International Journal of Safety and Security Engineering
Vol. 16, No. 6, June, 2026, pp. 1343-1359
Journal homepage: http://iieta.org/journals/ijsse

Identity Theft in Cybersecurity: A Systematic Literature Review of Attack Mechanisms, Identity Management Systems, Technological Solutions, and Human Factors

Martanto[1*], Dadang Sudrajat[2], Khaerul Anam[2], Arif Rinaldi Dikananda[3], Fatihanursari Dikananda[2]

[1] Department of Informatics Management Study Program, STMIK IKMI Cirebon, Cirebon 45131, Indonesia
[2] Department of Informatics Engineering, STMIK IKMI Cirebon, Cirebon 5131, Indonesia
[3] Software Engineering Study Program Department, STMIK IKMI Cirebon, Cirebon 45131, Indonesia

Corresponding Author Email: martantomusijo@gmail.com

Copyright: ©2026 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.160616

Received: 27 April 2026
Revised: 10 June 2026
Accepted: 22 June 2026
Available online: 30 June 2026

Keywords:
identity theft, cybersecurity, digital identity, identity management, phishing attacks, blockchain identity

ABSTRACT

Identity theft has become an increasingly complex cybersecurity challenge driven by the rapid expansion of digital ecosystems, artificial intelligence, cloud computing, IoT, and metaverse technologies. This systematic literature review (SLR) synthesizes recent research on identity theft by examining attack mechanisms, identity management systems, technological mitigation solutions, and human behavioral factors. Using the PRISMA framework, 49 Scopus-indexed studies published between 2021 and 2026 were systematically analyzed. The findings reveal that identity theft has evolved into a multidimensional socio-technical phenomenon characterized by sophisticated threats such as phishing, credential stuffing, deepfake impersonation, malware-based attacks, and large-scale data breaches. The review further shows that centralized identity systems face limitations related to privacy protection, interoperability, and vulnerability to credential compromise, particularly in distributed digital environments.

1. INTRODUCTION

1.1 Background and significance

The rapid advancement of digital technologies has fundamentally transformed how individuals, organizations, and governments manage and utilize digital identities. The proliferation of online services including e-commerce, mobile banking, cloud computing, and national digital identity systems has significantly increased reliance on identity-based authentication mechanisms. However, this transformation has simultaneously expanded the attack surface, making digital identities more vulnerable to exploitation. In this context, identity theft has emerged as one of the most critical threats in modern cybersecurity.

Recent studies indicate that identity theft has evolved into a sophisticated cyber threat driven by large-scale data breaches, social engineering, and AI-enabled impersonation attacks [1, 2]. The widespread adoption of digital services has increased exposure to phishing and credential based attacks, while darknet marketplaces have facilitated the rapid commercialization of stolen identities, accelerating cybercrime globally [3]. Moreover, mobile ecosystems and application level vulnerabilities further exacerbate risks, making personal data highly susceptible to compromise [4]. These developments illustrate that identity theft is no longer an isolated incident but a systemic issue embedded within digital infrastructures.

In addition, the emergence of interconnected technologies such as the Internet of Things (IoT), artificial intelligence (AI), cloud computing, and metaverse platforms has intensified identity-related risks. IoT environments introduce weak authentication mechanisms and large-scale device connectivity, increasing exposure to identity exploitation [5]. AI technologies, while enabling automation, are increasingly leveraged by attackers for deepfake based impersonation and identity inference attacks [6, 7]. Furthermore, immersive digital environments such as the metaverse introduce persistent and behavioral identities, raising concerns over unauthorized identity replication and privacy violations [8, 9]. These developments collectively highlight the growing complexity of identity theft in modern digital ecosystems.

Identity theft has significant economic, social, and security implications. Financial losses, reputational damage, and privacy violations are among the most immediate consequences affecting individuals and organizations. At a broader level, identity theft undermines trust in digital systems and threatens the stability of digital economies. The increasing reliance on digital identity frameworks in critical sectors such as healthcare, finance, and government services further amplifies the importance of robust identity protection mechanisms.

The relevance of identity theft is particularly pronounced in the era of emerging technologies. The convergence of AI, IoT, and metaverse platforms creates complex and dynamic threat environments where traditional security approaches are insufficient. As digital identities become more integrated into everyday activities, ensuring their security becomes a fundamental requirement for sustainable digital transformation.

1.2 Existing literature and research gaps

Existing literature has approached identity theft from multiple perspectives, including technical, behavioral, and contextual dimensions. From a technical standpoint, research highlights the evolution of attack vectors such as phishing, credential stuffing, and AI driven social engineering, demonstrating how attackers exploit system vulnerabilities and weak authentication mechanisms [10, 11]. Behavioral studies emphasize user susceptibility, showing that cognitive biases, lack of awareness, and risky online behaviors significantly increase identity theft risks [12, 13]. Meanwhile, contextual research situates identity theft within broader socio-technical systems, including digital transformation, regulatory frameworks, and organizational environments [14, 15].

Furthermore, technological countermeasures such as machine-learning-based detection systems and blockchain-based identity management solutions have been widely proposed to mitigate identity theft [16, 17]. While these approaches demonstrate promising results, the literature remains fragmented, with studies often focusing on isolated aspects rather than providing an integrated understanding of the phenomenon.

Despite the growing body of research, several limitations persist in the study of identity theft. A major issue is the lack of standardized datasets and benchmarking frameworks, which limits the comparability and reproducibility of research findings [18, 19]. Additionally, existing studies tend to focus heavily on technical detection mechanisms while underexploring socio behavioral factors such as user behavior and attacker psychology [20, 21].

Another critical gap lies in the limited integration of interdisciplinary approaches. Current research rarely combines technological, behavioral, and policy perspectives into a unified framework, resulting in fragmented solutions [22]. Moreover, emerging threats such as deepfake enabled identity fraud and synthetic identities remain insufficiently explored in empirical studies [23]. Existing solutions also face challenges related to scalability, real time implementation, and long term effectiveness [24, 25].

These limitations indicate that identity theft is not merely a technical problem but a complex, multi dimensional issue requiring integrated analysis and holistic solutions.

1.3 Objectives, research questions, and scope of the review

The primary objective of this systematic literature review (SLR) is to develop a comprehensive understanding of identity theft in cybersecurity by integrating multiple perspectives from existing research. Specifically, this study aims to:

(1) Identify and classify identity theft threats and attack mechanisms.
(2) Analyze identity management systems and digital identity technologies.
(3) Evaluate technological solutions for mitigating identity theft.
(4) Examine the role of human factors in identity-related risks.
(5) Develop an integrated conceptual framework linking these elements.

To achieve these objectives, this review addresses the following research questions, which guide the literature search, study selection, data extraction, thematic synthesis, and discussion.

This review focuses on peer reviewed studies related to identity theft in cybersecurity, covering various technological contexts such as IoT, cloud computing, artificial intelligence, and metaverse environments. The analysis includes both empirical and conceptual studies published in recent years to capture the latest developments in the field. Only English language articles within the domain of computer science and related disciplines are considered.

The research questions guiding this systematic literature review are summarized in Table 1. These questions define the scope of the review and provide the foundation for the literature search, study selection, data extraction, thematic synthesis, and discussion.

Table 1. Research question

Code	Research Question
RQ1	What types of identity theft threats and attack mechanisms are reported in recent cybersecurity literature?
RQ2	What identity management systems and digital identity technologies are used to prevent or reduce identity theft risks?
RQ3	What technological solutions have been proposed to detect, prevent, or mitigate identity theft?
RQ4	How do human factors influence identity theft vulnerability and mitigation effectiveness?
RQ5	What research gaps and future directions can be identified from the reviewed literature?

Although the review covers multiple domains including identity theft attack mechanisms, identity management systems, technological mitigation solutions, human factors, governance, and emerging digital environments, these topics were not examined as independent research streams. Instead, they were analyzed through a unified identity theft perspective.

The analytical focus of this review is the identity theft lifecycle, which consists of four interconnected dimensions: (1) attack mechanisms used to compromise digital identities, (2) identity management architectures that provide protection or create vulnerabilities, (3) technological mitigation approaches designed to detect, prevent, or respond to identity-related threats, and (4) human and organizational factors influencing both attack success and defensive effectiveness.

Consequently, technologies such as blockchain, Self-Sovereign Identity (SSI), artificial intelligence, IoT, cloud computing, and metaverse platforms were included only when they directly influenced identity theft risks, identity protection mechanisms, or identity management processes. This analytical structure enabled the integration of diverse research areas into a coherent socio-technical framework explaining how identity theft emerges, evolves, and can be mitigated across modern digital ecosystems.

1.4 Contributions and organization of the paper

This study contributes to the literature in several ways. First, it provides an integrated synthesis of identity theft research across technical, behavioral, and contextual dimensions. Second, it develops a comprehensive conceptual framework that links attack mechanisms, identity management systems, and human factors. Third, it identifies key research gaps and proposes directions for future research. Finally, it offers practical insights for organizations and policymakers in designing more effective identity protection strategies.

The remainder of this paper is organized as follows. Section 2 describes the research methodology, including search strategy, inclusion criteria, and the PRISMA based selection process. Section 3 presents the theoretical background related to identity management and cybersecurity threat models. Section 4 provides a thematic synthesis of the findings across four key areas: attack mechanisms, identity management systems, technological solutions, and human factors. Section 5 discusses the implications of the findings, and Section 6 concludes the study with key insights and future research directions.

2. METHODS

2.1 Search strategy

A SLR methodology was employed to identify, analyze, and synthesize relevant studies on identity theft in cybersecurity. The review followed a structured and reproducible approach aligned with established guidelines for systematic reviews in information systems and cybersecurity research. The search process was conducted using the Scopus database as the primary source due to its comprehensive coverage of high impact, peer reviewed journals.

The search query was constructed using Boolean operators to capture key concepts related to identity theft and cybersecurity, including variations such as digital identity, identity management, and identity security, for more complete boolean keywords as follows TITLE-ABS-KEY(("identity theft" OR "digital identity" OR "identity management" OR "identity security" OR "identity fraud") AND ("cybersecurity" OR "information security" OR "network security" OR "cyber attack*" OR "cyber threat*")). The final search string combined identity-related terms with cybersecurity related keywords to ensure broad yet relevant coverage of the literature. The search was limited to publications between 2021 and 2026 to capture recent developments in emerging technologies and identity-related threats.

This approach is consistent with recent studies emphasizing the importance of structured keyword design and database selection to capture evolving threats such as phishing, credential stuffing, and AI driven identity attacks [20, 26]. Furthermore, focusing on high quality indexed databases enhances the reliability and academic rigor of the selected literature [27].

To minimize the inclusion of studies discussing digital identity in a general or administrative context, an additional relevance filtering procedure was applied during the screening and eligibility stages. Although broad identity-related keywords such as “digital identity” and “identity management” were included to capture emerging identity protection technologies, studies were retained only when they explicitly addressed identity theft, identity fraud, authentication vulnerabilities, credential compromise, cyberattacks targeting identity systems, or identity protection mechanisms.

Articles focusing exclusively on digital transformation, e-government services, digital citizenship, identity policy, or identity management implementation without a clear connection to cybersecurity threats or identity theft risks were excluded. This relevance refinement ensured that the final dataset remained aligned with the review objective of understanding identity theft within cybersecurity environments rather than digital identity management in general.

2.2 Inclusion and exclusion criteria

To ensure the relevance and quality of the selected studies, rigorous inclusion and exclusion criteria were applied. The inclusion criteria required studies to be peer reviewed journal articles published between 2021 and 2026, written in English, and indexed in high impact databases such as Scopus. Additionally, studies were required to focus explicitly on identity theft, authentication vulnerabilities, cyberattack mechanisms, or identity protection technologies. Only studies demonstrating methodological transparency and reproducible results were included.

Furthermore, studies with a minimum citation threshold were prioritized to ensure scholarly impact, and open access publications were preferred to facilitate accessibility and verification. These criteria align with recent systematic reviews that emphasize methodological rigor, transparency, and relevance in cybersecurity research [27-29].

Exclusion criteria were applied to filter out non peer reviewed publications, conference abstracts without full papers, editorials, and non English studies. Articles lacking clear relevance to identity theft or cybersecurity frameworks were also excluded. Additionally, studies from discontinued journals or those with insufficient citation metrics were omitted to maintain quality standards. This structured filtering process enhances the reliability and comparability of the final dataset. For further details, please see Table 2.

Table 2. Inclusion and exclusion criteria

Criteria	Inclusion	Exclusion
Year	2021–2026	Outside 2021–2026
Language	English	Non English
Document Type	Peer reviewed journal article	Editorial, book chapter, conference abstract, non peer reviewed paper
Database	Scopus-indexed	Non Scopus
Topic	Identity theft, digital identity, IAM, cyberattack mechanisms, identity protection	Articles not discussing identity theft or cybersecurity
Field	Computer Science and related fields	Outside the scope of cybersecurity/digital identity

2.3 Screening and selection process

The study selection process followed the PRISMA framework, which ensures transparency and reproducibility in systematic reviews. The process consisted of four main stages: identification, screening, eligibility, and inclusion.

During the identification phase, records were retrieved from the Scopus database using the predefined search query. Duplicate records and irrelevant entries were removed before proceeding to the screening phase. In the screening stage, titles and abstracts were reviewed to assess relevance based on the inclusion criteria. The eligibility phase involved a full text assessment of the remaining studies to ensure alignment with the research objectives. Finally, only studies meeting all criteria were included in the final review.

The application of PRISMA enhances methodological rigor by enabling systematic filtering and clear documentation of

the selection process [27]. Previous studies have demonstrated that PRISMA based approaches improve consistency and reproducibility in cybersecurity research, particularly when combined with keyword refinement and bibliometric filtering [29, 30]. Additionally, PRISMA flow diagrams facilitate the identification and exclusion of low quality studies, ensuring that only relevant and high impact research is included.

To improve methodological transparency, the screening and selection process was conducted independently by two reviewers. During the title and abstract screening stage, each retrieved record was evaluated against the predefined inclusion and exclusion criteria. Articles that clearly focused on digital identity, identity management, authentication systems, cybersecurity threats, identity fraud, or identity theft were retained for further assessment. Studies addressing digital identity solely from administrative, social, legal, or e-government perspectives without discussing cybersecurity threats, identity misuse, authentication vulnerabilities, or identity theft risks were excluded.

In the eligibility stage, full-text articles were independently assessed by both reviewers. Disagreements regarding study relevance or eligibility were resolved through discussion and consensus. When consensus could not be reached, a joint reassessment of the article was performed until agreement was obtained. Reasons for exclusion during the full-text assessment included: (1) insufficient focus on identity theft or identity-related cyber threats, (2) lack of cybersecurity relevance, (3) absence of methodological information, and (4) duplication of research findings across multiple publications.

The final inclusion decision required that each article satisfy all eligibility criteria and contribute directly to at least one of the review themes: identity theft attack mechanisms, identity management systems, technological mitigation solutions, or human factors influencing identity security.

2.4 Quality assessment

To ensure the validity, reliability, and methodological rigor of the synthesized findings, a structured quality assessment process was conducted for all selected studies. Unlike PRISMA, which primarily functions as a reporting guideline for systematic reviews rather than an assessment instrument for individual studies, this review adopted a simplified and operational quality evaluation framework specifically designed for the objectives of this SLR. Nevertheless, PRISMA remained essential for ensuring transparency and reproducibility in the article selection and reporting process, while AMSTAR 2 and ROBIS were considered as supporting references for understanding methodological quality and risk of bias evaluation in evidence synthesis research [29, 30].

The quality assessment process focused on evaluating the relevance, methodological transparency, analytical rigor, and contribution of each selected study to the topic of identity theft and cybersecurity. Each article was independently reviewed using five predefined assessment criteria adapted from recent systematic review practices in cybersecurity and information systems research [24, 31]. The criteria are presented in Table 3.

Each criterion was evaluated using a three-point scoring scale:

0 = criterion not addressed,
1 = partially addressed,
2 = fully addressed.

Thus, each study could achieve a maximum total score of 10 points. Based on the cumulative score, the studies were categorized into three quality levels as shown in Table 4.

To improve objectivity and reduce reviewer bias, the quality assessment process was conducted independently by two reviewers. Disagreements in scoring were resolved through discussion and consensus evaluation. When differences persisted, the final score was determined through joint reassessment of the article content and methodological contribution.

Table 3. Quality assessment criteria

Code	Quality Assessment Criterion	Score
QA1	The study clearly states its aim or research problem	0–2
QA2	The method or analytical approach is clearly described	0–2
QA3	The study directly addresses identity theft, digital identity, IAM, or cybersecurity threats	0–2
QA4	The findings are supported by data, model, framework, or systematic argumentation	0–2
QA5	The limitations are stated or can be inferred	0–2

Table 4. Study quality categories

Total Score	Category
8–10	High quality
5–7	Moderate quality
0–4	Low quality
Total Score	Category

The assessment process was applied to all 49 eligible articles included in the final synthesis stage. Articles categorized as low quality were excluded from deeper thematic synthesis, while only studies classified as moderate and high quality were retained for the final analytical interpretation. This filtering strategy ensured that the review findings were supported by methodologically reliable and academically relevant evidence.

The results of the quality assessment indicated that most selected studies demonstrated adequate methodological transparency and strong relevance to identity theft and cybersecurity research. High-quality studies generally provided clear research objectives, well-defined analytical methods, empirical validation, and explicit discussion of limitations. Moderate-quality studies typically contributed useful conceptual or contextual insights despite limited empirical validation or methodological detail. Overall, the quality assessment process strengthened the credibility, consistency, and trustworthiness of the synthesized findings presented in this review.

Recent studies emphasized that structured quality assessment procedures improve transparency, reduce bias, and enhance the reliability of systematic reviews in cybersecurity and information systems research [24, 31]. Therefore, the adoption of a simplified and operational evaluation framework in this study provided a more practical and context-relevant approach for assessing heterogeneous cybersecurity literature related to identity theft, digital identity systems, and identity protection technologies.

Figure 1 in this study illustrates the systematic literature selection process conducted to obtain relevant articles related to identity theft in the context of cybersecurity. In the identification stage, the researchers performed a search using the Scopus database with a combination of keywords related to identity theft, digital identity, identity management, identity

security, and identity fraud combined with cybersecurity, information security, network security, cyber attack, and cyber threat. From this search process, a total of 2,274 records were identified.

In the screening stage, an initial filtering process was carried out based on the inclusion and exclusion criteria. A total of 1,479 records were excluded because they did not match the publication year range of 2021–2026. The selection process was then continued based on document type (article), English language, Computer Science subject area, and cybersecurity keywords, reducing the number of records gradually to 71 articles. During the manual screening process, 22 articles were identified as being outside the scope of the study and were therefore excluded.

In the final included stage, 49 articles were considered eligible and relevant to the research topic. These articles were subsequently used as the primary sources in the SLR to analyze the development of research related to identity theft, digital security threats, and identity management and cybersecurity approaches applied in previous studies.

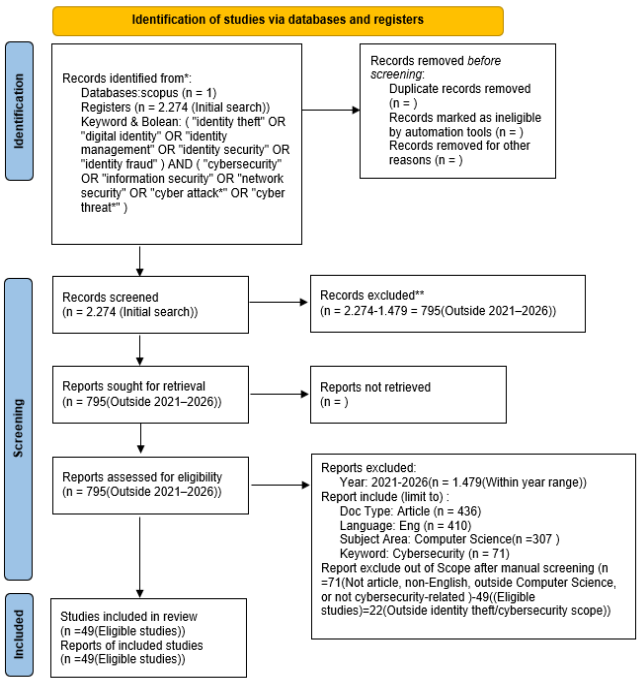

Figure 1. PRISMA flow diagram

2.5 Quality assessment results

The quality assessment was conducted for all 49 studies included in the final review. Each article was independently evaluated by two reviewers using the five predefined quality assessment criteria (QA1–QA5). The maximum achievable score was 10.

The assessment results indicated that 35 studies (71.4%) were classified as high quality (scores 8–10), 14 studies (28.6%) were classified as moderate quality (scores 5–7), and no studies were categorized as low quality (scores 0–4). Consequently, all 49 studies were retained for thematic synthesis because they met the minimum methodological quality threshold.

To evaluate consistency between reviewers, an inter-reviewer agreement analysis was performed. Initial scoring agreement reached 89.8%. Disagreements primarily involved the evaluation of methodological transparency (QA2) and reporting of study limitations (QA5). These differences were resolved through discussion and consensus review. The high level of agreement indicates satisfactory reliability and consistency in the quality assessment process.

A summary of the quality assessment results is presented in Table 5, while the complete individual quality assessment scores for all 49 included studies are provided in Appendix.

Table 5. Quality assessment results

Quality Category	Score Range	Number of Studies	Percentage
High Quality	8–10	35	71.4%
Moderate Quality	5–7	14	28.6%
Low Quality	0–4	0	0%
Total	–	49	100%

2.6 Data extraction and synthesis strategy

Data were extracted using a structured extraction form. The extracted information included author, year, publication source, research context, study method, type of identity theft or attack mechanism, identity management technology, mitigation technique, dataset or population, performance metric, key findings, and study limitations.

A thematic synthesis approach was applied to analyze the included studies. The studies were coded according to their main focus and grouped into four themes: identity theft attack mechanisms, identity management systems and technologies, technological mitigation solutions, and human factors. A cross theme synthesis was then conducted to identify relationships among attack vectors, identity architectures, mitigation technologies, and behavioral dimensions.

3. THEORETICAL BACKGROUND

3.1 Identity and digital identity theory

Digital identity refers to the collection of credentials, attributes, and behavioral information used to identify and authenticate individuals, devices, and entities in digital environments. As digital ecosystems become increasingly interconnected, identity has evolved from a static identifier into a dynamic and context-aware construct. Recent literature highlights a transition from traditional centralized identity management models toward decentralized and user-centric approaches that improve privacy, interoperability, and resilience against identity compromise [32, 33].

Decentralized Identity (DID), SSI, blockchain-based identity architectures, and Zero Trust frameworks have emerged as key paradigms for strengthening identity protection. Blockchain-enabled identity systems enhance trust, transparency, and tamper resistance while reducing reliance on centralized authorities [34, 35]. Similarly, Zero Trust architectures emphasize continuous verification and least-privilege access principles to minimize unauthorized access risks [36]. Multi-factor authentication, biometric verification, and privacy-enhancing technologies further contribute to protecting digital identities and mitigating identity theft threats [37, 38].

These developments provide the theoretical foundation for understanding how identity management architectures influence both identity theft vulnerabilities and identity

protection capabilities in contemporary cybersecurity ecosystems.

3.2 Cybersecurity threat and risk models

Identity theft is increasingly driven by sophisticated attack vectors including phishing, credential theft, malware, man-in-the-middle attacks, and large-scale data breaches. Phishing remains one of the most prevalent mechanisms because it exploits human behavior and authentication weaknesses simultaneously [39, 40]. Data breaches and credential exposure further facilitate identity fraud by providing attackers with access to personally identifiable information and authentication credentials [41, 42].

Recent studies also highlight the emergence of AI-enabled threats such as deepfake-based impersonation and automated social engineering attacks, which significantly increase the complexity of identity-related cyber risks [13, 43]. In parallel, the expansion of cloud computing, IoT environments, and distributed digital ecosystems has enlarged the attack surface and increased opportunities for identity compromise [44].

Contemporary cybersecurity risk models conceptualize identity theft as a socio-technical phenomenon resulting from interactions among technological vulnerabilities, organizational controls, and human behavior. Approaches such as Zero Trust, risk-based authentication, behavioral analytics, and machine-learning-driven anomaly detection have therefore been proposed to reduce identity-related risks through adaptive and context-aware security mechanisms [45-47].

3.3 Conceptual debates and paradigms

A major debate within the identity security literature concerns the relative advantages and limitations of centralized versus DID systems. Centralized architectures provide governance, operational simplicity, and regulatory control but introduce single points of failure that increase exposure to large-scale identity breaches [35]. Conversely, decentralized approaches such as SSI provide greater user control, privacy preservation, and reduced dependence on intermediaries, although challenges related to key management, usability, and interoperability remain significant [48, 49].

Another important debate contrasts technology-centric and human-centric cybersecurity approaches. Technology-centric perspectives emphasize automated detection systems, authentication technologies, artificial intelligence, and access control mechanisms as primary defenses against identity theft [50, 51]. Human-centric approaches focus on awareness, trust, usability, behavioral vulnerabilities, and socio-technical interactions that influence security outcomes [52].

The reviewed literature increasingly supports integrated socio-technical approaches that combine technological safeguards with behavioral and organizational interventions. Such hybrid approaches are considered more effective for addressing identity theft because they simultaneously address technical vulnerabilities and human factors that attackers frequently exploit [53-55].

3.4 Descriptive analysis of included studies

To provide a clearer overview of the evidence base, a descriptive analysis of the 49 included studies was conducted. The analysis examined publication year, research methodology, technology focus, application domain, and geographical distribution.

The results indicate a growing research interest in identity theft and digital identity security. Publication activity increased substantially after 2023, with the highest number of studies published between 2024 and 2025. This trend reflects the increasing concern regarding AI-enabled identity fraud, digital identity ecosystems, and emerging cybersecurity threats.

Regarding research methodology, conceptual and framework-based studies represented the largest group, followed by machine learning-based empirical studies, experimental cybersecurity evaluations, and systematic reviews. In terms of technological focus, artificial intelligence, blockchain-based identity systems, SSI, biometric authentication, and Zero Trust architectures emerged as the dominant themes.

The reviewed studies were applied across multiple domains, including IoT environments, cloud systems, healthcare, mobile platforms, e-commerce, digital government services, metaverse ecosystems, and cross-border digital identity infrastructures. Geographically, the evidence base demonstrated broad international representation, with significant contributions originating from Asia, Europe, North America, and Australia.

The distribution of the included studies according to research methodology is summarized in Table 6. The reviewed literature consists predominantly of conceptual and framework-based studies, followed by experimental, machine learning, systematic review, case study, and policy analysis research.

Table 7 summarizes the technological focus of the included studies. Artificial intelligence and machine learning represent the most frequently investigated technologies, followed by blockchain/SSI, authentication systems, biometrics, Zero Trust, and privacy-enhancing technologies.

Table 6. Distribution of included studies by research method

Method Type	Number
Conceptual/Framework	17
Experimental	12
Machine Learning / AI	10
Systematic Review	5
Case Study	3
Policy Analysis	2

Table 7. Distribution by technology focus

Technology	Number
AI / Machine Learning	14
Blockchain / SSI	11
Authentication Systems	8
Biometrics	5
Zero Trust	4
Privacy Technologies	4
Other	3

4. REVIEW OF FINDINGS

4.1 Identity theft types and attack mechanisms

Table 8 summarizes the identity theft attack mechanisms reported across the selected studies. As shown in Table 8, the cybersecurity landscape has evolved from isolated attack vectors toward increasingly sophisticated multi-stage identity

attacks. Based on the synthesis of the analyzed literature, attacks targeting digital identity have evolved alongside increasing system complexity, network integration, and the emergence of new digital environments such as the Internet of Things (IoT), Extended Reality (XR), and the Metaverse. Furthermore, advancements in artificial intelligence (AI) have significantly enhanced attackers' capabilities to perform impersonation, manipulation, and identity exploitation with greater sophistication. Therefore, it is essential to systematically classify the types of identity theft and their associated attack mechanisms in order to better understand the patterns and dynamics of emerging threats.

Based on Table 8, the findings indicate that identity theft mechanisms in cybersecurity can be categorized into several interrelated groups. First, social engineering based attacks such as phishing and behavioral manipulation emerge as dominant vectors, primarily due to their ability to exploit human vulnerabilities as entry points into systems. Second, network based attacks including man in the middle (MITM), ARP spoofing, and intrusion demonstrate that weaknesses in communication infrastructure remain a critical pathway for identity compromise.

In addition, data centric attacks such as data breaches and data leakage highlight that insecure data management practices directly contribute to identity theft. The literature shows that residual data stored on devices or leaked through distributed systems can be exploited for identity misuse. Furthermore, technological advancements have introduced a new category of AI driven attacks, including deepfakes and prompt injection, which enable highly realistic and difficult to detect identity impersonation.

The findings also reveal a significant shift from single vector attacks to multi layered attack strategies that combine multiple techniques. For instance, phishing attacks may be enhanced with deepfake technologies to increase their effectiveness, while network intrusions in IoT environments can provide broader access to sensitive identity data. Moreover, the emergence of new digital environments such as the Metaverse and XR expands the concept of identity itself, introducing new targets such as avatar identities and behavioral data.

Overall, these findings underscore that identity theft is an evolving and dynamic phenomenon driven by technological advancements and increasingly complex human system interactions. Consequently, partial or isolated security approaches are no longer sufficient, and a holistic mitigation strategy is required one that integrates technological, human, and contextual dimensions of cybersecurity.

Table 8. Synthesis of identity theft types and attack mechanisms

Ref. (Year)	Context	Method	Attack Type	Key Findings	Limitations
Molitor et al. [56] (2023)	Data breach litigation	ML-based text analytics	Data breach, identity theft	Identifies identity theft as a major cluster alongside phone scams and cybersecurity issues	Focuses on litigation rather than technical mechanisms
El-Hajj [57] (2025)	Extended Reality (XR)	Conceptual + adversary model	Identity theft, behavioral data leakage	XR introduces new risks such as profiling and behavioral manipulation	Lacks empirical validation
Kustiawan & Ghauth [58] (2025)	Web security	ML framework	Phishing (URL-based)	ML model (CatBoost) achieves 99.48% accuracy in phishing detection	Dataset-dependent
Raza et al. [59] (2022)	Digital forensics	Deep learning	Deepfake-based identity theft	Deepfakes enable highly realistic impersonation and fraud	Focus limited to detection
Odeh et al. [60] (2025)	AI-based detection	Hybrid AI models	Deepfake attack	Hybrid AI outperforms humans in detecting deepfakes (91.3%)	Limited to visual domain
Mvah et al. [61] (2024)	Software-defined networks	Game theory	ARP spoofing, identity fraud	ARP spoofing acts as a foundation for MITM and identity compromise	Network-specific focus
Raich & Gadicha [62] (2024)	Authentication systems	Blockchain-based model	MITM attack	MITM exploits weaknesses in traditional authentication protocols	Simulation-based study
Mahmood et al. [63] (2023)	5G networks	ML-based IDS	Intrusion, identity theft	IoT and 5G increase exposure to identity theft via network intrusion	Not identity-specific
Rustam et al. [64] (2023)	Malware analysis	ML + transfer learning	Malware-based credential theft	Malware serves as a primary vector for credential theft	Focus on detection only
Taherdoost [65] (2024)	Cybercrime review	Literature review	Phishing, ransomware, identity theft	Detection and response time are critical for mitigation	Not identity-system focused
Oladokun et al. [66] (2024)	Metaverse	Narrative review	Identity theft, social engineering	User behavior (e.g., weak passwords) amplifies risks	Lacks quantitative data
Sallam et al. [67] (2024)	Healthcare AI	Case-based analysis	Deepfake, prompt injection	GenAI introduces new identity theft vectors	Limited case scope
Kim et al. [68] (2022)	Android systems	Digital forensics	Data leakage, identity theft	Residual data recovery can lead to identity theft	Platform-specific
Al-Saeedi et al. [69] (2024)	AI & legal	Conceptual	Identity fraud, data misuse	AI-generated identities increase fraud and privacy risks	No technical validation
Alshboul et al. [70] (2021)	Smart home IoT	Experimental	Sensor identity theft	IoT sensors are vulnerable to identity exposure	Limited scale
Kuru & Kuru [71] (2025)	Metaverse	Blockchain + FL	Identity impersonation	Avatar identities are vulnerable to impersonation	Conceptual framework

4.2 Identity management systems and technologies

Table 9 summarizes the identity management systems and technologies identified in the reviewed studies.. The increasing complexity of cybersecurity threats, particularly identity theft, has driven the rapid evolution of identity management systems and supporting technologies. Traditional centralized identity management approaches are increasingly challenged by issues related to scalability, privacy, single points of failure, and vulnerability to cyberattacks. As a result, recent literature has explored a wide range of technological solutions, including blockchain-based identity systems, cryptographic frameworks, digital identity wallets, and DID models. These technologies aim to enhance authentication, ensure data integrity, and provide users with greater control over their digital identities. Therefore, a systematic synthesis of identity management systems and technologies is essential to understand their architectures, capabilities, and limitations in mitigating identity-related threats.

The synthesis presented in Table 9 highlights a clear transition from traditional centralized identity management systems toward more decentralized, flexible, and intelligent architectures. DID models, particularly those based on blockchain and SSI, have emerged as prominent solutions for enhancing user control, privacy, and trust. These systems eliminate reliance on centralized authorities and reduce single points of failure, thereby improving resilience against identity theft.

In contrast, centralized and federated identity systems continue to play an important role, particularly in regulated environments such as banking and government services. These systems provide structured governance and interoperability but remain vulnerable to large-scale breaches due to their centralized nature. Hybrid approaches attempt to combine the strengths of both models, integrating centralized control with decentralized verification mechanisms.

From a technological perspective, cryptographic techniques including public key infrastructure, elliptic curve cryptography, and post quantum cryptography remain fundamental in securing identity systems. Additionally, biometric authentication systems have demonstrated high accuracy in identity verification, although they raise significant privacy concerns. Emerging architectures such as Zero Trust further redefine identity management by emphasizing continuous verification and adaptive access control.

Moreover, the integration of artificial intelligence and machine learning into identity management systems enables dynamic threat detection and adaptive security responses. However, these advancements also introduce new challenges, including computational overhead, system complexity, and potential biases in automated decision making.

Table 9. Synthesis of identity management systems and technologies

Ref. (Year)	Technology	Architecture	Security Features	Key Findings	Limitations
Rattanawiboonsom & Khan [72] (2024)	Blockchain (SSI)	Decentralized	Cryptography, trustless verification	Blockchain enhances identity security and privacy in mobile payments	Scalability and usability challenges
Fiaz et al. [73] (2024)	Self-Sovereign Identity (SSI)	Fully decentralized	User-controlled identity, privacy preservation	SSI improves control over personal data in Metaverse environments	Conceptual validation
Li et al. [74] (2023)	Lightweight authentication	Hybrid (ECC + CLC)	Mutual authentication, key update	Efficient for resource-constrained systems	Limited real-world deployment
Neppolian & Kumar [75] (2025)	Public Key Cryptography	Centralized + distributed	Encryption, digital signatures	Enhances trust and secure communication in e-commerce	Implementation complexity
Belhocine et al. [76] (2024)	Biometric authentication	Centralized	Palmprint recognition, deep learning	High accuracy in identity verification	Privacy concerns
Naohiro et al. [77] (2021)	Digital identity platform	Federated	API-based identity sharing	Enables secure cross-organization identity verification	Regulatory dependency
Comandè & Varilek [78] (2024)	Digital Identity Wallet	Hybrid	PQC-ready encryption, authentication	Wallets enable secure and portable identity management	Privacy risks (linkability)
Álvarez et al. [79] (2026)	Digital Identity Wallet (EUDI)	Centralized-regulated	Privacy-enhancing technologies (ZKP)	Identifies privacy risks in wallet architecture	Design limitations
Ismail et al. [80] (2024)	Blockchain + ML framework	Decentralized	Smart contracts, trust management	Combines prevention and detection in identity management	Computational overhead
Supangkat et al. [81] (2025)	Cross-border identity systems	Hybrid	Interoperability, governance	Highlights challenges in global identity systems	Regulatory fragmentation
Joshi [82] (2025)	Zero Trust Architecture	Distributed	Continuous verification, least privilege	Enhances dynamic identity validation	Complexity in implementation
Alruwies et al. [83] (2021)	Identity Governance Framework	Centralized	Access control, policy enforcement	Improves management of privileged identities	Limited scalability
Kayes et al. [84] (2025)	Privacy protection frameworks	Hybrid	Risk assessment, AI-based analysis	Provides comprehensive identity protection strategies	Generalized approach

Overall, the findings indicate that no single identity management solution is universally optimal. Instead, effective identity protection requires a combination of technologies tailored to specific contexts, balancing security, usability, privacy, and scalability. This reinforces the need for a holistic and multi layered approach to identity management in modern cybersecurity ecosystems.

4.3 Technological solutions for identity theft mitigation

Table 10 presents the technological solutions proposed for mitigating identity theft.. In response to the increasing sophistication of identity theft attacks, a wide range of technological solutions has been developed to enhance detection, prevention, and mitigation capabilities. These solutions leverage advancements in artificial intelligence, machine learning, cryptography, and anomaly detection to address evolving cybersecurity threats. Unlike identity management systems, which focus on structuring and governing identities, technological mitigation solutions primarily aim to detect malicious activities, prevent unauthorized access, and respond to security incidents in real time. Therefore, it is essential to systematically examine these technologies to evaluate their effectiveness, performance, and limitations in combating identity theft across different digital environments.

The synthesis in Table 10 demonstrates that technological solutions for mitigating identity theft are increasingly driven by data centric and intelligence based approaches. Machine learning and deep learning techniques dominate the landscape, particularly in detecting phishing attacks, malware, and deepfake based identity fraud. These approaches achieve high levels of accuracy, often exceeding 90%, indicating their effectiveness in identifying complex attack patterns that are difficult to detect using traditional rule based systems.

In addition to detection focused solutions, hybrid approaches that integrate multiple technologies such as blockchain combined with machine learning have emerged as promising strategies. These approaches enable both prevention and detection by securing identity data while simultaneously identifying anomalous behaviors within the system. Similarly, game theory based models introduce predictive defense mechanisms that anticipate attacker strategies and optimize defensive responses.

However, the findings also highlight several limitations. Many solutions are highly dependent on specific datasets, which limits their generalizability across different environments. Computational complexity is another major concern, particularly for deep learning and hybrid AI models, which may hinder real time deployment. Furthermore, while detection accuracy is often emphasized, fewer studies address response strategies and system level integration.

Another important insight is that technological solutions are increasingly tailored to specific contexts, such as IoT, 5G networks, healthcare systems, and mobile platforms. This contextual dependency suggests that there is no one size fits all solution, and effective mitigation requires adaptive and context aware technologies.

Overall, the results indicate that while technological advancements have significantly improved the ability to detect and mitigate identity theft, challenges related to scalability, generalization, and integration remain. This underscores the need for future research to focus on developing unified, efficient, and context adaptive security solutions that can operate effectively across diverse cybersecurity environments.

Table 10. Synthesis of technological solutions for identity theft mitigation

Ref. (Year)	Technique	Dataset/Context	Performance Metrics	Key Findings	Limitations
Rustam et al. [64] (2023)	Transfer learning (VGG16, ResNet)	Malware dataset	Accuracy (100%)	Hybrid models enhance malware detection significantly	Overfitting risk
Taherdoost [65] (2024)	IDS & phishing detection	Cybercrime datasets	Detection time, response time	Faster detection improves mitigation effectiveness	Lacks unified framework
Odeh et al. [60] (2025)	Hybrid AI (CNN + ViT)	Deepfake dataset	Accuracy (91.3%)	AI outperforms humans in deepfake detection	Computational complexity
Raza et al. [59] (2022)	Deep learning (CNN)	Deepfake images	Accuracy (94–95%)	Effective detection of identity fraud via deepfake	Limited generalization
Kustiawan & Ghauth [58] (2025)	ML (CatBoost)	Phishing URLs	Accuracy (99.48%)	Highly accurate phishing detection model	Dataset dependency
Ismail et al. [80] (2024)	Blockchain + ML	IoT networks	Precision, recall, F1-score	Combines prevention and detection mechanisms	High computational cost
Mvah et al. [61] (2024)	Game theory-based detection	SDN networks	Detection efficiency	Predictive defense improves mitigation	Complex implementation
Sallam et al. [67] (2024)	AI risk analysis	Healthcare systems	CIA triad analysis	Identifies vulnerabilities in AI-driven systems	Case-based limitation
Alshboul et al. [70] (2021)	Sensor identity protection	Smart home IoT	Performance evaluation	Protects identity through communication obfuscation	Context-specific
Kim et al. [68] (2022)	Digital forensic analysis	Android systems	Data recovery analysis	Highlights need for secure data deletion	Platform limitation

4.4 Human factors and behavioral aspects

Table 11 summarizes the human factors and behavioral aspects influencing identity theft. While technological advancements play a critical role in addressing identity theft, the human factor remains one of the most significant vulnerabilities in cybersecurity systems. Users often act as the weakest link due to limited awareness, cognitive biases, lack of security knowledge, and risky online behaviors. Recent literature increasingly emphasizes the importance of human centric cybersecurity, highlighting how user perceptions, motivations, trust, and behavioral intentions influence the effectiveness of identity protection mechanisms. Therefore, understanding the behavioral and psychological dimensions of

cybersecurity is essential to complement technological solutions and develop more holistic mitigation strategies.

The synthesis presented in Table 11 highlights that human factors play a crucial role in shaping both vulnerability and resilience to identity theft. Across the reviewed studies, awareness consistently emerges as a central determinant of secure behavior. Users with higher levels of cybersecurity awareness are more likely to adopt protective measures, while low awareness increases susceptibility to attacks such as phishing and social engineering.

Motivational and psychological constructs, such as perceived risk, self efficacy, and trust, are also shown to significantly influence user behavior. The application of theories such as Protection Motivation Theory (PMT) and Expectancy Value Theory demonstrates that individuals are more likely to engage in protective behaviors when they perceive threats as severe and believe they have the capability to mitigate them. Conversely, resistance to change and usability challenges can hinder the adoption of secure practices.

Another important finding is the role of contextual and environmental factors, particularly in emerging digital ecosystems such as the Metaverse and cross border identity systems. In these environments, the complexity of interactions and the novelty of technologies amplify behavioral risks, making users more vulnerable to identity theft. Additionally, trust and privacy concerns play a decisive role in shaping user acceptance and engagement with digital identity systems.

The findings also indicate that human factors are not isolated but interact dynamically with technological and organizational elements. For instance, even the most advanced security technologies can fail if users do not understand or properly utilize them. Similarly, policy and governance frameworks influence user behavior by shaping perceptions of security and trust.

Overall, the results emphasize that addressing identity theft requires a human centric approach that integrates behavioral insights with technological solutions. Future research should focus on developing adaptive security systems that account for user behavior, as well as designing interventions to improve awareness, motivation, and trust in digital identity ecosystems.

Cross-theme synthesis. Across the reviewed studies, identity theft appears as a socio-technical cybersecurity problem shaped by the interaction between attack sophistication, identity system design, technological mitigation capacity, and user behavior. Attack mechanisms exploit weaknesses in identity management systems, while mitigation technologies depend on both technical robustness and user adoption. This cross-theme relationship provides the basis for the conceptual framework discussed in Section 5.

Table 11. Synthesis of human factors and behavioral aspects

Ref. (Year)	Population/Context	Theory Used	Variables	Key Findings	Limitations
Alhelaly et al. [85] (2023)	Mobile users	Expectancy-Value Theory	Awareness, motivation, capability	Awareness mediates the gap between user expectations and protection behavior	Context limited to mobile users
Al Humaid Alneyadi & Normalini [86] (2023)	UAE organizations	Protection Motivation Theory (PMT)	Perceived risk, self-efficacy, resistance	Behavioral intention strongly influenced by perceived efficacy and risk	Country-specific
Hilowle et al. [87] (2023)	National digital identity users	Human-centric cybersecurity	Trust, privacy, usability	Adoption depends on trust and perceived risk	Conceptual synthesis
Hilowle et al. [88] (2024)	Australian NDID users	Qualitative approach	User experience, trust	Human factors significantly influence system adoption	Limited sample size
Al-Emran et al. [89] (2024)	Metaverse users	TTAT + fsQCA	Privacy concern, response cost	Multiple configurations influence secure behavior	Complex model interpretation
Oladokun et al. [66] (2024)	Metaverse environment	Narrative review	User behavior, awareness	Weak passwords and social engineering increase identity theft risk	No empirical validation
Supangkat et al. [81] (2025)	Cross-border identity systems	SLR approach	Trust, governance, inclusion	Adoption influenced by social and regulatory factors	Broad scope
Mishra et al. [90] (2022)	Multi-country policy	Policy analysis	Governance, regulation	Policy gaps influence identity protection effectiveness	Not user-focused
Malezis [91] (2023)	Healthcare organizations	Conceptual	Identity awareness, system use	Digital identity adoption supports cybersecurity resilience	Limited empirical data

5. DISCUSSION

5.1 Synthesis of key findings across themes

The findings of this review demonstrate that identity theft has evolved into a complex socio-technical cybersecurity challenge driven by the interaction between attack mechanisms, identity management architectures, technological mitigation solutions, and human behavioral factors. Across the reviewed studies, phishing, credential theft, malware, deepfake impersonation, and data breaches emerged as the dominant identity theft vectors. At the same time, DID systems, blockchain-based identity management, artificial intelligence, behavioral analytics, and adaptive authentication mechanisms have increasingly been proposed to strengthen identity protection.

The synthesis further indicates that identity theft cannot be effectively mitigated through isolated technological interventions. Instead, cybersecurity resilience depends on the alignment of secure identity architectures, intelligent detection technologies, organizational governance, and user behavior. These findings support the need for integrated and multi-layered approaches capable of addressing both technological and human vulnerabilities.

5.2 Proposed socio-technical framework for identity theftmitigation

Based on the synthesis of the reviewed literature, this study proposes an integrated socio-technical framework that explains how identity theft emerges, evolves, and can be mitigated within modern digital ecosystems.

Figure 2 presents the proposed socio-technical framework of identity theft. The framework illustrates that identity theft results from the dynamic interaction between four interconnected dimensions: attack mechanisms, identity management systems, technological mitigation solutions, and human factors. Attack mechanisms exploit vulnerabilities in identity infrastructures through phishing, malware, credential theft, deepfake impersonation, social engineering, and data breaches. Identity management systems influence the resilience of authentication and authorization processes through centralized, federated, and decentralized architectures.

The framework further highlights the role of technological mitigation mechanisms, including artificial intelligence, blockchain-based security, behavioral analytics, anomaly detection, and adaptive authentication. However, the effectiveness of these technologies is strongly influenced by user awareness, trust, security behavior, organizational governance, and regulatory environments. Consequently, identity theft prevention requires a coordinated socio-technical strategy rather than purely technical countermeasures.

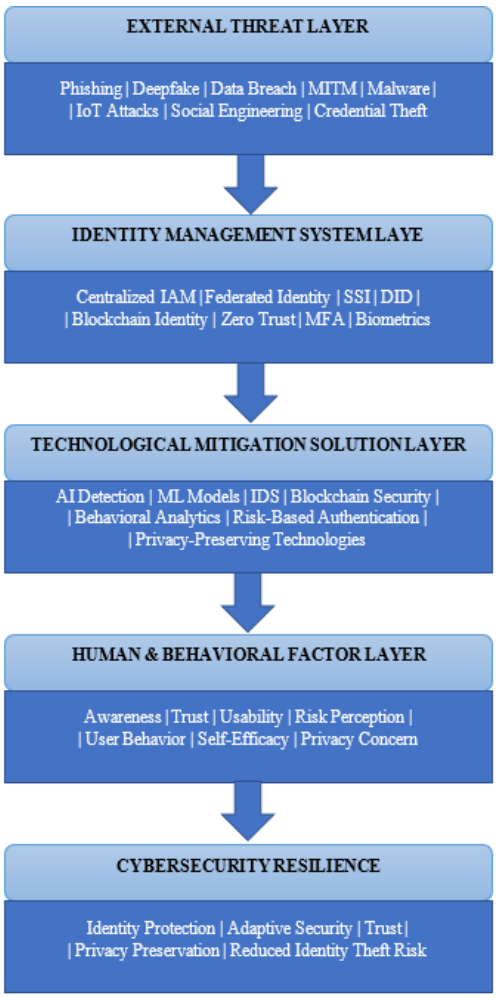

Figure 2. Conceptual framework

The proposed framework contributes to the literature by integrating previously fragmented research streams into a unified analytical perspective and providing a foundation for future identity protection research.

5.3 Implications for research and practice

From a theoretical perspective, the findings reinforce the view that identity theft should be understood as a socio-technical phenomenon rather than solely a technical cybersecurity issue. The review demonstrates that attack evolution, identity system design, technological defenses, and human behavior are interdependent factors that collectively shape cybersecurity outcomes. The proposed framework therefore contributes to the development of more integrated identity theft theories and provides a conceptual basis for future interdisciplinary research.

From a practical perspective, the findings suggest that organizations should adopt multi-layered identity protection strategies that combine strong authentication, continuous monitoring, user awareness programs, behavioral analytics, and adaptive access control mechanisms. Policymakers should promote interoperable digital identity standards, privacy-preserving identity architectures, and effective governance frameworks. Technology developers should prioritize not only security performance but also usability, scalability, transparency, and privacy when designing identity protection systems.

5.4 Future research directions

Several opportunities for future research were identified. First, there is a need for standardized benchmarking datasets to improve comparability and reproducibility across identity theft studies. Second, future studies should conduct longitudinal and real-world evaluations of identity protection technologies beyond laboratory environments. Third, additional research is needed to address emerging threats such as synthetic identities, AI-generated impersonation attacks, adversarial machine learning, and identity risks within metaverse and IoT ecosystems. Finally, future work should further explore the integration of technological, behavioral, organizational, and policy perspectives into unified identity protection frameworks.

5.5 Limitations

This SLR contributes to the theoretical development of cybersecurity and digital identity research by demonstrating that identity theft should no longer be conceptualized solely as a technical security issue, but rather as a complex socio-technical phenomenon shaped by the interaction between technological infrastructures, human behavior, organizational governance, and evolving cyber threats. The findings extend existing cybersecurity theories by integrating attack mechanisms, identity management architectures, technological mitigation strategies, and behavioral dimensions into a unified conceptual perspective. This integrated view advances prior literature that has traditionally examined these dimensions in isolation.

In response to the theoretical gaps identified in RQ1–RQ4, the review demonstrates that contemporary identity theft mechanisms increasingly challenge conventional assumptions underlying centralized security and authentication models.

Existing theories of identity management have historically emphasized static authentication, perimeter defense, and centralized trust structures. However, the findings reveal that modern cyber threats including AI-driven impersonation, deepfake attacks, credential stuffing, and multi-vector social engineering attacks operate within dynamic and highly distributed digital ecosystems. Consequently, traditional theoretical frameworks are insufficient to explain how identity risks evolve in environments characterized by cloud computing, IoT, metaverse platforms, and decentralized digital interactions.

The review also contributes to the conceptual refinement of digital identity theory by reinforcing the transition from centralized identity paradigms toward decentralized and adaptive identity ecosystems. The emergence of SSI, blockchain-based identity systems, Zero Trust architectures, and context-aware authentication models suggests that identity should be understood as a dynamic, continuously verified, and context-dependent construct rather than a static credential-based entity. This finding extends contemporary debates within identity and access management literature regarding trust distribution, user sovereignty, privacy preservation, and adaptive authentication.

Furthermore, the findings strengthen human-centric cybersecurity theory by demonstrating that technological effectiveness is fundamentally mediated by behavioral and psychological factors. Existing technology-centric models frequently assume that stronger technical controls automatically produce stronger security outcomes. However, this review indicates that user awareness, trust, perceived risk, cognitive biases, motivation, and usability significantly shape the effectiveness of identity protection mechanisms. This supports and extends theories such as PMT, socio-technical systems theory, and behavioral cybersecurity frameworks by showing that identity theft prevention depends on the alignment between technological systems and human decision-making processes.

Another important theoretical implication lies in the recognition of co-adaptive dynamics between attackers and defensive systems. The findings suggest that identity theft evolves through continuous interaction between adversarial innovation and defensive adaptation. As organizations implement AI-driven detection systems, behavioral biometrics, and decentralized authentication mechanisms, attackers simultaneously develop more sophisticated evasion strategies using automation, deepfakes, adversarial AI, and social engineering techniques. This dynamic supports emerging perspectives in adaptive cybersecurity theory, which conceptualize cybersecurity not as a static protection mechanism but as an evolving ecosystem characterized by continuous technological and behavioral competition.

The review also highlights the need for greater interdisciplinary theoretical integration within identity theft research. Existing studies remain fragmented across computer science, behavioral psychology, information systems, digital governance, and cybersecurity management domains. By synthesizing these perspectives, this study proposes a broader socio-technical conceptualization capable of bridging disciplinary boundaries and improving theoretical coherence within the field. Such integration is particularly important for understanding emerging cybersecurity environments where technical vulnerabilities, governance structures, ethical concerns, and human behaviors interact simultaneously.

Overall, the theoretical implications of this review suggest that future cybersecurity theories should move beyond purely technology-centric approaches toward adaptive, interdisciplinary, and context-aware frameworks capable of explaining the evolving relationship between identity systems, cyber threats, technological innovation, and human behavior in modern digital ecosystems.

6. CONCLUSION

This SLR provides a comprehensive synthesis of identity theft research in cybersecurity by integrating perspectives related to attack mechanisms, identity management systems, technological mitigation strategies, and human behavioral factors. The findings demonstrate that identity theft has evolved into a complex and multidimensional socio-technical phenomenon shaped by the interaction between technological vulnerabilities, adversarial innovation, digital identity architectures, and user behavior. Emerging threats such as AI-driven deepfake impersonation, phishing-as-a-service, credential stuffing, and large-scale data breaches illustrate that contemporary identity attacks are increasingly adaptive, intelligent, and difficult to detect using conventional security approaches.

The review further reveals that traditional identity management systems are becoming increasingly insufficient in highly distributed digital ecosystems such as cloud computing, IoT environments, and metaverse platforms. In response to these evolving threats, recent studies have proposed DID architectures, blockchain-based identity management, Zero Trust frameworks, behavioral biometrics, and AI-driven anomaly detection systems as more adaptive mitigation approaches. However, the effectiveness of these technologies remains constrained by challenges related to scalability, interoperability, usability, privacy, and integration complexity.

Another important conclusion of this review is that human factors continue to represent one of the most critical dimensions of identity theft vulnerability and mitigation effectiveness. User awareness, trust, risk perception, cognitive behavior, and security culture significantly influence the success or failure of cybersecurity mechanisms. Therefore, identity protection should not be approached solely from a technology-centric perspective, but rather through integrated socio-technical strategies combining technical safeguards, organizational governance, behavioral adaptation, and policy coordination.

This study contributes theoretically by proposing an integrated socio-technical conceptual framework that connects attack mechanisms, identity systems, technological solutions, and human-centered cybersecurity dimensions within a unified perspective. Practically, the findings provide guidance for organizations, cybersecurity practitioners, and policymakers in developing adaptive, multi-layered, and user-centric identity protection strategies capable of responding to rapidly evolving digital threats.

In response to RQ5, this review identifies four major future research directions: standardized benchmarking datasets, real-world and longitudinal validation, interdisciplinary socio-technical models, and deeper investigation of synthetic identities and AI-enabled impersonation threats. Future studies should also prioritize adaptive and context-aware cybersecurity frameworks capable of balancing security, usability, privacy, and governance requirements across

increasingly interconnected digital ecosystems.

Overall, this review advances the understanding of identity theft by demonstrating that cybersecurity resilience depends on the continuous integration of technological innovation, human-centric design, and adaptive governance mechanisms within modern digital identity ecosystems.

REFERENCES

[1] Liu, Y., Zhang, T., Jin, X., Cheng, X. (2015). Personal privacy protection in the era of big data. Journal of Computer Research and Development, 52(1): 229-247. https://doi.org/10.7544/issn1000-1239.2015.20131340

[2] Alzahrani, R.A., Aljabri, M., Mohammad, R.A.M. (2025). Ad click fraud detection using machine learning and deep learning algorithms. IEEE Access, 13: 12746-12763. https://doi.org/10.1109/ACCESS.2025.3532200

[3] Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. Journal of Global Information Technology Management, 22(2): 77-81. https://doi.org/10.1080/1097198X.2019.1603527

[4] Eleftherakis, S., Giustiniano, D., Kourtellis, N. (2025). SoK: Evaluating 5G-Advanced protocols against legacy and emerging privacy and security attacks. In 18th ACM Conference on Security and Privacy in Wireless and Mobile Networks, New York, NY, USA, pp. 196-210. https://doi.org/10.1145/3734477.3734716

[5] Alrawais, A., Alhothaily, A., Hu, C., Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 21(2): 34-42. https://doi.org/10.1109/MIC.2017.37

[6] Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76: 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

[7] Mirsky, Y., Lee, W. (2020). The creation and detection of deepfakes: A survey. ACM Computing Surveys (CSUR), 54(1): 1-41. https://doi.org/10.1145/3425780

[8] Nguyen, T.T., Nguyen, Q.V.H., Nguyen, D.T., Nguyen, D.T., et al. (2022). Deep learning for deepfakes creation and detection: A survey. Computer Vision and Image Understanding, 223: 103525. https://doi.org/10.1016/j.cviu.2022.103525

[9] Falchuk, B., Loeb, S., Neff, R. (2018). The social metaverse: Battle for privacy. IEEE Technology and Society Magazine, 37(2): 52-61. https://doi.org/10.1109/MTS.2018.2826060

[10] Bada, M., Nurse, J.R. (2020). The social and psychological impact of cyberattacks. In Emerging Cyber Threats and Cognitive Vulnerabilities, pp. 73-92. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

[11] Polychronaki, M., Xevgenis, M.G., Kogias, D.G. (2024). Decentralized identity management for metaverse-enhanced education: A literature review. Electronics, 13(19): 3887. https://doi.org/10.3390/electronics13193887

[12] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In IFIP International Information Security Conference, Auckland, New Zealand, pp. 366-378. https://doi.org/10.1007/978-3-642-39218-4_27

[13] Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khurram, M., Choo, K.R. (2020). Blockchain-based identity management systems: A review. Journal of Network and Computer Applications, 166: 102731. https://doi.org/10.1016/j.jnca.2020.102731

[14] Sule, M., Zennaro, M., Thomas, G. (2021). Technology in Society Cybersecurity through the lens of digital identity and data protection: Issues and trends. Technology in Society, 67: 101734. https://doi.org/10.1016/j.techsoc.2021.101734

[15] Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7): e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[16] Ahmed, R., Islam, A.K.M.M., Member, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. IEEE Access, 10: 113436-113481. https://doi.org/10.1109/ACCESS.2022.3216643

[17] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., Hong, J. (2008). Lessons from a real world evaluation of anti-phishing training. In 2008 eCrime Researchers Summit, Atlanta, GA, USA, pp. 1-12. https://doi.org/10.1109/ECRIME.2008.4696970

[18] Radanliev, P., De Roure, D., Maple, C., Nurse, J.R., Nicolescu, R., Ani, U. (2024). AI security and cyber risk in IoT systems. Frontiers in Big Data, 7: 1402745. https://doi.org/10.3389/fdata.2024.1402745

[19] Bada, M., Nurse, J.R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). Information & Computer Security, 27(3): 393-410. https://doi.org/10.1108/ICS-07-2018-0080

[20] Alharbi, A., Dong, H., Yi, X., Tari, Z., Khalil, I. (2021). Social media identity deception detection: A survey. ACM Computing Surveys (CSUR), 54(3): 1-35. https://doi.org/10.1145/3446372

[21] Sharma, S., Dwivedi, R. (2024). A survey on blockchain deployment for biometric systems. IET Blockchain, 4(2): 124-151. https://doi.org/10.1049/blc2.12063

[22] Alshamrani, A., Myneni, S., Chowdhary, A., Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2): 1851-1877. https://doi.org/10.1109/COMST.2019.2891891

[23] Agarwal, V. (2021). Identity theft detection using machine learning. International Journal for Research in Applied Science and Engineering Technology, 9(8): 1943-1946. https://doi.org/10.22214/ijraset.2021.37696

[24] Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F., Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. Geneva Papers on Risk and Insurance - Issues and Practice, 47(3): 698-736. https://doi.org/10.1057/s41288-022-00266-6

[25] Compagnino, A.A., Maruccia, Y., Cavuoti, S., Riccio, G., Tutone, A., Crupi, R., Pagliaro, A. (2025). An introduction to machine learning methods for fraud detection. Applied Sciences, 15(21): 11787. https://doi.org/10.3390/app152111787

[26] Chen, Y., Zhao, C., Xu, Y., Nie, C., Zhang, Y. (2026). Deep learning in financial fraud detection: Innovations, challenges, and applications. Data Science and

Management, 9(2): 100162. https://doi.org/10.1016/j.dsm.2025.08.002
[27] Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372. https://doi.org/10.1136/bmj.n71
[28] Kitchenham, B., Brereton, O.P., Budgen, D. (2009). Systematic literature reviews in software engineering—A systematic literature review. Information and Software Technology, 51(1): 7-15. https://doi.org/10.1016/j.infsof.2008.09.009
[29] Shea, B.J., Reeves, B.C., Wells, G., Thuku, M., et al. (2017). AMSTAR 2: A critical appraisal tool for systematic reviews that include randomised or non-randomised studies of healthcare interventions, or both. BMJ, 358. https://doi.org/10.1136/bmj.j4008
[30] Higgins, J.P.T., Caldwell, D.M., Whiting, P., Savovi, J. (2016). ROBIS: A new tool to assess risk of bias in systematic reviews was developed. Journal of Clinical Epidemiology, 69: 225-234. https://doi.org/10.1016/j.jclinepi.2015.06.005
[31] Bhuiyan, J.U. (2026). Information technology, cybersecurity, and artificial intelligence evaluating the effectiveness of cyber security frameworks in preventing banking fraud. Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 3(3): 75-94. https://doi.org/10.70715/jitcai.2026.v3.i3.068
[32] Seo, J., Park, S. (2025). Self-sovereign identity framework with user-friendly private key generation and rule table. Future Generation Computer Systems, 167: 107757. https://doi.org/10.1016/j.future.2025.107757
[33] Xian, J., You, L., Yi, Q., Wang, J., Hu, G. (2025). A survey on decentralized identity management systems. Computer Science Review, 58: 100811. https://doi.org/10.1016/j.cosrev.2025.100811
[34] Ferdous, M.S., Chowdhury, F., Alassafi, M.O. (2019). In search of self-sovereign identity leveraging blockchain technology. IEEE Access, 7: 103059-103079. https://doi.org/10.1109/ACCESS.2019.2931173
[35] Alanzi, H.M., Alkhatib, M. (2025). Blockchain-based identity management system prototype for enhanced privacy and security. Electronics, 14(13): 2605. https://doi.org/10.3390/electronics14132605
[36] Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). Zero trust architecture. NIST Special Publication, 800(207): 1-52. https://doi.org/10.6028/NIST.SP.800-207
[37] Zyskind, G., Nathan, O., Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. IEEE Security and Privacy Workshops. pp. 180-184. https://doi.org/10.1109/SPW.2015.27
[38] Aloul, F., Zahidi, S., El-Hajj, W. (2009). Two factor authentication using mobile phones. In IEEE/ACS International Conference on Computer Systems and Applications. pp. 641-644. https://doi.org/10.1109/AICCSA.2009.5069395
[39] Saeed, T., Nafees, M. (2024). A systematic literature review on phishing attacks and countermeasures. Soc. Transform. AI Big Data Journal, 2(1): 48-66. https://doi.org/10.20547/aibd.242105
[40] Osamor, J., Ashawa, M., Shahrabi, A., Phillip, A., Iwend, C. (2025). The evolution of phishing and future directions: A review. In International Conference on Cyber Warfare and Security, pp. 361-368.
[41] Abdullah, M., Nawaz, M.M., Saleem, B., Zahra, M., Ashfaq, E., Muhammad, Z. (2025). Evolution cybercrime—Key trends, cybersecurity threats, and mitigation strategies from historical data. Analytics, 4(3): 25. https://doi.org/10.3390/analytics4030025
[42] Bisogni, F., Asghari, H. (2020). More than a suspect: An investigation into the connection between data breaches, identity theft, and data breach notification laws. Journal of Information Policy, 10: 45-82. https://doi.org/10.5325/jinfopoli.10.2020.0045
[43] Nassif, A.B., Talib, M.A., Nasir, Q., Dakalbab, F.M. (2021). Machine learning for anomaly detection: A systematic review. IEEE Access, 9: 78658-78700. https://doi.org/10.1109/ACCESS.2021.3083060
[44] Ali, S., Ahmed, S., Yichiet, A., Lee, M., Kang, C. (2024). Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing. Egyptian Informatics Journal, 27(2): 100519. https://doi.org/10.1016/j.eij.2024.100519
[45] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98: 102003. https://doi.org/10.1016/j.cose.2020.102003
[46] Van Haastrecht, M., Yigit Ozkan, B., Brinkhuis, M., Spruit, M. (2021). Respite for SMEs: A systematic review of socio-technical cybersecurity metrics. Applied Sciences, 11(15): 6909. https://doi.org/10.3390/app11156909
[47] Kumar, V., Paul, K. (2023). Device fingerprinting for cyber-physical systems: A survey. ACM Computing Surveys, 55(14s): 1-41. https://doi.org/10.1145/3584944
[48] Čučko, Š., Keršič, V., Turkanović, M. (2023). Towards a catalogue of self-sovereign identity design patterns. Applied Sciences, 13(9): 5395. https://doi.org/10.3390/app13095395
[49] Fathalla, E., Azab, M., Xin, C., Wu, H. (2026). Self-sovereign identity as a secure and trustworthy approach to digital identity management: A comprehensive survey. ACM Computing Surveys, 58(7): 190. https://doi.org/10.1145/3785466
[50] Finnegan, O.L., White III, J.W., Armstrong, B., Adams, E.L., et al. (2024). The utility of behavioral biometrics in user authentication and demographic characteristic detection: A scoping review. Systematic Reviews, 13(1): 61. https://doi.org/10.1186/s13643-024-02451-1
[51] Khan, A.R., Kashif, M., Jhaveri, R.H., Raut, R., Saba, T., Bahaj, S.A. (2022). Deep learning for intrusion detection and security of Internet of Things (IoT): Current analysis, challenges, and possible solutions. Security and Communication Networks, 2022(1): 4016073. https://doi.org/10.1155/2022/4016073
[52] Varghese, B.B., Bui, Q.N. (2026). An integrated framework for information security risk management: A mixed-methods systematic literature review. Computers & Security, 168: 104957. https://doi.org/10.1016/j.cose.2026.104957
[53] Khayer, B., Mirzaei, S., Alavizadeh, H., Salehi Shahraki, A. (2025). Blockchain for secure IoT: A review of identity management, access control, and trust mechanisms. IoT, 6(4): 65. https://doi.org/10.3390/iot6040065
[54] Kuzior, A., Tiutiunyk, I., Zielińska, A., Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2): 220-

239. https://doi.org/10.14254/2071-8330.2024/17-2/12
[55] Gökstorp, S., Katsikeas, S., Johnson, P. (2026). Machine learning for cybersecurity: A comprehensive literature review. ACM Computing Surveys, 58(9): 1-36. https://doi.org/10.1145/3796543
[56] Molitor, D., Raghupathi, W., Saharia, A., Raghupathi, V. (2023). Exploring key issues in cybersecurity data breaches: Analyzing data breach litigation with ML-based text analytics. Information, 14(11): 600. https://doi.org/10.3390/info14110600
[57] El-Hajj, M. (2025). Cybersecurity and privacy challenges in extended reality: Threats, solutions, and risk mitigation strategies. Virtual Worlds, 4(1): 1. https://doi.org/10.3390/virtualworlds4010001
[58] Kustiawan, Y.A., Ghauth, K.I. (2025). PhishOFE: A novel machine learning framework for real-time phishing URL detection with optimized feature engineering. IEEE Access, 13: 169606-169627. https://doi.org/10.1109/ACCESS.2025.3614126
[59] Raza, A., Munir, K., Almutairi, M. (2022). A novel deep learning approach for deepfake image detection. Applied Sciences, 12(19): 9820. https://doi.org/10.3390/app12199820
[60] Odeh, A., Al-Haj Hassan, O., Abu Taleb, A. (2025). Hybrid AI approaches for detecting deepfake faces. Signal, Image and Video Processing, 19(18): 1457. https://doi.org/10.1007/s11760-025-05051-1
[61] Mvah, F., Tchendji, V.K., Djamegni, C.T., Anwar, A.H., Tosh, D.K., Kamhoua, C. (2024). Countering ARP spoofing attacks in software-defined networks using a game-theoretic approach. Computers & Security, 139: 103696. https://doi.org/10.1016/j.cose.2023.103696
[62] Raich, A., Gadicha, V. (2024). Enhancing authentication security against MITM attacks through bioinspired identity management & blockchain-enhanced protocols. International Journal of Intelligent Systems and Applications in Engineering, 12(10s): 468-476.
[63] Mahmood, I., Alyas, T., Abbas, S., Shahzad, T., Abbas, Q., Ouahada, K. (2023). Intrusion detection in 5G cellular network using machine learning. Computer Systems Science and Engineering, 47(2): 2439-2453. https://doi.org/10.32604/csse.2023.033842
[64] Rustam, F., Ashraf, I., Jurcut, A.D., Bashir, A.K., Zikria, Y.B. (2023). Malware detection using image representation of malware data and transfer learning. Journal of Parallel and Distributed Computing, 172: 32-50. https://doi.org/10.1016/j.jpdc.2022.10.001
[65] Taherdoost, H. (2024). Insights into cybercrime detection and response: A review of time factor. Information, 15(5): 273. https://doi.org/10.3390/info15050273
[66] Oladokun, B.D., Enakrire, R.T., Ukubeyinje, E.S., Oyighan, D., Okeke, O.C., Ajani, Y.A. (2024). Cybersecurity behavior in the metaverse: Opportunities, challenges and future trends for libraries. Library Hi Tech News, 43(3): 6-12. https://doi.org/10.1108/LHTN-09-2024-0159
[67] Sallam, M., Al-Mahzoum, K., Sallam, M. (2024). Generative artificial intelligence and cybersecurity risks: Implications for healthcare security based on real-life incidents. Mesopotamian Journal of Artificial Intelligence in Healthcare, 2024: 184-203. https://doi.org/10.58496/MJAIH/2024/019
[68] Kim, H., Shin, Y., Kim, S., Jo, W., Kim, M., Shon, T. (2022). Digital forensic analysis to improve user privacy on Android. Sensors, 22(11): 3971. https://doi.org/10.3390/s22113971
[69] Al-Saeedi, L.A.E., Albo Mohammed, D.F.G., Shakir, F.J., Hasan, F.K., Hasan, F.K., Khaleel, Y.L., Habeeb, M.A. (2024). Artificial intelligence and cybersecurity in face sale contracts: Legal issues and frameworks. Mesopotamian Journal of Cybersecurity, 4(2): 129-142. https://doi.org/10.58496/MJCS/2024/0012
[70] Alshboul, Y., Bsoul, A.A.R., Al Zamil, M., Samarah, S. (2021). Cybersecurity of smart home systems: Sensor identity protection. Journal of Network and Systems Management, 29(3): 22. https://doi.org/10.1007/s10922-021-09586-9
[71] Kuru, K., Kuru, K. (2025). Internet of things and cyber-physical systems UMetaBE-DPPML: Urban metaverse & blockchain-enabled decentralised privacy-preserving machine learning verification and authentication with metaverse immersive devices. Internet of Things and Cyber-Physical Systems, 5: 47-86. https://doi.org/10.1016/j.iotcps.2025.02.001
[72] Rattanawiboonsom, V., Khan, N. (2024). Blockchain technology in mobile payments: A systematic review of security enhancements in mobile commerce. International Journal of Interactive Mobile Technologies, 18(21): 134-148. https://doi.org/10.3991/ijim.v18i21.52099
[73] Fiaz, F., Sajjad, S.M., Iqbal, Z., Yousaf, M., Muhammad, Z. (2024). Metassi: A framework for personal data protection, enhanced cybersecurity and privacy in metaverse virtual reality platforms. Future Internet, 16(5): 176. https://doi.org/10.3390/fi16050176
[74] Li, X., Jiang, C., Du, D., Fei, M., Wu, L. (2023). A novel revocable lightweight authentication scheme for resource-constrained devices in cyber-physical power systems. IEEE Internet of Things Journal, 10(6): 5280-5292. https://doi.org/10.1109/JIOT.2022.3221943
[75] Neppolian, K., Kumar, M.R. (2025). Applying public key cryptography to enhance content protection in maritime logistics and e-commerce. Journal of Internet Services and Information Security, 15(2): 88-102. https://doi.org/10.58346/JISIS.2025.I2.007
[76] Belhocine, Y., Meraoumia, A., Abderrazak, K., Saigaa, M. (2024). Efficient contactless palmprint recognition system based on deep rule-based classification. Acta Informatica Pragensia, 13(2): 193-212. https://doi.org/10.18267/j.aip.236
[77] Naohiro, K., Kenichiro, Y., Ryouichi, S. (2021). Multi-bank identity confirmation platform—A new way to verify user identity using digital technology. NEC Technical Journal, 15(1): 23-26.
[78] Comandè, G., Varilek, M. (2024). The many features which make the eIDAS 2 digital wallet either risky or the ideal vehicle for the transition to post-quantum encryption. Computer Law & Security Review, 54: 106022. https://doi.org/10.1016/j.clsr.2024.106022
[79] Álvarez, I.A., Hölzmer, P., Sedlmeir, J. (2026). Privacy evaluation of the European digital identity wallet's architecture and reference framework. Computers & Security, 160: 104707. https://doi.org/10.1016/j.cose.2025.104707
[80] Ismail, S., Nouman, M., Dawoud, D.W., Reza, H. (2024). Blockchain: Research and applications towards a lightweight security framework using blockchain and

machine learning. Blockchain: Research and Applications, 5(1): 100174. https://doi.org/10.1016/j.bcra.2023.100174
[81] Supangkat, S.H., Firmansyah, H.S., Rizkia, I., Kinanda, R. (2025). Challenges in implementing cross-border digital identity systems for global public infrastructure: A comprehensive analysis. IEEE Access, 13: 42083-42098. https://doi.org/10.1109/ACCESS.2025.3547373
[82] Joshi, H. (2024). Emerging technologies driving zero trust maturity across industries. IEEE Open Journal of the Computer Society, 6: 25-36. https://doi.org/10.1109/OJCS.2024.3505056
[83] Alruwies, M.H., Mishra, S., AlShehri, M.A.R. (2022). Identity governance framework for privileged users. Computer Systems Science & Engineering, 40(3): 995-1005. https://doi.org/10.32604/csse.2022.019355
[84] Kayes, A.S.M., Rahayu, W., Dillon, T., Shahraki, A.S., Alavizadeh, H. (2024). Safeguarding individuals and organizations from privacy breaches: A comprehensive review of problem domains, solution strategies, and prospective research directions. IEEE Internet of Things Journal, 12(2): 1247-1265. https://doi.org/10.1109/JIOT.2024.3481316
[85] Alhelaly, Y., Dhillon, G., Oliveira, T. (2023). When expectation fails and motivation prevails: the mediating role of awareness in bridging the expectancy-capability gap in mobile identity protection. Computers & Security, 134: 103470. https://doi.org/10.1016/j.cose.2023.103470
[86] Al Humaid Alneyadi, M.R.M., Normalini, M.K. (2023). Factors influencing user's intention to adopt AI-based cybersecurity systems in the UAE. Interdisciplinary Journal of Information, Knowledge, and Management, 18: 459-486. https://doi.org/10.28945/5166
[87] Hilowle, M., Yeoh, W., Grobler, M., Pye, G., Jiang, F. (2023). Users' adoption of national digital identity systems: Human-centric cybersecurity review. Journal of Computer Information Systems, 63(5): 1264-1279. https://doi.org/10.1080/08874417.2022.2140089
[88] Hilowle, M., Yeoh, W., Grobler, M., Pye, G., Jiang, F. (2024). Leveraging human-centric cybersecurity to improve usage of national digital identity systems in Australia. Computer, 57(7): 87-98. https://doi.org/10.1109/MC.2024.3395523
[89] Al-Emran, M., Al-Sharafi, M.A., Foroughi, B., Iranmanesh, M., Alsharida, R. A., Al-Qaysi, N., Ali, N.A. (2024). Evaluating the barriers affecting cybersecurity behavior in the metaverse using PLS-SEM and fuzzy sets (fsQCA). Computers in Human Behavior, 159: 108315. https://doi.org/10.1016/j.chb.2024.108315
[90] Mishra, A., Alzoubi, Y.I., Anwar, M.J., Gill, A.Q. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Computers & Security, 120: 102820. https://doi.org/10.1016/j.cose.2022.102820
[91] Malezis, G. (2023). Digital identity: Healthcare's path forward. Network Security, 2023(5). https://doi.org/10.12968/S1353-4858(23)70020-2

APPENDIX

The quality assessment was independently conducted by two reviewers using the five predefined quality assessment criteria (QA1–QA5). Each criterion was scored using a three-point scale (0 = not addressed, 1 = partially addressed, and 2 = fully addressed), resulting in a maximum score of 10. Studies with scores of 8–10 were categorized as High Quality, scores of 5–7 as Moderate Quality, and scores below 5 as Low Quality. All 49 studies satisfied the minimum quality threshold and were therefore included in the thematic synthesis.

Table A1. Individual quality assessment scores

Ref.	First Author (Year)	QA1	QA2	QA3	QA4	QA5	Total	Quality
56	Molitor (2023)	2	2	2	2	1	9	High
57	El-Hajj (2025)	2	2	2	1	2	9	High
58	Kustiawan (2025)	2	2	2	2	1	9	High
59	Raza (2022)	2	2	2	2	1	9	High
60	Odeh (2025)	2	2	2	2	1	9	High
61	Mvah (2023)	2	2	2	2	1	9	High
62	Raich (2024)	2	2	2	2	1	9	High
63	Mahmood (2023)	2	2	2	2	1	9	High
64	Rustam (2023)	2	2	2	2	1	9	High
65	Taherdoost (2024)	2	1	2	2	2	9	High
66	Oladokun (2024)	2	2	2	1	2	9	High
67	Sallam (2024)	2	2	2	2	1	9	High
68	Kim (2022)	2	2	2	2	1	9	High
69	Al-Saeedi (2024)	2	2	2	1	2	9	High
70	Alshboul (2021)	2	2	2	2	1	9	High
71	Kuru (2025)	2	2	2	2	1	9	High
72	Rattanawiboonsom (2024)	2	2	2	2	1	9	High
73	Fiaz (2024)	2	2	2	2	1	9	High
74	Li (2023)	2	2	2	2	1	9	High
75	Neppolian (2025)	2	2	2	2	1	9	High
76	Belhocine (2024)	2	2	2	2	1	9	High
77	Naohiro (2021)	2	1	2	2	2	9	High
78	Comandè (2024)	2	2	2	2	1	9	High
79	Álvarez (2026)	2	2	2	2	1	9	High
80	Ismail (2024)	2	2	2	2	1	9	High
81	Supangkat (2025)	2	2	2	2	1	9	High
82	Joshi (2024)	2	2	2	2	1	9	High

83	Alruwies (2022)	2	2	2	2	1	9	High
84	Kayes (2024)	2	2	2	2	1	9	High
85	Alhelaly (2023)	2	2	2	1	1	8	High
86	Alneyadi (2023)	2	2	2	1	1	8	High
87	Hilowle (2023)	2	2	2	1	1	8	High
88	Hilowle (2024)	2	2	2	1	1	8	High
89	Al-Emran (2024)	2	2	2	1	1	8	High
90	Mishra (2022)	2	2	2	1	1	8	High
91	Malezis (2023)	2	2	2	1	1	8	High
32	Seo (2025)	2	2	1	1	1	7	Moderate
33	Xian (2025)	2	2	1	1	1	7	Moderate
34	Ferdous (2019)	2	1	2	1	1	7	Moderate
35	Alanzi (2025)	2	2	1	1	1	7	Moderate
36	Rose (NIST)	2	1	2	1	1	7	Moderate
37	Zyskind (2015)	2	2	1	1	1	7	Moderate
38	Aloul (2009)	2	1	2	1	1	7	Moderate
39	Saeed (2024)	2	2	1	1	1	7	Moderate
40	Osamor (2025)	2	2	1	1	1	7	Moderate
41	Abdullah (2025)	2	1	2	1	1	7	Moderate
42	Investigation Between Data Breaches (2020)	2	2	1	1	1	7	Moderate
43	Nassif (2021)	2	2	1	1	1	7	Moderate
44	Ali (2024)	2	1	2	1	1	7	Moderate
45	Alshaikh (2020)	2	2	1	1	1	7	Moderate

Table A2. Summary of quality assessment results

Quality Category	Score	Number of Studies	Percentage
High Quality	8–10	35	71.4%
Moderate Quality	5–7	14	28.6%
Low Quality	0–4	0	0%
Total	–	**49**	**100%**