongoing evolution of AI tools and algorithms for fraud detection

(Bello *et al*., 2023; Malhotra, 2023; Shapiro, & Hassett, 2012; Lane, 2020). These advancements enable real-time fraud detection across various financial settings, providing organisations with adaptive tools that can proactively address fraud risks. From a RAT perspective, these advancements strengthen capable guardianship by equipping entities with comprehensive and proactive defences against fraud.

2. Machine learning

   Machine learning applications, a key theme with numerous citations, emphasise the versatility of machine learning in identifying fraudulent behaviours. Tools such as neural networks, supervised learning, and reinforcement learning are instrumental in analysing complex datasets and predicting fraudulent activities (Ali *et al*., 2024; Dayyabu *et al*., 2023; Kumar, 2023; Malhotra, 2023). The adaptability of machine learning models, particularly supervised learning, and neural networks, enhances the resilience of fraud detection by allowing quick adaptation to emerging fraud patterns. Through the lens of the RAT, machine learning strengthens capable guardianship by increasing detection systems' adaptability and responsiveness.

3. Data security

   Data security in fraud detection focuses on securing data within AI systems to prevent unauthorised access and ensure robust fraud prevention. With 224 mentions, this theme stresses the importance of safeguarding sensitive information through measures like encryption and fraud monitoring algorithms. (Olugbenga, 2021; Kim *et al*., 2022) Effective data security practices enhance trust in AI-driven fraud detection systems and align with the RAT’s emphasis on capable guardianship, as they contribute to a resilient and secure fraud detection framework.

4. Automation

   Automation in fraud detection reflects AI's role in automating repetitive tasks, allowing for uninterrupted fraud monitoring without constant manual oversight. Automation, frequently cited in the literature, improves the efficiency of fraud detection enabling real-time alerts essential for swift responses (Ekwonwune *et al*., 2022; Natarajan & Ashara 2024; Pramod, 2022; Salaudeen *et al*., 2022). By providing continuous, automated oversight, AI-driven automation reinforces capable guardianship, creating an enduring protective barrier against fraud attempts.

Based on the analysis, several AI techniques stand out for their contributions to fraud detection, as shown in Figure 33 and Figure 34. Anomaly detection, a prominent technique, involves training machine learning models to flag deviations from normal behavioural patterns, thereby identifying potential fraud in real time (Zhao, 2021). However, while effective, anomaly detection models can produce false positives, occasionally impacting legitimate user activities (D'Alessandro et al., 2014).

Supervised learning models, such as decision trees and support vector machines, are commonly applied in fraud detection, using labelled datasets to distinguish between legitimate and fraudulent transactions (Adedoyin, 2018; Malhotra *et al*., 2023). Although highly accurate with sufficient data, these models can struggle with novel fraud tactics absent from their training data. To address these limitations, unsupervised and semi-supervised learning techniques are often deployed, particularly in dynamic environments where fraud patterns are evolving (Abbott et al., 2002). However, these methods may lack precision when managing complex data relationships (Malhotra, *et al*., 2023; Sanni *et al.*, 2023; Kumar et al., 2023).

Neural networks, including deep learning models like recurrent neural networks, offer advanced capabilities in processing complex data to detect fraud patterns in real time (Adewumi and Akinyelu, 2016; Malhotra *et al*., 2019; Nama & Obaid

2024). However, the "black box" nature of deep learning models raises transparency challenges, as it can be difficult to interpret their decision-making processes (Assey v. Vodacom Tanzania, 2023; Malhotra *et al*., 2020).

Natural language processing is another AI application in fraud prevention, often used to detect suspicious language in communications such as phishing emails and chat logs. Natural language processing techniques enable systems to identify linguistic cues indicative of fraud, allowing organisations to pre-emptively thwart scams (Nguyen *et al*., 2021). However, natural language processing models require regular updates to keep pace with the evolving language tactics of fraudsters.

Additional AI applications, such as risk scoring systems and behavioural biometrics, further expand fraud detection capabilities. Risk scoring systems evaluate fraud likelihood by analysing multiple factors, while behavioural biometrics examine unique user patterns, such as typing speed and mouse movement (Kim *et al*., 2022; Bandi & Yalamarthi, 2022; Sharma, 2020; Sood *et al*., 2023). While these tools enhance security, challenges around algorithmic bias and privacy considerations remain.

AI's integration into fraud detection has transformed organisational capabilities, providing faster, more accurate, and automated solutions. Machine learning and automation enable real-time anomaly detection, allowing systems to respond to fraud trends with agility. However, challenges persist, including data dependency, interpretability, and resource demands, as well as ethical considerations around privacy and fairness (Adjaoute, 2013; Miller, 2001; Nicholls *et al*., 2021).

In summary, AI has become a cornerstone of fraud detection, utilising tools like machine learning, deep learning, natural language processing, and behavioural biometrics to enhance security within financial systems. These technologies strengthen capable guardianship by equipping organisations with adaptive, automated, and accurate mechanisms for preventing fraud. However, ethical

concerns around data security, privacy, and transparency remain critical considerations for responsible AI deployment.

The RAT highlights the importance of capable guardianship in fraud prevention, and themes like Technological Advancements, Machine Learning Applications, and Data Security align well with this concept by providing tools that enhance detection accuracy and data protection. Automation adds further strength by ensuring constant monitoring and reinforcing fraud defences without requiring continuous manual intervention. These AI applications collectively spotlight how capable guardianship can be enhanced through technological innovation, although continued advancements and ethical vigilance are essential for AI's responsible use in fraud prevention.

6.4.4 AI techniques for SIM swap fraud

This section investigates the specific AI techniques employed in detecting, preventing, and analysing SIM swap fraud, addressing the question: What AI techniques are currently utilised for identifying and mitigating SIM swap fraud? As outlined and discussed above, in the context of fraud prevention, AI has become indispensable, offering a suite of sophisticated tools that enhance the ability to identify suspicious patterns and respond rapidly to potential fraud cases.

The analysis of codes related to AI techniques for SIM swap fraud, as depicted in Figure 35, highlights several prominent themes, including AI, machine learning, neural networks, and accuracy in detection. These themes draw attention the prolific application of AI tools in enhancing SIM swap fraud prevention.

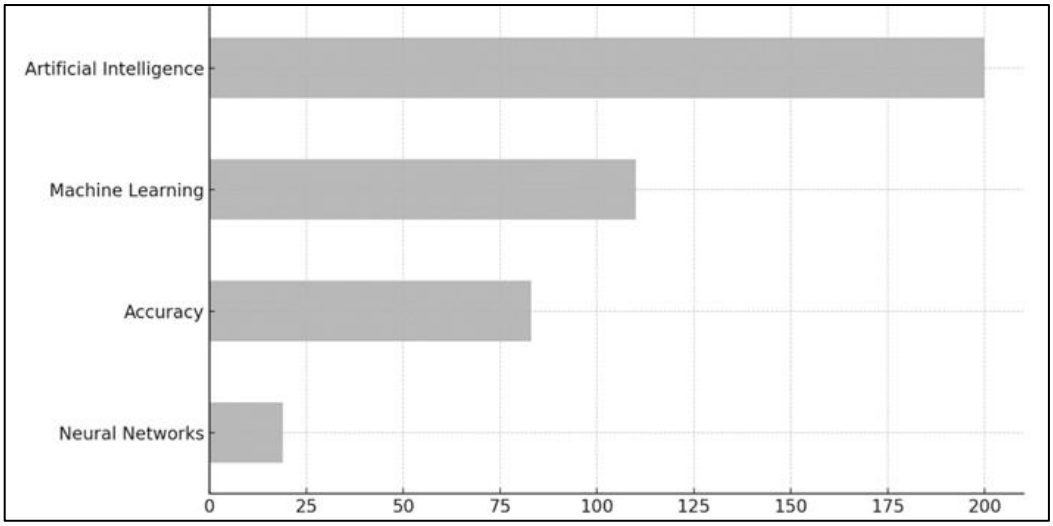


Figure 35: AI techniques for SIM swap fraud - Most prominent codes

1. Artificial intelligence

   AI, the most frequently cited theme, encapsulates the range of AI-driven technologies that bolster SIM swap fraud detection. AI supports sophisticated pattern recognition, real-time fraud analysis, and automated responses, all of which are essential in pre-empting fraud (Fang & Fang, 2024; Harinath, 2023; Malhotra *et al*., 2023). Through quick adaptation and analysis of varied fraud scenarios, AI enhances capable guardianship, reducing the opportunities for fraudulent behaviour. Within the RAT, AI mitigates the lack of capable guardianship by minimising the time and space available for fraudulent actions, allowing for rapid intervention when threats are detected.

2. Machine learning

   Machine learning, a significant theme, involves algorithms that autonomously learn from data and evolve to detect new fraud patterns. Key models, such as support vector machines and random forest, are used to analyse behavioural data and transaction history, effectively flagging potential SIM swap fraud cases. Kashir and Bashir (2019) demonstrated the efficacy of support vector machine models with optimised kernels, achieving a 99.24% accuracy rate in detecting SIM box fraud. Such adaptability highlights Machine Learning's

proactive role in fraud prevention, strengthening capable guardianship by continuously updating to counter emerging fraud tactics.

3. Neural networks

   Neural networks, a specialised subset of machine learning, are particularly effective for complex fraud detection tasks. Models such as multi-layer perceptron and convolutional neural networks can process sophisticated data patterns, capturing subtle indicators of fraud. Sallehuddin *et al*. (2014) showed that neural networks achieved a high classification accuracy of 98.71% in detecting SIM box fraud, underscoring their relevance for SIM swap scenarios. However, these black box models are often challenging to interpret (Singh & Kumar, 2020), presenting a trade-off between accuracy and transparency. Nonetheless, they offer a high level of capable guardianship by enhancing the depth and precision of fraud detection.

4. Accuracy in detection

   Accuracy, a central theme, emphasises the importance of precision in SIM swap fraud detection. High accuracy rates reduce false positives and negatives, ensuring robust protection without interrupting the user experience. By focusing on genuine fraud indicators, accurate AI models enhance capable guardianship by safeguarding users effectively while minimising disruptions. Accuracy is critical in SIM swap detection, where errors can carry significant financial and reputational costs.

Delving into the details of the data beyond these core techniques reveals several advanced AI applications are also making notable contributions to SIM swap fraud prevention:

- Behavioural biometrics: AI-powered behavioural biometrics create user profiles based on unique patterns like finger movements and typing speed, offering an additional layer of fraud protection (Stephens, 2020). Although

this approach is effective, it requires careful balancing of user convenience and security within the SIM swap process.

- Real-time anomaly detection: AI systems monitor for atypical activities, such as sudden IP address changes, flagging them as potentially fraudulent. Harinath (2023) highlights how real-time detection allows immediate response to suspicious SIM swap attempts, reinforcing proactive defence with timely data.
- Natural language processing: This form of processing is used to analyse unstructured data, including SMS and call logs, to identify language indicative of SIM swap fraud. Sood *et al*. (2023) discuss natural language processing's capacity to detect malicious language, providing a preventive layer by examining large volumes of communication data for red flags.
- Graph-based anomaly detection: Graph-based techniques analyse the relationships between entities to uncover organised fraud networks. Nicholls, Kuppa, and Le-Khac (2021) illustrate how these models identify fraud rings by mapping connections between individuals attempting SIM swaps, although they require substantial computational resources for large-scale implementation.
- Predictive analytics: Predictive models use historical data to assess fraud risks, with AI-based risk scoring prioritising cases for further investigation. As Pratima (2023) notes, while predictive analytics are powerful, they can introduce bias if training data does not represent diverse fraud scenarios.

To address the interpretability challenges associated with complex AI models, explainable AI techniques are being explored. Bandi and Yalamarthi (2022) emphasise the importance of explainable AI in making AI models' decision-making processes transparent, especially in regulatory settings. Trustworthy AI further focuses on ethical deployment, ensuring fairness and transparency in fraud detection systems, although consistency across platforms remains an issue.

AI has fundamentally transformed SIM swap fraud detection, bringing advanced capabilities in pattern recognition, real-time monitoring, and predictive analytics. Techniques like machine learning, neural networks, behavioural biometrics, and natural language processing offer a multi-faceted approach to fraud prevention, adapting to evolving fraud patterns with high levels of accuracy and speed. Nevertheless, challenges around resource demands, interpretability, and ethical considerations persist, requiring a balanced approach that ensures both effectiveness and fairness. Figure 36 illustrates these challenges in greater detail, as captured through a concept mapping of related literature.

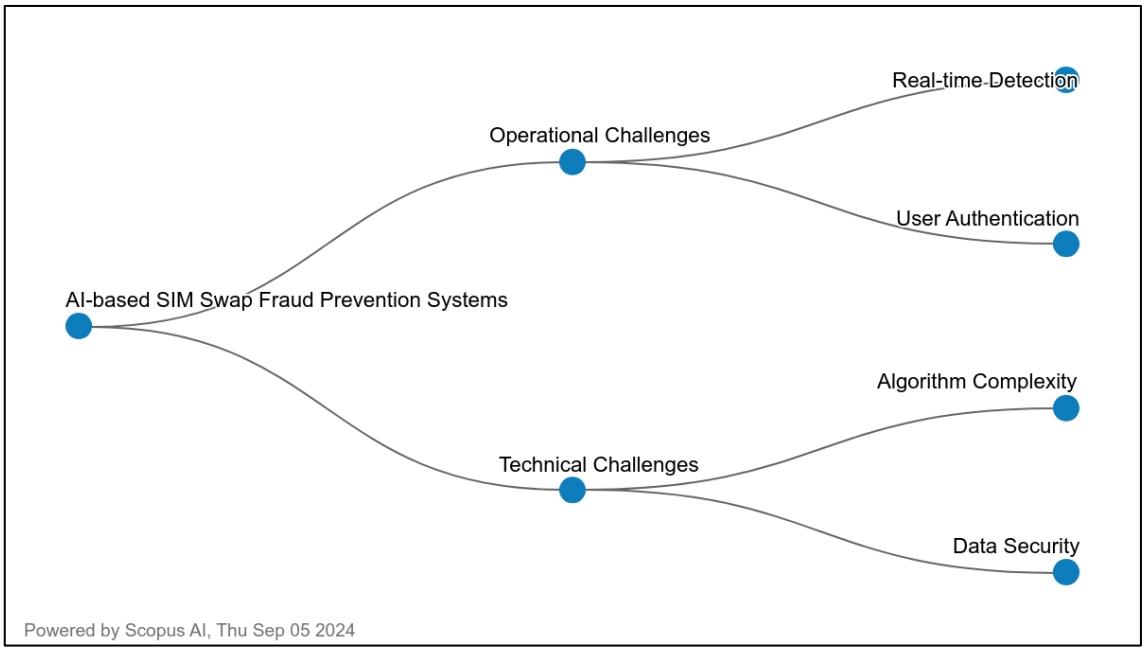


Figure 36: Challenges for AI in SIM swap concept map

In the context of the RAT, AI reinforces capable guardianship by enhancing system responsiveness and accuracy, thus providing an immediate and effective defence against SIM swap fraud. By reducing the window of opportunity for fraudsters and increasing detection precision, AI supports proactive strategies that protect users more effectively.

This analysis makes clear the substantial benefits of AI-driven systems in SIM swap fraud prevention, emphasising the importance of accuracy, adaptability, and transparency. AI techniques like machine learning and neural networks have

established a robust foundation for secure, AI-enabled fraud detection systems, laying the groundwork for further advancements in this field.

6.4.5 Effectiveness of AI solutions

This section examines the effectiveness of AI solutions in mitigating SIM swap fraud, addressing the question: How is the effectiveness of AI in preventing SIM swap fraud measured? While the reviewed literature does not offer studies solely dedicated to AI's role in combating SIM swap fraud, there is a broad consensus on the growing necessity for advanced AI-based approaches to address the rising incidence of SIM swap attacks (Marakalala, 2023; Assolini, 2019). This section, therefore, synthesises insights on evaluating AI's effectiveness in fraud prevention, focusing on critical performance metrics that are adaptable to the context of SIM swap fraud.

Key themes in assessing AI for fraud prevention, highlighted in Figure 37, are organised around terms like Performance, Achievement, and Evaluation. These metrics provide a framework for understanding how AI solutions are assessed in terms of their utility in detecting and mitigating SIM swap fraud.

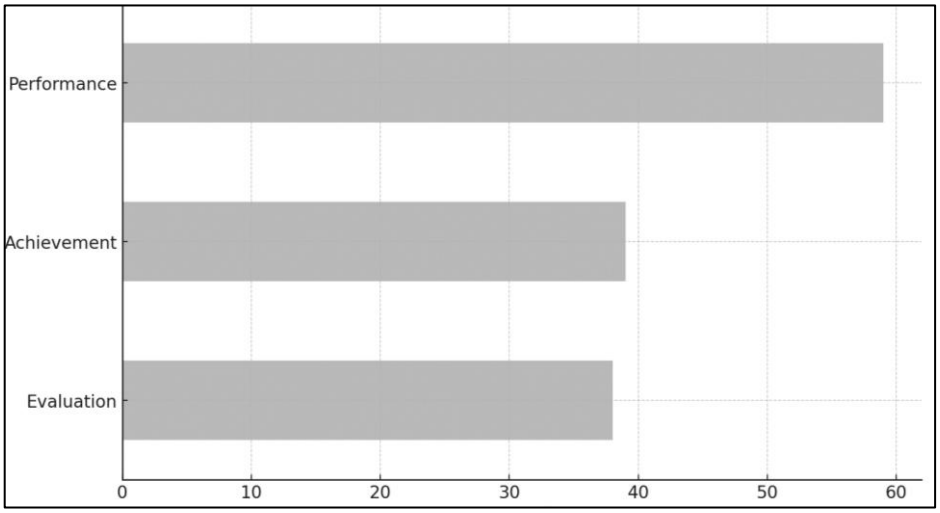


Figure 37: Effectiveness of AI solutions - themes

1. Performance

Performance, the most frequently discussed theme, pertains to operational metrics such as detection accuracy, speed, and scalability – fundamental attributes that enable AI to counter fraud in real time. Kashir and Bashir (2019) emphasise that metrics like classification accuracy, regression rates, and algorithm comparisons are essential for gauging AI's performance. For instance, their study revealed that support vector machines and neural networks performed particularly well in distinguishing genuine from fraudulent SIM swap attempts, with certain support vector machine kernels, including Radial and Sigmoid, demonstrating superior accuracy. This reinforces the importance of optimising and fine-tuning algorithms to enhance fraud detection capabilities.

Furthermore, Sallehuddin *et al.* (2014) tested 240 neural network models in fraud detection, achieving a classification accuracy of 98.71%. Their study underscored how parameter adjustments, such as generalisation error, precision, and recall, are crucial for model robustness. By balancing high detection accuracy with minimal false positives, these metrics reinforce a positive user experience and secure fraud detection.

Ultimately, performance metrics suggest that the effectiveness of AI in fraud prevention relies on accuracy, speed, and scalability, which are foundational to a robust fraud defence system. From the perspective of the RAT, high-performance AI systems function as capable guardians, strengthening the security framework against fraud by effectively identifying and counteracting threats.

2. Achievement

The theme of achievement centres on measurable outcomes such as heightened accuracy, decreased fraud rates, and lower operational costs. AI's capacity to monitor user behaviour and identify anomalies is another key performance indicator. Malek *et al.* (2008) developed an AI model based on artificial neural networks to analyse user behaviour, issuing real-time alerts

when anomalies are detected. This approach added an extra layer of defence, enhancing the system's ability to detect SIM swap fraud.

Similarly, Harinath (2023) highlights the ability of AI to trigger alerts for sudden changes in user activity, such as unusual IP address shifts, enabling mobile network operators (MNOs) to intercept fraud attempts pre-emptively. Fang's (2024) Telecom Fraud Detection model, which covers the entire fraud lifecycle, from pre-warning to post-monitoring, further drawing attention to AI's role in real-time intervention, helping to block fraudulent activity as it arises.

Thus, achievement in real-time monitoring and fraud detection captures AI's tangible contributions to reducing fraud and enhancing system reliability. This theme underscores AI's role in meeting critical performance benchmarks, establishing it as an effective guardian in the fight against SIM swap fraud.

3. Evaluation

Evaluation encompasses systematic assessments of AI models, encompassing factors such as algorithm performance, accuracy, and overall effectiveness in fraud prevention. Evaluation methods ensure that AI models remain agile and effective against new fraud risks, aligning with the RAT's concept of capable guardianship.

Comparative studies have shown that AI models consistently outperform traditional fraud detection methods. For example, Chitroub *et al*. (2018) compared AI-based systems to conventional techniques, assessing aspects like detection speed and accuracy. Their results demonstrated that AI models offered a marked advantage in identifying SIM swap fraud, underscoring their ability to handle complex datasets. Metrics like false-positive and false-negative rates are also essential, as Assolini (2019) highlights, emphasising the need for user-friendly, accurate systems that balance effectiveness with minimising user friction.

Testing AI models across varying network conditions further reveals their adaptability. For instance, Bijani and Kazemitabar (2008) tested a hybrid intrusion detection system that combined host-based and network-based approaches, assessing its effectiveness against different attack types, including SIM cloning and denial-of-service (DoS) attacks. The system's ability to adapt to diverse threats showss the importance of rigorous evaluation and ongoing refinement.

A deeper analysis of AI applications in SIM swap fraud mentioned in the supporting data reveals several advanced AI techniques have demonstrated efficacy in preventing SIM swap fraud:

- Anomaly detection: AI-based anomaly detection systems monitor user behaviour to quickly flag deviations, allowing timely interventions against SIM swap fraud. Natarajan and Ashara (2024) highlight AI's ability to detect unusual account activity in real time, thus enhancing fraud detection capabilities.
- Case-based reasoning: Case-based reasoning models integrate historical data with real-time inputs, continuously refining their accuracy. Hilas (2009) developed an expert system using case-based reasoning that adapts to new fraud cases, offering an adaptable and high-detection solution.
- Consumer protection efforts: Although less frequently discussed, AI applications in consumer education bolster user awareness and resilience, indirectly reinforcing capable guardianship by reducing users' vulnerability to SIM swap fraud.

Assessing AI's effectiveness in detecting SIM swap fraud involves a comprehensive set of performance metrics, achievement milestones, and systematic evaluations. High performance in terms of accuracy, speed, and scalability underscores AI's operational strengths, while achievements like reduced fraud rates highlight its real-world impact on fraud prevention. Regular

evaluations ensure that AI models remain responsive to emerging threats, which is crucial in maintaining AI's role as a capable guardian in fraud prevention.

The themes of performance, achievement, and evaluation form a robust framework for assessing AI's effectiveness in SIM swap fraud prevention. In the context of the RAT, effective AI systems fulfil the role of a capable guardian by detecting fraud efficiently and responding swiftly. Continuous fine-tuning of these systems is essential to sustain their protective role, as AI solutions need to evolve alongside the fast-paced landscape of digital fraud.

Looking ahead, stakeholders must prioritise consistent assessment methods that combine quantitative metrics with user feedback to enhance the resilience and adaptability of AI in fraud detection. As AI technology advances, ongoing evaluation and recalibration will be essential to maintain a strong and dynamic defence against fraud, ensuring a secure and adaptable digital environment.

6.4.6 Future of AI in SIM swap fraud management

This section examines the future of AI-driven solutions for preventing SIM swap fraud in mobile networks, guided by the question: What new AI technologies are being suggested or implemented to prevent SIM swap fraud? Emerging methods include biometric verification, advanced machine learning analytics, and blockchain-enabled transaction tracking. These innovations are geared toward creating a more proactive and secure mobile environment by minimising unauthorised access (Jordaan & Von Solms, 2011; Lokanan, 2023). Key themes from the literature, as shown in Figure 38, include authentication, technological advancements, artificial intelligence, data security, trust, and automation.

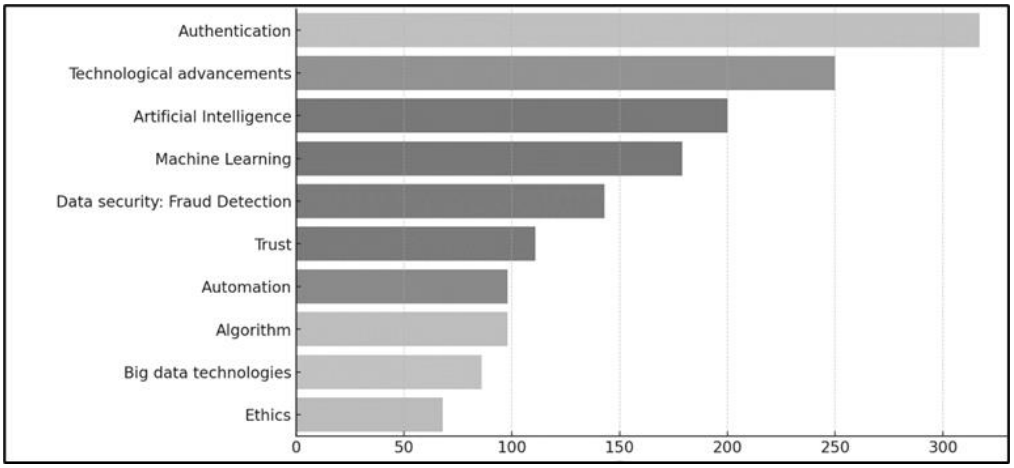


Figure 38: Future of AI - Most prominent codes

1. Authentication

   The authentication theme, referenced extensively, highlights the importance of advanced verification methods such as biometrics and multi-factor authentication in fraud prevention. Biometric systems use unique physical characteristics, such as fingerprints or facial recognition, to ensure that only verified individuals can perform SIM swaps, creating secure barriers that are challenging for fraudsters to bypass. These advanced methods embody the RAT's capable guardianship dimension by reinforcing security against unauthorised access.

   Recent shifts in authentication practices are moving away from traditional passwords toward biometrics, recognised for their non-repudiable nature, which binds access to each user's unique attributes. This technology is increasingly advocated to reduce the effectiveness of social engineering tactics and unauthorised SIM swaps, reinforcing the security layer (Jordaan & Von Solms, 2011).

2. Technological advancements

   The technological advancement theme highlights tools like blockchain, real-time monitoring, and cloud-based security solutions. Blockchain technology,

for instance, offers a secure ledger for tracking SIM-related transactions, enhancing transparency and reducing fraud risks (Singh & Kumar, 2020). AI-powered real-time monitoring systems allow continuous oversight of network activity, enabling rapid responses to suspicious patterns.

Research supports blockchain integration as a powerful method for transparent transaction records, while AI-driven anomaly detection provides real-time alerts to prevent fraud. Together, these technologies represent a tech-augmented guardianship, capable of evolving alongside sophisticated fraud tactics.

3. Artificial intelligence

AI, a pivotal theme, encompasses machine learning, deep learning, and neural networks, which are instrumental in detecting fraud patterns and anomalies. Machine learning plays a vital role in predictive fraud modelling, enabling systems to anticipate and identify fraud trends before they materialise.

AI's ability to detect complex patterns in real time significantly enhances fraud detection, enabling dynamic adaptation to emerging threats. This evolution of AI represents a form of intelligent guardianship in fraud prevention, aligning with the RAT's concept of capable guardianship by proactively identifying suspicious activities.

4. Data security

The theme of data security emphasises encryption, secure databases, and cybersecurity protocols to protect sensitive user information from unauthorised access. These foundational security measures are critical for preventing SIM swap fraud, as they limit fraudsters' access to data that could be exploited in fraudulent transactions.

By employing encryption and robust data-sharing protocols, AI-driven fraud prevention strategies help create a secure digital environment, reinforcing digital guardianship against potential breaches and strengthening overall fraud resilience.

5. Trust

   The theme of trust highlights the importance of fostering customer confidence in AI-driven fraud prevention technologies. Transparent and effective security measures are crucial for encouraging user adoption and compliance with advanced authentication and verification methods (Buzzard, 2023; LexisNexis Risk Solutions, 2024; Jentzsch, 2012; Jimenez *et al.*, 2016; Jover 2018).

   Trust acts as both a preventive factor and an outcome of effective AI-based security, reducing fraud vulnerability while promoting user engagement and confidence. The RAT suggests that customer trust in fraud prevention systems can play a significant role in reducing fraud opportunities by enhancing compliance and minimising attempts to bypass these systems.

The details of the base literature reveal several emerging AI solutions and their applications:

- Federated learning: Abuhamoud *et al*. (2021) propose federated learning as an approach to improve privacy in fraud detection, as it trains machine learning models across decentralised devices without sharing raw data. This method preserves user privacy while enhancing predictive accuracy.
- Explainable AI: With increasingly complex AI models, transparency is essential. Explainable AI allows network operators and users to understand the decision-making processes behind fraud detection, fostering regulatory compliance and building trust in AI systems, particularly in disputed cases (Bandi & Yalamarthi, 2022).
- Trustworthy AI: Future AI solutions will focus on fairness and avoiding bias. Bello *et al*. (2023) advocate for bias-detection algorithms to ensure that fraud

prevention measures do not disproportionately impact specific user groups, fostering equitable fraud prevention.

- Blockchain and smart contracts: By securing transaction records with blockchain and automating SIM swap validation with smart contracts, stakeholders can reduce human error and social engineering risks (Singh & Kumar, 2020).
- Behavioural biometrics and continuous authentication: Behavioural biometrics analyse user-specific patterns, such as typing speed and mouse movement, to detect anomalies (Stephens, 2020). Continuous authentication verifies user identity throughout a session, offering a dynamic, ongoing security check (Marakalala, 2023).
- Quantum computing: Quantum computing has the potential to rapidly process vast datasets, identifying complex fraud patterns. However, it also introduces new challenges, necessitating quantum-resistant security measures (Abuhamoud *et al*., 2021).
- Edge AI and 5G networks: Edge computing and 5G networks enable AI to operate closer to data sources, which enhances detection speed and efficiency. This setup allows immediate responses to threats and reduces latency, which is particularly valuable for fraud detection in complex environments (Fang & Fang, 2024).
- Risk scoring and context-aware systems: AI-driven risk scoring leverages contextual data, such as location and device history, to assess fraud risk and tailor security measures (Pratima, 2023). Context-aware systems adjust fraud protocols based on environmental cues, improving detection accuracy while minimising disruptions.

The future of SIM swap fraud prevention is set to benefit from a wide range of AI-driven innovations, from federated learning to edge computing. Each solution enhances fraud prevention, strengthening AI's role as a capable guardian in digital security frameworks. By advancing authentication mechanisms, incorporating cutting-edge technologies, and ensuring transparency, stakeholders can address evolving fraud tactics with greater agility and resilience.

These advancements highlight AI's essential role in fraud prevention, aligning with the RAT's emphasis on capable guardianship. As fraud methods continue to evolve, maintaining robust, transparent AI systems will be essential in preventing SIM swap fraud and sustaining user trust. Through continual innovation and comprehensive security strategies, AI-driven solutions are well-positioned to secure the future of mobile fraud prevention.

6.5 Conclusion

This chapter has provided a comprehensive thematic analysis of SIM swap fraud, structured through the lens of the RAT, to shed light on key factors influencing both the prevalence of this type of fraud and the effectiveness of measures designed to counter it. By examining SIM swap fraud through the dimensions of a motivated offender, suitable target, and lack of capable guardianship, we gain a nuanced understanding of the behaviours of fraudsters, the vulnerabilities of potential victims, and the strengths and limitations of existing and emerging security measures.

Within the motivated offender dimension, SIM swap fraudsters emerge as individuals with notable technical expertise, adept social engineering skills, and, in many cases, ties to organised cybercrime networks. The themes of impersonation and resilience suggest that these offenders are not only skilled manipulators but also highly adaptable, often refining their techniques to bypass evolving security measures. This adaptability indicates the need for targeted, dynamic prevention strategies that address both the technical and psychological tactics used by fraudsters.

The suitable target dimension highlights factors that increase users' susceptibility to SIM swap fraud, with a particular focus on confidentiality risks, general vulnerabilities, and data accessibility. The analysis illustrates a critical knowledge gap in cybersecurity awareness, especially among users with inconsistent access to protective resources, such as those in rural areas. Although community

initiatives and regulatory efforts exist to mitigate these issues, significant gaps remain, particularly in user education and equitable access to fraud prevention tools, which may leave certain groups more vulnerable than others.

In exploring the lack of capable guardianship dimension, this chapter examined the preparedness of key stakeholders, including telecom operators, regulatory bodies, and law enforcement agencies, in addressing SIM swap fraud. Foundational security measures, such as access control, cybersecurity protocols, and verification processes, represent the primary line of defence. Additionally, AI-driven solutions are increasingly enhancing fraud detection capabilities through advanced technologies like machine learning, predictive modelling, and automation, thereby improving the speed and precision of fraud detection efforts. However, challenges persist, particularly in the uneven adoption of these technologies across underserved areas, indicating a need for enhanced cooperation among stakeholders to address regional disparities and achieve consistent protections.

Furthermore, this chapter evaluated the role of AI in detecting and preventing SIM swap fraud, with a focus on metrics such as accuracy, performance, and detection delay as benchmarks for assessing AI's effectiveness. Advanced technologies, including multi-factor authentication, big data analytics, and biometric verification, are now integral components of AI-enhanced fraud prevention systems. However, the themes of trust and ethics remain crucial, as the effectiveness of AI solutions hinges not only on technical performance but also on user confidence and ethical deployment, ensuring that these tools operate fairly and transparently across diverse user demographics.

Overall, this chapter reveals that effectively combating SIM swap fraud requires a multi-dimensional approach that combines technical defences, regulatory support, user education, and innovative AI solutions. By integrating these elements into a cohesive defence framework, stakeholders can better adapt to the rapidly evolving tactics of fraudsters and work toward resilient, equitable protection for all users. This comprehensive approach, rooted in continuous

adaptation and collaboration, points out the importance of both technological and human factors in creating a robust and sustainable defence against SIM swap fraud.

While the findings confirm AI's potential in detecting SIM swap fraud, a critical review reveals notable blind spots. Many studies emphasise technical performance metrics (e.g. accuracy, precision) but give little attention to ethical or practical implementation challenges, such as the availability of training data, resource constraints, or user trust. Moreover, most empirical evidence stems from developed markets, limiting the transferability of findings to South Africa's context. This imbalance in the literature not only narrows the scope of AI solutions proposed but also risks exacerbating digital inequalities if applied uncritically.

CHAPTER 7. CONCLUSION AND RECOMMENDATIONS

The thematic analysis in Chapter 6 reinforced and expanded upon the patterns identified in Chapter 5, offering grounded insights into the behavioural, technical, and institutional dimensions of SIM swap fraud. Building on these findings, Chapter 7 presents a synthesis of conclusions and recommendations. These are designed to address both the research gaps identified in the bibliometric review and the network migrations related SIM swap fraud vulnerabilities surfaced in the thematic analysis. By examining SIM swap fraud across three dimensions, namely motivated offender, suitable target, and lack of capable guardianship, the study has revealed insights into the underlying dynamics, risk factors, and potential interventions. Here, these insights are translated into targeted recommendations, particularly emphasising regulatory measures, and AI-driven solutions to fortify defences against SIM swap fraud.

7.1 Foundational literature enquiry and theoretical focus

The initial literature review and subsequent discussion chapters served distinct but complementary purposes within this study. The literature review provided foundational knowledge on SIM swap fraud and the role of AI in fraud prevention, particularly within the context of the 2G/3G network shutdown. It offered a broad synthesis, identifying how transitions in network infrastructure can heighten fraud risks and exploring the potential of AI as a countermeasure.

In contrast, the discussion chapters built on this foundation, employing the RAT to dissect SIM swap fraud through the dimensions of a motivated offender, suitable target, and lack of capable guardianship. This framework enabled a more refined analysis, highlighting specific offender traits such as adaptability and technical skills that go beyond the broader concepts presented in the literature review. Additionally, the discussions delved into tailored AI techniques, like machine learning for anomaly detection and behavioural biometrics for user

authentication, providing concrete examples of advanced AI implementations that address the unique challenges of SIM swap fraud amid network transitions.

While the literature review established a general understanding of AI's potential across various fraud contexts, the discussions move toward specific, empirically grounded insights and critiques. This layered approach allowed for a cohesive narrative, progressing from theoretical overviews to specialised, action-oriented analysis. Together, the literature review and discussions contextualised the study's specific focus on SIM swap fraud, forming a comprehensive foundation for the targeted recommendations that follow.

7.2 Summary of findings

The study identified SIM swap fraud as a multi-faceted challenge that combines technical manipulation with social engineering tactics. Findings indicated that offenders often possess both advanced technical skills and a keen understanding of psychological manipulation, underscoring the need for security strategies that are as adaptable and sophisticated as the tactics employed by fraudsters.

The analysis also highlighted vulnerabilities within the suitable target dimension, particularly among users in rural and underserved regions who may have limited access to cybersecurity resources. Such disparities heighten their exposure to SIM swap fraud. While community initiatives aim to bridge these gaps, there remains an urgent need for more comprehensive user education and equitable access to preventive measures.

In terms of guardianship, the study found that existing measures, including access control, cybersecurity protocols, and verification processes, provide a foundational defence. However, the uneven adoption of these technologies, particularly in less connected areas, suggests that greater collaboration among telecom providers, financial institutions, and regulatory bodies is necessary to achieve consistent protection.

Figure 39 provides a summary of the research analytical overview, findings and discussions, as well as the recommendations and conclusion as discussed here.

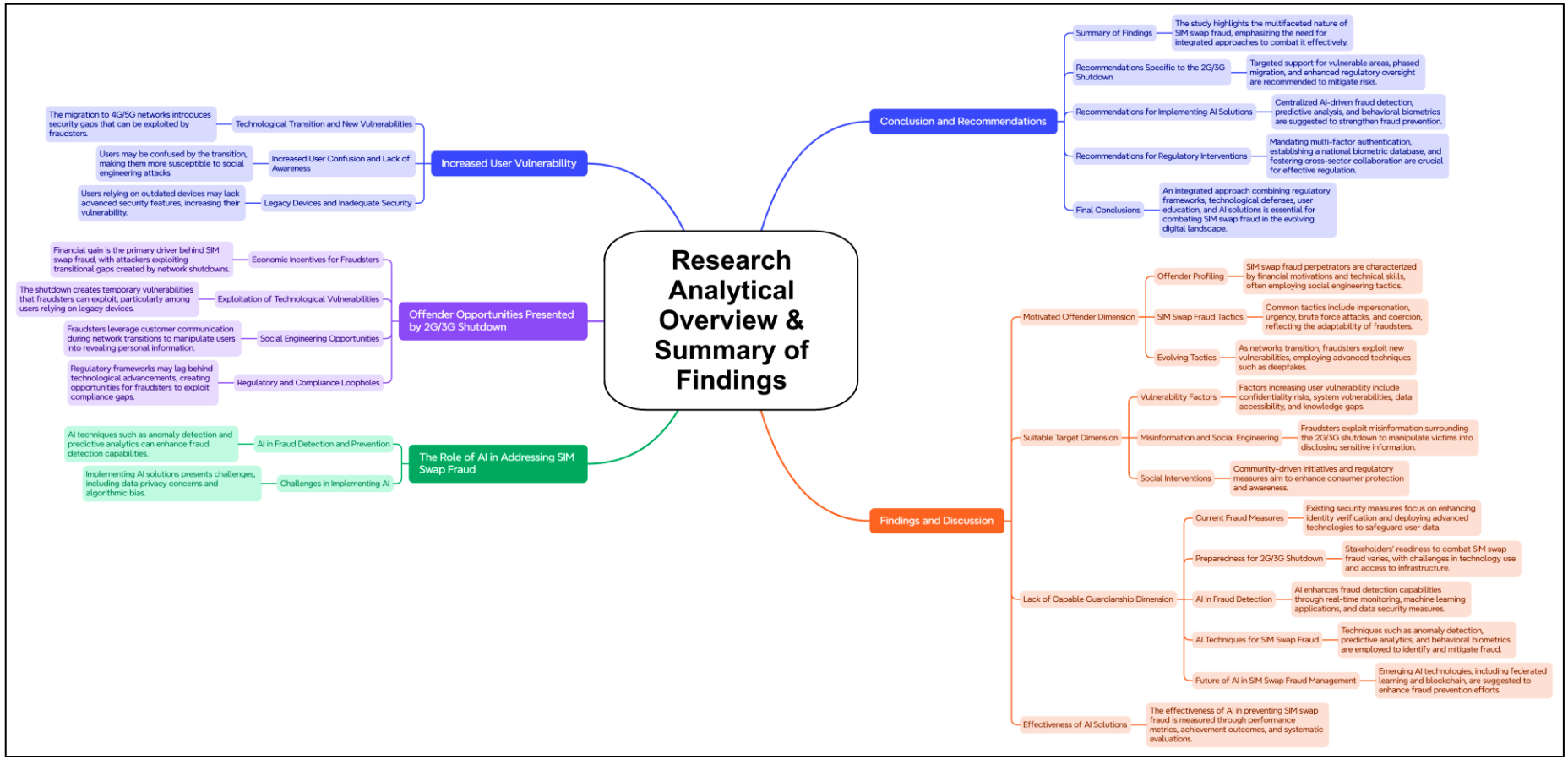


Figure 39: Analytical overview and summary of findings

This research confirms the three propositions aligned with the Routine Activity Theory:

1. Proposition 1: 2G/3G shutdown will lead to an increase in SIM swap fraud due to a larger pool of potentially motivated offenders.
    - 2G/3G to 4G/5G transition creates new incentives for cybercriminals, with technical gaps and social confusion increasing attack feasibility.
2. Proposition 2: 2G/3G shutdown will lead to an increase in SIM swap fraud due to a larger pool of suitable targets.
    - Users, particularly those with legacy devices or low digital literacy, become vulnerable due to unclear migration processes.
3. Proposition 3: Implementing AI as a capable guardian will reduce the overall rate of successful SIM swap fraud attempts.
    - AI can serve as a dynamic and proactive guardian, though implementation is constrained by ethical, infrastructural, and regulatory considerations.

These findings collectively highlight AI's potential as a fraud deterrent when deployed ethically and transparently.

Informed by the analysis in Chapters 5 and 6, which revealed both promising AI capabilities and implementation challenges, the following sections outline targeted recommendations for AI deployment in the telecommunications sector. The intent is to align technical innovation with practical realities such as regulatory readiness, digital literacy, and fraudster adaptation tactics.

7.3 Recommendations specific to the 2G/3G shutdown

The process of transitioning from 2G/3G to more advanced network technologies presents distinct challenges and risks in the context of SIM swap fraud. Key findings suggest that the shutdown of older networks exacerbates vulnerabilities

in underserved areas, while temporary security gaps may arise as older protections are phased out.

The following recommendations are proposed based on this study's findings:

- Targeted support for vulnerable areas: Increase investment in rural infrastructure to ensure seamless adoption of 4G/5G security measures, bridging the digital divide and mitigating fraud risk.
- Phased migration and continuous monitoring: Implement a staggered network shutdown with real-time monitoring to identify and address emerging security vulnerabilities.
- Enhanced regulatory oversight: Regulators should mandate that telecom operators uphold robust security standards throughout and after the transition.
- AI-driven solutions for transitional monitoring: Deploy real-time monitoring and anomaly detection AI tools in areas of ongoing 4G/5G adoption to identify potential fraud activities.
- Cross-sector collaboration: Foster data-sharing and coordination among telecoms, financial institutions, and law enforcement for a unified approach to fraud prevention.

7.4 Recommendations for implementing AI solutions in SIM swap fraud prevention

Advanced AI solutions are essential to pre-emptively addressing the sophisticated tactics of SIM swap fraud. The following strategies provide a framework for the effective deployment of AI in fraud prevention.

Based on the findings of this study, the following recommendations are put forward:

- Centralised AI-driven fraud detection: Establish a centralised monitoring system across networks to detect fraud in real time.

- Predictive analysis and anomaly detection: Use machine learning algorithms to predict high-risk accounts based on historical patterns, pre-emptively triggering preventive measures.
- Behavioural biometrics: Incorporate AI-driven behavioural biometrics for continuous identity verification.
- Explainable AI: Use explainable AI to clarify AI-driven decisions for regulatory compliance and user trust, particularly in disputed cases.
- Adaptive multi-factor authentication: Deploy multi-factor authentication that adjusts verification requirements based on dynamic risk assessment.
- Federated learning: Use federated learning to train machine learning models without sharing raw data, preserving user privacy while enhancing fraud detection.
- Edge computing with AI: Employ edge computing with AI for real-time monitoring, particularly beneficial during network transitions.
- Blockchain integration: Leverage blockchain for transparent logging of SIM swap requests, creating an immutable record to deter social engineering.
- Risk-scoring systems: Develop AI-driven risk scores based on contextual factors, like geolocation, to trigger additional verifications when needed.
- Ethics in AI deployment: Conduct regular ethics audits to ensure fairness in AI-driven fraud prevention and to mitigate potential biases.

7.5 Recommendations for regulatory interventions

Regulatory measures play a vital role in standardising fraud prevention protocols and fostering collaboration among stakeholders.

This study's results have informed the following proposed recommendations:

- Mandate multi-factor authentication: Require consistent multi-factor authentication implementation for SIM swaps and financial transactions.

- National biometric database for mobile registration: Create a central biometric database to verify users before SIM swaps, strengthening identity verification.
- Real-time monitoring requirements: Enforce real-time monitoring and reporting of suspicious activity to regulatory authorities.
- Compliance penalties: Impose penalties for non-compliance to incentivise robust security measures.
- Cross-sector data sharing: Mandate secure data sharing among telecoms, banks, and government agencies to facilitate comprehensive fraud prevention.
- National and regional fraud task forces: Establish multi-sector task forces to enhance response times and information sharing.

7.6 Recommendations for future studies

Building on the limitations and challenges identified in this study, several directions are proposed for future research to strengthen the evidence base and enhance the responsible, context-specific application of AI in SIM swap fraud detection, particularly in the context of South Africa's digital landscape.

First, future studies should broaden the scope of literature reviewed to address publication bias and gaps in grey literature inclusion. While PRISMA guidelines were followed, the tendency for journals to publish studies with positive outcomes may have inflated perceptions of AI effectiveness. Researchers are encouraged to expand their search strategies to include regulatory filings, industry white papers, pre-print repositories, and conference abstracts. Additionally, applying capture–recapture techniques can help estimate the proportion of potentially "missing" studies, allowing for a more balanced synthesis of both successful and less favourable implementations of AI-based fraud detection.

To address heterogeneity across existing studies future work should adopt formal meta-analytic techniques. Using random-effects or meta-regression models that

incorporate contextual variables would allow researchers to identify how AI performance varies across different environments. Such approaches would improve the generalisability of findings to emerging market contexts.

Regarding the limitations associated with thematic analysis, to further mitigate bias future research should continue to use the applied hybrid approaches that combine human coding with automated or AI-assisted coding pipelines which can offer triangulated insights and help distinguish between human subjectivity and algorithmic bias.

Given the limited generalisability of in-depth, context-specific qualitative findings, future studies should incorporate multiple comparative case studies across different regions in the Global South. For example, a comparative analysis involving operators in South Africa, Kenya, and Nigeria could illuminate both universal success factors and context-specific challenges. Such research would enhance the transferability and practical utility of AI-based fraud prevention strategies.

Finally,future studies should incorporate mixed-methods approaches to assess how factors such as user interface design, regulatory readiness, and trust affect adoption and effectiveness. Field experiments and stakeholder interviews can provide valuable insights into behavioural and institutional barriers that may hinder successful deployment.

7.7 Implications for the South African market

By adopting these recommendations, South Africa’s telecommunications sector can develop a multi-faceted strategy to curb SIM swap fraud effectively. Leveraging AI, enhancing public awareness, reinforcing regulatory frameworks, and addressing privacy concerns can collectively reduce the occurrence of SIM swap fraud and protect consumers during the 2G/3G network shutdowns and beyond. These recommendations provide a blueprint for building a resilient

telecom infrastructure that can adapt to the evolving fraud landscape and safeguard users across all segments of society.

As South Africa increasingly relies on AI-driven solutions for fraud prevention, it is critical to address potential ethical issues, including data privacy and algorithmic bias. Policies ensuring that AI models are transparent, explainable, and periodically reviewed can help mitigate unintended harms, particularly for vulnerable populations. Implementing safeguards that prevent AI-driven tools from discriminating against specific user groups is essential to build trust and promote equitable access to secure telecom services.

The findings of this research clearly highlight AI's potential as a capable guardian in the fight against SIM swap fraud. However, this promise must be viewed critically. AI systems, while technically robust, are not neutral actors (Bertolini, 2022; Xavier, 2025). Their deployment is shaped by organisational priorities, regulatory frameworks, and data limitations, all of which may compromise fairness, transparency, or effectiveness (Varsha, 2023). Moreover, fraud is a moving target; as AI tools evolve, so too will the tactics of offenders. This dynamic brings in the need for continuous adaptation and oversight, lest today's solutions become tomorrow's vulnerabilities.

7.8 Conclusions

This study has demonstrated that mitigating SIM swap fraud requires an integrated approach, combining regulatory frameworks, technological defences, user education, and inter-sectoral collaboration. Regulatory recommendations target standardised verification processes, real-time monitoring, and robust compliance, while AI-based recommendations focus on centralised monitoring, behavioural biometrics, and predictive analytics. Together, these strategies represent a capable guardianship approach, as defined by the RAT, equipping stakeholders with the tools necessary to counter SIM swap fraud.

By embracing AI and fortifying regulatory structures, stakeholders can create a resilient and equitable defence system that adapts to an evolving fraud landscape, ultimately fostering a secure digital environment for all users. The implementation of AI is critical in establishing a proactive defence against fraud. A multi-layered AI approach incorporating centralised monitoring, machine learning, behavioural biometrics, and blockchain can enhance detection accuracy and response times. Advanced methods, like federated learning and edge computing, could make fraud prevention systems more adaptive and transparent. By embracing AI solutions and strengthening regulatory frameworks, stakeholders can build a resilient and user-centric approach to fraud prevention that adapts to the rapidly evolving digital landscape, providing equitable protection across all regions and demographics.

REFERENCES

Abbott, D., Matkovsky, I., & Elder, J. (2002). An evaluation of high-end data mining tools for fraud detection. *SMC'98 Conference Proceedings. 1998 IEEE International Conference on Systems, Man, and Cybernetics (Cat. No.98CH36218)*, *3*, 2836–2841. https://doi.org/10.1109/icsmc.1998.725092

Abuhamoud, N., Alsadi, I., & Ali, S. (2021). Detecting SIMBox fraud using CDR files and Neo4J technology. *2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA*, *17*, 259–263. https://doi.org/10.1109/mi-sta52233.2021.9464510

ACMA. (2022). Reducing the impact of unauthorised high-risk customer transactions. In *Australian Communications and Media Authority - Regulation Impact Statement*. https://www.acma.gov.au/sites/default/files/2022-04/RIS%20-%20Reducing%20the%20impact%20of%20unauthorised%20high-risk%20customer%20transactions.pdf

Adekunle, A., & Jaiyeola, H. (2025). The emerging threat of AI powered fraud. In *PricewaterhouseCoopers Incorporated*. https://www.pwc.com/ng/en/assets/pdf/the-emerging-threat-of-ai-powered-fraud%20.pdf

Adedoyin, A. (2018). *Predicting fraud in mobile money transfer* (Doctoral dissertation, University of Brighton). https://cris.brighton.ac.uk/ws/portalfiles/portal/6145772/13831870_PhD_Thesis.pdf

Adewumi, A. O., & Akinyelu, A. A. (2016). A survey of machine-learning and nature-inspired based credit card fraud detection techniques. *International Journal of Systems Assurance Engineering and Management*, *8*(S2), 937–953. https://doi.org/10.1007/s13198-016-0551-y

Adjaoute, A. (2013). *U.S. Patent No. 8,458,069*. Washington, DC: U.S. Patent and Trademark Office. https://patentimages.storage.googleapis.com/42/dc/18/a3ccf98d21c023/US8458069.pdf

African Wireless Communications. (2024, February 9). *South Africa extends 2G/3G shutdown to end-2027*. AWC. https://www.africanwirelesscomms.com/news-details?itemid=7249&post=south-africa-extends-2g3g-shutdown-to-end-2027-729387

Agrawal, J., Patel, R., P. Mor, P. Dubey, & J.M. Keller. (2015). Evolution of mobile communication network: From 1G to 4G. *International Journal of Multidisciplinary and Current Research*, *3*. http://ijmcr.com/wp-content/uploads/2015/11/Paper11100-11031.pdf

Akbar, S., Chandulal, J. A., Rao, K. N., & Kumar, G. S. (2012, December). Improving network security using machine learning techniques. In *2012 IEEE International Conference on Computational Intelligence and Computing Research* (pp. 1-5). IEEE. https://doi.org/10.1109/ICCIC.2012.6510197

Akers, R. (2017). *Social learning and social structure: A general theory of crime and deviance*. Routledge. https://doi.org/10.4324/9781315129587

Akhtar, S. (2009). 2G-5G networks: Evolution of technologies, standards, and deployment. *Encyclopedia of Multimedia Technology and Networking*, 522-532. https://doi.org/10.4018/978-1-60566-014-1.ch070

Al-Humaigani, M., Dunn, D. B., & Brown, D. (2009). Security transition roadmap to 4G and future generations wireless networks. In *Southeastern Symposium on System Theory at the University of Tennessee Space Institute* (2008th ed., pp. 94–97). https://doi.org/10.1109/ssst.2009.4806852

Ali, N. T., Hasan, S. J., Ghandour, A., & Al-Hchimy, Z. S. (2024). Improving credit card fraud detection using machine learning and GAN technology. *BIO Web of Conferences*, *97*, 00076. https://doi.org/10.1051/bioconf/20249700076

Ammayappan, K. (2013). Seamless interoperation of LTE-UMTS-GSM requires flawless UMTS and GSM. In *International Conference on Advanced Computing, Networking and Security* (2nd ed.). https://doi.org/10.1109/adcons.2013.53

Asmare, F. M., & Ayalew, L. G. (2023). Security challenges in the transition to 4G mobile systems in developing countries. *Cogent Engineering*, *10*(1), 2166214. https://www.tandfonline.com/doi/pdf/10.1080/23311916.2023.2166214

Assey v. Vodacom Tanzania, Civil case no. 8 (2023). Legal Judgement - High Court of the Republic of Tanzania. https://tanzlii.org/akn/tz/judgment/tzhc/2023/22054/eng@2023-10-20/source

Assolini, F. (2019). SIM swap fraud: a new wave of attacks targeting financial services and online services in Africa. In *M2 Presswire*. Proquest. https://www.proquest.com/telecomms/wire-feeds/sim-swap-fraud-new-wave-attackstargeting/ docview/2220115094/sem-2?accountid=15083

Bagga, S., Goyal, A., Gupta, N., & Goyal, A. (2020). Credit Card Fraud Detection using Pipeling and Ensemble Learning. *Procedia Computer Science*, *173*, 104–112. https://doi.org/10.1016/j.procs.2020.06.014

Bandi, A., & Yalamarthi, S. (2022). Towards artificial intelligence empowered security and privacy issues in 6G communications. *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. https://doi.org/10.1109/icscds53736.2022.9760857

Bao, Y., Hilary, G., & Ke, B. (2022). Artificial intelligence and fraud detection. *Innovative Technology at the Interface of Finance and Operations.* Volume I, 223-247. https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3738618

Bertolini, A. (2022). Artificial Intelligence does not exist! Defying the technology-neutrality narrative in the regulation of civili liability for advanced technologies. *Europa e diritto privato*, (2), 369-420. https://hdl.handle.net/11382/552651

Bhavana, S., Miriam, D. D. H., & Robin, C. R. (2024). Understanding the implications of SIM card swap fraud in India: a comprehensive study. *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, *21*, 1–8. https://doi.org/10.1109/ic3iot60841.2024.10550217

Barocas, S., Hardt, M., & Narayanan, A. (2023). *Fairness and machine learning: Limitations and opportunities*. MIT. https://fairmlbook.org/pdf/fairmlbook.pdf

Becker, R. A., Volinsky, C., & Wilks, A. R. (2011). Fraud detection in telecommunications: History and lessons learned. *Quality Engineering*, *56*(1), 143–144. https://dialnet.unirioja.es/servlet/articulo?codigo=3965981

Behrad, S., Bertin, E., & Crespi, N. (2018, February). Securing authentication for mobile networks, a survey on 4G issues and 5G answers. In *2018 21st*

conference on innovation in clouds, internet and networks and workshops (ICIN) (pp. 1-8). IEEE. https://ieeexplore.ieee.org/iel7/8392644/8401570/08401619.pdf

Bello, O. A., Folorunso, A., Onwuchekwa, J., Ejiofor, O. E., Budale, F. Z., & Egwuonwu, M. N. (2023). Analysing the Impact of advanced analytics on Fraud Detection: A Machine Learning perspective. *European Journal of Computer Science and Information Technology*, *11*(6). https://tudr.org/id/eprint/3105/1/Analysing%20the%20Impact%20of%20Advanced%20Analytics.pdf

BEREC Europa. (2023). Report on practices and challenges of the phasing out of 2G and 3G. In *BEREC Europa*. https://www.berec.europa.eu/system/files/2023-06/BoR%20%2823%29%20111%20BEREC%20Draft%20Report%20on%20practices%20and%20challenges%20of%20the%20phasing%20out%20of%202G%20and%203G.pdf

Bhargavi, K., & Shivani, B. M. (2024). Detection of fraudulent phone calls detection in mobile applications. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *15*(2), 1-5. https://doi.org/10.61841/turcomat.v15i2.14644

Bhavana, S. U., Miriam, D. D. H., & Robin, C. R. (2024, April). Understanding the implications of sim card swap fraud in India: A comprehensive study. In *2024 International Conference on Communication, Computing and Internet of Things (IC3IoT)* (pp. 1-8). IEEE. https://doi.org/10.1109/ic3iot60841.2024.10550217

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602–613. https://doi.org/10.1016/j.dss.2010.08.008

Bijani, S., & Kazemitabar, M. (2008). HIDMN: a Host and Network-Based Intrusion Detection for mobile networks. In *2008 International Conference on Computer and Electrical Engineering* (Vols. 204–208, pp. 204–208). https://doi.org/10.1109/iccee.2008.183

Booth, A., James, M. S., Clowes, M., & Sutton, A. (2021). *Systematic approaches to a successful literature review*. Los Angeles. http://lib.ugent.be/en/catalog/rug01:002101878/items/000010929920/

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Buzzard, J. (2023). 2023 Identity Fraud Study: The Butterfly Effect. In *Javelin Strategy*. https://www.javelinstrategy.com/research/2023-identity-fraud-study-butterfly-effect

Cardoso, N. A. D. M. L. (2021). *User behavior analytics in the contact center: Insider threat assessment and fraud detection* (Master's thesis). https://estudogeral.uc.pt/bitstream/10316/96092/1/Tese_UEBA_2.1.pdf

Celebi, M. E., & Aydin, K. (Eds.). (2016). Unsupervised learning algorithms. In *Springer eBooks* (Vol. 9, p. 103). https://doi.org/10.1007/978-3-319-24211-8

Cheng, D., Wang, X., Zhang, Y., & Zhang, L. (2020). Graph neural network for fraud detection via spatial-temporal attention. *IEEE Transactions on Knowledge and Data Engineering*, *34*(8), 3800-3813. https://doi.org/10.1109/tkde.2020.3025588

Chigbu, U. E., Atiku, S. O., & Du Plessis, C. C. (2023). The science of literature reviews: Searching, identifying, selecting, and synthesising. *Publications*, *11*(1), 2. https://doi.org/10.3390/publications11010002

Chitre, P., & Sriramulu, S. (2022). Analysis and evaluation of security and privacy threats in high speed communication network. In *Lecture notes in networks and systems* (pp. 519–531). https://doi.org/10.1007/978-981-19-2535-1_39

Chitroub, S., Zidouni, N., Aouadia, H., Blaid, D., & Laouar, R. (2018). SIM card of the next-generation wireless networks: Security, potential vulnerabilities and solutions. *2018 2nd European Conference on Electrical Engineering and Computer Science (EECS) (pp. 502-509)*. https://doi.org/10.1109/eecs.2018.00098

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608. https://doi.org/10.2307/2094589

Cooper, M. (2024, July 12). SIM swap fraud in South Africa 2024: Essential information for enterprises. *Sekura.id*. https://sekura.id/SIM-swap-fraud-in-south-africa-2024/

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: choosing among five approaches*. Sage Publications.

D'Alessandro, S., Johnson, L., Gray, D., & Carter, L. (2014). Consumer satisfaction versus churn in the case of upgrades of 3G to 4G cell networks. *Marketing Letters*, *26*(4), 489–500. https://doi.org/10.1007/s11002-014-9284-3

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

Dayyabu, Y. Y., Arumugam, D., & Balasingam, S. (2023). The application of artificial intelligence techniques in credit card fraud detection: A quantitative study. *E3S Web of Conferences*, *389*, 07023. https://doi.org/10.1051/e3sconf/202338907023

Department of Communications and Digital Technologies [Alfred Mashishi] (Director). (2023). National Artificial Intelligence Strategy of South Africa: Adoption of AI by government. In *Department of Communications and Digital Technologies*. https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf

Dixon-Woods, M., Cavers, D., Agarwal, S., Annandale, E., Arthur, A., Harvey, J., ... & Sutton, A. J. (2006). Conducting a critical interpretive synthesis of the literature on access to healthcare by vulnerable groups. *BMC Medical Research Methodology*, *6*, 1-13. https://doi.org/10.1186/1471-2288-6-35

Ekeh, G. E., Afolabi, Y. I., Uche-Nwachi, E. O., & Eze-Udu, E. (2021). Awareness of BVN, SIM swap and Clone Frauds: Methods and controls. *African Journals Online*, *17*(2), 200–206. https://www.ajol.info/index.php/swj/article/download/231307/218470

Ekwonwune, E. N., Chukwuebuka, U. C., Duroha, A. E., & Duru, A. N. (2022). Analysis of Global System for Mobile Communication (GSM) Subscription Fraud Detection System. *International Journal of Communications Network and System Sciences*, *15*(10), 167–180. https://doi.org/10.4236/ijcns.2022.1510012

Ettiane, R., Elkouch, R., & Chaoub, A. (2016). Protection Mechanisms for signaling DOS attacks on 3G mobile Networks: Comparative study and Future Perspectives. In *IEEE International colloquium on information science and*

technology (CiSt) (4th ed., Vol. 1, pp. 860–866). https://doi.org/10.1109/cist.2016.7805009

Faircloth, C., Hartzell, G., Callahan, N., & Bhunia, S. (2022). A study on brute force attack on T-Mobile leading to SIM-Hijacking and Identity-Theft. *2022 IEEE World AI IoT Congress (AIIoT)*, 501–507. https://doi.org/10.1109/aiiot54504.2022.9817175

Fang, P., & Fang, Q. (2024). Research on anti-telecom fraud based on artificial intelligence and edge computing. In *IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA)* (3rd ed.). https://doi.org/10.1109/eebda60612.2024.10486050

Ganesan, M., Deepika, C., Harievashini, B., Krithikha, A. S., & Lokhratchana, B. (2020). A survey on chatbots using artificial intelligence. In *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)* (pp. 1-5). IEEE. https://doi.org/10.1109/icscan49426.2020.9262366

Gareth, J., Daniela, W., Trevor, H., & Robert, T. (2013). *An Introduction to statistical learning: With applications.* In R. Springer. https://link.springer.com/content/pdf/10.1007/978-1-0716-1418-1.pdf

Global Cybersecurity Index (GSI) 2020. (2021). International Telecommunication Union https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. In *MIT Press eBooks*. https://dl.acm.org/citation.cfm?id=3086952

Grassi, P., Garcia, M., & Fenton, J. (2017). *Digital identity guidelines (Revised draft)*. https://csrc.nist.gov/publications/detail/sp/800-63/3/archive/2017-03-31

GSMA. (2021). *The Mobile Economy 2021*. GSMA Intelligence. https://data.gsmaintelligence.com/research/research/research-2021/the-mobile-economy-2021

GSMA. (2023). *The mobile economy Sub-Saharan Africa 2023*. GSMA Intelligence. https://event-assets.gsma.com/pdf/20231017-GSMA-Mobile-Economy-Sub-Saharan-Africa-report.pdf

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (pp.

105–117). Sage Publications, Inc*. https://psycnet.apa.org/record/1994-98625-005*

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. Wiley. https://openlibrary.org/books/OL26963465M/Social_engineering

Haidine, A., Aqqal, A., & Ouahmane, H. (2016). Modeling the migration of mobile networks towards 4G and beyond. In *Lecture notes in electrical engineering* (pp. 355–363). https://doi.org/10.1007/978-3-319-30301-7_37

Hallman, R. A. (n.d.) SIM swapping attacks for digital identity theft: A threat to financial services and beyond. *Researchgate*. https://www.researchgate.net/profile/Roger-Hallman/publication/376612643_SIM_Swapping_Attacks_for_Digital_Identity_Theft_A_threat_to_financial_services_and_beyond/links/658091b20bb2c7472bf3dd84/SIM-Swapping-Attacks-for-Digital-Identity-Theft-A-threat-to-financial-services-and-beyond.pdf

Harinath, D. (2023). SIM - swap technique - a legitimate customer request. International Journal of Science and Research (IJSR), 12(3), 392–396. https://doi.org/10.21275/sr23308172146

Higgins, J. P. T., & Green, S. (2008). Cochrane handbook for systematic reviews of interventions. In *Wiley eBooks*. https://doi.org/10.1002/9780470712184

Hilas, C. S. (2009). Designing an expert system for fraud detection in private telecommunications networks. *Expert Systems With Applications*, *36*(9), 11559–11569. https://doi.org/10.1016/j.eswa.2009.03.031

Holtrup, G., Lacube, W., David, D. P., Mermoud, A., Bovet, G., & Lenders, V. (2021). 5G system security analysis. *arXiv preprint* arXiv:2108.08700.

Hosseini, M., Gordijn, B., Wafford, Q. E., & Holmes, K. L. (2023). A systematic scoping review of the ethics of contributor role ontologies and taxonomies. *Accountability in Research*, *31*(6), 678-705. https://www.tandfonline.com/doi/pdf/10.1080/08989621.2022.2161049

Ighneiwa, I., & Mohamed, H. (2017). Bypass fraud detection: Artificial intelligence approach. *arXiv Preprint* https://arxiv.org/pdf/1711.04627

iiDENTIFii. (2024, May 20). Why SA’s networks need to defend against the devastating effect of SIM swap fraud. *ITWeb*. https://www.itweb.co.za/article/why-sas-

networks-need-to-defend-against-the-devastating-effect-of-SIM-swap-fraud/mQwkoM6YRNX73r9A

Independent Communications Authority of South Africa. (2023). *State of the ICT sector in South Africa - 2023 Report.* Independent Communications Authority of South Africa. https://www.icasa.org.za/legislation-and-regulations/state-of-ict-sector-report-2023-report

Internet Organised Crime Threat Assessment (IOCTA) | *Europol*. (2020). Europol. https://www.europol.europa.eu/iocta-report

Jackson, D. (2020). New SIM-swap hacks highlight carriers' wobbly security. In *Urgent Communications*. US Federal Government. https://urgentcomm.com/

Jain, A. K., & Gupta, B. (2021). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527–565. https://doi.org/10.1080/17517575.2021.1896786

Jentzsch, N. (2012). Implications of mandatory registration of mobile phone users in Africa. *Telecommunications Policy*, *36*(8), 608–620. https://doi.org/10.1016/j.telpol.2012.04.002

Jimenez, N., San-Martin, S., & Azuela, J. I. (2016). Trust and satisfaction: the keys to client loyalty in mobile commerce. *Academia Revista Latinoamericana De Administración*, *29*(4), 486–510. https://doi.org/10.1108/arla-12-2014-0213

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389-399. https://arxiv.org/pdf/1906.11668

Jordaan, L., & Von Solms, B. (2011). A Biometrics-based solution to combat SIM swap fraud. In *Lecture Notes in Computer Science* (pp. 70–87). https://doi.org/10.1007/978-3-642-19228-9_7

Jover, R. P. (2019). The current state of affairs in 5G security and the main remaining security challenges. *arXiv preprint arXiv:1904.08394*.

Jurafsky, D., & Martin, J. H. (2000). Speech and language processing: An introduction to natural language processing, computational linguistics, and speech recognition. In *Prentice Hall eBooks*. https://nats-www.informatik.uni-hamburg.de/pub/CDG/JurafskyMartin00Comments/JurafskyMartin00-Review.pdf

Kashir, M., & Bashir, S. (2019). Machine learning techniques for SIM box fraud detection. In *International Conference on Communication Technologies*. https://doi.org/10.1109/comtech.2019.8737828

Kazembe, M. (2023). Eliminating use of non-traceable identity cards to reduce cyber security incidents: focus on Malawi. *Authorea Preprints*. https://www.techrxiv.org/doi/pdf/10.36227/techrxiv.21859197.v1

Khogali, H. O., & Mekid, S. (2023). The blended future of automation and AI: Examining some long-term societal and ethical impact features. *Technology in Society*, *73*, 102232. https://doi.org/10.1016/j.techsoc.2023.102232

Kibuuka, A. (2024, April 24). *DFS Security recommendations for regulators and providers* [Slide show; Presentation slides]. Regional Digital Financial Services Security Clinic for Asia Pacific Region, Seoul, Korea, Republic of. ITU. https://www.itu.int/en/ITU-T/webinars/dfs/sc/20240424/Documents/Arnold%20Kibuuka%20session%205.pdf

Kim, M., Suh, J., & Kwon, H. (2022). A study of the emerging trends in SIM swapping crime and effective countermeasures. In *IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD)* (pp. 240–245). https://doi.org/10.1109/bcd54882.2022.9900510

Kotak, J., Habler, E., Brodt, O., Shabtai, A., & Elovici, Y. (2023). Information Security Threats and Working from Home Culture: Taxonomy, Risk Assessment and Solutions. *Sensors*, *23*(8), 4018. https://doi.org/10.3390/s23084018

Koul, S., Raj, Y., & Koul, S. (2020). Analyzing Cyber Trends in Online Financial Frauds using digital Forensics Techniques. *International Journal of Innovative Technology and Exploring Engineering*, *9*(9), 446–451. https://doi.org/10.35940/ijitee.i7185.079920

Krishnan, P., Jain, K., Poojara, S. R., Srirama, S. N., Pandey, T., & Buyya, R. (2024). eSIM and blockchain integrated secure zero-touch provisioning for autonomous cellular-IoTs in 5G networks. *Computer Communications*, *216*, 324–345. https://doi.org/10.1016/j.comcom.2023.12.023

Kumar, V. (2024). Smishing, Phishing and SIM Swap: Seminar uncovers evolving Cyber fraud landscape. In *Asia News Monitor*. Proquest. https://www.proquest.com/newspapers/india-smishing-phishing-sim-swap-seminaruncovers/ docview/3081784067/se-2?accountid=15083

Lane, A. (2020). White Paper: Preparing for the phase out of 2G/3G cellular. In *Instrumentation*. Westermo. https://www.instrumentation.co.za/papers/J6163.pdf?a

Lasierra, O., Garcia-Aviles, G., Municio, E., Skarmeta, A., & Costa-Pérez, X. (2023). European 5G security in the wild: Reality versus expectations. In *16th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 13–18). https://doi.org/10.1145/3558482.3581776

Lawler, J., & Waldner, D. (2023). Interpretivism versus positivism in an age of causal inference. *Oxford handbook of philosophy of political Science*, 221-242. http://dx.doi.org/10.1093/oxfordhb/9780197519806.013.11

Lee, K., Kaiser, B., Mayer, J. R., & Narayanan, A. (2020). An empirical study of wireless carrier authentication for SIM swaps. *Symposium on Usable Privacy and Security*, 61–79. https://www.usenix.org/system/files/soups2020-lee.pdf

LexisNexis Risk Solutions. (2024). AI Exploit and Threat Landscape Cybersecurity Guide: Mitigate artificial intelligence and generative AI cyber threats and identity fraud risk [eBook]. In *LexisNexis Risk Solutions*. https://risk.lexisnexis.com/government/government-fraud-detection-and-prevention

Lin, K., Wu, Y., Sun, I. Y., & Qu, J. (2023). Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory. *Criminology & Criminal Justice*, 174889582211461. https://doi.org/10.1177/17488958221146144

Lincoln, Y. S., Guba, E. G., & Pilotta, J. J. (1985). Naturalistic inquiry. *International Journal of Intercultural Relations*, *9*(4), 438–439. https://doi.org/10.1016/0147-1767(85)90062-8

Lokanan, M. E. (2023). Predicting mobile money transaction fraud using machine learning algorithms. *Applied AI Letters*, *4*(2). https://doi.org/10.1002/ail2.85

Long, G., Tan, Y., Jiang, J., & Zhang, C. (2020). Federated learning for open banking. In *Lecture notes in computer science* (pp. 240–254). https://doi.org/10.1007/978-3-030-63076-8_17

Malhotra, S., Arora, G., & Bathla, R. (2023). Detection and analysis of fraud phone calls using artificial intelligence. In *2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies*

(REEDCON) (pp. 592–595). https://doi.org/10.1109/reedcon57544.2023.10150631

Manhide, T. C., & Nkomo, D. J. (2023). Determination of factors influencing the upsurge of electronic banking frauds in Zimbabwe. *Journal of Research and Innovation for Sustainable Society*, *5*(2), 189–199. https://doi.org/10.33727/jriss.2023.2.23:189-199

Malek, W. W. Z., Mayes, K., & Markantonakis, K. (2008). Fraud detection and prevention in smart card-based environments using artificial intelligence. In *Lecture notes in computer science* (pp. 118–132). https://doi.org/10.1007/978-3-540-85893-5_9

Marakalala, M. C. (2023). Forensic Intelligence: The Effectiveness of the Biometric-based Solution to Combat Mobile Fraud. *OIDA International Journal of Sustainable Development*, *16*(05), 19-30. https://oidaijsd.com/wp-content/uploads/2023/12/16-05-2-01-SPA-23.pdf

Mason, P. (2005). Visual data in applied qualitative research: lessons from experience. *Qualitative Research*, *5*(3), 325–346. https://doi.org/10.1177/1468794105054458

Masrub, A., & Alahemar, M. (2020). SIM Boxing problem: ALMADAR ALJADID Case Study. In *International Conference on Next Generation Mobile Applications, Services, and Technologies* (2nd ed., Vol. 4, pp. 1–5). https://doi.org/10.1109/icee49691.2020.9249872

Mattord, H., Kotwica, K., Whitman, M., & Battaglia, E. (2023). Organizational perspectives on converged security operations. *Information and Computer Security*, *32*(2), 218–235. https://doi.org/10.1108/ics-03-2023-0029

Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative research: A guide to design and implementation*. John Wiley & Sons.

McPhail, L. L., & McPhail, J. E. (2021). Machine learning implications for banking regulation. In *Routledge eBooks* (pp. 395–415). https://doi.org/10.4324/9780429292903-29

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 205395171667967. https://doi.org/10.1177/2053951716679679

Malhotra, S., Arora, G., & Bathla, R. (2023, May). Detection and analysis of fraud phone calls using artificial intelligence. In *2023 International Conference on*

Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON) (pp. 592-595). IEEE. https://ieeexplore.ieee.org/iel7/10150432/10150438/10150631.pdf

MTN Group. (2022). *MTN Group Integrated Annual Report 2022*. MTN Group. https://www.mtn.com/wp-content/uploads/2023/04/MTN-Group-FY-22-Integrated-Annual-Report.pdf

Mtuze, S. S. K., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*(3), 299–323. https://doi.org/10.1365/s43439-023-00089-8

Murugalakshmi, S., Doreen, H. M. D., & Rene, R. C. R. (2023). Advancements in mobile security: A comprehensive study of SIM card swapping and cloning - trends, challenges and innovative solutions. *I-manager S Journal on Mobile Applications and Technologies*, *10*(1), 23. https://doi.org/10.26634/jmt.10.1.20103

Nahar, L., Amir, I., & Shabnam, S. (2015). A comprehensive survey of fraud detection techniques. *International Journal of Applied Information Systems*, *10*(2), 26–32. https://doi.org/10.5120/ijais2015451471

Natarajan, S., & Ashara, P. (2024). Whitepaper: Payment Scams - AI to Rescue. In *Quinte Financial Technologies*. https://quinteft.com/wp-content/uploads/2024/07/Qunite-Scams-AI-to-Rescue-Whitepaper.pdf

Nagin, D. S. (1998). Criminal deterrence research at the outset of the twenty-first century. *Crime and Justice*, *23*, 1–42. https://doi.org/10.1086/449268

Nama, F. A., & Obaid, A. J. (2024). Financial fraud identification using deep learning techniques. *Al-Salam Journal for Engineering and Technology*, *3*(1), 141–147. https://doi.org/10.55145/ajest.2024.03.01.012

Ngai, E., Hu, Y., Wong, Y., Chen, Y., & Sun, X. (2010). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Nguyen, M., To, L. N. H., & Viet, H. N. (2022). A model for detecting accounting frauds by using machine learning. *Proceedings of the . . . Annual Hawaii International Conference on System Sciences/Proceedings of the Annual Hawaii*

International Conference on System Sciences. https://doi.org/10.24251/hicss.2022.193

Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, *9*, 163965-163986. https://ieeexplore.ieee.org/iel7/6287639/6514899/09642993.pdf

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1). https://doi.org/10.1177/1609406917733847

Oh, B., Ahn, J., Bae, S., Son, M., Lee, Y., Kang, M. S., & Kim, Y. (2023). Preventing SIM box fraud using device model fingerprinting. In *Network and Distributed System Security (NDSS) Symposium*. https://doi.org/10.14722/ndss.2023.24416

Olugbenga, A. A. (2020). *Fraudulent detection model using machine learning techniques using unstructured supplementary service data* [Masters dissertation, Universiti Teknologi Malaysia]. http://eprints.utm.my/96376/1/AyoAkinjeMSC2021.pdf.pdf

Omotubora, A. (2020). Crafting the phishing offence in the cybercrime act: A drafter's inelegance that is the court's nightmare. *NIALS International Journal of Legislative Drafting*, *3*(3), 139-180. https://journal.nials.edu.ng/index.php/nijld/article/download/58/58

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., . . . Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Parmar, J. D., & Patel, J. T. (2017). Anomaly detection in data mining: a review. *International Journal of Advanced Research in Computer Science and Software Engineering*, *7*(4), 32-40. http://www.ijarcsse.com/ (ISSN: 2277 128X)

Patel, K. (2023). Credit card analytics: a review of fraud detection and risk assessment techniques. *International Journal of Computer Trends and Technology*, 71(10), 69-79. https://doi.org/10.14445/22312803/IJCTT-V71I10P109

Pramod, D. (2021). Robotic process automation for industry: adoption status, benefits, challenges and research agenda. *Benchmarking an International Journal*, *29*(5), 1562–1586. https://doi.org/10.1108/bij-01-2021-0033

Pratima, H. (2023). Spam is a tricky problem to solve. In *Voice & Data*. Voice & Data, New Delhi. https://www.proquest.com/trade-journals/spam-is-tricky-problem-solve/docview/2829334037/se-2

Question to the Minister of Communications and Digital Technologies - NW442 | PMG. (n.d.). https://pmg.org.za/committee-question/25047/

Rana, P., & Baria, J. (2015). A survey on Fraud Detection Techniques in e-commerce. *International Journal of Computer Applications*, *113*(14), 5–7. https://doi.org/10.5120/19892-1898

Razak, S. A., Nazari, N. H. M., & Al-Dhaqm, A. (2020). Data anonymization using pseudonym system to preserve data privacy. *IEEE Access*, *8*, 43256–43264. https://doi.org/10.1109/access.2020.2977117

Regulatory analysis of Over-The-Air provisioning of SIM profiles including its impact on number portability. (2018). In *Electronic Communications Committee*. Electronic Communications Committee. https://docdb.cept.org/download/1320

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rosa, L. G. (2024). *Modeling the SIM swap ceremony - integrating human behavior and formal analysis* [Bachelors dissertation, Universidade Federal de Santa Catarina]. https://repositorio.ufsc.br/bitstream/handle/123456789/255696/TCC2___Larissa%20%283%29%20%281%29.pdf?sequence=1

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach*, *4th US ed.* Alternative Investment Management Association. https://aima.cs.berkeley.edu/

Regulation governing the SIM card registration in Rwanda. (2024). In *Rwanda Utilities Regulation Authority*. Rwanda Utilities Regulation Authority. https://www.rura.rw/fileadmin/Documents/ICT/Laws/Amended_Draft__Regulation_governing_SIM_cards_registration_for_22_April_2024.pdf

Saadia, B., Tawfiq, K., & Ali, A. (2021). The use of artificial intelligence in the banking sector, referring to the case of the United Arab Emirates. *Journal of Economics*

and Sustainable Development, *7*(1), 279–291. https://www.asjp.cerist.dz/en/downArticle/598/7/1/243714

SABRIC. (2022). *Annual Crime Stats 2022*. SABRIC. https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2022/

Salaudeen, L. G., Yauri, A. R., Muhammad, G., Suru, H. U., Al-Maru'f, A. O., Gabi, D., Argungun, S. M., & Aliyu, M. S. (2022). A plethoric literature survey on SIMBox fraud detection in telecommunication industry. *Direct Research Journal of Engineering and Information Technology*, *9*(1), 16. https://doi.org/10.26765/drjeit14035036

Sallehuddin, R., Ibrahim, S., Zain, A. M., & Elmi, A. H. (2014). Classification of SIM box fraud detection using support vector machine and artificial neural network. *International Journal of Innovative Computing*, *4*(2). https://doi.org/10.11113/ijic.v4n2.95

Sanni, M. L., Akinyemi, B. O., Olalere, D. A., Olajubu, E. A., & Aderounmu, G. A. (2023). A predictive cyber threat model for mobile money services. *Annals of Emerging Technologies in Computing*, *7*(1), 40–60. https://doi.org/10.33166/aetic.2023.01.004

Shapiro, R. J., & Hassett, K. A. (2012). The employment effects of Advances in internet and wireless technology: Evaluating the transitions from 2G to 3G and from 3G to 4G. In *New Policy Institute and NDN*. SONECON. https://www.sonecon.com/docs/studies/Wireless_Technology_and_Jobs-Shapiro_Hassett-January_2012.pdf

Sharma, N. P. (2024). Algorithms and strategies for fraud prevention on online platforms. *World Journal of Advanced Research and Reviews*, *23*(2), 2220–2225. https://doi.org/10.30574/wjarr.2024.23.2.2462

Singh, S., & Kumar, S. (2020). The times of cyber attacks. *Acta Technica Corviniensis-Bulletin of Engineering*, *13*(3), 133-137. http://acta.fih.upt.ro/pdf/2020-3/ACTA-2020-3-25.pdf

Singh, T. (2023). A novel secure identity management for 5G ultra-dense communication networks. In *2023 4th IEEE Global Conference for Advancement in Technology (GCAT)* (Vol. 15, pp. 1–6). https://doi.org/10.1109/gcat59970.2023.10353539

Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021). AI and 6G security: opportunities and challenges. In *2021 Joint European Conference on*

Networks and Communications & 6G Summit (EuCNC/6G Summit). https://doi.org/10.1109/eucnc/6gsummit51104.2021.9482503

Sood, P., Sharma, C., Nijjer, S., & Sakhuja, S. (2023). Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing. *International Journal of Systems Assurance Engineering and Management*, *14*(6), 2120–2135. https://doi.org/10.1007/s13198-023-02043-7

Statista. (2024, March 8). *Number of mobile connections in South Africa 2017-2023*. https://www.statista.com/statistics/1347388/number-of-mobile-connections-south-africa/

Stephens, C. (2020). Why are SMS codes still the global ID solution? *Biometric Technology Today*, *2020*(8), 8–10. https://doi.org/10.1016/s0969-4765(20)30110-7

Strauss, A. L., & Corbin, J. M. (1998). Basics of qualitative research : techniques and procedures for developing grounded theory. In *Sage eBooks* (Issue 1). http://lib.tums.ac.ir/site/catalogue/61151

Sule, P., & Joshi, A. (2014). Architectural shift from 4G to 5G wireless mobile networks. *International Journal of Computer Science and Mobile Computing*, *3*(9), 715-721. www.ijcsmc.com (ISSN 2320–088X)

Tambunan, D. A., Suryadi, M., & Hamid, S. (2021). Cyber policing in preventing SIM swap attacks, a new threat to digital economy transactions. *Management Technology and Security International Journal*, *1*, 127–138. https://www.ctrs-stik-mtsij.ac.id/wp-content/uploads/2021/05/cyber-policing-in-preventing-sim-swap-attacks-a-new-threat-to-digital-economy-transactions.pdf

Telecom Regulatory Authority of India. (2023). Draft Telecommunication Mobile Number Portability (Ninth Amendment) Regulations of 2023. In *Telecom Regulatory Authority of India*. https://trai.gov.in/sites/default/files/Regulation_27092023.pdf

Toorani, M., & Beheshti, A. (2008). Solutions to the GSM security weaknesses. In *2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies* (pp. 576-581). IEEE. https://ieeexplore.ieee.org/iel5/4756388/4756389/04756489.pdf

Urbas, G., & Krone, T. (2007). Mobile and wireless technologies: security and risk factors. *Trends and Issues in Crime and Criminal Justice*, *329*, 1. https://apo.org.au/node/8481

Uttley, L., Quintana, D. S., Montgomery, P., Carroll, C., Page, M. J., Falzon, L., ... & Moher, D. (2023). The problems with systematic reviews: a living systematic review. *Journal of Clinical Epidemiology*, *156*, 30-41. https://doi.org/10.1016/j.jclinepi.2023.01.011

Van Looy, A. (2021). A quantitative and qualitative study of the link between business process management and digital innovation. *Information & Management*, *58*(2), 103413. https://doi.org/10.1016/j.im.2020.103413

Varsha, P. S. (2023). How can we manage biases in artificial intelligence systems–A systematic literature review. *International Journal of Information Management Data Insights*, *3*(1), 100165. https://doi.org/10.1016/j.jjimei.2023.100165

Vodacom Group. (2022). *Integrated Annual Report 2022*. Vodacom Group. https://www.vodacom.com/annual-results.php

Voigt, P., & Von Dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). In *Springer eBooks*. https://doi.org/10.1007/978-3-319-57959-7

Wanyonyi, E., & Bird, L. (2021). Constructing crime risks, vulnerabilities and opportunities in Africa's communications infrastructure. In *ENACT Africa*. https://enact-africa.s3.amazonaws.com/site/uploads/2021-12-06-infrastructure-series-research-paper-telecoms.pdf

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

William, F. K. A. (2024). Interpretivism or constructivism: Navigating research paradigms in social science research. International Journal of Research Publications, 143(1), 134-138. http://dx.doi.org/10.47119/IJRP1001431220246122

Wilson, R. D., & Creswell, J. W. (1996). Research Design: Qualitative and quantitative approaches. *Journal of Marketing Research*, *33*(2), 252. https://doi.org/10.2307/3152153

World Bank. (2024). *World Development Indicators*. World Bank. https://databank.worldbank.org/source/world-development-indicators

Xavier, B. (2025). Biases within AI: challenging the illusion of neutrality. *AI & SOCIETY*, *40*(3), 1545-1546. https://doi.org/10.1007/s00146-024-01985-1

Zaeifi, M., Kalantari, F., Oest, A., Sun, Z., Ahn, G., Shoshitaishvili, Y., Bao, T., Wang, R., & Doupé, A. (2024). Nothing personal: Understanding the spread and use of personally identifiable information in the financial ecosystem. In *ACM Conference on Data and Application Security and Privacy* (14th ed.). https://doi.org/10.1145/3626232.3653266

Zhao, J., Ding, B., Guo, Y., Tan, Z., & Lu, S. (2021). SecureSIM. *Proceedings of the 28th Annual International Conference on Mobile Computing and Networking*. https://doi.org/10.1145/3447993.3483254

APPENDIX A: PRISMA 2020 CHECKLIST

Section and Topic	Item #	Checklist item	Location where item is reported
TITLE			
Title	1	Identify the report as a systematic review.	Y
ABSTRACT			
Abstract	2	See the PRISMA 2020 for Abstracts checklist.	N
INTRODUCTION			
Rationale	3	Describe the rationale for the review in the context of existing knowledge.	Y
Objectives	4	Provide an explicit statement of the objective(s) or question(s) the review addresses.	Y
METHODS			
Eligibility criteria	5	Specify the inclusion and exclusion criteria for the review and how studies were grouped for the syntheses.	Y
Information sources	6	Specify all databases, registers, websites, organisations, reference lists and other sources searched or consulted to identify studies. Specify the date when each source was last searched or consulted.	Y
Search strategy	7	Present the full search strategies for all databases, registers, and websites, including any filters and limits used.	Y
Selection process	8	Specify the methods used to decide whether a study met the inclusion criteria of the review, including how many reviewers screened each record and each report retrieved, whether they worked independently, and if applicable, details of automation tools used in the process.	Y
Data collection process	9	Specify the methods used to collect data from reports, including how many reviewers collected data from each report, whether they worked independently, any processes for obtaining or confirming data from study investigators, and if applicable, details of automation tools used in the process.	Y
Data items	10a	List and define all outcomes for which data were sought. Specify whether all results that were compatible with each outcome domain in each study were sought (e.g., for all measures, time points, analyses), and if not, the methods used to decide which results to collect.	Y
	10b	List and define all other variables for which data were sought (e.g., participant and intervention characteristics, funding sources). Describe any assumptions made about any missing or unclear information.	Y
Study risk of bias assessment	11	Specify the methods used to assess risk of bias in the included studies, including details of the tool(s) used, how many reviewers assessed each study and whether they worked independently, and if applicable, details of automation tools used in the process.	Y
Effect measures	12	Specify for each outcome the effect measure(s) (e.g., risk ratio, mean difference) used in the synthesis or presentation of results.	N
Synthesis methods	13a	Describe the processes used to decide which studies were eligible for each synthesis (e.g., tabulating the study intervention characteristics and comparing against the planned groups for each synthesis (item #5)).	Y
	13b	Describe any methods required to prepare the data for presentation or synthesis, such as handling of missing summary statistics, or data conversions.	Y
	13c	Describe any methods used to tabulate or visually display results of individual studies and syntheses.	Y
	13d	Describe any methods used to synthesize results and provide a rationale for the choice(s). If meta-analysis was performed, describe the model(s), method(s) to identify the presence and extent of statistical heterogeneity, and software package(s) used.	Y
	13e	Describe any methods used to explore possible causes of heterogeneity among study results (e.g., subgroup analysis, meta-regression).	Y
	13f	Describe any sensitivity analyses conducted to assess robustness of the synthesised results.	Y

Section and Topic	Item #	Checklist item	Location where item is reported
Reporting bias assessment	14	Describe any methods used to assess risk of bias due to missing results in a synthesis (arising from reporting biases).	Y
Certainty assessment	15	Describe any methods used to assess certainty (or confidence) in the body of evidence for an outcome.	Y
RESULTS			
Study selection	16a	Describe the results of the search and selection process, from the number of records identified in the search to the number of studies included in the review, ideally using a flow diagram.	Y
	16b	Cite studies that might appear to meet the inclusion criteria, but which were excluded, and explain why they were excluded.	Y
Study characteristics	17	Cite each included study and present its characteristics.	Y
Risk of bias in studies	18	Present assessments of risk of bias for each included study.	Y
Results of individual studies	19	For all outcomes, present, for each study: (a) summary statistics for each group (where appropriate) and (b) an effect estimate and its precision (e.g., confidence/credible interval), ideally using structured tables or plots.	Y
Results of syntheses	20a	For each synthesis, briefly summarise the characteristics and risk of bias among contributing studies.	Y
	20b	Present results of all statistical syntheses conducted. If meta-analysis was done, present for each the summary estimate and its precision (e.g., confidence/credible interval) and measures of statistical heterogeneity. If comparing groups, describe the direction of the effect.	Y
	20c	Present results of all investigations of possible causes of heterogeneity among study results.	Y
	20d	Present results of all sensitivity analyses conducted to assess the robustness of the synthesised results.	Y
Reporting biases	21	Present assessments of risk of bias due to missing results (arising from reporting biases) for each synthesis assessed.	Y
Certainty of evidence	22	Present assessments of certainty (or confidence) in the body of evidence for each outcome assessed.	Y
DISCUSSION			
Discussion	23a	Provide a general interpretation of the results in the context of other evidence.	Y
	23b	Discuss any limitations of the evidence included in the review.	Y
	23c	Discuss any limitations of the review processes used.	Y
	23d	Discuss implications of the results for practice, policy, and future research.	Y
OTHER INFORMATION			
Registration and protocol	24a	Provide registration information for the review, including register name and registration number, or state that the review was not registered.	N
	24b	Indicate where the review protocol can be accessed, or state that a protocol was not prepared.	N
	24c	Describe and explain any amendments to information provided at registration or in the protocol.	N
Support	25	Describe sources of financial or non-financial support for the review, and the role of the funders or sponsors in the review.	N/A
Competing interests	26	Declare any competing interests of review authors.	N/A
Availability of data, code, and other materials	27	Report which of the following are publicly available and where they can be found: template data collection forms; data extracted from included studies; data used for all analyses; analytic code; any other materials used in the review.	N

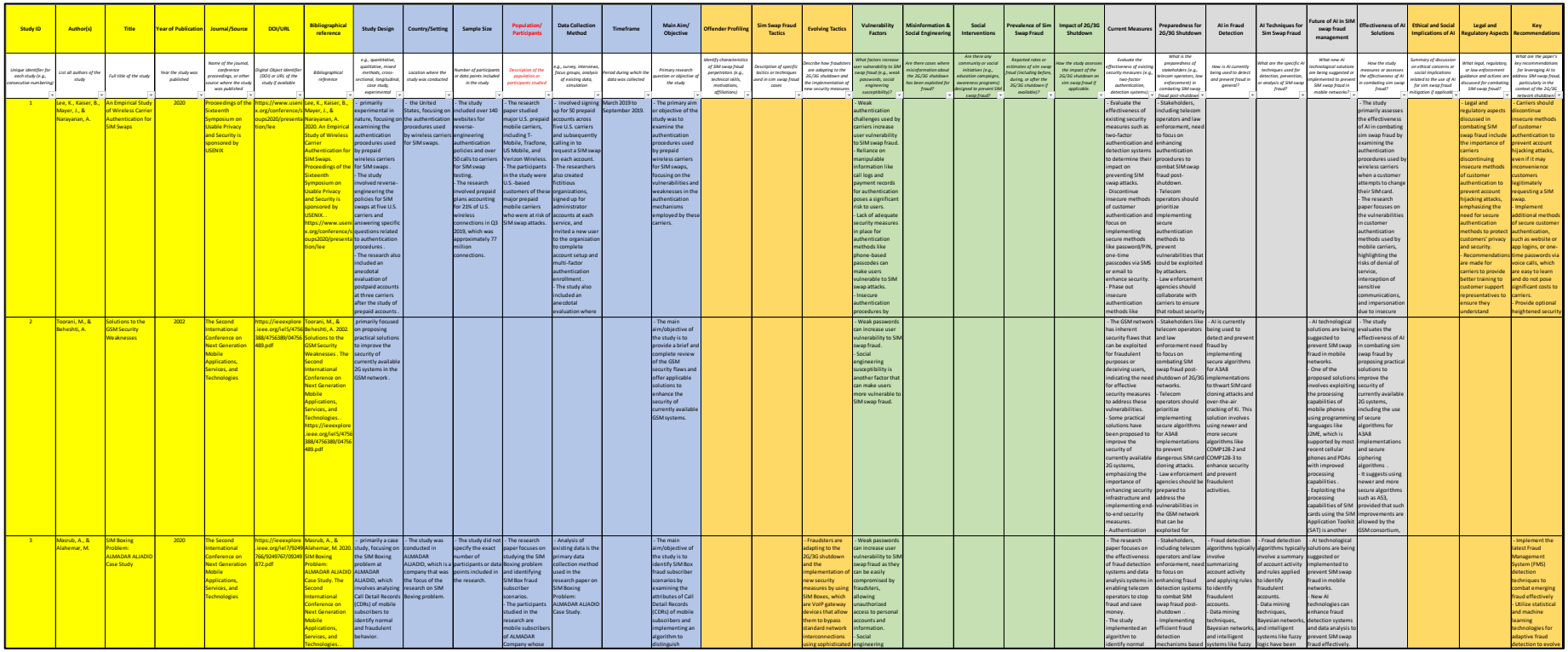
From: Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, *et al.* The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 2021;372:n71. doi: 10.1136/bmj.n71

APPENDIX B: LIST OF SELECTED SOURCES

ID	Author(s)	Title	Year
1	Lee, K., Kaiser, B., Mayer, J., & Narayanan, A.	An Empirical Study of Wireless Carrier Authentication for SIM Swaps	2020
2	Toorani, M., & Beheshti, A.	Solutions to the GSM Security Weaknesses	2002
3	Masrub, A., & Alahemar, M.	SIM Boxing Problem: ALMADAR ALJADID Case Study	2020
4	Al-Humaigani, M., Dunn, D. B., & Brown, D.	Security Transition Roadmap to 4G and Future Generations Wireless Networks	2009
5	Behrad, S., Bertin, E., & Crespi, N.	Securing Authentication for Mobile Networks, A Survey on 4G issues and 5G answers	2020
6	Ammayappan, K.	Seamless interoperation of LTE-UMTS-GSM requires flawless UMTS and GSM	2013
7	Sood, P., Sharma, C., Nijjer, S., & Sakhuja, S.	Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing	2023
8	Fang, P.	Research on Anti-telecom Fraud Based on Artificial Intelligence and Edge Computing	2024
9	Vesa, J.	Regulatory framework and industry clockspeed: Lessons from the Finnish mobile services industry	2004
10	Qiu, T., Ji, L., Pei, D., Wang, J., Jun (Jim) Xu, & Ballani, H.	Locating Prefix Hijackers using LOCK	2009
11	Chitre, P., & Sriramulu, S.	Analysis and Evaluation of Security and Privacy Threats in High Speed Communication Network	2022
12	Ettiane, R., Elkouch, R., & Chaoub, A. (2016, October)	Protection Mechanisms for Signaling DoS Attacks on 3G mobile networks: comparative study and future perspectives	2016
13	Mir, A., Zuhairi, M. F., Musa, S., Syed, T. A., & Alrehaili, A.	POSTER: A Survey of Security Challenges with 5G-IoT	2020
14	Henda, N.	Overview on the Security in 5G Phase 2	2020
15	Angelogianni, A., Politis, I., Mohammadi, F., & Xenakis, C.	On Identifying Threats and Quantifying Cybersecurity Risks of MNOs Deploying Heterogeneous RATs	2020
16	Oh, B., Ahn, J., Bae, S., Son, M., Lee, Y., Kang, M. S., & Kim, Y.	Preventing SIM Box Fraud Using Device Model Fingerprinting	2023
17	LexisNexis Risk Solutions	AI Exploit and Threat Landscape Cybersecurity Guide: Mitigate Artificial Intelligence and generative AI cyber threats and identity fraud risk	2024
18	Lin, K., Wu, Y., Sun, I. Y., & Qu, J.	Telecommunication and cyber fraud victimisation among Chinese college students: An application of routine activity theory	2023
19	Tu, G. H., Li, C. Y., Peng, C., & Lu, S.	How Voice Call Technology Poses Security Threats in 4G LTE Networks	2015
20	Bijani, S., & Kazemitabar, M.	HIDMN: A Host and Network-based Intrusion Detection for Mobile Networks	2008
21	Malek, W. W. Z., Mayes, K., & Markantonakis, K.	Fraud Detection and Prevention in Smart Card Based Environments Using Artificial Intelligence	2008
22	Elmi, A. H., Ibrahim, S., & Sallehuddin, R.	Detecting SIM Box Fraud Using Neural Network	2013
23	Kwon, H. Y., & Kim, S.	Effects of the development of competition framework and legal environment for media contents on the generational transition of mobile networks	2021
24	Dayyabu, Y. Y., Arumugam, D., & Balasingam, S.	The application of artificial intelligence techniques in credit card fraud detection: a quantitative study	2023
25	Abuhamoud, N., Alsadi, I., & Ali, S.	Detecting SIMBox Fraud Using CDR Files And Neo4j Technology	2021
26	Ali, N. T., Hasan, S. J., Ghandour, A., & Al-Hchimy, Z. S.	Improving credit card fraud detection using machine learning and GAN technology	2024
27	Xiang, Y., Wang, Z., Yin, X., & Wu, J.	Argus: An Accurate and Agile System to Detecting IP Prefix Hijacking	2011
28	Nyika, G., Eric, P	Legal Judgements: Adella Stanslaus Assey ta Mount Kibo Phamarcy 2012 vs VODACOM Tanzania Public Ltd Company and Another	2023
29	Lam, L. C., Li, W., & Chiueh, T. C.	Accurate and Automated System Call Policy-Based Intrusion Prevention	2006
30	Kim, M., Suh, J., & Kwon, H.	A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures	2022
31	Jentzsch, N.	Implications of Mandatory Registration of Mobile Phone Users in Africa	2012
32	Kumar, V., Bhardwaj, V., & Anbarasu, V.	Credit Card Fraud Detector for Lower Ranged Transactions using AI Algorithms	2023
33	Kouam, A. J., Viana, A. C., & Tchana, A.	Battle of Wits: To What Extent Can Fraudsters Disguise Their Tracks in International bypass Fraud?	2024
34	Zhao, J., Ding, B., Guo, Y., Tan, Z., & Lu, S.	SecureSIM: Rethinking Authentication and Access Control for SIM/eSIM	2021
35	Van Den Broek, F., Verdult, R., & De Ruiter, J.	Defeating IMSI Catchers	2015
36	Raza, M. T., Anwar, F. M., & Lu, S.	Exposing LTE Security Weaknesses at Protocol Inter-layer, and Inter-radio Interactions	2018
37	Poplavska, Z., & Komarynets, S.	Modelling the External Economic Environment Instability Impact on the Organizational Flexibility of the Enterprise	2021
38	Jimenez, N., San-Martin, S., & Azuela, J. I.	Trust and satisfaction: the keys to client loyalty in mobile commerce	2016
39	Lokanan, M. E., & Maddhesia, V.	Supply Chain Fraud Prediction with Machine Learning and Artificial Intelligence	2024
40	David Jensen	Prospective assessment of AI technologies for fraud detection: A case study	1994
41	Shapiro, R. J., & Hassett, K. A.	The Employment Effects of Advances in Internet and Wireless Technology: Evaluating the Transitions from 2G to 3G and from 3G to 4G	2012
42	Kusuma, A. A., & Suryanegara, M.	Upgrading Mobile Network to 5G: The Technoeconomic Analysis of Main Cities in Indonesia	2019
43	Jover, R. P.	The current state of affairs in 5G security and the main remaining security challenges	2018
44	Chitroub, S., Zidouni, N., Aouadia, H., Blaid, D., & Laouar, R.	SIM card of the next-generation wireless networks: Security, potential vulnerabilities and solutions	2018
45	Depavath Harinath	SIM - Swap Technique -A Legitimate Customer Request	2023
46	Asmare, F. M., & Ayalew, L.	Security challenges in the transition to 4G mobile systems in developing countries	2023
47	Adjaoute, A.	Systems and Methods for Adaptive Identification of Sources of Fraud	2013
48	Zhuk, S., Gepko, I.	Mobile Phone Multi-Factor Authentication with Robustness of Clone Detection	2016
49	Haidine, A., Aqqal, A., & Ouahmane, H.	Modeling the Migration of Mobile Networks Towards 4G and Beyond	2016
50	Gepko, I.	General Requirements and Security Architecture for Mobile Phone Anti-Cloning Measures	2015
51	Miller, S. K.	Facing the Challenge of Wireless Security	2001
52	Mazurkevich, D. O., & Orlov, V. G.	Evolution of security systems in different generations of cellular networks	2011
53	Duan, L., Huang, J., & Walrand, J.	Economic analysis of 4G upgrade timing	2015
54	Malhotra, S., Arora, G., & Bathla, R.	Detection and Analysis of Fraud Phone Calls using Artificial Intelligence	2023
55	Tejpal, K., Vidyapeeth, D. P., Pimpri, P., & Patole, J.	Cybersecurity: Pressing priority in India	2023
56	D'Alessandro, S., Johnson, L., Gray, D., & Carter, L.	Consumer satisfaction versus churn in the case of upgrades of 3G to 4G cell networks	2015
57	Awale, S. M., & Gupta, D. P.	Awareness of Sim Swap Attack	2019
58	Sule, P., & Joshi, A.	Architectural Shift from 4G to 5G Wireless Mobile Networks	2014
59	Shah, K., Martinez, P., Tepedelenlioglu, E., Hasan, S., Festin, C., Blumenstock, J., ... & Heimerl, K.	An Investigation of Phone Upgrades in Remote Community Cellular Networks	2017
60	Adedoyin, A.	Predicting fraud in mobile money transfer	2018
61	Malhotra, S., Arora, G., & Bathla, R.	Detection and Analysis of Fraud Phone Calls using Artificial Intelligence: A Machine Learning Approach	2023
62	Lasierra, O., Garcia-Aviles, G., Municio, E., Skarmeta, A., & Costa-Pérez, X.	European 5G Security in the Wild: Reality versus Expectations	2023
63	Holtrup, G., Lacube, W., David, D. P., Mermoud, A., Bovet, G., & Lenders, V.	5G System Security Analysis	2021
64	Ighneiwa, I., & Mohamed, H.	Bypass Fraud Detection: Artificial Intelligence Approach	2017
65	Sallehuddin, R., Ibrahim, S., & Hussein Elmi, A.	Classification of SIM box fraud detection using support vector machine and artificial neural network	2014
66	Radisys Corporation.	3G to 4G Core Network Migration	2010
67	Akhtar, S.	2G-5G networks: Evolution of technologies, standards, and deployment	2009
68	Andrews, N.	" Can I Get Your Digits?": Illegal Acquisition of Wireless Phone Numbers for Sim-Swap Attacks and Wireless Provider Liability	2018
69	Nanda, A., Jeong, J. J., Shah, S. W. A., Nosouhi, M., & Doss, R.	Computers & Security	2024
70	Krishnan, P., Jain, K., Poojara, S. R., Srirama, S. N., Pandey, T., & Buyya, R.	eSIM and blockchain integrated secure zero-touch provisioning for autonomous cellular-IoTs in 5G networks	2024
71	FCC	Uniform Compliance SIM swap and Port out Rules	2024
72	Singh, S., & Kumar, S.	The times of cyber attacks	2020
73	Lee, K.	The Research-Practice Gap in User Authentication	2022
74	Pramod, D.	Robotic process automation for industry: adoption status, benefits, challenges and research agenda	2022
75	Jackson, D.	New SIM-swap hacks highlight carriers' wobbly security	2020
76	Shetty, M.	Drop OTP? You'll still need phone	2024
77	Richard Detura, Carla Ioshiura, Adrian Murphy, Bryan Richardson, Sebastian Scheurle, Eric Schweikert, Max Vancauwenberghe	A new approach to fighting fraud while enhancing customer experience	2022
78	Ashish Laddha	The pivotal role of AI in supercharging business intelligence capabilities within mobile apps Express Computer	2024
79	Pratima, H	Spam is a tricky problem to solve	2023
80	Srivastava, A.	Online fraud: A raging menace: Your phone has now become an instrument in the hands of the cyber criminal to rob you of your hard-earned money. What you can do to protect yourself	2023
81	Kumar, V.	Smishing, Phishing And SIM Swap: Seminar Uncovers Evolving Cyber Fraud Landscape	2024
82	Assolini, F	SIM swap fraud: A New Wave of Attacks Targeting Financial Services and online services in Africa	2019
83	Hawken, C	Growth in Fintech Drives Growth in Cyberattacks	2019

84	iiDENTIFii	Why South Africa's networks need to defend against the devastating effect of SIM swap fraud	2024
85	Paul McGuire, P., Nadalin, E.	New SIM swap check from tru.ID, the mobile authentication platform, stops the growing menace of SIM swap fraud	2021
86	Kotak, J., Habler, E., Brodt, O., Shabtai, A., & Elovici, Y.	Information Security Threats and Working from Home Culture: Taxonomy, Risk Assessment and Solutions	2023
87	Ali, G., Ally Dida, M., & Elikana Sam, A.	Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda	2021
88	FCC	Draft FCC Item Aims to Combat SIM Swap, Port-Out Fraud	2023
89	CTIA	CTIA Seeks Reconsideration Of SIM Swap, Fraud Item	2024
90	Sharma, P.	Algorithms and strategies for fraud prevention on online platforms	2024
91	Vodacom SA	Vodacom's Submission on ICASA Draft Amendments to Numbering Plan Regulations of 2016, Gazette 46080 of 23 March 2022	2022
92	Vodacom S.A.	Vodacom's written submission in response to ICASA's inquiry into the role and responsibilities of the Independent Communications Authority of South Africa in Cybersecurity	2018
93	Adekunle, A., Jaiyeola, H.	The-emerging-threat-of-AI-powered-fraud	2024
94	Home Office, UK	Telecommunications Fraud Sector Charter	2022
95	Buzzard, J.	2023 Identity Fraud Study: The Butterfly Effect	2023
96	Amadiba Community Network	Response to the Next Generation Radio Frequency Spectrum for Economic Development	2022
97	SABRIC	sabric-annual-crime-stats-2022	2022
98	RSPG Secretariat - EU	DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY Connectivity Radio Spectrum Policy Group RSPG Secretariat	2023
99	ACMA	RIS - Reducing the impact of unauthorised high-risk customer transactions	2021
100	National Identity Management Commission	REVISED NATIONAL IDENTITY POLICY FOR SIM CARD REGISTRATION	2021
101	Telecom Regulatory Authority of India	Draft Telecommunication Mobile Number Portability (Ninth Amendment) Regulations	2023
102	Natarajan, S., Ashara, P.	Whitepaper: Payment Scams - AI to Rescue	2024
103	Federal Communications Commission	Plan Ahead for Phase Out of 3G Cellular Networks and Service	2022
104	GSMA	2G-3G Sunset Guidelines Version 2.0	2024
105	GSMA	2G-3G Sunset Guidelines	2021
106	Media Monitoring Africa	Submission by Media Monitoring Africa	2021
107	Legal Brief Forensic	More customers lose cash in SIM-swap fraud	2024
108	Westermo	White paper: Preparing for the phase out of 2G/3G cellular	2021
109	GSMA	Mobile money fraud typologies and mitigation strategies	2024
110	Federal Communications Commission	Report: Protecting Consumers from SIM Swap and PortOut Fraud	2023
111	Electronic Communications Committee	Regulatory Analysis of Over-The-Air Provisioning of SIM profiles including its impact on Number Portability	2018
112	ICASA	Draft Amendment Numbering Plan Regulations	2016
113	Federal Communications Commission	FCC ADOPTS RULES TO PROTECT CONSUMERS' CELL PHONE ACCOUNTS	2023
114	Telefónica Innovación Digital	API Datasheet: SIM Swap	2024
115	Commission for Communications Regulation	2G/3G Switch off - Guidance for Mobile Network Operators	2024
116	Telecom Regulatory Authority of India	Draft Telecommunication Mobile Number Portability (Ninth Amendment) Regulations, 2023	2023
117	CellC SA	INQUIRY INTO THE ROLES AND RESPONSIBILITIES OF ICASA IN RELATION TO CYBERSECURITY (GAZETTE 41944 OF 28 SEPTEMBER 2018)	2018
118	BEREC Europa	Report on practices and challenges of the phasing out of 2G and 3G	2023
119	Kibuuka, A.	DFS Security recommendations for regulators and providers	2024
120	Wilson, S.	RESEARCH STRATEGY REPORT: 2G AND 3G MIGRATION: CHALLENGES AND INVESTMENT CASES FOR SOLUTIONS	2017
121	Rwanda Utilities Regulatory Authority	REGULATION GOVERNING THE SIM CARD REGISTRATION IN RWANDA	2024
122	AmaBhungane	AmaBhungane submission on the draft Numbering Plan Regulations	2016
123	ICASA	NOTICE REGARDING THE DRAFT INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) ROADMAP	2024
124	Luhanga, E., Sowon, K., Cranor, L. F., Fanti, G., Tucker, C., & Gueye, A.	User Experiences with Third-Party SIM Cards and ID Registration in Kenya and Tanzania	2023
125	Federal Communications Commission	Protecting Consumers from SIM-Swap and Port-Out Fraud AGENCY: Federal Communications Commission. ACTION: Final rule	2023
126	GSMA	Mobile Telecommunications Security Threat Landscape	2024
127	Stephens, C.	Why are SMS codes still the global ID solution	2020
128	Bhavana, S. U., Miriam, D. D. H., & Robin, C. R.	Understanding the Implications of SIM Card Swap Fraud in India: A Comprehensive Study	2024
129	Zaeifi, M., Kalantari, F., Oest, A., Sun, Z., Ahn, G. J., Shoshitaishvili, Y., ... & Doupé, A.	Nothing Personal: Understanding the Spread and Use of Personally Identifiable Information in the Financial Ecosystem	2024
130	Bandi, A., & Yalamarthi, S.	Towards Artificial Intelligence Empowered Security and Privacy Issues in 6G Communications	2022
131	SAADIA, B., TAWFIQ, K., & ALI, A.	THE USE OF ARTIFICIAL INTELLIGENCE IN THE BANKING SECTOR, REFERRING TO THE CASE OF THE UNITED ARAB EMIRATES	2024
132	Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P.	Survey of Fraud Detection Techniques	2004
133	Dupuis, D., & Gleason, K. C.	Old Frauds with a New Sauce: Digital Coins and Behavioral Paradigms	2021
134	Hallman, R. A.	SIM Swapping Attacks for Digital Identity Theft: A threat to financial services and beyond	2023
135	Samunderu, T.	SIM swap fraud: no way out?: financial law	2014
136	Wanyonyi, E., de Lugo, L. B. R. B.	Constructing crime Risks, vulnerabilities and opportunities in Africa's communications infrastructure	2021
137	Ramatar, N.	Artificial Intelligence-driven transformation of risk management function in the South African Telecommunications Industry	2022
138	Melendez, J., Noriega, J., Tiznado, J., Calderon, P., Benites, Y., Rivera, L., ... & Mayhuasca, J.	Sectrabank Model to Mitigate Computer Fraud in Electronic Operations through Banking Applications on Android Devices	2024
139	Omotubora, A.	Crafting the phishing offence in the cybercrime act: A drafter's inelegance that is the court's nightmare	2020
140	Rosa, L. G.	Modeling the SIM Swap Ceremony - Integrating Human Behavior and Formal Analysis	2024
141	Urbas, G., & Krone, T.	Mobile and wireless technologies: security and risk factors	2006
142	Ekwonwune, E. N., Chukwuebuka, U. C., Duroha, A. E., & Duru, A. N.	Analysis of Global System for Mobile Communication (GSM) Subscription Fraud Detection System	2022
143	brahim, I. A., Mohammed, I., & Saidu, B.	Fraud Management System in Detecting Fraud in Cellular Telephone Networks	2015
144	Becker, R. A., Volinsky, C., & Wilks, A. R.	Fraud Detection in Telecommunications: History and Lessons Learned	2010
145	Xu, W., Pang, Y., Ma, J., Wang, S. Y., Hao, G., Zeng, S., & Qian, Y. H.	FRAUD DETECTION IN TELECOMMUNICATION: A ROUGH FUZZY SET BASED APPROACH	2008
146	Moudani, W., & Chakik,	Fraud detection in mobile telecommunication	2013
147	Marakalala, M. C.	Forensic Intelligence: The Effectiveness of the Biometric-based Solution to Combat Mobile Fraud	2023
148	Abbott, D. W., Matkovsky, I. P., & Elder, J. F.	An Evaluation of High-end Data Mining Tools for Fraud Detection	1998
149	Kazembe, M.	Eliminating use of non-traceable identity cards to reduce cyber security incidents: focus on Malawi	2023
150	Hilas, C. S.	Designing an expert system for fraud detection in private telecommunications networks	2009
151	Madiajagan, M., & Dheeba, J.	International Innovative Research Journal of Engineering and Technology	2020
152	Tambunan, D. A., Suryadi, M. T., Hamid, S.,	Cyber Policing In Preventing Sim Swap Attacks, A New Threat To Digital Economy Transactions	2021
153	Hui, S. Y., & Yeung, K. H.	Challenges in the migration to 4G mobile systems	2003
154	OLUGBENGA, A. A.	FRAUDULENT DETECTION MODEL USING MACHINE LEARNING TECHNIQUES USING UNSTRUCTURED SUPPLEMENTARY SERVICE DATA	2021
155	Lokanan, M. E.	Predicting mobile money transaction fraud using machine learning algorithms	2023
156	Koul, S., Raj, Y., & Koul, S.	Analyzing Cyber Trends in Online Financial Frauds using digital Forensics Techniques	2020
157	Stęchły, A., & Szpunar, A.	Analysis of Potential Risks of SMS-Based Authentication	2023
158	Bello, O. A., Folorunso, A., Onwuchekwa, J., Ejiofor, O. E., Budale, F. Z., & Egwuonwu, M. N.	Analysing the Impact of Advanced Analytics on Fraud Detection: A Machine Learning Perspective	2023
159	Ekeh, G. E., Afolabi, Y. I., Uche-Nwachi, E. O., Ekeh, L. K., & Eze-Udu, E.	Awareness of BVN, SIM swap and clone frauds: Methods and controls	2022
160	Nama, F. A., & Obaid, A. J.	Financial Fraud Identification Using Deep Learning Techniques	2024
161	Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M.	AI and 6G Security: Opportunities and Challenges	2021
162	Salaudeen, L. G., Yauri, A. R., Muhammad, G., Umar, H., & Aliyu, S.	A Plethoric Literature Survey on SIMBox Fraud Detection in Telecommunication Industry	2022
163	Kim, M., Suh, J., & Kwon, H.	A Study of the Emerging Trends in SIM Swapping - Crime and Effective Countermeasures	2022
164	Sanni, M. L., Akinyemi, B. O., Akinwuyi, D., Olajubu, E. A., & Aderounmu, G. A.	A Predictive Cyber Threat Model for Mobile Money Services	2023
165	Jordaan, L., & Von Solms, B.	A Biometrics-based Solution to Combat SIM Swap Fraud	2011
166	Adedoyin, A., Kapetanakis, S., Samakovitis, G., & Petridis, M.	Predicting fraud in mobile money transfer using case-based reasoning	2017
167	Manhide, T. C., & Nkomo, D. J.	Determination of Factors Influencing the Upsurge of Electronic Banking Frauds in Zimbabwe	2023
168	Keykhaie, S., & Pierre, S.	Mobile match on card active authentication using touchscreen biometric	2020
169	Singh, R. R., Moreira, J., Chothia, T., & Ryan, M. D.	Security Properties and Attacks Modelling of 802.11 4-Way Handshake Attacks and Analysis of Security Properties	2020
170	Rana, P. J., & Baria, J.	A Survey on Fraud Detection Techniques in Ecommerce	2015
171	Kashir, M., & Bashir, S.	Machine Learning Techniques for SIM Box Fraud Detection	2019
172	Nicholls, J., Kuppa, A., & Le-Khac, N. A.	Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape	2021
173	Yamaguchi, S., Gomi, H., & Uehara, T.	In 2023 IEEE 23rd International Conference on Software Quality, Reliability, and Security Companion (QRS-C) (pp. 532-539)	2023
174	Faircloth, C., Hartzell, G., Callahan, N., & Bhunia, S.	A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft	2022

APPENDIX C: DATA COLLECTION AND QUALITY ASSESSMENT TOOL



Study ID	Author(s)	Title	Year of Publication	Journal/Source	DOI/URL	Bibliographical reference	Study Design	Country/Setting	Sample Size	Population/ Participants	Data Collection Method	Timeframe	Main Aim/ Objective	Offender Profiling	Sim Swap Fraud Tactics	Evolving Tactics	Vulnerability Factors	Misinformation & Social Engineering	Social Interventions	Prevalence of Sim Swap Fraud	Impact of 2G/3G Shutdown	Current Measures	Preparedness for 2G/3G Shutdown	AI in Fraud Detection	AI Techniques for Sim Swap Fraud	Future of AI in SIM swap fraud management	Effectiveness of AI Solutions	Ethical and Social Implications of AI	Legal and Regulatory Aspects	Key Recommendations
Unique identifier for each study (e.g., consecutive numbering)	*List all authors of the study*	*Full title of the study*	*Year the study was published*	*Name of the journal, conference proceedings, or other source where the study was published*	*Digital Object Identifier (DOI) or URL of the study if available*	*Bibliographical reference*	*e.g., quantitative, qualitative, mixed methods, cross-sectional, longitudinal, case study, experimental*	*Location where the study was conducted*	*Number of participants or data points included in the study*	*Description of the population or participants studied*	*e.g., survey, interviews, focus groups, analysis of existing data, simulation*	*Period during which the data was collected*	*Primary research question or objective of the study*	*Identify characteristics of SIM swap fraud perpetrators (e.g., technical skills, motivations, affiliations)*	*Description of specific tactics or techniques used in sim swap fraud cases*	*Describe how fraudsters are adapting to the 2G/3G shutdown and the implementation of new security measures*	*What factors increase user vulnerability to SIM swap fraud (e.g., weak passwords, social engineering susceptibility)?*	*Are there cases where misinformation about the 2G/3G shutdown has been exploited for fraud?*	*Are there any community or social initiatives (e.g., education campaigns, awareness programs) designed to prevent SIM swap fraud?*	*Reported rates or estimates of sim swap fraud (including before, during, or after the 2G/3G shutdown) if available?*	*How the study assesses the impact of the 2G/3G shutdown on sim swap fraud if applicable.*	*Evaluate the effectiveness of existing security measures (e.g., two-factor authentication, detection systems).*	*What is the preparedness of stakeholders (e.g., telecom operators, law enforcement) in combating SIM swap fraud post-shutdown?*	*How is AI currently being used to detect and prevent fraud in general?*	*What are the specific AI techniques used for detection, prevention, or analysis of SIM swap fraud?*	*What new AI technological solutions are being suggested or implemented to prevent SIM swap fraud in mobile networks?*	*How the study measures or assesses the effectiveness of AI in combating sim swap fraud?*	*Summary of discussion on ethical concerns or social implications related to the use of AI for sim swap fraud. mitigation if applicable*	*What legal, regulatory, or law enforcement guidance and actions are discussed for combating SIM swap fraud?*	*What are the paper's key recommendations for leveraging AI to address SIM swap fraud, particularly in the context of the 2G/3G network shutdown?*
1	Lee, K., Kaiser, B., Mayer, J., & Narayanan, A.	An Empirical Study of Wireless Carrier Authentication for SIM Swaps	2020	Proceedings of the Sixteenth Symposium on Usable Privacy and Security is sponsored by USENIX	https://www.usenix.org/conference/soups2020/presentation/lee	Lee, K., Kaiser, B., Mayer, J., & Narayanan, A. 2020. An Empirical Study of Wireless Carrier Authentication for SIM Swaps. Proceedings of the Sixteenth Symposium on Usable Privacy and Security is sponsored by USENIX. https://www.usenix.org/conference/soups2020/presentation/lee	- primarily experimental in nature, focusing on examining the authentication procedures used by prepaid wireless carriers for SIM swaps . - The study involved reverse-engineering the policies for SIM swaps at five U.S. carriers and answering specific questions related to authentication procedures . - The research also included an anecdotal evaluation of postpaid accounts at three carriers after the study of prepaid accounts .	- the United States, focusing on the authentication procedures used by wireless carriers for SIM swaps.	- The study included over 140 websites for reverse-engineering authentication policies and over 50 calls to carriers for SIM swap testing. - The research involved prepaid plans accounting for 21% of U.S. wireless connections in Q3 2019, which was approximately 77 million connections.	- The research paper studied major U.S. prepaid mobile carriers, including T-Mobile, Tracfone, US Mobile, and Verizon Wireless. - The participants in the study were U.S.-based customers of these major prepaid mobile carriers who were at risk of SIM swap attacks.	- involved signing up for 50 prepaid accounts across five U.S. carriers and subsequently calling in to request a SIM swap on each account. - The researchers also created fictitious organizations, signed up for administrator accounts at each service, and invited a new user to the organization to complete account setup and multi-factor authentication enrollment . - The study also included an anecdotal evaluation where	March 2019 to September 2019.	- The primary aim or objective of the study was to examine the authentication procedures used by prepaid wireless carriers for SIM swaps, focusing on the vulnerabilities and weaknesses in the authentication mechanisms employed by these carriers.				- Weak authentication challenges used by carriers increase user vulnerability to SIM swap fraud. - Reliance on manipulable information like call logs and payment records for authentication poses a significant risk to users. - Lack of adequate security measures in place for authentication methods like phone-based passcodes can make users vulnerable to SIM swap attacks. - Insecure authentication procedures by					- Evaluate the effectiveness of existing security measures such as two-factor authentication and detection systems to determine their impact on preventing SIM swap attacks. - Discontinue insecure methods of customer authentication and focus on implementing secure methods like password/PIN, one-time passcodes via SMS or email to enhance security. - Phase out insecure authentication methods like	- Stakeholders, including telecom operators and law enforcement, need to focus on enhancing authentication procedures to combat SIM swap fraud post-shutdown. - Telecom operators should prioritize implementing secure authentication methods to prevent vulnerabilities that could be exploited by attackers. - Law enforcement agencies should collaborate with carriers to ensure that robust security					- Legal and regulatory aspects discussed in combating SIM swap fraud include the importance of carriers discontinuing insecure methods of customer authentication to prevent account hijacking attacks, emphasizing the need for secure authentication methods to protect customers' privacy and security. - Recommendations are made for carriers to provide better training to customer support representatives to ensure they understand	- Carriers should discontinue insecure methods of customer authentication to prevent account hijacking attacks, even if it may inconvenience customers legitimately requesting a SIM swap. - Implement additional methods of secure customer authentication, such as website or app logins, or one-time passwords via voice calls, which are easy to learn and do not pose significant costs to carriers. - Provide optional heightened security
2	Toorani, M., & Beheshti, A.	Solutions to the GSM Security Weaknesses	2002	The Second International Conference on Next Generation Mobile Applications, Services, and Technologies	https://ieeexplore.ieee.org/iel5/4756388/4756389/04756489.pdf	Toorani, M., & Beheshti, A. 2002. Solutions to the GSM Security Weaknesses . The Second International Conference on Next Generation Mobile Applications, Services, and Technologies . https://ieeexplore.ieee.org/iel5/4756388/4756389/04756489.pdf	primarily focused on proposing practical solutions to improve the security of currently available 2G systems in the GSM network.						- The main aim/objective of the study is to provide a brief and complete review of the GSM security flaws and offer applicable solutions to enhance the security of currently available GSM systems.				- Weak passwords can increase user vulnerability to SIM swap fraud. - Social engineering susceptibility is another factor that can make users more vulnerable to SIM swap fraud.					- The GSM network has inherent security flaws that can be exploited for fraudulent purposes or deceiving users, indicating the need for effective security measures to address these vulnerabilities. - Some practical solutions have been proposed to improve the security of currently available 2G systems, emphasizing the importance of enhancing security infrastructure and implementing end-to-end security measures. - Authentication	- Stakeholders like telecom operators and law enforcement need to focus on combating SIM swap fraud post-shutdown of 2G/3G networks. - Telecom operators should prioritize implementing secure algorithms for A3A8 implementations to prevent dangerous SIM card cloning attacks. - Law enforcement agencies should be prepared to address the vulnerabilities in the GSM network that can be exploited for	- AI is currently being used to detect and prevent fraud by implementing secure algorithms for A3A8 implementations to thwart SIM card cloning attacks and over-the-air cracking of Ki. This solution involves using newer and more secure algorithms like COMP128-2 and COMP128-3 to enhance security and prevent fraudulent activities.		- AI technological solutions are being suggested to prevent SIM swap Fraud in mobile networks. - One of the proposed solutions involves exploiting the processing capabilities of mobile phones using programming languages like J2ME, which is supported by most recent cellular phones and PDAs with improved processing capabilities . - Exploiting the processing capabilities of SIM cards using the SIM Application Toolkit (SAT) is another	- The study evaluates the effectiveness of AI in combating sim swap fraud by proposing practical solutions to improve the security of currently available 2G systems, including the use of secure algorithms for A3A8 implementations and secure ciphering algorithms . - It suggests using newer and more secure algorithms such as A53, provided that such improvements are allowed by the GSM consortium,			
3	Masrub, A., & Alahemar, M.	SIM Boxing Problem: ALMADAR ALIADID Case Study	2020	The Second International Conference on Next Generation Mobile Applications, Services, and Technologies	https://ieeexplore.ieee.org/iel7/9049766/9049767/09049872.pdf	Masrub, A., & Alahemar, M. 2020. SIM Boxing Problem: ALMADAR ALIADID Case Study. The Second International Conference on Next Generation Mobile Applications, Services, and Technologies .	- primarily a case study, focusing on the SIM Boxing problem at ALMADAR ALIADID, which involves analyzing Call Detail Records (CDRs) of mobile subscribers to identify normal and fraudulent behavior.	- The study was conducted in ALMADAR ALIADID, which is a company that was the focus of the research on SIM Boxing problem.	- The study did not specify the exact number of participants or data points included in the research.	- The research paper focuses on studying the SIM Boxing problem and identifying SIM box fraud subscriber scenarios. - The participants studied in the research are mobile subscribers of ALMADAR Company whose	- Analysis of existing data is the primary data collection method used in the research paper on SIM Boxing Problem: ALMADAR ALIADID Case Study.		- The main aim/objective of the study is to identify SIM Box fraud subscriber scenarios by examining the attributes of Call Detail Records (CDRs) of mobile subscribers and implementing an algorithm to distinguish			- Fraudsters are adapting to the 2G/3G shutdown and the implementation of new security measures by using SIM Boxes, which are VoIP gateway devices that allow them to bypass standard network interconnections using sophisticated	- Weak passwords can increase user vulnerability to SIM swap fraud as they can be easily compromised by fraudsters, allowing unauthorized access to personal accounts and information. - Social engineering					- The research paper focuses on the effectiveness of fraud detection systems and data analysis systems in enabling telecom operators to stop fraud and save money. - The study implemented an algorithm to identify normal	- Stakeholders, including telecom operators and law enforcement, need to focus on enhancing fraud detection systems to combat SIM swap fraud post-shutdown . - Implementing efficient fraud detection mechanisms based	- Fraud detection algorithms typically involve summarizing account activity and applying rules to identify fraudulent accounts. - Data mining techniques, Bayesian networks, and intelligent systems like fuzzy	- Fraud detection algorithms typically involve a summary of account activity and rules applied to identify fraudulent accounts. - Data mining techniques, Bayesian networks, and intelligent systems like fuzzy logic have been	- AI technological solutions are being suggested or implemented to prevent SIM swap Fraud in mobile networks. - New AI technologies can enhance fraud detection systems and data analysis to prevent SIM swap Fraud effectively.				- Implement the latest Fraud Management System (FMS) detection techniques to combat emerging fraud effectively . - Utilize statistical and machine learning technologies for adaptive fraud detection to evolve

Figure 40: Data capture tool

Study Identification			Motivated Offender Themes			Suitable Target Themes					Lack of Capable Guardianship Themes						
Study ID	Author(s)	Year of Publication	Offender Profiling	Sim Swap Fraud Tactics	Evolving Tactics	Vulnerability Factors	Misinformation & Social Engineering	Social Interventions	Prevalence of Sim Swap Fraud	Impact of 2G/3G Shutdown	Current Measures	Preparedness for 2G/3G Shutdown	AI in Fraud Detection	AI Techniques for Sim Swap Fraud	Future of AI in SIM swap fraud management	Effectiveness of AI Solutions	
Unique identifier for each study	*List all authors of the study*	*Year the study was published*	QUALITY SCORING														Paper Quality Score (n/14)
1	Lee, K., Kaiser, B.,	2020	0	0	0	1	0	0	0	0	1	1	0	0	0	1	4
2	Toorani, M., &	2002	0	0	0	1	0	0	0	0	1	1	1	0	1	1	6
3	Masrub, A., &	2020	0	0	1	1	0	0	0	0	1	1	1	1	1	0	7
4	Al-Humaigani, M.,	2009	0	0	1	1	0	0	0	0	1	1	0	0	1	0	5
5	Behrad, S., Bertin,	2020	0	1	1	1	0	0	0	0	0	0	0	0	0	0	3
6	Ammayappan, K.	2013	0	0	0	1	0	0	0	0	0	1	0	0	0	0	2
7	Sood, P., Sharma,	2023	0	1	0	0	0	0	0	0	1	0	1	1	1	0	5
8	Fang, P.	2024	0	1	0	1	0	0	0	0	1	1	1	1	1	1	8
9	Vesa, J.	2004	0	0	0	0	0	0	0	0	0	0	1	0	1	0	2
10	Qiu, T., Ji, L., Pei,	2009	0	0	0	1	0	0	0	0	1	0	1	0	1	0	4
11	Chitre, P., &	2022	1	0	1	1	0	0	0	0	0	0	0	0	0	0	3
12	Ettiane, R.,	2016	0	0	0	1	0	0	0	0	1	1	0	0	1	0	4
13	Mir, A., Zuhairi, M.	2020	0	0	0	1	0	0	0	0	0	0	0	0	1	0	2
14	Henda, N.	2020	0	0	0	1	0	0	0	0	0	1	0	0	1	0	3
15	Angelogianni, A.,	2020	0	0	1	1	0	0	0	0	1	0	1	0	1	0	5
16	Oh, B., Ahn, J., Bae,	2023	0	0	0	1	0	0	1	0	0	0	0	0	0	0	2
17	LexisNexis Risk	2024	1	1	0	1	1	1	0	0	1	1	1	0	1	0	9
18	Lin, K., Wu, Y., Sun,	2023	0	0	0	1	0	0	0	0	1	0	1	0	1	0	4
19	Tu, G. H., Li, C. Y.,	2015	0	0	0	1	0	0	0	0	0	1	0	0	1	0	3
20	Bijani, S., &	2008	1	0	0	1	0	0	0	0	0	0	1	0	0	1	4
21	Malek, W. W. Z.,	2008	0	0	0	1	0	0	0	0	1	1	1	1	1	1	7

Figure 41: Quality assessment tool

APPENDIX D: SOURCE LOCAL IMPACT

Source	h_index	g_index	m_index	TC	NP	PY_start
IEEE ACCESS	2	2	0,4	56	2	2020
LECTURE NOTES IN COMPUTER SCIE	2	3	0,11764706	14	3	2008
2015 IEEE CONFERENCE ON COMMU	1	1	0,1	23	1	2015
2019 16TH INTERNATIONAL CONFEI	1	1	0,16666667	12	1	2019
2019 INTERNATIONAL CONFERENCI	1	1	0,16666667	10	1	2019
2021 IEEE 1ST INTERNATIONAL MAC	1	1	0,25	2	1	2021
2021 JOINT EUROPEAN CONFERENC	1	1	0,25	153	1	2021
2022 IEEE WORLD AI IOT CONGRESS	1	1	0,33333333	5	1	2022
2023 INTERNATIONAL CONFERENCI	1	1	0,5	1	1	2023
21ST CONFERENCE ON INNOVATIO	1	1	0,14285714	15	1	2018
30TH ANNUAL NETWORK AND DIST	1	1	0,5	2	1	2023
ACADEMIA REVISTA LATINOAMERI	1	1	0,11111111	43	1	2016
ACM INTERNATIONAL CONFERENCI	1	2	0,125	8	2	2017
ANNALS OF EMERGING TECHNOLO	1	1	0,5	2	1	2023
APPLIED AI LETTERS	1	1	0,5	4	1	2023
BENCHMARKING	1	1	0,33333333	32	1	2022
BIOMETRIC TECHNOLOGY TODAY	1	1	0,2	3	1	2020
COGENT ENGINEERING	1	1	0,5	2	1	2023
COLLOQUIUM IN INFORMATION SC	1	1	0,11111111	3	1	2016
COMPUTER COMMUNICATIONS	1	1	1	4	1	2024
CONFERENCE PROCEEDING - IEEE IN	1	1	0,04761905	312	1	2004
CONTRIBUTIONS TO ECONOMICS	1	1	0,05263158	3	1	2006
CRIMINOLOGY AND CRIMINAL JUST	1	1	0,5	4	1	2023
E3S WEB OF CONFERENCES	1	1	0,5	7	1	2023
EXPERT SYSTEMS WITH APPLICATIO	1	1	0,0625	54	1	2009
IEEE COMMUNICATIONS MAGAZINI	1	1	0,04545455	306	1	2003
IEEE TRANSACTIONS ON MOBILE CO	1	1	0,1	18	1	2015
INFORMATION (SWITZERLAND)	1	1	0,2	13	1	2020
INTERNATIONAL CONFERENCE ON S	1	1	0,33333333	8	1	2022
INTERNATIONAL JOURNAL OF PROI	1	1	1	1	1	2024
INTERNATIONAL JOURNAL OF SYST	1	1	0,5	5	1	2023
JOURNAL OF ICT STANDARDIZATIOI	1	1	0,16666667	4	1	2019
LECTURE NOTES IN ELECTRICAL ENG	1	2	0,08333333	16	2	2013
LECTURE NOTES IN NETWORKS AND	1	1	0,5	1	1	2023
LECTURE NOTES OF THE INSTITUTE I	1	1	0,14285714	22	1	2018
MARKETING LETTERS	1	1	0,1	7	1	2015
MM 2020 - PROCEEDINGS OF THE 28	1	1	0,2	174	1	2020
MODERN PROBLEMS OF RADIO ENG	1	1	0,11111111	2	1	2016
PROCEEDINGS - 2018 2ND EUROPEA	1	1	0,14285714	3	1	2018
PROCEEDINGS - 2020 1ST INTERNAT	1	1	0,2	5	1	2020
PROCEEDINGS - 2022 IEEE/ACIS 7TH	1	1	0,33333333	2	1	2022
PROCEEDINGS - 2ND INTERNATION	1	1	0,08333333	5	1	2013
PROCEEDINGS - INTERNATIONAL CO	1	1	0,07142857	14	1	2011
PROCEEDINGS - THE 2ND INTERNAT	1	1	0,05882353	53	1	2008
PROCEEDINGS OF THE 16TH SYMPO	1	1	0,2	32	1	2020
PROCEEDINGS OF THE 18TH USENIX	1	1	0,0625	22	1	2009
PROCEEDINGS OF THE 2008 INTERN	1	1	0,05882353	3	1	2008
PROCEEDINGS OF THE 7TH INTERNA	1	1	0,05882353	19	1	2008
PROCEEDINGS OF THE ACM CONFEI	1	1	0,1	49	1	2015
PROCEEDINGS OF THE ANNUAL INT	1	1	0,25	13	1	2021
PROCEEDINGS OF THE ANNUAL SOU	1	1	0,0625	3	1	2009
PROCEEDINGS OF THE IEEE INTERN	1	1	0,03703704	24	1	1998
PROCEEDINGS OF THE INTERNATIO	1	1	0,05263158	18	1	2006
SENSORS	1	1	0,5	6	1	2023
TECHNOMETRICS	1	1	0,06666667	54	1	2010
TELECOMMUNICATIONS POLICY	1	1	0,07692308	14	1	2012
TELEMATICS AND INFORMATICS	1	1	0,25	2	1	2021
WISEC 2023 - PROCEEDINGS OF THE	1	1	0,5	4	1	2023

APPENDIX E: AUTHOR LOCAL IMPACT

Author	h_index	g_index	m_index	TC	NP	PY_start
LU S	3	3	0,3	58	3	2015
ABBOTT DW	1	1	0,03703704	24	1	1998
ABUHAMOUD N	1	1	0,25	2	1	2021
ADEDOYIN A	1	1	0,125	9	1	2017
ADEROUNMU GA	1	1	0,5	2	1	2023
AHN J	1	1	0,5	2	1	2023
AKINYEMI BO	1	1	0,5	2	1	2023
AL-HUMAIGANI M	1	1	0,0625	3	1	2009
ALI G	1	1	0,2	13	1	2020
ALI S	1	1	0,25	2	1	2021
ALREHAILI A	1	1	0,2	5	1	2020
ALSADI I	1	1	0,25	2	1	2021
AMMAYAPPAN K	1	1	0,08333333	5	1	2013
ANGELOGIANNI A	1	1	0,2	8	1	2020
ANWAR FM	1	1	0,14285714	22	1	2018
AOUADIA H	1	1	0,14285714	3	1	2018
AQQAL A	1	1	0,11111111	1	1	2016
ARORA G	1	1	0,5	1	1	2023
ARUMUGAM D	1	1	0,5	7	1	2023
ASMARE FM	1	1	0,5	2	1	2023
AYALEW LG	1	1	0,5	2	1	2023
AZUELA JI	1	1	0,11111111	43	1	2016
BAE S	1	1	0,5	2	1	2023
BALASINGAM S	1	1	0,5	7	1	2023
BALLANI H	1	1	0,0625	22	1	2009
BANDI A	1	1	0,33333333	8	1	2022
BASHIR S	1	1	0,16666667	10	1	2019
BATHLA R	1	1	0,5	1	1	2023
BECKER RA	1	1	0,06666667	54	1	2010
BEHRAD S	1	1	0,14285714	15	1	2018
BERTIN E	1	1	0,14285714	15	1	2018
BHUNIA S	1	1	0,33333333	5	1	2022
BIJANI S	1	1	0,05882353	3	1	2008
BLAID D	1	1	0,14285714	3	1	2018
BLUMENSTOCK J	1	1	0,125	8	1	2017
BRODT O	1	1	0,5	6	1	2023
BROWN D	1	1	0,0625	3	1	2009
BUYYA R	1	1	1	4	1	2024
CALLAHAN N	1	1	0,33333333	5	1	2022
CARTER L	1	1	0,1	7	1	2015
CHAOUB A	1	1	0,11111111	3	1	2016
CHEN R	1	1	0,2	174	1	2020
CHEN X	1	1	0,2	174	1	2020
CHITRE P	1	1	0,5	1	1	2023
CHITROUB S	1	1	0,14285714	3	1	2018
CHIUEH TC	1	1	0,05263158	18	1	2006
COSTA-PÉREZ X	1	1	0,5	4	1	2023
CRESPI N	1	1	0,14285714	15	1	2018
D'ALESSANDRO S	1	1	0,1	7	1	2015
DAYYABU YY	1	1	0,5	7	1	2023
DE RUITER J	1	1	0,1	49	1	2015
DIDA MA	1	1	0,2	13	1	2020
DING B	1	1	0,25	13	1	2021
DIONISIO J	1	1	0,125	8	1	2017
DUAN L	1	1	0,1	18	1	2015
DUNN DB	1	1	0,0625	3	1	2009
ELDER JFIV	1	1	0,03703704	24	1	1998
ELKOUCH R	1	1	0,11111111	3	1	2016
ELMI AH	1	1	0,08333333	15	1	2013
ELOVICI Y	1	1	0,5	6	1	2023
ETTIANE R	1	1	0,11111111	3	1	2016
FAIRCLOTH C	1	1	0,33333333	5	1	2022
FESTIN C	1	1	0,125	8	1	2017
GANG H	1	1	0,05882353	19	1	2008
GARCIA-AVILES G	1	1	0,5	4	1	2023
GE Y	1	1	0,2	174	1	2020
GEPKO I	1	1	0,11111111	2	1	2016
GRAY D	1	1	0,1	7	1	2015
GUO Y	1	1	0,25	13	1	2021
HABLER E	1	1	0,5	6	1	2023
HAIDINE A	1	1	0,11111111	1	1	2016
HARTZELL G	1	1	0,33333333	5	1	2022
HASAN S	1	1	0,125	8	1	2017
HEIMERL K	1	1	0,125	8	1	2017
HENDA NB	1	1	0,16666667	4	1	2019
HILAS CS	1	1	0,0625	54	1	2009
HUANG J	1	1	0,1	18	1	2015
HUANG YP	1	1	0,04761905	312	1	2004
HUI SY	1	1	0,04545455	306	1	2003
IBRAHIM S	1	1	0,08333333	15	1	2013
JAIN K	1	1	1	4	1	2024
JENTZSCH N	1	1	0,07692308	14	1	2012
JI L	1	1	0,0625	22	1	2009
JIMENEZ N	1	1	0,11111111	43	1	2016
JOHNSON L	1	1	0,1	7	1	2015
JORDAAN L	1	1	0,07142857	1	1	2011
KAISER B	1	1	0,2	32	1	2020
KANG M	1	1	0,5	2	1	2023
KAPETANAKIS S	1	1	0,125	9	1	2017
KASHIR M	1	1	0,16666667	10	1	2019
KIM M	1	1	0,33333333	2	1	2022
KIM S	1	1	0,25	2	1	2021
KIM Y	1	1	0,5	2	1	2023
KOTAK J	1	1	0,5	6	1	2023
KRISHNAN P	1	1	1	4	1	2024
KUPPA A	1	1	0,25	48	1	2021
KUSUMA AA	1	1	0,16666667	12	1	2019
KWON H	1	1	0,33333333	2	1	2022
KWON HY	1	1	0,25	2	1	2021
LAM LC	1	1	0,05263158	18	1	2006
LAOUAR R	1	1	0,14285714	3	1	2018
LASIERRA O	1	1	0,5	4	1	2023
LE-KHAC NA	1	1	0,25	48	1	2021
LEE K	1	1	0,2	32	1	2020
LEE Y	1	1	0,5	2	1	2023
LI CY	1	1	0,1	23	1	2015
LI W	1	1	0,05263158	18	1	2006
LIN K	1	1	0,5	4	1	2023
LIYANAGE M	1	1	0,25	153	1	2021
LOKANAN ME	1	2	0,5	5	2	2023
LU CT	1	1	0,04761905	312	1	2004
MA J	1	1	0,05882353	19	1	2008
MADDHESIA V	1	1	1	1	1	2024
MALEK WWZ	1	1	0,05882353	4	1	2008
MALHOTRA S	1	1	0,5	1	1	2023
MARKANTONAKIS K	1	1	0,05882353	4	1	2008
MARTINEZ P	1	1	0,125	8	1	2017
MARYAMOSADAT KA	1	1	0,05882353	3	1	2008
MATKOVSKY IP	1	1	0,03703704	24	1	1998
MAYER J	1	1	0,2	32	1	2020
MAYES K	1	1	0,05882353	4	1	2008
MIR A	1	1	0,2	5	1	2020
MOHAMMADI F	1	1	0,2	8	1	2020
MUNICIO E	1	1	0,5	4	1	2023
MUSA S	1	1	0,2	5	1	2020
NARAYANAN A	1	1	0,2	32	1	2020
NI B	1	1	0,2	174	1	2020
NICHOLLS J	1	1	0,25	48	1	2021
NIJJER S	1	1	0,5	5	1	2023
OH B	1	1	0,5	2	1	2023
OLAJUBU EA	1	1	0,5	2	1	2023
OLALERE DA	1	1	0,5	2	1	2023
OUAHMANE H	1	1	0,11111111	1	1	2016
PANDEY T	1	1	1	4	1	2024
PANG YE	1	1	0,05882353	19	1	2008
PEI D	1	1	0,0625	22	1	2009
PENG C	1	1	0,1	23	1	2015
PETRIDIS M	1	1	0,125	9	1	2017
POLITIS I	1	1	0,2	8	1	2020
POOJARA SR	1	1	1	4	1	2024
PORAMBAGE P	1	1	0,25	153	1	2021
PRAMOD D	1	1	0,33333333	32	1	2022
QIAN YH	1	1	0,05882353	19	1	2008
QIU T	1	1	0,0625	22	1	2009
QU J	1	1	0,5	4	1	2023
RAZA MT	1	1	0,14285714	22	1	2018
SAKHUJA S	1	1	0,5	5	1	2023
SALLEHUDDIN R	1	1	0,08333333	15	1	2013
SAM AE	1	1	0,2	13	1	2020
SAMAKOVITIS G	1	1	0,125	9	1	2017
SAN-MARTIN S	1	1	0,11111111	43	1	2016
SANNI ML	1	1	0,5	2	1	2023
SHABTAI A	1	1	0,5	6	1	2023
SHAH K	1	1	0,125	8	1	2017
SHARMA C	1	1	0,5	5	1	2023
SHIRAZI AAB	1	1	0,05882353	53	1	2008
SIRIWARDHANA Y	1	1	0,25	153	1	2021
SIRWONGWATTANA S	1	1	0,04761905	312	1	2004
SKARMETA A	1	1	0,5	4	1	2023
SON M	1	1	0,5	2	1	2023
SOOD P	1	1	0,5	5	1	2023
SRIRAMA SN	1	1	1	4	1	2024
SRIRAMULU S	1	1	0,5	1	1	2023
STEPHENS C	1	1	0,2	3	1	2020
SUH J	1	1	0,33333333	2	1	2022
SUN IY	1	1	0,5	4	1	2023
SURYANEGARA M	1	1	0,16666667	12	1	2019
SYED TA	1	1	0,2	5	1	2020
TAN Z	1	1	0,25	13	1	2021
TEPEDELENLIOGLU E	1	1	0,125	8	1	2017
TOORANI M	1	1	0,05882353	53	1	2008
TU GH	1	1	0,1	23	1	2015
VAN DEN BROEK F	1	1	0,1	49	1	2015
VERDULT R	1	1	0,1	49	1	2015
VESA J	1	1	0,05263158	3	1	2006
VOLINSKY C	1	1	0,06666667	54	1	2010
VON SOLMS B	1	1	0,07142857	1	1	2011
WALRAND J	1	1	0,1	18	1	2015
WANG J	1	1	0,0625	22	1	2009
WANG SY	1	1	0,05882353	19	1	2008
WANG Z	1	1	0,07142857	14	1	2011
WILKS AR	1	1	0,06666667	54	1	2010
WU J	1	1	0,07142857	14	1	2011
WU Y	1	1	0,5	4	1	2023
XENAKIS C	1	1	0,2	8	1	2020
XIANG Y	1	1	0,07142857	14	1	2011
XU J	1	1	0,0625	22	1	2009
XU W	1	1	0,05882353	19	1	2008
YALAMARTHI S	1	1	0,33333333	8	1	2022
YEUNG KH	1	1	0,04545455	306	1	2003
YIN X	1	1	0,07142857	14	1	2011
YLIANTTILA M	1	1	0,25	153	1	2021
ZENG S	1	1	0,05882353	19	1	2008
ZHAO J	1	1	0,25	13	1	2021
ZHUK S	1	1	0,11111111	2	1	2016
ZIDOUNI N	1	1	0,14285714	3	1	2018
ZUHAIRI MF	1	1	0,2	5	1	2020

APPENDIX F: KEY WORD PLUS CO-OCCURRENCE

Occurrences	Words	Cluster	Cluster_L	btw_cent	clos_cent	pagerank
7	fraud detecti	1	fraud detecti	1063,09539	0,00186916	0,01134441
5	artificial inte	1	fraud detecti	524,069698	0,00179533	0,00748323
5	neural netwo	1	fraud detecti	558,80583	0,00191571	0,009899
4	data mining	1	fraud detecti	687,420246	0,00194175	0,00658206
4	learning syst	1	fraud detecti	497,740822	0,00192308	0,00820936
4	telecommun	1	fraud detecti	1080,36787	0,00188679	0,0081237
2	deep learnin	1	fraud detecti	151,489834	0,0015748	0,00526002
2	behavioral re	1	fraud detecti	23,731371	0,00149925	0,00405687
2	classification	1	fraud detecti	99,4342765	0,00165289	0,00457585
2	cybernetics	1	fraud detecti	143,653585	0,00179211	0,00443146
2	fraudsters	1	fraud detecti	281,075712	0,00191205	0,00426611
2	machine lear	1	fraud detecti	50,1299474	0,00156986	0,00445762
2	quality of se	1	fraud detecti	273,570185	0,0017452	0,00386584
2	smart cards	1	fraud detecti	135,58372	0,00191571	0,00355977
2	telecom frau	1	fraud detecti	107,962389	0,00158228	0,00463126
2	telecom prov	1	fraud detecti	189,367672	0,00170358	0,0042936
2	telecommun	1	fraud detecti	63,497402	0,00167785	0,00428356
2	voip - techno	1	fraud detecti	96,53468	0,00158983	0,00386595
21	crime	2	crime	6726,97254	0,00223714	0,03778609
14	authenticati	2	crime	1638,05955	0,00194553	0,01927732
6	cybersecurit	2	crime	240,34472	0,00161031	0,01227571
6	machine lear	2	crime	1665,59199	0,00204918	0,01111703
5	computer cri	2	crime	1389,84025	0,00194932	0,01156956
3	risk assessme	2	crime	572,972373	0,0019685	0,00577374
4	cyber-crimes	2	crime	174,689832	0,00169779	0,00892732
4	finance	2	crime	287,995947	0,00179856	0,00739258
3	cyber securit	2	crime	356,682421	0,00182149	0,00685653
3	economic an	2	crime	364,151119	0,00198807	0,00476052
3	electronic m	2	crime	336,965156	0,0017762	0,005846
3	machine-lea	2	crime	128,37099	0,0015625	0,00525413
3	network prot	2	crime	455,795637	0,0020202	0,00523106
3	sim cards	2	crime	189,105195	0,00153139	0,00584186
3	surveys	2	crime	413,544314	0,00186567	0,00564506
3	telephone se	2	crime	398,899468	0,00178891	0,00421635
2	anomaly det	2	crime	120,826545	0,00163666	0,00513707
2	authenticati	2	crime	95,8225205	0,00189394	0,00288696
2	cyber-attack	2	crime	63,3125564	0,00172712	0,00387559
2	cyberspaces	2	crime	120,345861	0,00171527	0,00527748
2	detection me	2	crime	157,782456	0,00185529	0,00344129
2	ecosystems	2	crime	78,955616	0,0016835	0,00453193
2	financial loss	2	crime	25,8705742	0,00148148	0,00383925
2	identity thef	2	crime	63,3125564	0,00172712	0,00387559
2	losses	2	crime	25,8705742	0,00148148	0,00383925
2	mobile mone	2	crime	141,351367	0,00174216	0,00451874
2	personal con	2	crime	22,6099974	0,00145985	0,00478566
2	phone numb	2	crime	123,742097	0,00176678	0,00365768
2	prevention n	2	crime	141,995126	0,00168634	0,0036212
2	risk analysis	2	crime	337,959248	0,00184502	0,00398107
2	sales	2	crime	51,4853585	0,00175131	0,00343109
2	sensitive dat	2	crime	69,9616081	0,00172414	0,00394833
2	threat	2	crime	67,2766054	0,0015456	0,00439435
2	policy maker	3	policy maker	76,2042898	0,00144718	0,00379194
2	wireless syst	3	policy maker	298,474283	0,00163132	0,00372035
15	network secu	4	network secu	3389,43488	0,00211416	0,02552103
10	5g mobile co	4	network secu	1772,38602	0,00178253	0,01693069
5	security	4	network secu	466,557795	0,0017452	0,00911436
5	security syste	4	network secu	655,36569	0,0018018	0,00845249
4	security and	4	network secu	427,433288	0,00195695	0,0064674
3	internet of th	4	network secu	187,574944	0,00163934	0,00564907
2	'current	4	network secu	57,484123	0,00153139	0,00425314
2	authenticati	4	network secu	174,75585	0,00172712	0,00313224
2	block-chain	4	network secu	53,8547544	0,0017094	0,00446226
2	blockchain	4	network secu	53,8547544	0,0017094	0,00446226
2	cellulars	4	network secu	283,911929	0,00195313	0,00407931
2	embedded s	4	network secu	412,520616	0,00194932	0,0043144
2	g-networks	4	network secu	31,5158946	0,00143472	0,00339052
2	multi-factor	4	network secu	39,3964535	0,0015456	0,00305966
2	next generat	4	network secu	40,9257675	0,00161551	0,00324821
2	privacy	4	network secu	77,7715169	0,00176056	0,00381302
2	queueing ne	4	network secu	31,9931556	0,00147275	0,00412159
2	security chal	4	network secu	60,0973502	0,00154083	0,00346138
2	security feat	4	network secu	122,114009	0,00166389	0,00403583
2	security mec	4	network secu	76,1115553	0,00167224	0,00331908
2	gateways (co	5	gateways (co	549,66829	0,0015456	0,00435038
2	prefix hijacki	5	gateways (co	729	0,00124844	0,00515265
16	mobile telec	6	mobile telec	2384,16209	0,00196078	0,02579595
14	mobile secur	6	mobile telec	1984,28752	0,0019305	0,02206488
14	wireless net	6	mobile telec	2360,41714	0,00196078	0,02215323
6	cellular netw	6	mobile telec	521,514262	0,00175439	0,00968915
4	mobile netw	6	mobile telec	192,791896	0,00169779	0,00660001
4	wireless tele	6	mobile telec	192,5057	0,00169779	0,00508662
3	global syster	6	mobile telec	135,873243	0,00158983	0,00410792
3	smartphones	6	mobile telec	272,182775	0,00181488	0,00593699
2	3g mobile co	6	mobile telec	61,8548793	0,00149477	0,00407548
2	3gpp	6	mobile telec	123,448999	0,00161551	0,00306748
2	automation	6	mobile telec	294,43921	0,00191571	0,00425481
2	cloning	6	mobile telec	31,8963051	0,0015361	0,00243922
2	denial-of-se	6	mobile telec	52,1961344	0,00162866	0,00355928
2	denial of ser	6	mobile telec	52,1961344	0,00162866	0,00355928
2	fraud preven	6	mobile telec	70,9169686	0,00167785	0,00355073
2	security vuln	6	mobile telec	16,6754065	0,00163666	0,00177088
2	fraud	7	security of da	200,946807	0,00171233	0,00542412
3	security of da	7	security of da	874,93534	0,00182149	0,00592234
2	internet	7	security of da	1619,58429	0,00175131	0,00621139
2	websites	7	security of da	270,606113	0,00185185	0,00485544
2	cellular oper	8	cellular oper	620,981148	0,00185874	0,00494072
2	commerce	8	cellular oper	138,720348	0,0015873	0,00436411
2	multimedia s	8	cellular oper	118,279348	0,0015674	0,00397821
2	data privacy	9	data privacy	227,291166	0,00161812	0,00343566