IST-Africa
IST-Africa 2026 Conference Proceedings
Miriam Cunningham and Paul Cunningham (Eds)
IST-Africa Institute and IIMC, 2026
ISSN: 2576-8581
ISBN: 978-1-905824-76-2
DOI: https://doi.org/10.67725/IST-Africa.2026.VCYR4216

A Comprehensive Analysis of Identity Theft: Definitions, Types, and Impacts

Cynthia S. NTSHNAGASE[1,2], Adriana A. STEYN[1]
[1]*University of Pretoria, Pretoria, 0001, South Africa*
[2]*The Council for Scientific and Industrial Research, Pretoria, 0001, South Africa*
Email: u25772342@tuks.co.za/smlambo@csir.co.za

Abstract: Identity theft is a complex and evolving phenomenon spanning physical, digital, algorithmic, and hybrid domains. This paper presents a systematic literature review following PRISMA guidelines to consolidate definitions, identify major and emerging subtypes, and assess impacts on individuals, organisations, and society. The study proposes a comprehensive definition that unifies fragmented and subtype-specific descriptions in the literature and explicitly encompasses document-based, child, offline, familial, criminal, synthetic, biometric, and algorithmic identity theft. We clarify that our bibliometric analysis reflects research attention rather than real-world incidence and explain the practical implications of this distinction. To enhance applied value, we discuss Africa-specific identity-management challenges, including persistent identity document fraud, and the rise of synthetic identities, and outline how the taxonomy supports national ID authorities, policy makers, financial institutions, and fraud-prevention bodies in South Africa and across the continent. Benefits include improved incident-response categorisation, more comprehensive compliance checklists, enhanced risk assessments, and clearer cross-sector communication. The review highlights a research focus bias toward financial theft and calls for further empirical work on underexplored subtypes (e.g., familial, child, algorithmic, deceased). We conclude with future research that triangulates bibliometric signals with incident statistics and operational data to inform resilient identity-management frameworks.

Keywords: Identity theft, definitions, types of identity theft, impact of identity theft

1. Introduction

Identity theft has become increasingly complex and common in both physical and digital environments [1]. The frequency of identity theft is driven by systemic requirements for identity verification in diverse service environments, both online and offline, using traditional or digital identity systems. Malicious actors exploit these verification processes by appropriating or manipulating the identities of legitimate individuals to obtain unauthorised access or illegal benefits [2]. Identity theft is generally referred to as the unauthorised acquisition of personal information, such as names, surname, identity number, account credentials and identification cards [3]. However, definitions of identity theft in the literature are often fragmented, narrow, or implicitly biased toward specific environments (e.g., financial systems or digital platforms). This creates ambiguities and exclusions that ripple through practice: incident misclassification, inconsistent reporting standards, gaps in risk assessment, and misaligned preventive controls across sectors [4]. These shortcomings are especially consequential in contexts where traditional documentation and offline impersonation remain prevalent alongside rapidly digitising ecosystems (e.g., South Africa and other African countries) [5] [6].

This study addresses this gap by proposing a comprehensive definition of identity theft. Additionally, by examining how impact differs across contexts and types. The outcome of this study will contribute to the proposal of inclusive solutions that consider the realities of South African society, while drawing on global best practices. This study closes the gap by addressing the following research questions: i): What are the definitions, types, and impacts of identity theft? ii) How can identity theft be defined comprehensively to encompass different types and impacts? The primary beneficiaries of this research are researchers, policy makers and regulators, national ID authorities, financial and insurance institutions, and cybersecurity and fraud-prevention professionals.

The structure of this paper is as follows. Section 2 presents the methodology on how the research was conducted, which includes data collection, inclusion, and exclusion criteria. Section 3 presents the findings based on the defined research questions. Section 4 is a discussion, and then the conclusions are provided in Section 5.

2. Methodology

This study explores the definition and classification of identity theft. To answer the defined research questions, this study adopts a systematic literature review approach, guided by the Preferred Reporting Items for Systematic Reviews and Meta Analysis (PRISMA) framework [7]. This methodology ensures a transparent, replicable and structured process for identifying and analysing sources of academic articles and reports to answer research questions. This framework is commonly used in studies that explore or explain scientific knowledge [8]. It comprises four primary stages, namely, identification, screening, eligibility, and inclusion.

During the identification stage, relevant articles, books and reports were obtained from academic databases through Google Schoolar and directly from Google Search, using a combination of keywords “identity theft”, “types of identity”.

All records were screened using defined inclusion and exclusion criteria to ensure quality and relevance.

- Inclusion: Peer-reviewed publications (journal articles, theses, books and conference articles), government or organisational reports, and industry white papers from recognised institutions, published in English between 2020 and 2025, and directly relevant to the research questions.
- Exclusion: Sources lacking academic credibility (e.g., blogs, personal websites), pre-2020 publications, non-English materials, duplicates, or inaccessible full texts.

Articles deemed eligible were evaluated for methodological consistency and relevance to research questions. This stage specifically addresses the second research question, which aims to identify and examine the various forms of identity theft. Each article was classified according to the forms of identity theft described.

The final selection was analysed to extract key definitions, types, and impacts of identity theft. The synthesis aligned the findings with the research questions and applied a quality assessment framework to ensure reliability and validity.

A PRISMA approach guided the process, as illustrated in Figure 1. Of 356 total records (332 database and 24 other sources (reports searched directly from Google)), 51 were removed as duplicates or inaccessible. After screening 305 titles and abstracts, 53 full texts were reviewed and 30 met the inclusion criteria for qualitative synthesis.

3. Findings

The final selection was analysed to extract key definitions, types, and impacts of identity theft. The synthesis aligned findings with the research questions and applied a quality assessment framework to ensure reliability and validity.

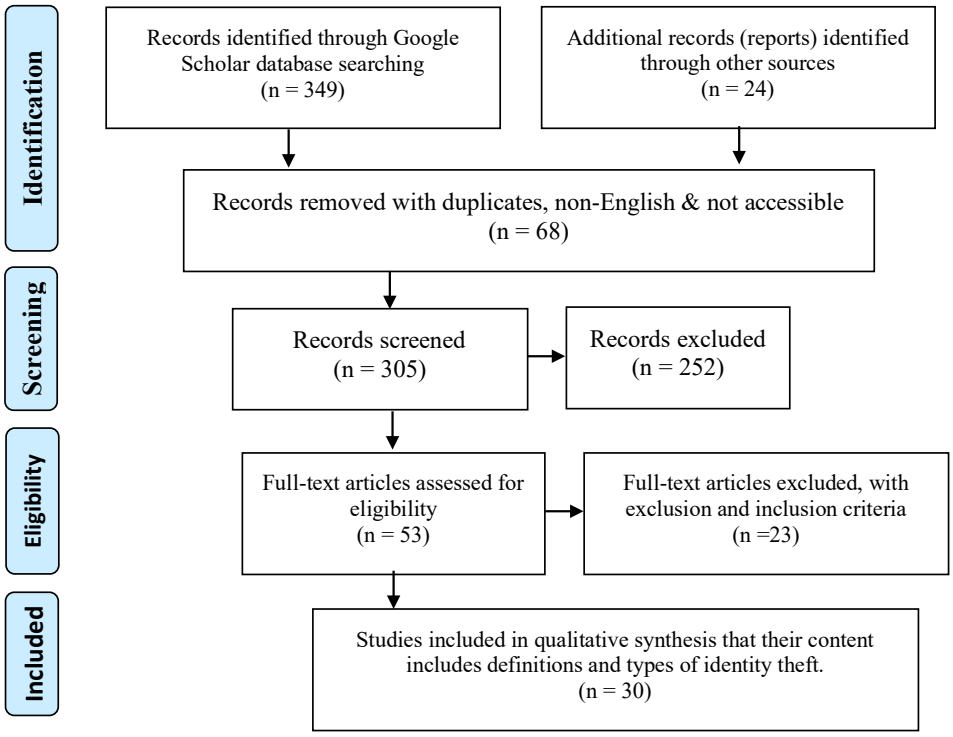

Figure 1: The PRISMA systematic process for selecting articles.

The literature review indicates substantial diversity in the way identity theft is defined and conceptualised. Among the 30 sources analysed, different types of identity theft were identified and explained. The sources analysed included 14 journal articles, 4 conference papers, 6 reports, 5 books or book chapters, and 1 academic thesis, as indicated in Table 1.

Table 1:Number of articles per type of publication.

Publication Type	Count
Journal Articles	14
Conference Proceedings	4
Reports	6
Book Chapter / Books	5
Thesis	1
Total	30

3.1 Definitions and Conceptualisation

There are different definitions of identity theft identified and discussed in the reviewed articles. Most studies described different types of identity theft based on the objectives of the study. Academic articles in [2], [3] and [6] provided detailed theoretical definitions, whereas industry reported like Entrust, South African Fraud Prevention Services (SAFPS) and KPMG, adopted pragmatic descriptions emphasising detection, prevention, and policy implications[1], [5] and [31].

3.2 Different types of identity theft

Table 2 shows different types of identity theft discussed in the reviewed articles. Analysis of the reviewed studies reveals a diverse spectrum of types of identity theft. Financial identity theft is the most frequently reported and discussed type, followed by child identity theft, medical identity theft, and synthetic identity theft. These four types collectively dominate the literature, indicating a convergence between traditional identity theft and digitally mediated forms.

Table 2: Different types of identity theft identified.

Identity Theft Type	Reference
Financial identity theft	[2], [5], [6], [11], [13], [15], [16], [17], [20], [21], [24], [25], [29], [32]
Child identity theft	[2], [4], [13], [21], [25], [27], [28], [29], [30], [31]
Medical identity theft	[2], [3], [6], [13], [21], [25], [29]
Synthetic identity theft	[1], [5], [4], [6], [12], [21], [28], [29], [31]
Criminal identity theft	[6], [10], [11], [13], [17], [21], [29]
Digital identity theft	[9], [14], [17], [19], [20], [22], [23]
Document-based identity theft	[5], [10],[16], [18], [26]
Familial identity theft	[3], [4], [8]
Social media identity theft	[5], [13], [17], [24]
Algorithmic identity theft	[9], [12], [20]
Biometric identity theft	[12], [20], [23]
Deceased identity theft	[2], [5]
Internal identity theft	[5],[11]
Employment identity theft	[5], [21]
Offline identity theft	[16], [26]
Tax identity theft	[25], [26]

Figure 2 visualises the share of reviewed sources that mention each subtype. It is a bibliometric indicator of research attention, not a measure of real-world prevalence. Financial identity theft accounts for the largest share of documented cases, reflecting its significant economic impact. Child and medical identity theft, although less prevalent, pose unique challenges due to delayed detection and implications for the integrity of healthcare. Synthetic identity theft, which combines real and fabricated data, is increasingly recognised for its complexity and detection difficulties.

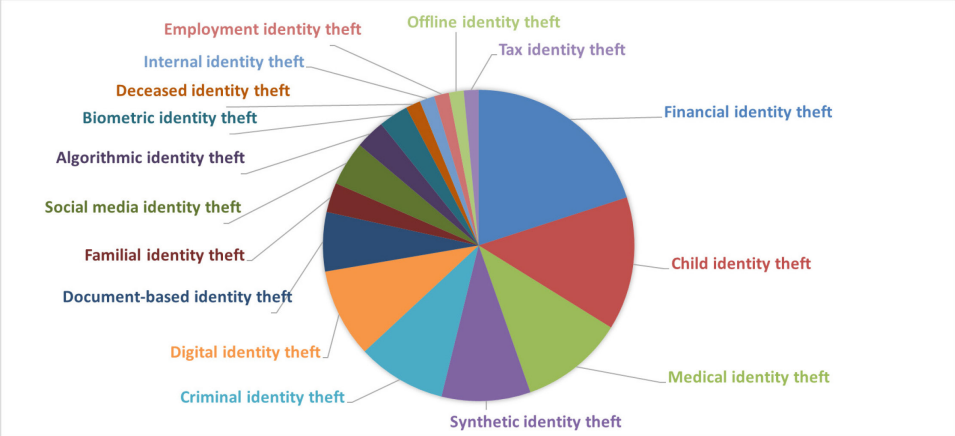

Figure 2: Bibliometric distribution of identity-theft subtypes in the reviewed literature (2020–2025).

Evolving types such as algorithmic and biometric identity theft, though less frequently discussed, underscore the evolving nature of identity-related crimes in the digital era. This diversity highlights the need for a comprehensive conceptual framework and comprehensive mitigation strategies that address both established and emerging threats.

4. Discussion

This section discusses identified definitions, different types of identity theft, and their impacts. This discussion is structured around the defined research questions.

4.1 Research Question 1: What are the definitions of identity theft, types, and impacts?

In this study, a comprehensive definition is proposed by first delineating various types of identity theft. Subsequently, the existing definitions are examined to determine the existing gaps and close the gaps through the formulation of an comprehensive definition.

The general definition of identity theft is predominantly described as the unauthorised acquisition or access of another person's PII. Researchers in [2] offer one of the most comprehensive definitions, describing identity theft as "the unauthorised acquisition, transfer, retention, or use of information relating to a natural or legal person for the purpose of committing further criminal acts such as theft, fraud, and other similar crimes through computer systems and networks." They distinguish between a narrow sense (obtaining data) and a broad sense (obtaining and using or selling such data on illicit markets). However, this definition excludes identity theft conducted without using a computer system and networks, such as the misuse of birth certificates (as an identity for children) related theft [29]. This definition also excludes other types of identity theft performed by criminals stealing credential of other criminals [15]. To understand the gap, this discussion firstly delves into definitions of different types of identity theft based on the findings.

The findings and analysis of identity theft types show a clear concentration of scholarly and professional attention on financially related crimes. This type of crime is referred to as financial identity theft, which is defined as the unauthorised acquisition and use of another person's financial credentials, such as banking details, credit card information, or account identifiers, with the intent to commit fraudulent transactions or obtain monetary benefits [2]. Financial identity theft emerges as the most frequently researched subtype [11]. The research reflects the high economic impact and global prevalence of financial theft, which often involves unauthorised transactions, credit misuse, and breach of banking details [5]. On the other hand, financial identity theft can be extended to a use of stolen personal identifiable information for the purpose of gaining finance [32]. This leads to an explanation of other types of identity theft, an example of this extended definition is when parents or guardians use identities of their children to obtain their financial gains such as opening credit accounts or opening loans, this is referred to as child identity theft [4].

Child identity theft may be performed not only by relatives but even strangers who have access to the child's identity [30]. This form of identity theft is particularly insidious due to the delayed detection of fraud, often discovered years after the initial compromise [27]. This theft exerts a detrimental influence on the professional and financial development of children, while simultaneously inducing stress within familial members [25]. Moreover, it affects associated organisations where stolen identities are utilised, potentially leading to financial losses [31]. The findings emphasise the need for proactive monitoring systems and legal safeguards to protect minor's identities, whose digital footprints are increasingly exposed through educational platforms and social media [13]. In addition, technology and regulation are required to protect children against the perpetrators related to a child [3].

Another type of identity theft mostly discussed is medical identity theft, representing a growing concern in health informatics [9]. Medical identity theft is defined as the unauthorised use of another person's health-related personal identifiable information, such as medical records, insurance or medical aid details or healthcare identifiers [25]. This type of identity theft primarily impacts individuals, as victims may face compromised medical records, incorrect treatments and financial liabilities [2]. However, it also significantly affects organisations, such as healthcare providers and medical insurance companies, by introducing fraudulent claims, disrupting patient data integrity, and increasing operational costs [13]. The digitisation of healthcare records has expanded the attack surface for malicious actors, leading to fraudulent online insurance claims and potentially life-threatening inaccuracies in patient records [6]. This indicates the urgent need for secure

health data infrastructure and interdisciplinary research bridging cybersecurity, healthcare, and ethics.

Emerging identity theft types such as synthetic, criminal, and digital identity theft, reflect the evolving nature of identity crimes in the digital age [1]. Synthetic identity theft involves the creation of fictitious identities using real and fabricated data, for example, using a legitimate national ID number with a fake name or address to open accounts, apply for loans or commit fraud [31]. Its complexity and detection challenges call for advanced analytics and machine learning-based detection systems. Its impact varies across levels, such as individuals often face delayed discovery, credit damage, and financial stress, organisations incur losses from unpaid loans and increased fraud risk due to identities passing verification checks; and society experiences weakened trust in identity systems, complex law enforcement challenges, and heightened risks amplified by AI-driven platforms, necessitating advanced analytics and machine learning for detection [11].

Criminal identity theft illustrates the legal and reputational consequences of identity misuse, where victims may be falsely associated with criminal records [6]. Unlike financial or synthetic identity theft, its primary purpose is to evade accountability rather than gain money [17]. The impacts on individuals may suffer wrongful arrests, reputational harm, and costly legal battles, while involved organisations, including law enforcement and judicial systems, face resource-intensive investigations and delays in justice, and society experiences weakened trust in identity verification and legal systems, along with systemic vulnerabilities that criminals exploit, underscoring the need for stronger identity validation and inter-agency data sharing [21], [29].

Digital identity theft captures the vulnerabilities of online authentication systems and the growing reliance on digital credentials in both public and private sectors [9]. Digital identity theft refers to the unauthorised capture or misuse of personal or digital identifiers, such as usernames, passwords, biometric profiles, or online credentials, within digital platforms and authentication systems [14]. It exploits vulnerabilities in online services, social media, and cloud-based environments, often leading to account takeovers, fraudulent transactions, and privacy breaches [19]. The impacts vary across levels, the individuals face financial loss, reputational harm, and compromised privacy. Involved organisations incur costs from fraud remediation, data breaches, and reputational damage; and society experiences weakened trust in digital ecosystems and heightened cybersecurity risks, amplified by the growing reliance on AI-driven and interconnected identity systems [20], [22].

Moderately studied types such as document-based identity theft and social media identity theft remain relevant, particularly in contexts where physical documentation and online impersonation are prevalent [10]. Document-based identity theft involves the misuse or forgery of physical identity documents, such as ID cards, passports, or birth certificates, to impersonate individuals or create fraudulent identities [5]. Its impacts include financial loss and reputational harm for victims, operational risks for organisations relying on document verification, and systemic vulnerabilities in regions where physical documentation remains dominant [26]. These findings suggest that while digital threats dominate the discourse, traditional and hybrid forms of identity theft persist and require continued vigilance. Social media identity theft occurs when attackers impersonate individuals on social platforms by hijacking accounts or creating fake profiles [13]. This often leads to reputational damage, privacy breaches, and scams targeting victims' contacts [17]. Organisations face brand impersonation risks, while society experiences increased misinformation and erosion of trust in online interactions [24].

Specialised and underexplored categories such as familial identity theft, algorithmic identity theft, and biometric identity theft, point to emerging threats that intersect with artificial intelligence, interpersonal dynamics, and biometric technologies [4]. Familial

identity theft occurs when a family member or close relative uses another person's identity, often a child's or dependent's, to gain financial benefits or evade obligations [3]. Its impacts include long-term credit damage and emotional strain for victims, financial liability for families, and legal complications for institutions handling fraudulent accounts [30].

Algorithmic identity theft is an emerging form of identity crime that exploits weaknesses in Artificial Intelligence-driven identity verification systems. Attackers manipulate algorithms used for authentication or fraud detection to bypass security checks or create fraudulent profiles [20]. Unlike traditional identity theft, which targets personal data directly, algorithmic identity theft focusses on exploiting the logic and decision-making processes of automated systems. It differs from synthetic identity theft because synthetic identity theft creates a fictitious identity using real and fabricated data, whereas algorithmic identity theft goes further by attacking the underlying verification algorithms themselves, enabling fraud even when identity data appears legitimate [18]. This makes it more sophisticated and harder to detect, as it undermines the integrity of automated identity management frameworks rather than just exploiting data gaps. [12]. This emerging threat impacts individuals through privacy breaches, organisations via compromised security systems, and society by eroding trust in automated identity management frameworks [19].

Biometric identity theft involves stealing or forging biometric data, such as fingerprints, facial scans, or voice patterns, to impersonate individuals [20]. Its impacts include irreversible loss of privacy for victims, high remediation costs for organisations, and systemic risks as biometric technologies become central to identity verification [23]. These areas are currently underrepresented in the literature but are likely to grow in significance as AI and biometric systems become more integrated into identity verification processes.

Other low-frequency subtypes, including internal identity theft, employment identity theft and offline identity theft, which highlight the continued relevance of organisational and physical vulnerabilities in identity management [11]. Employment identity theft occurs when someone uses another person's identity, such as national ID numbers, to gain employment or work-related benefits [5]. Impacts include tax and legal complications for victims, compliance risks for employers, and systemic vulnerabilities in labour and tax systems [21]. Internal identity theft happens within organisations, where employees misuse access privileges to steal or manipulate identity data [11]. This leads to privacy breaches and reputational harm for individuals, poor service delivery to citizens, operational and compliance risks for organisations, and broader trust issues in corporate governance [5]. Offline identity theft involves impersonation or misuse of identity in physical environments, such as forging signatures or using stolen documents in face-to-face transactions [26]. Its impacts include financial loss and reputational damage for victims, verification challenges for organisations, and persistent vulnerabilities in regions reliant on manual identity checks [16].

Conclusively, deceased identity theft and tax identity theft, are among the least represented in the literature [2]. Despite their low research attention, these subtypes have significant implications for public trust and institutional integrity. Deceased identity theft exploits gaps in death record synchronisation, while tax identity theft targets government systems, often resulting in delayed victim recovery and financial loss [5]. Their limited visibility may reflect data scarcity rather than a lack of importance. Deceased identity theft occurs when criminals exploit gaps in death record synchronisation to use identities of deceased individuals for fraudulent activities [2]. Impacts include financial loss for estates, operational challenges for institutions, and weakened public trust in civil registration systems. Tax identity theft targets government systems by using stolen or fabricated identity information to file fraudulent tax returns or claim benefits [25]. Victims face delayed refunds and financial stress, organisations incur administrative burdens, and society suffers from reduced confidence in tax systems.

4.2 Proposed Comprehensive Definition

Different authors have provided general definitions of identity theft. In [24] authors build their definition on Federal Trade Commission and Bureau of Justice Statistics definitions, and define identity theft as "a fraud committed or attempted using a person's identifying information without authority," encompassing unauthorised access or attempted use of existing accounts, personal information, or the creation of new accounts.

Shah & Capstone [6], Okeke & Eiza [11] describe identity theft as the illicit acquisition of another's personal or organisational data without consent, focusing on theft of names, identification numbers, financial details, or biometric identifiers.

Some definitions rely on the advancement of technology, leaving out the physical traditional and off-line forms of identification, this includes studies in [12] and [9], where researchers emphasise the role of digital identity theft, defining it as the unlawful capture of personal or digital identifiers, including algorithmic and biometric profiles, for malicious purposes. While industry reports such as Entrust [1], SAFPS [5], and Smile ID [22] broaden this view to include synthetic identity theft, in which real and fabricated data are combined to create new, hybrid identities. Other scholars, such as in [13] and [32], link identity theft directly to financial credential theft, especially in banking and payments ecosystems.

In a collective analysis, these perspectives outline identity theft as the unlawful or unauthorised procurement of personal related information, which exclude other types of identity theft. Thus, a comprehensive, integrative definition that reflects these varied interpretations can be proposed as follows:

> *Identity theft is the unauthorised acquisition, access, possession, transfer, or misuse of a natural or legal person's identifying attributes, across physical, digital, financial, biometric, or algorithmic contexts, with the intent to obtain unlawful benefit, evade accountability, or enable further criminal activity.*

This definition covers traditional and offline forms (e.g., document-based fraud and in-person impersonation), digitally mediated forms (e.g., account takeover, credential abuse), emerging AI and analytics-enabled abuses (e.g., algorithmic manipulation, synthetic identities), and inter-personal or insider-facilitated forms (e.g., familial, internal).

This encompasses both traditional forms (such as document-based and offline impersonation) and digital forms (including algorithmic and biometric exploitation), as well as emerging types like synthetic identity theft, which combines real and fabricated data, and internal or familial misuse. The proposed comprehensive definition bridges the current research perspectives, providing a unified conceptual foundation to understand the evolving ecosystem of identity theft in both physical and digital contexts.

4.3. Benefits

Identity management in Africa, particularly in South Africa, operates within a dual ecosystem where traditional document-based identification coexists with expanding digital and mobile identity systems. This creates distinct vulnerabilities. Document-based identity theft remains widespread due to reliance on physical credentials such as ID books, ID cards, and birth certificates, which are susceptible to theft, forgery, and alteration. These weaknesses directly intersect with child identity theft, as fraudulent use or manipulation of birth certificates enables offenders to create or exploit children's identities for financial or administrative gain.

Within this context, the proposed comprehensive taxonomy provides value to a diverse set of stakeholders. Researchers benefit from a unified conceptual structure that supports comparative studies and measurement frameworks. Policy makers and regulators gain consistent terminology for legislation, reporting, and oversight. National ID authorities can apply clearer categorisation methods to improve verification, data-sharing practices, and registry reconciliation. Financial institutions and insurers are supported through harmonised

fraud typologies that enhance case management and reduce loss attributed to misclassification. Telecommunications and mobile-money providers can use the taxonomy to refine SIM-swap countermeasures and strengthen identity-linking across channels. Cybersecurity and fraud-prevention professionals gain a foundation for developing more robust detection rules, response playbooks, and cross-sector coordination.

The practical benefits include more accurate incident-response categorisation, improved compliance and assurance frameworks, stronger risk-assessment models across both offline and digital attack paths, enhanced cross-sector communication, and clearer benchmarking for monitoring fraud trends and public-reporting practices.

5. Conclusions

This study consolidates fragmented descriptions of identity theft into a comprehensive definition and taxonomy that spans physical, digital, algorithmic, and hybrid forms. This is a PRISMA-guided review, showing that scholarly attention clusters around financial identity theft, while important subtypes, such as familial, child, algorithmic, and deceased identity theft, remain underexplored. It has been clarified that this visual summary reflects bibliometric attention, not population incidence, and it is recommended that for future works the literature will be integrated with operational incident data. To improve practical relevance, Africa-specific identity-management challenges were articulated and discussed on how the taxonomy supports national ID authorities, policy makers, financial institutions, telecoms, and fraud-prevention bodies in standardising incident categorisation, tightening controls, and aligning cross-sector communication. By providing a shared definitional foundation, the study aims to reduce ambiguity, enhance comparability, and inform the design of resilient identity-management frameworks suited to both traditional documentation environments and rapidly digitising ecosystems.

Acknowledgements

Declaration of use of content generated by Artificial Intelligence (AI) (including but not limited to Generative-AI) in the paper

The authors acknowledge the use of content generated by AI (including but not limited to text) in the paper entitled " An Comprehensive Analysis of Identity Theft: Definitions, Types, and Impacts" in the following ways:
Open Writefull - used for grammar and to rephrase some sentences for clarity.

References

[1] Entrust, "Identity fraud report," Entrust Cybersecurity Institute, 2025.
[2] B. Merdovic and B. Jojanovic, "Understanding identity theft and fraud," Kultura Polisa, vol. 21, pp. 17–43, 2024.
[3] Y. Irvin-Erickson, "Identity fraud victimization: a critical review of the literature of the past two decades," Crime Science, vol. 13, pp. 1–26, 2024.
[4] B. Green, S. Gies, A. Bobnis, N. Leeper-Piquero, A.R. Piquero and E. Velasquez, "Exploring identity-based crime victimizations: Assessing threats and victim services among a sample of professionals," Deviant Behaviour, vol. 42, pp. 1086–1099, 2021.
[5] SAFPS, "South African Fraud Prevention System 2024 Annual Report," SAFPS, 2025.
[6] S. Shah and A. Capstone, "Identity theft and prevention," New York: Routledge, 2023.
[7] M.J. Page, J.E. Mckenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, L. Shamseer, J.M. Tetzlaff, E.A. Akl, S.E. Brennan, R. Chou, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, vol. 372, 2021.
[8] R.B. Sağlam, V. Miller and V.N.L. Franqueira, "A systematic literature review on cyber security education for children," Computers & Security, Elsevier, 2023.
[9] E. Huseynov, "Chapter 60 - Identity Theft," in Computer and Information Security Handbook (Fourth Edition), J.R. Vacca, Morgan Kaufmann, pp. 993–1006, 2025.

[10] S. Baechler, "Document fraud: Will your identity be secure in the twenty-first century?" European Journal on Criminal Policy and Research, vol. 26, pp. 379–398, 2020.
[11] R. I. Okeke, and M. H. Eiza. “The application of role-based framework in preventing internal identity theft related crimes: A qualitative case study of UK retail companies.” Information Systems Frontiers, vol. 25, no. 2, pp. 451-472, Springer, 2023.
[12] T. Gorichanaz, "Data selves and identity theft in the age of AI," in The De Gruyter Handbook of Artificial Intelligence, Identity and Technology Studies, A. Elliott, Walter de Gruyter GmbH & Co KG, pp. 181–196, 2024.
[13] H.M. Salman, "Identity theft in the banking system," in Online Identity - An Essential Guide, London: IntechOpen, 2024.
[14] S.A.A. Shah, "Digital identity theft and privacy concerns in the metaverse," Journal of Social Sciences and Management Studies, vol. 1, 2024.
[15] J. Brensinger, "Identity theft, trust breaches, and the production of economic insecurity," American Sociological Review, vol. 88, pp. 844–871, 2023.
[16] A.J. Vanhee and R. McNealey, "Individual residence and identity theft: how residential characteristics shape exposure and risk of offline and online identity theft victimization," Journal of Financial Crime, vol. 31, pp. 594–607, 2023.
[17] S.N. Prasetyo and C. Monique, "Identity theft and personal data protection in Indonasian Criminal Law," in Proceedings of the International Conference on Law Reform (5th Inclar 2024), S.A. Fatih, H. Tegnan, M.H.B.M. Said, N.R. Yunus, A. Saeed and F.J. Fernhout, Springer Nature, 2025.
[18] C.A.L. Montesinos and E.J.E. Cárdenas, "Verification of peruvian identity document fraud through OCR, hash algorithm, and simulated blockchain database," in Knowledge Management and Artificial Intelligence for Growth: Cases from Emerging and Developed Economies, I. Bianchi and G.A. Dávila, Cham: Springer Nature Switzerland, pp. 165–188, 2024.
[19] N. Khalifa, W. Elmedany and S. Sharif, "Leveraging digital identity and open banking data for fraud prevention in the financial industry," in 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 286–291, 2024.
[20] A.Y.A.B. Ahmad, "Fraud prevention in insurance: Biometric identity verification and AI-based risk assessment," in 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), pp. 1–6, 2024.
[21] S.R. Ahmed, “Preventing identity crime: identity theft and identity fraud: An identity crime model and legislative analysis with recommendations for preventing identity crime,” Leiden: Brill Nijhoff, pp. 1 online resource (xiii, 765 pages), 2020.
[22] Smile ID, "2025 Digital identity: Fraud in Africa report," Nairobi: Smile identity, 2025.
[23] T. Jabeen, Y. Mehmood, H. Khan, M.F. Nasim and S.A.A. Naqvi, "Identity theft and data breaches how stolen data circulates on the dark web: A systematic approach," Spectrum of Engineering Sciences, vol. 3, pp. 143–161, 2025.
[24] E. Harrell and A. Thompson, "Victims of identity theft, 2021," Bureau of Justice Statistics, 2023.
[25] H. M. Mosharraf and H. Fatemeh, "Exploring identity theft: Motives, techniques, and consequents on different age groups," Journal of Innovations in Computer Science and Engineering (JICSE), vol. 1, pp. 63–74, 2023.
[26] D.C. Pheiffer, and J. Naude, "An Exploration of the use of software technology to combat identify theft in South Africa," International Journal of Social Science Research and Review, vol. 7, pp. 191–202. 2024.
[27] Mike Bolhuis, "Project: Child identity theft," Mike Bolhuis specialised security services, Pretoria, 2024.
[28] N.L. Piquero, A.R. Piquero, S. Gies, B. Green, A. Bobnis and E. Velasquez, "Preventing identity theft: Perspectives on technological solutions from industry insiders," Victims and Offenders, vol. 16, pp. 444–463, Routledge, 2021.
[29] E. Huseynov and J.R. Vacca, "Identity theft," in Computer and Information Security Handbook 4th edition, Elsevier Science & Technology, 2024.
[30] Javelin, "Child identity fraud: The perils of too many screens and social media," Javelin Strategy & Research, 2022.
[31] KPMG, "Synthetic-identity-fraud: A $6 billion problem," Klynveld Peat Marwick Goerdeler, 2022.
[32] N. Jahan Sarna, F. Ahmed Rithen, U. Salma Jui, S. Belal, A. Amin, T. Kabir Oishee and A.K.M. Muzahidul Islam, "AI Driven Fraud Detection Models in Financial Networks: A Comprehensive Systematic Review," IEEE Access, vol. 13, pp. 141204–141233, 2025.
[33] H. Ho, R. Ko and L. Mazerolle, "Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review," Computers & Security, vol. 115, Art. no. 102611, 2022.