مجلة جامعة الشارقة للعلوم الإنسانية والاجتماعية

جامعة الشارقة
UNIVERSITY OF SHARJAH

University of Sharjah Journal of Humanities & Social Sciences

A Refereed Scientific journal

Vol. 22, No. 3
Rabi' al-Awwal 1447 A.H. / September 2025 A.D.

ISSN : 1996-2339

University of Sharjah Journal for Humanities & Social Sciences, Volume 22, No. 3 September 2025
https//:doi.org/10.36394/jhss/22/3/12

The Role of National Digital Identity in Accelerating the Processes of Digital Transformation: "A Review"

Abdelrahman Ahmed Alhammadi(1)

Saadat M. Alhashmi(2)

Mohammad Lataifeh(3)

John Lewis Rice(4)

Received on: 30 - 01 - 2024 **Accepted on: 07 - 08 - 2024**

Abstract:

This paper examines the increasing prevalence of National Digital Identity (NDI) systems, with a focus on their design, application, and the obstacles to their implementation across various nations. Digital identification systems are indispensable for national security, surveillance, and efficient service management. Systems like Aadhaar in India, MERNIS in Turkey, RENIEC in Peru, and CNIC in Pakistan are used for security management, criminal investigations, and population data collection. However, legislative, ethical, and legal issues, particularly privacy and data protection concerns, have impeded their deployment.

This study aims to describe the concept of NDI, its impact on digital

(1) College of Arts, Humanities and Social Sciences - University of Sharjah (Sharjah - U.A.E.) U20102623@Sharjah.ac.ae

(2) Computing and Informatics - University of Sharjah (Sharjah - U.A.E.)

(3) Computing and Informatics - University of Sharjah (Sharjah - U.A.E.)

(4) College of Business Administration - University of Sharjah (Sharjah - U.A.E.)

transformation, and evaluate its alignment with digital agendas. The problem statement addresses challenges in implementing NDI, including privacy, data protection, legislation, and technological infrastructure. A systematic literature review elucidates the reasons for implementing NDI systems and provides insights into their potential benefits and limitations as part of a country's digital transformation agenda.

Keywords: Digital Identification Systems, National Digital Identity (NDI), Biometric Identity Systems, Digital Transformation, Identity Management Systems

1. Introduction

Digital identification systems have become vital to different aspects of society, including education, welfare services, elections, financial services, employment, and security. Technological advancements have made these identification systems integral to national surveillance and security strategies worldwide (Gelb & Metz, 2018). An identity encompasses features that distinguish a person or an entity from others (Crossman, 2017). While identity has several features, its primary purpose is to provide proof of individual uniqueness, establish trust and ensure accountability. An identity (ID) is a collection of economic, social, and legal transactions involving individuals or entities. IDs can be foundational or functional (Tinyakova & Morozova, 2020). Foundational IDs are multipurpose identification systems or features that identify the entire population, thus providing the basis for public and private sector decision-making. Functional IDs have specific roles, encompassing driving permits, ration cards, tax ID numbers, and voter IDs (Geteloma et al., 2019). These IDs only cover a small subset of the population. Regardless of the ID type, there has been an enhanced clamour to digitise these systems and identification features. Proponents of digital IDs argue that they provide several benefits for individuals, businesses, and the government (Eke et al., 2022). This paper examines various designs, use cases, and challenges of NDI systems and determines their relevance to different countries' digital transformational agendas.

National Digital Identity (NDI) systems are electronic platforms that capture and store information about individuals or entities to help identify them uniquely. These systems use digital tools to validate, store, transfer, authenticate, and verify credentials. Identity management systems link individuals with offline and online identities, providing a digital framework.

Many countries are registering their citizens on digital systems, with some maintaining foundational identification systems that allow private and public sectors to identify people using national IDs (Eke et al., 2022).

National biometric identity systems are gaining popularity in many countries for various reasons, such as security management, criminal investigations, and population data gathering. India's national biometric identity system, Aadhaar, was approved by the Supreme Court to support taxation and financial purposes but not for student registration, banking, or private phone systems (Tinyakova & Morozova, 2020). Turkey's Turkish electronic ID card and Peru's National Registry of Identification and Civil Status (RENIEC) are national digital ID systems linked to other official databases (Kwiringira, 2017). Pakistan's Computerised National Identity Card (CNIC) is the legal digital ID for all Pakistani citizens and is used for financial inclusion, social programs, pension disbursement, voting, and offline and online identification (Bhandari, 2020). Other countries that have launched digital IDs include Mexico, Bangladesh, Kazakhstan, Uruguay, and Chile.

Some countries have yet to be able to adopt identity management systems due to legislative, ethical, and legal issues (Kwiringira, 2017). For example, the court halted Kenya's identity management system because there was no proper legislative framework to handle biometric identity systems, especially regarding data protection and privacy issues. Similarly, in the UK, citizens opposed the proposed Identity Act, citing government overreach. Privacy and data protection concerns have also slowed the development of similar systems in the United States.

However, some countries have enacted laws on national identity systems or have already implemented their digital ID systems (Jain & Rangaswamy, 2020). Jamaica passed the National Identification and Registration Act (NIRA), which the government argued would pave the way for a new national identification system (NIDS). According to Jamaican authorities, the new system would help verify citizens' identities and provide better services efficiently. However, the Act faced opposition as it intruded on people's biometric data and introduced criminal sanctions for non-compliance. The Jamaican Supreme Court declared NIRA null and void for various reasons. Similar identification systems have been challenged in Japan, Australia, and Canada (Eke et al., 2022). This systematic literature review establishes why countries implement NDI systems and whether they are consistent with their digital transformation agenda. Therefore, this work attempted to answer the following research question:

Research Question: How do governments, businesses, and individuals use NDI systems worldwide?

Problem Statement: Many countries face significant challenges in implementing National Digital Identity as part of their efforts to accelerate the process of achieving digital transformation. These challenges include issues related to privacy, data protection, legislation, and technological infrastructure.

In line with the research question and the problem statement, this work is set to achieve the following objectives:

1. Describe the concept of National Digital Identity, its objectives, and impact on accelerating the process of digital transformation.
2. Explain the different types and perspectives related to National Digital Identity in the context of digital transformation.
3. Evaluate the relationship between National Digital Identity and the digital transformation agenda of different countries, focusing on challenges and potential solutions.
4. Analyze the potential benefits and limitations associated with adopting National Digital Identity as part of the national digital transformation agenda.
5. Identify research gaps and propose future areas for research and development in the field of National Digital Identity and digital transformation.

The rest of the paper consists of three sections, i.e., systematic literature review methodology, results, discussions, and conclusions. The systematic literature review section described the study design, including how the data was collected, synthesised and analysed. It explained the value of using the PRISMA process for the literature review. The results and discussion section presents the articles selected for the review, their contents and discussions of various themes they express. The conclusion section summarises the research findings, describes its limitations and provides insights into the study's implications.

2. Systematic literature review methodology

A systematic literature review allows researchers to identify and evaluate relevant studies on a topic. It involves carefully reviewing and analysing existing data to answer specific research questions. This method is effective in studies where data already exist, and a systematic review is chosen for its ability to review high-quality studies in a transparent and replicable manner.

To conduct a comprehensive systematic literature review, researchers collect, filter, and review different articles based on their scope, clarity, and objectivity. They use structured criteria to identify, retrieve, and evaluate relevant published articles within the scope of the study. This review helps to evaluate past studies on the objectives of digital identity for the government, businesses, and individuals, as well as the limitations of existing studies.

The literature review process involves quantitative, qualitative, and empirical studies on digital identity. Conceptual studies suggest different digital identity constructs and relationships, providing in-depth insights into the multidisciplinary nature of NDI.

2.1. PRISMA Process

In the previous section, we discussed how Systematic Literature Review (SLR) helps identify relevant studies. One commonly used method for conducting SLR is the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) methodology. As Xiao and Watson (2019) described, PRISMA is a systematic process for selecting and synthesising literature. We adopt PRISMA to ensure valid, reliable, and pertinent studies are included in our research analysis (Selçuk, 2019). Effective PRISMA methodology involves ten steps (see Figure 1).

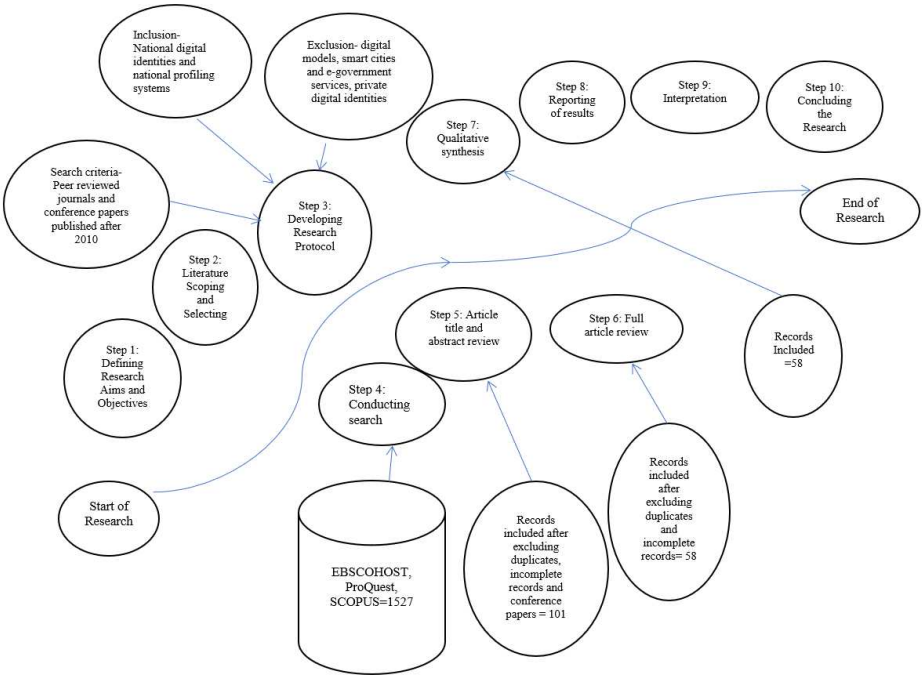

Figure 1: PRISMA Methodology

2.2. Research Aim and Objectives

This SLR aims to describe NDI, its various elements, and how it is implemented in different countries. This work achieved this goal by evaluating literature, including case studies, empirical data, and theories on NDI, its potential benefits, and challenges.

2.3. Literature Scoping and Selecting

The literature scoping and selection encompassed identifying appropriate keywords and a combination of keyword strings that can be used to conduct literature searches to achieve the study objectives. The keywords were derived from various components of the digital ecosystem (see Figure 2).

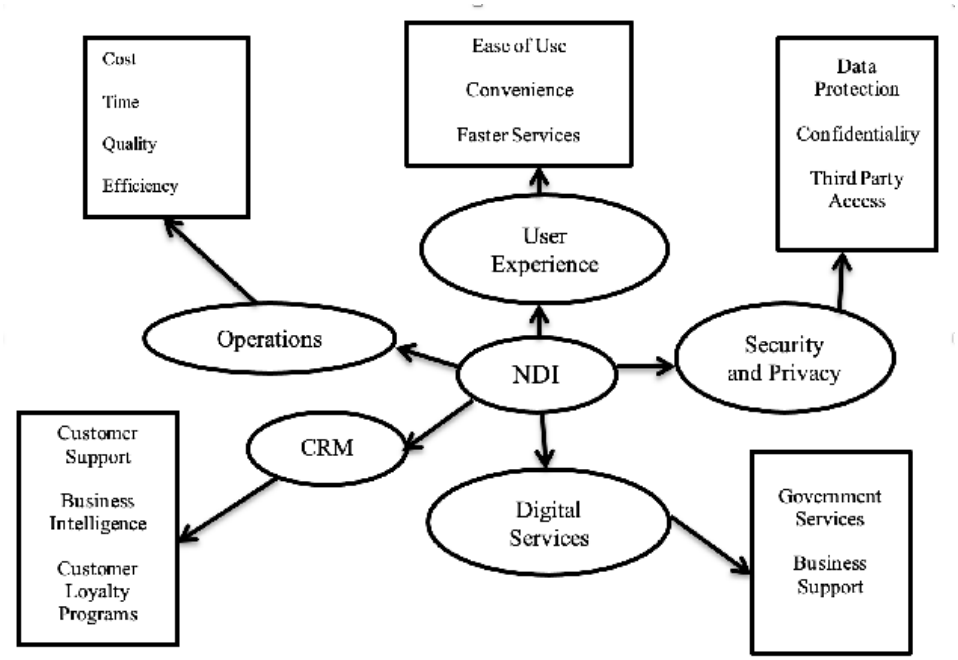

Figure 2: Digital Identity Ecosystem

Following the digital ecosystem shown in Figure 2, a combination of eight keyword strings (Table 1) was used to conduct a literature search on EBSCOhost, SCOPUS, and ProQuest. The data from these databases are reliable and justified for academic research. Furthermore, these databases contain hundreds of thousands of resources on digital technology, thus appropriate for the current study. The search strings included digital identities, NDI, national profiling systems, and national digitalisation programs.

The keyword strings used in the systematic literature review are summarized in Table 1.

RQ	How do governments, businesses, and individuals use national digital identities and profiling systems worldwide?	EBSCOHOST	ProQuest	SCOPUS	Total
SLR	ALL (national digital identity OR national profiling systems OR e-government identity) AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp")) AND (LIMIT-TO (LANGUAGE, "English")) AND (LIMIT-TO (SRCTYPE, "j") OR LIMIT-TO (SRCTYPE , "p"))	566	268	693	1527

Table 1: Keyword Strings for Systematic Literature Review

2.4. Developing Research Protocol

The research protocol outlined search and inclusion/exclusion criteria. EBSCOhost, SCOPUS, and ProQuest were selected for their reliable, current peer-reviewed articles. Peer review ensures article validity and quality. Data from these databases underwent rigorous screening before inclusion in our synthesis.

Since NDI is relatively new, records from 2000 onwards were reviewed. Search criteria included English peer-reviewed articles and conference papers. Inclusion criteria covered qualitative, quantitative, and mixed-method studies on NDI and its aspects. Exclusion criteria involved non-English papers, duplicates, editorials, and non-peer-reviewed publications.

2.5. Conducting Search

The inclusion and exclusion process of articles is summarized in Figure 3.

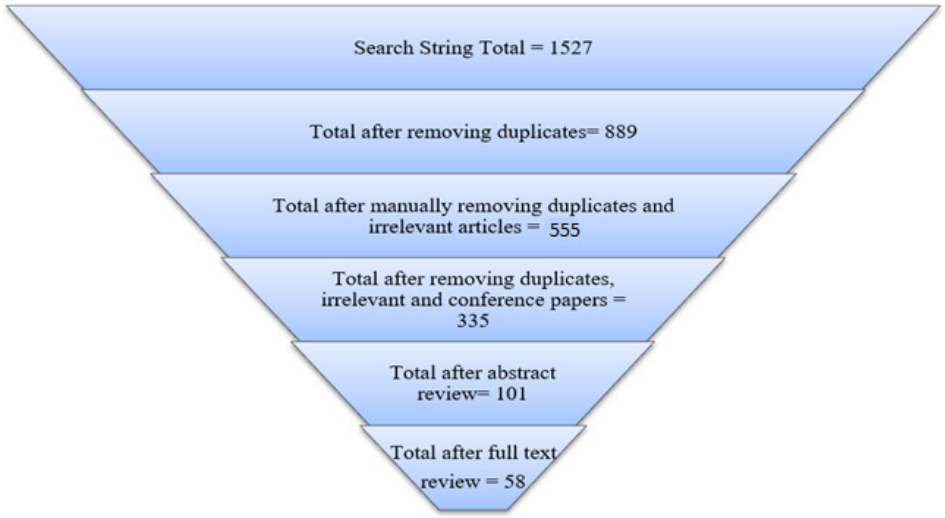

Figure 3: Summary of Inclusion and Exclusion Process

The search targeted databases likely yielded numerous articles, resulting in 1527 records from SCOPUS, EBSCOhost, and ProQuest (Figure 2). These comprised 566 from EBSCOhost, 268 from ProQuest, and 693 from SCOPUS, reflecting various combinations of search keywords (Table 2.1). To streamline the process, duplicates were removed using EndNote, leaving 889 records. The manual review further refined the selection, eliminating

334 records unrelated to NDI, profiling systems, and digital transformation (Borissov et al., 2022). Additionally, 220 conference papers were excluded due to concerns about academic credibility (Scherer & Saldanha, 2019). This step reduced the pool to 335 relevant records. Subsequent scrutiny of titles and abstracts narrowed the selection to 101 articles meeting predefined criteria (Khabsa et al., 2015). These articles were further categorised based on their alignment with different elements of the NDI ecosystem outlined in Figure 2 and Table 2.

The records are categorized based on research objectives in Table 2.

Category	Number of records	Significance of the record
NDI concept	Broekhuizen et al. (2021), Eke et al. (2022), Geteloma et al. (2019), Gorensek & Kohont (2019), Mcloughlin et al. (2013), Medaglia et al. (2022). Mergel et al. (2019), Rao & Nair (2019), Scaria (2022), Aichholzer & Strauß (2010), Mir et al. (2020), Mukhopadhyay et al. (2019), Sullivan (2016), Sullivan (2018), Ajana (2015), Al Sulaimani & Ozuem (2022), Leese (2020), Mavriki & Karydan (2022)	Explain the concept of NDI.
Profiling system concept	Krishna (2020), Sullivan (2009), Sullivan (2014), De Andrés et al. (2015), Gastil & Richards (2017), Salmasi & Gillam (2010), Noack & Kubicek (2010), Rao & Nair (2019).	Describe the available profiling systems around the world.

e-government	Aichholzer & Strauß (2010), Dutton et al. (2005), Guenduez et al. (2022), Sullivan (2018), Al Sulaimani & Ozuem (2022), Arun (2017), Gastil & Richards (2017), Sharma & Panigrahi (2015), Srivastava & Teo (2009). Althunibat et al. (2021), Goede (2019), Kassen (2019), Kumari & Khan (2013), Kurfalı et al. (2017), Nasri (2019), Tomura et al. (2021).	Examine how digital identities influence access to e-government services.
NDI/profiling system from an operational perspective	Aichholzer & Strauß (2010), Dutton et al. (2005), Guenduez (2020), Mir et al. (2020), Mukhopadhyay et al. (2019), Rössler (2008), Skierka (2023), Sule et al. (2021), Sullivan (2014), Sullivan (2016), Sullivan (2018), Ajana (2015), Al Sulaimani & Ozuem (2022), Arun (2017), Gao & Hu (2021), Gastil & Richards (2017), Marino & Lo Presti (2018), Sharma & Panigrahi (2015), Leese (2020), Mavriki & Karyda (2022), Broekhuizen et al. (2021), Jain & Gabor (2020), Kumari & Khan (2013), Wolfond (2017).	Discuss how NDI or profiling systems work, their efficiency, and their effectiveness.

NDI/profiling system from the user experience perspective	Krishna (2020), Mukhopadhyay et al. (2019), Rössler (2008), Sule et al. (2021), Ajana (2015), Al Sulaimani & Ozuem (2022), De Andrés et al. (2015), Dunn (2020), Gao & Hu (2021), Gastil & Richards (2017), Makarychev & Wishnick (2022), Srivastava & Teo (2009), Stepančič & Blažic (2018).	Explain how users feel or perceive NDI/profiling system applications.
NDI/profiling system from privacy and security perspective	Dutton et al. (2005), Guenduez et al. (2022), Sule et al. (2021), Sullivan (2014), Sullivan (2016), Sullivan (2018), Arun (2017), Dunn (2020), Gastil & Richards (2017), Salmasi & Gillam (2010), Sharma & Panigrahi (2015), Leese (2020), Mavriki & Karyda (2022), Stepančič & Blažič (2018), Beduschi (2019), Eke et al. (2022), Holt & Malčić (2015), Joshi et al. (2001).	Discuss the privacy and security issues that influence the application of NDI/profiling systems.
NDI/profiling system and digital services	Mir et al. (2020), Mukhopadhyay et al. (2019), Rössler (2008), Ajana (2015), Al Sulaimani et al. (2022), Dunn (2020), Marino & Lo Presti (2018), Salmasi & Gillam (2010), Sharma & Panigrahi (2015), Stepančič & Blažič (2018).	Examine how NDI/profiling system impacts digital services.

NDI and customer relationship management (CRM)	Althunibat et al. (2021), Jain & Gabor (2020), Kassen (2019), Kumari & Khan (2013), Manesh et al. (2016), Mcloughlin et al. (2013), Mergel et al. (2019), Nasri (2019), Noack & Kubicek (2010), Wolfond, G. (2017).	Discuss how NDI and profiling systems affect the relationship between the government and users such as businesses and individuals.

Table 2: Categorization of Records by Research Objectives

2.6. Full Article Review

Following the initial screening, 101 peer-reviewed journal articles were further categorised into five groups, each addressing different aspects of the NDI ecosystem. These categories encompass user experience, digital services, government services, customer relationship management (CRM), operations, and security and privacy perspectives. Notably, articles could address multiple aspects simultaneously. Subsequently, articles were ranked into quartiles to gauge their value for the study. Q1 included systematic literature reviews and quantitative studies with large sample sizes (more than 500 participants), ensuring robust data reliability and generalizability. Q2 comprised other quantitative studies, literature reviews, and qualitative studies based on expert opinions, providing additional insights. Q3 and Q4 encompassed qualitative studies and opinion-based papers, offering supplemental understanding but less robust evidence. These articles were assessed individually for their relevance to the research.

The ranking of articles is summarized in Table 3.

Category of articles	Ranking				Total
	Q1	Q2	Q3	Q4/No Quartile	
User experience	11	9	7	3	30
Digital services/e-government services	14	12	17	5	51
CRM	2	4	5	1	11
Operations	17	9	10	4	45
Security and privacy	10	7	8	4	29
Total number of articles per ranking level	*33*	*25*	*34*	*9*	*101*

Table 3: Ranking of Articles

NB: One article can address more than the NDI or national profiling system perspective.

Out of the 101 reviewed articles, 58 (33 Q1, 25 Q2) addressed the research question effectively. Articles categorised as Q3 and Q4 were excluded. Specific categories included 30 on user experience, 51 on digital/ e-government services, 11 on CRM, 45 on NDI operation, and 29 on NDI security/privacy. These 58 articles were divided into NDI perspectives as shown in Figure 4.

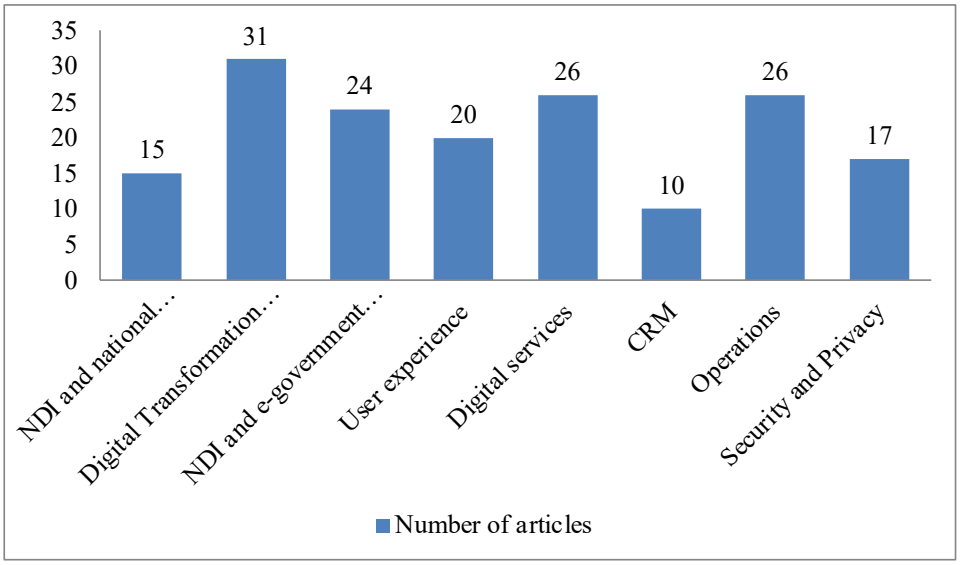

Figure 4: NDI from Different Perspectives

2.7. Qualitative synthesis

Qualitative synthesis encompassed analysis and comparison of the 58 articles selected after a full review. At first, we conducted a template analysis that involved three stages. In stage 1, we developed a priori template, (see Table 4).

1. NDI concept
1.1. NDI and National Profiling System Concept
1.2. Digital Transformation Agenda
1.3. NDI and e-government services
2. Features of NDI and National Profiling System
2.1. NDI from a user experience perspective
2.2. NDI from a digital services perspective
2.3. NDI from a customer relationship management (CRM) perspective
2.4. NDI from a privacy and security perspective
2.5. NDI from an operations perspective

Table 4: Priori Template

In stage 2, all the publications are divided to examine the NDI phenomenon and how they are discussed in the literature. The data extraction method includes the type of study, including quantitative, qualitative, mixed method, and abstract methods are shown in Figure 5.

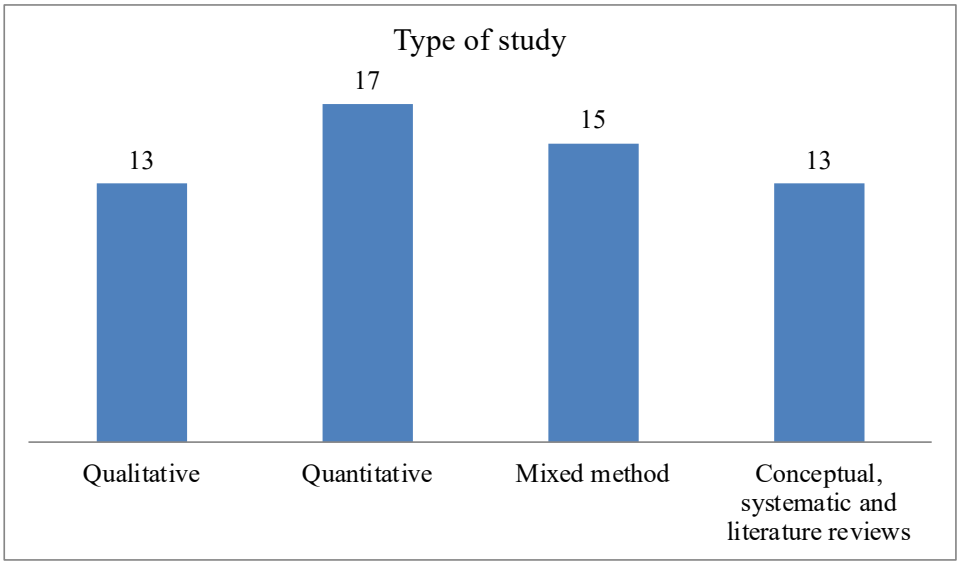

Figure 5: Types of Study Included in the Research

We used a grounded theory approach in analysing the articles. The process began by reading and evaluating five papers to identify themes and codes for analysis. After that, another set of five papers compared them with the earlier sets. The themes were then reorganised and discussed based on how various authors conceptualised and discussed various ideas. After that, the synthesised results are reported in the following sections.

3. Results

At this stage, we presented the results of the analysis. The section includes descriptive statistics, content analysis, and qualitative synthesis results.

3.1. Descriptive statistics

The review included 58 articles, all of which were journal articles. The most common outlets were Computer Law & Security Review (5), Government Information Quarterly (4), and Information Polity (4), (see Table 5).

Journals	***Count***
Information Polity	2
Archives of Business Research	1
Big Data & Society	1
Communications of the Association for Information Systems	1
Computer	1
Computer Law & Security Review	5
Computers in Human Behavior	1
Digital Government at Work	1
Geopolitics	1
Government Information Quarterly	4
Identity in the Information Society	1
Information Systems Journal	1
Information Technology for Development	2
International Journal for Applied Information Management	2
International Journal of Electronic Governance	2
International Journal of Euro-Mediterranean Studies	1

International Journal of Public Administration in the Digital Age	1
ISACA Journal	1
Journal of Business Research	1
Journal of Information Policy	3
Journal of Information	3
Communication and Ethics in Society	3
Journal of Physics	1
Journal of Responsible Technology	1
Journal of South Asian Studies	1
Kuwait Chapter of Arabian Journal of Business and Management Review	1
New political economy	1
Online Information Review	1
PS: Political Science & Politics	1
Security and Communication Networks	1
Social Sciences	1
Surveillance & Society	1
Sustainability	1
Technology in Society	1
Technology Innovation Management Review	1
Transforming Government: People	1
Process and Policy	3
Urban Studies	1
Wireless Communications and Mobile Computing	1

Table 5: Articles Included in the Analysis

The articles included in the study were published between 2001 and 2022. The year of publications is summarized in Figure 6..

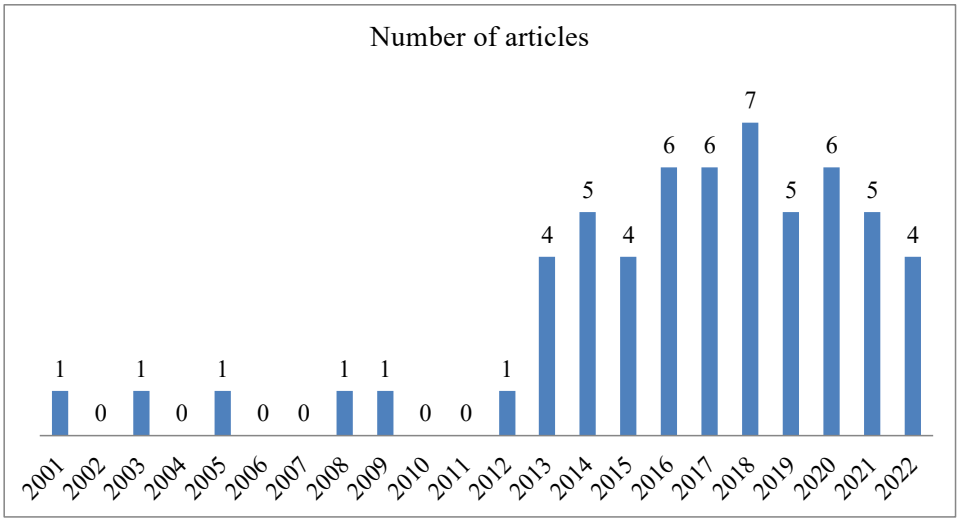

Fig. 6: Year of Publications

Most articles were published between 2016 and 2022 (39), with 70% published in that period. Most discussions on NDI and national profiling systems are relatively recent.

3.2. Content Analysis

Deriving from the digital identity ecosystem in Figure 2 and the contents of the articles under synthesis, we identified the themes and summarised the codes. (see Table 6).

Conceptual Themes	Organising Themes	Codes	References

NDI Concept	NDI and National Profiling System	Digital Identity in Estonia The digital identity used in Japan, Germany Blockchain digital identities Localised digital identities Features and uses of the Aadhar system in India	(Aichholzer & Strauß, 2010, Al-Khouri, 2012, Breslo Geteloma, Ayo & Goddy-Wurlu, 2019, Goede, 2019, 2020, Noack & Kubicek, 2010, Scaria, 2022, Sullivar Sullivan, 2016, Sullivan, 2018, Wolfond, 2017)
	Digital Transformation Agenda	Effectiveness of digital identity in different countries India's Aadhar system Authentication and verification protocols Efficacy of government service provision	(Aichholzer & Strauß, 2010, Ajana, 2015, Al-Khouri, Ozuem, 2022, Al-Shboul et al., 2014, Bradford et al., Broekhuizen et al., 2021, De Andrés et al., 2015, Dun Ebrahim & Irani, 2005, Eke, D., Oloyede et al., 2022, Gunawong & Gao, 2017, Holt & Malčić, 2015, Jain & al., 2001, Kassen, 2019, Krishna, 2020, Kumari & Kh Wishnick, 2022, Manesh et al., 2016, Mergel, Edelma 2020, Mukhopadhyay et al., 2019, Rao & Nair, 2019, Gillam, 2010, Srivastava & Teo, 2009, Stepančič & B
	NDI and e-government services	Access to government services Perceived Quality and Usefulness of the Digital Identity	(Aichholzer & Strauß, 2010, Ajana, 2015, Al-Khouri, Ebrahim & Irani, 2005, Eke et al., 2022, Gao & Hu, 2 Goede, 2019, Guenduez, Mettler, & Schedler, 2022, G & Malčić, 2015, Jain & Gabor, 2020, Joshi et al., 200 al., 2017, Mavriki & Karyda, 2022, Mcloughlin, Wils et al., 2022, Nasri, 2019, Scaria, 2022, Sharma & Pan Zulkifli et al., 2015)

Features of NDI	User experience perspective	Client or user's perceptions of digital identities Effect on access to government services Digital Identities and democracy Legitimacy and legal perspectives regarding digital identities	(Al Sulaimani & Ozuem, 2022, Al-Shboul et al., 2014 2019, Breslow, 2020, Broekhuizen et al., 2021, De An 2020, Guenduez, Mettler & Schedler, 2022, Gunawon & Wishnick, 2022, Manesh, Hadavand & Tahmasbiza Mukhopadhyay et al., 2019, Nasri, 2019, Rössler, 200 Srivastava & Teo, 2009, Stepančič & Blažič, 2018, Su 2021, Sullivan, 2014, Sullivan, 2016, Wolfond, 2017,
	Digital services perspective	Government identification services Digital identity in healthcare access Social protection and security services Education sector Security issues	(Aichholzer & Strauß, 2010, Ajana, 2015, Al-Khouri, Ebrahim & Irani, 2005, Eke et al., 2022, Gao & Hu, 2 Goede, 2019, Guenduez, Mettler, & Schedler, 2022, G & Malčić, 2015, Jain & Gabor, 2020, Joshi et al., 200 al., 2017, Mavriki & Karyda, 2022, Mcloughlin, Wils et al., 2022, Nasri, 2019, Scaria, 2022, Sharma & Pan Zulkifli et al., 2015, Goede, 2019, Gorensek & Kohont, 2019)
	CRM perspective	Access to services in some businesses Financial sector applications Marketing and telecommunication applications	(Ajana, 2015, Bradford, Earp & Grabski, 2014, De An 2020, Gorensek & Kohont, 2019, Jain & Gabor, 2020 Manesh et al., 2016, Mcloughlin, Wilson & Martin, 2 2018)
	Privacy and Security Perspective Operational Perspective	Privacy regulations Security vulnerabilities Users' privacy perceptions Users' security perceptions Recommendations for data protection Cost advantages Time savings Quality of the system Efficiency NDI infrastructure NDI design	(Al-Shboul et al., 2014, Arun, 2017, Beduschi, 2019, 2005, Gastil & Richards, 2017, Leese, 2020, Mavriki Kubicek, 2010, Salmasi & Gillam, 2010, Sule, Zenna 2009, Sullivan, 2016, Tomura et al., 2021, Остроушк Sharma & Panigrahi, 2015) (Aichholzer & Strauß, 2010, Bradford, Earp & Grabs Ebrahim & Irani, 2005, Eke et al., 2022, Gao & Hu, 2 Guenduez, Mettler & Schedler, 2022, Gunawong & C 2015, Joshi, J., Ghafoor et al., 2001, Kassen, 2019, K Mavriki & Karyda, 2022, Mcloughlin et al., 2013, Mc 2020, Noack & Kubicek, 2010, Rao & Nair, 2019, Rö Sullivan, 2016, Sullivan, 2018, Wolfond, 2017, Zulki

Table 6: Conceptual and Organizing Themes with Corresponding Codes and References

	4, Arun, 2017, Beduschi, ndrés et al., 2015, Dunn, ng & Gao, 2017, Makarychev adeh, 2016, Mir et al., 2020, 08, Salmasi & Gillam, 2010, ule, Zennaro & Thomas, Остроушко, 2022)
	2012, Althunibat et al., 2021, 2021, Geteloma et al., 2019, Gunawong & Gao, 2017, Holt 1, Kassen, 2019, Kurfalı et son & Martin, 2013, Medaglia igrahi, 2015, Skierka, 2023,
	ndrés et al., 2015, Dunn, , Kumari & Khan, 2013, 013, Stepančič & Blažič,
	Dunn, 2020, Dutton et al., & Karyda, 2022, Noack & ro & Thomas, 2021, Sullivan, o, 2022, Scaria, 2022,
	ki, 2014, Dunn, 2020, 2021, Geteloma et al., 2019, Gao, 2017, Holt & Malčić, rishna, 2020, Leese, 2020, edaglia et al., 2022, Mir et al., össler, 2008, Sullivan, 2009, fli et al., 2015)

The themes are discussed as follows:

3.2.1. NDI concept

The review broadly defines NDI as the creation and implementation of digital identities by governments to authenticate citizens' identities (Aichholzer & Strauß, 2010; Goede, 2019; Krishna, 2020; Mir et al., 2020; Noack & Kubicek, 2010; Scaria, 2022; Sullivan, 2016, 2018; Wolfond, 2017). It reveals that digital identities can be localised, centralised, or decentralised for various purposes (Al-Khouri, 2012; Breslow, 2020; Eke et al., 2022; Geteloma, Ayo & Goddy-Wurlu, 2019; Sullivan, 2009, 2014). Localised and decentralised identities serve specific areas or purposes (Geteloma, Ayo & Goddy-Wurlu, 2019), while centralised identities are managed globally by governments to deliver services (Aichholzer & Strauß, 2010; Goede, 2019; Krishna, 2020; Scaria, 2022). These discussions lead to three sub-themes in the NDI concept.

NDI and the national profiling system

The national profiling system is a system innovation (Aichholzer & Strauß, 2010) that helps the government achieve its digital governance objectives (Breslow, 2020), such as ensuring that all citizens can access services on a single platform (Mir et al., 2020), surveillance and reaching minority communities (Krishna, 2020). The profiling system can either be centralised or nationalised, like the Aadhar system in India (Krishna, 2020) and the e-identity system of Austria (Aichholzer & Strauß, 2010). NDI can also be decentralised and localised, such as the UAE Smart Pass system (Al-Khouri, 2012) or the Canadian system that uses blockchain technology (Wolfond, 2017). NDI, the national profiling system's primary objective, ensures convenient, accurate, and efficient identification, authentication,

and verification of people accessing certain services (Mir et al., 2020, Noack & Kubicek, 2010, Scaria, 2022).

While the private sector developed digital identities to enable their customers to access services (Geteloma, Ayo & Goddy-Wurlu, 2019), NDIs have become an emerging legal identity that can be used in place of physical identity documents such as social security cards (Sullivan, 2009, Sullivan, 2014, Sullivan, 2016, Sullivan, 2018). Other studies noted that national profiling systems and NDIs use features such as fingerprints, facial recognition, DNA samples, etc. which makes them more accurate, convenient, and accessible compared to conventional IDs (Breslow, 2020; Eke et al., 2022; Geteloma, Ayo & Goddy-Wurlu, 2019; Goede, 2019; Krishna, 2020; Mir et al., 2020: Noack & Kubicek, 2010).

Digital Transformation Agenda

The national profiling system, considered a system innovation (Aichholzer & Strauß, 2010), serves the government's digital governance goals (Breslow, 2020). It enables universal service access (Mir et al., 2020) and facilitates surveillance and outreach to minority communities (Krishna, 2020). Systems can be centralised or nationalised, like India's Aadhar and Austria's e-identity system (Krishna, 2020; Aichholzer & Strauß, 2010). NDI can also be decentralised, as seen in the UAE Smart Pass and Canadian blockchain-based systems (Al-Khouri, 2012; Wolfond, 2017). NDIs aim to ensure convenient, accurate, and efficient identification, authentication, and verification (Mir et al., 2020; Noack & Kubicek, 2010; Scaria, 2022).

While the private sector develops digital identities for customer service access (Geteloma, Ayo & Goddy-Wurlu, 2019), NDIs emerge as legal identities replacing physical documents like social security cards (Sullivan,

2009, 2014, 2016, 2018). National profiling and NDI systems utilise features such as fingerprints and facial recognition, enhancing accuracy, convenience, and accessibility (Breslow, 2020; Eke et al., 2022; Geteloma, Ayo & Goddy-Wurlu, 2019; Goede, 2019; Krishna, 2020; Mir et al., 2020; Noack & Kubicek, 2010).

NDI and e-government services

NDIs are integral to many governments' digital visions. Their use evolves (Sharma & Panigrahi, 2015; Skierka, 2023; Zulkifli et al., 2015), with dynamic interactions between governments and stakeholders in e-government projects (Sharma & Panigrahi, 2015; Zulkifli et al., 2015). Government IT professionals develop and manage systems, including profiling systems and digital identities, to support policy decisions and enhance business processes (Geteloma et al., 2019; Goede, 2019; Guenduez, Mettler, & Schedler, 2022).

Governments utilise web-based digital identity systems for various purposes, such as electronic payments, health records, passports, licenses, and voting (Mcloughlin, Wilson & Martin, 2013; Medaglia et al., 2022; Nasri, 2019; Mavriki & Karyda, 2022). These systems incorporate biometric data, one-time passwords, and smart cards for user identification and authentication (Mavriki & Karyda, 2022; Mcloughlin, Wilson & Martin, 2013; Medaglia et al., 2022; Nasri, 2019).

The use of NDIs varies across states. Autocratic regimes like Russia and China employ these technologies for surveillance purposes Ajana (2015), while democratic nations like Estonia and Taiwan utilise digital identity tools to prevent draconian measures (Aichholzer & Strauß, 2010; Althunibat et al., 2021; Guenduez, Mettler, & Schedler, 2022; Kassen, 2019; Kurfalı et al., 2017).

These systems play critical roles in health emergencies, as seen in Taiwan's effective Covid-19 response using digital identity for lockdown enforcement and case tracking (Gao & Hu, 2021). Furthermore, digital identities facilitate citizen-government interactions, enhancing engagement and trust (Medaglia et al., 2022; Nasri, 2019; Scaria, 2022).

3.2.2. Features of NDI

The focused literature revealed that NDIs were deployed differently in different countries, with various implications for users and policymakers. Therefore, we divided the features of NDI into the sub-themes discussed below:

NDI from an operational perspective

The review revealed multiple designs and infrastructure for NDI and national profiling systems. The designs included centralised, national identity systems such as Aadhar in India (Krishna, 2020), Singapore system (Gunawong & Gao, 2017), Taiwan system (Gao & Hu, 2021), Estonia system (Aichholzer & Strauß, 2010) and the proposed Nigerian system (Eke et al., 2022). These systems are designed to enable citizens to access multiple government services under a single platform (Bradford, Earp & Grabski, 2014; Dunn, 2020). It enabled the government to trace its citizens during disasters such as pandemics (Mavriki & Karyda, 2022).

National centralised identity systems, utilising unique numbers and biometric data, streamline citizen identification (Mir et al., 2020), enhancing authentication and verification for accessing government services (Eke et al., 2022; Gao & Hu, 2021; Geteloma et al., 2019). These systems reduce the time and costs associated with service access (Noack & Kubicek, 2010; Rao & Nair, 2019; Rössler, 2008).

Decentralised and localised digital identity systems serve specific purposes like smart city projects and health information systems (Al-Khouri, 2012; Mcloughlin et al., 2013; Rao & Nair, 2019). Often serving as legal identification, they offer users greater control over their data, particularly with blockchain-based systems (Wolfond, 2017). These decentralised systems minimise data manipulation opportunities by distributing data across various databases (Wolfond, 2017).

NDI from a user experience perspective

Users' perceptions of digital identities vary. Research indicates that digital identities enhance convenience and efficiency in accessing government services (Mukhopadhyay et al., 2019; Nasri, 2019; Rössler, 2008; Salmasi & Gillam, 2010; Srivastava & Teo, 2009; Stepančič & Blažič, 2018), allowing simultaneous access to multiple services via computers or mobile phones (Stepančič & Blažič, 2018). Studies highlight benefits such as ease of use, convenience, and faster services (Arun, 2017; Beduschi, 2019; Breslow, 2020; Broekhuizen et al., 2021; De Andrés et al., 2015; Dunn, 2020; Guenduez, Mettler & Schedler, 2022; Gunawong & Gao, 2017; Makarychev & Wishnick, 2022; Manesh, Hadavand & Tahmasbizadeh, 2016).

NDIs and digital profiling systems foster democracy by facilitating public participation in decision-making and political engagement (Mir et al., 2020; Mukhopadhyay et al., 2019; Nasri, 2019; Srivastava & Teo, 2009; Stepančič & Blažič, 2018; Sullivan, 2014; Dunn, 2020; Guenduez, Mettler & Schedler, 2022; Gunawong & Gao, 2017; Al Sulaimani & Ozuem, 2022; Al-Shboul et al., 2014). They serve as legitimate legal identities, replacing physical forms of identification (Sullivan, 2014; Sullivan, 2016). Despite user concerns about privacy and security, these systems enable verification

and authentication of personal data with greater accuracy, convenience, and efficacy (Sullivan, 2016; Wolfond, 2017).

NDI from a government digital services perspective

NDIs are used to support government services and business support (Aichholzer & Strauß, 2010, Ajana, 2015, Al-Khouri, 2012, Mcloughlin, Wilson & Martin, 2013, Medaglia et al., 2022, Nasri, 2019, Scaria, 2022). The review indicated that digital IDs provided reliable authentication that enabled service delivery using web and mobile applications. They ensure legitimate access to government services that require identity proof. Digital identity offers governments several social and economic benefits, such as low costs (Althunibat et al., 2021) and political and financial inclusion (Medaglia et al., 2022). NDI enables modernising public services such as healthcare, licenses (Joshi et al., 2001), certifications, and welfare payments (Holt & Malčić, 2015; Jain & Gabor, 2020).

NDI systems provide a convenient platform for access to government services, thus eliminating potential costs and reducing waiting times through remote online authentication (Kassen, 2019; Kurfalı et al., 2017; Mavriki & Karyda, 2022). E-government platforms based on NDI enhance administrative efficiency (Ebrahim & Irani, 2005; Eke et al., 2022; Gao & Hu, 2021; Geteloma et al., 2019; Goede, 2019) and reduce paperwork (Guenduez, Mettler, & Schedler, 2022; Gunawong & Gao, 2017; Holt & Malčić, 2015). They speed up processing and reduce identity fraud risks (Medaglia et al., 2022; Nasri, 2019, Scaria, 2022; Sharma & Panigrahi, 2015; Skierka, 2023). The review supported citizen participation through electronic voting (Zulkifli et al., 2015; Goede, 2019; Gorensek & Kohont, 2019).

NDI from a CRM perspective

Businesses can leverage NDI platforms to promote customer support, business intelligence, and loyalty programs (Ajana, 2015; Bradford, Earp & Grabski, 2014). Digital technology connects the public to the business and creates customer trust (Jain & Gabor, 2020; Kumari & Khan, 2013). NDI acts as an online identity verification that is safe and easy to use, thus providing customers with digital trust (De Andrés et al., 2015). The digital identity verification process help in the acquisition of customers and make it easier to access services via mobile applications or the web (Dunn, 2020; Gorensek & Kohont, 2019; Jain & Gabor, 2020; Kumari & Khan, 2013; Manesh et al., 2016). In addition, NDIs promote financial sector inclusions by enabling authentication and verification when accessing financial services (McLoughlin, Wilson & Martin, 2013; Stepančič & Blažič, 2018).

NDI from a security and privacy perspective

NDI raises concerns regarding third-party access, confidentiality, and data protection (Mavriki & Karyda, 2022; Noack & Kubicek, 2010; Salmasi & Gillam, 2010). Threats such as bots, malware, and phishing could compromise digital citizens' ability to safeguard their information (Salmasi & Gillam, 2010). Centralised NDIs are susceptible to attacks, leading to significant data breaches and potential human rights violations (Sullivan, 2009, 2016; Tomura et al., 2021).

New technologies like 4G/5G digital initiatives exacerbate security risks, consolidating diverse communities into a single database yet posing limitations and vulnerabilities (Kumari & Khan, 2013). Outdated security controls increase susceptibility to identity theft and data breaches (Kumari & Khan, 2013).

Privacy and security are crucial aspects of digital citizenship, necessitating multi-stakeholder policies for digital competence (Noack & Kubicek, 2010; Salmasi & Gillam, 2010; Sule, Zennaro & Thomas, 2021). Government officials play a key role in promoting digital citizenship while safeguarding rights and responsibilities (Al-Shboul et al., 2014; Arun, 2017; Beduschi, 2019; Dunn, 2020; Dutton et al., 2005; Gastil & Richards, 2017; Leese, 2020; Mavriki & Karyda, 2022). Integration of blockchain technology into NDI systems enhances security, privacy, and data protection (Wolfond, 2017; Остроушко, 2022; Scaria, 2022; Sharma & Panigrahi, 2015).

4. Discussion

The review found that national digital transformation is a common phenomenon worldwide, as many countries are adopting digital technologies to improve administrative efficiency and enhance convenience in service access.

The digitalisation of government services, as highlighted by Остроушко (2022), has revolutionised governmental operations worldwide. NDI systems are pivotal in this digital transformation agenda across many nations (Mir et al., 2020). These systems facilitate the consolidation of digital data, enhancing user access to various resources and e-government services under a single identity (Mir et al., 2020). This convenience mainly benefits users accessing healthcare and welfare programs, improving user experiences (Müller & Skau, 2015).

Digital identities streamline access and foster citizens' sense of ownership and democratic participation, enabling more efficient engagement with government entities (Müller & Skau, 2015). While the designs and objectives of digital identity management systems may vary, their fundamental application remains similar (Müller & Skau, 2015).

Regulations governing the information required for digital identities vary, raising operational and technical questions regarding NDI implementation, such as the choice between centralised or decentralised databases and control of the NDI system (Sule et al., 2021). However, the review found that authorisation and authentication protocols in different NDI systems ensure users access appropriate government services (Sule et al., 2021).

Digital engagements enhance user experiences and foster engagement, benefiting governments, businesses, and individuals (Tomura et al., 2021). NDIs facilitate operational excellence, as exemplified by Estonia, and enhance security surveillance while providing services to vulnerable communities, as demonstrated by India's Aadhar system (Tomura et al., 2021). Governments leverage NDIs to improve healthcare, education, and welfare programs, while financial institutions benefit from enhanced identity authentication and data protection (Zhang et al., 2014). Citizens perceive NDIs as safer and more secure than physical alternatives, enabling faster access to services in both public and private sectors (Zhang et al., 2014).

Despite the widespread adoption of NDIs, significant gaps persist in their implementation. Data security and privacy concerns have been raised, particularly in countries like India (Sullivan, 2018). Instances of data breaches could lead to identity fraud and other violations of individuals' rights (Althunibat et al., 2021). Weaknesses in NDI systems, including susceptibility to human errors and weak passwords, undermine their quality, security, and reliability (Beduschi, 2019).

In response to these concerns, some countries, such as Canada, have turned to blockchain-based identity management systems (Wolfond, 2017). Blockchain technology ensures data integrity by recording

transaction history on an immutable ledger, enhancing security and privacy (Wolfond, 2017). Decentralised NDI concepts, like those adopted in Canada, offer greater accountability and privacy than centralised systems (Wolfond, 2017). Nonetheless, achieving trusted digital identification remains a significant challenge amidst the pervasive use of the internet (Wolfond, 2017). Concerns persist regarding potential failure factors, including central agencies' production, processing, and control of identities.

4.1. Researchers' Opinions

Research indicates that enhancing efficiency and transparency in government services can be achieved through the implementation of National Digital Identity systems, which also foster trust between citizens and governments (Al-Khouri, 2012; Eke et al., 2022). Moreover, researchers suggest that adopting National Digital Identity can improve transparency and reduce administrative corruption, thereby contributing to the increased effectiveness of electronic services (Mukhopadhyay et al., 2019; Nasri, 2019).

4.2. Recommendations

1. Goverments investment in developing the necessary infrastructure to support National Digital Identity systems and ensure their reliability and security. Aichholzer & Strauß (2010) highlight that improving infrastructure can contribute to enhancing government operational efficiency and reducing costs.

2. Governments should develop and implement strong cybersecurity policies to protect personal data and ensure information confidentiality (Eke et al., 2022; Nasri, 2019). Zhang et al. (2014) emphasize the importance of robust security policies to protect digital identity from cyber threats.

3. A legal and regulatory framework should be established to support the implementation of National Digital Identity and ensure the protection of individuals' privacy and security. Ajana (2015) underscores the necessity of a comprehensive legal framework to support and guide the use of National Digital Identity.

4. Encouraging the improvement of digital identity verification processes to ensure system effectiveness and reduce security risks. Weerakkody et al. (2013) demonstrate that enhancing verification processes can reduce fraud and improve system reliability.

5. Countries should invest in developing a National Digital Identity system that is a comprehensive National Profiling System representing personal accounts for all individuals. Al Sulaimani & Ozuem (2022) suggest that an integrated identity accounts system can enhance efficiency and transparency in government service delivery and improve digital identity management

4.3. Strengths and Weaknesses

The full article review provided insights into various NDIs and profiling systems aspects. Strengths identified include conceptualisation (Aichholzer & Strauß, 2010), description of features (Ebrahim & Irani, 2005; Kumari & Khan, 2013), success factors (Sedlmeir et al., 2021), and different approaches (Layne and Lee, 2001; Wolfond, 2017) related to NDIs. Additionally, the review highlighted how NDI systems facilitate access to government services (Althunibat et al., 2021; Krishna, 2020; Kurfalı et al., 2017), acting as data management systems for e-government services.

However, certain weaknesses were observed in the reviewed articles. Some focused narrowly on specific systems without considering broader perspectives (Aichholzer & Strauß, 2010; Krishna, 2020). Many articles lacked discussion on the weaknesses of NDIs or profiling systems (Al Sulaimani & Ozuem, 2022; Bekkers, 2012; Ebrahim & Irani, 2005). Others failed to convincingly demonstrate the benefits of digital transformation associated with NDIs or e-government services (Sargeant & Lee, 2002; Sauermann et al., 2007). Furthermore, some articles overlooked legal, technical, and organisational challenges (Schaupp & Carter, 2005), economic costs (Rao & Nair, 2019), and planning and monitoring phases of these systems (Al-Shboul et al., 2014). These limitations underscore the need for a comprehensive and balanced approach in future research on NDIs and profiling systems.

4.4. Contributions and Limitations

The paper examined the adoption of NDIs by various entities and their diverse implementation strategies within digital transformation agendas. It reviewed 58 articles, case studies, and innovative government digital service delivery approaches (Aichholzer & Strauß, 2010; Althunibat et al., 2021; Krishna, 2020). While NDIs are widely used for authentication and verification to enhance service delivery, their adoption as profiling systems has been limited, facing legal challenges in several countries (Krishna, 2020). Concerns persist regarding the privacy, security, and reliability of current identity infrastructure (Mavriki & Karyda, 2022).

Nonetheless, NDIs have improved identification efficiency and enabled access to multiple services, albeit with security concerns (Eke et al., 2022). To address these issues, some countries have opted for localised, decentralised NDIs or blockchain-based technologies (Wolfond, 2017). Such models

aim to mitigate weaknesses observed in centralised systems and pave the way for NDI integration from a profiling perspective (Zulkifli et al., 2015). The review highlighted the impact of human-centric cybersecurity factors on user experiences and perceptions of security and privacy (Salmasi & Gillam, 2010).

It synthesised the literature on NDI design and implementation perspectives, showcasing their benefits in supporting customer relationships and facilitating e-government services (Sule et al., 2021). However, the review had limitations. It primarily focused on conceptual and empirical literature, lacking in-depth analysis of specific case studies (Sullivan, 2018). Only a small percentage of papers met inclusion criteria, and there was a dearth of studies on NDI profiling systems, particularly from diverse jurisdictions (Sule et al., 2021). Access to databases may have influenced the scope of the review (Sule et al., 2021).

Future research should focus on examining the successes and failures of NDIs across various contexts, exploring the benefits of decentralised, blockchain-based systems, and addressing the gaps in NDI implementation (Wolfond, 2017; Beduschi, 2019).

5. Conclusion

The review examined the influence of NDI and national profiling systems on accelerating digital transformation processes in different countries. The review showed that the goal of digital government is to provide appropriate information and ensure convenient and efficient access to government services by citizens. The review showed that most governments used NDI for authentication and verification purposes, not necessarily profiling perspectives. While the NDI concept can be used as a profiling tool, the application has faced legal hurdles in many countries, including Nigeria, Jamaica, and others, due to privacy and security systems. A few countries, namely India and Estonia, have successfully applied it from a profiling perspective. The review showed that the NDI had become an indispensable tool for governments seeking to improve service delivery by enhancing authentication and verification processes. NDI helps to identify individuals in the digital environment and promotes citizen engagement.

References

Aichholzer, G., & Strauß, S. (2010). Electronic identity management in e-government 2.0: Exploring a system innovation exemplified by Austria. Information Polity, 15(1,2), 139-152. https://doi.org/10.3233/ip-2010-0203

Ajana, B. (2015). Augmented borders: Big data and the ethics of immigration control. Journal of Information, Communication and Ethics in Society, 13(1), 58-78. https://doi.org/10.1108/jices-01-2014-0005

Al Sulaimani, A. H., & Ozuem, W. (2022). Understanding the role of transparency, participation, and collaboration for achieving open digital government goals in Oman. Transforming Government: People, Process and Policy, 16(4), 595-612. https://doi.org/10.1108/tg-04-2022-0044

AlHammadi, A. A., & Lataifeh, M. (n.d.). Examining the influence of national digital identity and smart pass platform on accelerating the processes of digital transformation. The University of Sharjah.

Al Khouri, A. M. (2011). An innovative approach for e-government transformation. International Journal of Managing Value and Supply Chains, 2(1), 22-43. https://doi.org/10.5121/ijmvsc.2011.2102

Al-Shboul, M., Rababah, O., Ghnemat, R., & Al-Saqqa, S. (2014). Challenges and factors affecting the implementation of e-government in Jordan. Journal of Software Engineering and Applications, 07(13), 1111-1127. https://doi.org/10.4236/jsea.2014.713098

Althunibat, A., Binsawad, M., Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Rahmi, W., & Seliaman, M. E. (2021). Sustainable applications of smart-government services: A model to understand smart-government adoption. Sustainability, 13(6), 3028. https://doi.org/10.3390/su13063028

, P. (2017). Uncertainty and insecurity in Privacyless India: A despotic push towards digitalisation. Surveillance & Society, 15(3/4), 456-464. https://doi.org/10.24908/ss.v15i3/4.6618

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2), 1-6. https://doi.org/10.1177/2053951719855091

Bekkers, V. (2012). Why does e-government looks as it does? looking beyond the explanatory emptiness of the e-government concept. Information Polity, 17(3,4), 329-342. https://doi.org/10.3233/ip-2012-0279

Bhandari, V. (2020). Use of digital ID for delivery of welfare. Centre for Internet & Society, Digital Identities Project.. https://dx.doi.org/10.2139/ssrn.3668118

Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralised end-to-end identity and access management and ERP systems: A multi-case analysis using the technology organisation environment framework. International Journal of Accounting Information Systems, 15(2), 149-165. https://doi.org/10.1016/j.accinf.2014.01.003

Breslow, H. (2020). The smart city and the containment of informality: The case of Dubai. Urban Studies, 58(3), 471-486. https://doi.org/10.1177/0042098020903233

Broekhuizen, T., Emrich, O., Gijsenberg, M., Broekhuis, M., Donkers, B., & Sloot, L. (2021). Digital platform openness: Drivers, dimensions and outcomes. Journal of Business Research, 122, 902-914. https://doi.org/10.1016/j.jbusres.2019.07.001

Crossman, G. (2017). The ID problem. In Digital identity management (pp. 193-200). Routledge.

De Andrés, J., Pariente, B., Gonzalez-Rodriguez, M., & Fernandez Lanvin, D. (2015). Towards an automatic user profiling system for online information sites. Online Information Review, 39(1), 61-80. https://doi.org/10.1108/oir-06-2014-0134

Dul, J., & Hak, T. (2008). Case study methodology in business research. Routledge.

Dunn, H. S. (2020). Risking identity: A case study of Jamaica's short-lived national ID system. Journal of Information, Communication and Ethics in Society, 18(3), 329-338. https://doi.org/10.1108/jices-04-2020-0040

Dutton, W., Guerra, G. A., Zizzo, D. J., & Peltu, M. (2005). The cyber trust tension in e-government: Balancing identity, privacy, security. Information Polity, 10(1,2), 13-23. https://doi.org/10.3233/ip-2005-0066

Ebrahim, Z., & Irani, Z. (2005). E□government adoption: Architecture and barriers. Business Process Management Journal, 11(5), 589-611. https://doi.org/10.1108/14637150510619902

Eke, D., Oloyede, R., Ochang, P., Borokini, F., Adeyeye, M., Sorbarikor, L., Wale-Oshinowo, B., & Akintoye, S. (2022). Nigeria's digital identification (ID) management program: Ethical, legal and socio-cultural concerns. Journal of Responsible Technology, 11, 100039. https://doi.org/10.1016/j.jrt.2022.100039

Gao, C., & Hu, X. (2021). Design and implementation of home health system based on ID card identification and Multidevice access. Wireless Communications and Mobile Computing, 2021, 1-11. https://doi.org/10.1155/2021/5514687

Gastil, J., & Richards, R. C. (2017). Embracing digital democracy: A call for building an online civic Commons. PS: Political Science & Politics, 50(03), 758-763. https://doi.org/10.1017/s1049096517000555

Gelb, A., & Metz, A. D. (2018). Identification revolution: Can digital ID be harnessed for development?. Brookings Institution Press.

Geteloma, V., Ayo, C. K., & Goddy-Wurlu, R. N. (2019). A proposed unified digital id framework for access to electronic government services. Journal of Physics, 1378(4), 39-45. IOP Publishing.

Goede, M. (2019). E-Estonia: The e-government cases of Estonia, Singapore, and Curaçao. Archives of Business Research, 7(2), 225–227. https://doi.org/10.14738/abr.72.6174

Gorensek, T., & Kohont, A. (2019). Conceptualisation of the Digitalization: Opportunities and Challenges for sorganisations in the Euro-Mediterranean Area. International Journal of Euro-Mediterranean Studies, 12(2), 93-115.

Guenduez, A. A., Mettler, T., & Schedler, K. (2022). The role of trust in e-credentials markets. Information Polity, 1-17. https://doi.org/10.3233/ip-211508

Gunawong, P., & Gao, P. (2017). Understanding e-government failure in the developing country context: A process-oriented study. Information

دور الهوية الرقمية الوطنية في تسريع عمليات التحول الرقمي "مراجعة"

عبد الرحمن أحمد الحمادي[1]

سعادت م. الهاشمي[2]

محمد لطيفه[3]

جون رايس[4]

ملخص البحث:

تُعنى هذه الورقة البحثية بفحص الانتشار المتزايد لأنظمة الهوية الرقمية الوطنية (NDI)، مع التركيز على تصميمها وتطبيقها والعقبات التي تواجه تنفيذها في مختلف الدول. أصبحت أنظمة التعريف الرقمية أدوات لا غنى عنها للأمن الوطني والمراقبة وإدارة الخدمات بكفاءة. تُستخدم أنظمة الهوية البيومترية مثل Aadhaar في الهند، وMERNIS في تركيا، وRENIEC في بيرو، وCNIC في باكستان لإدارة الأمن والتحقيقات الجنائية وجمع بيانات السكان. ومع ذلك، عرقلت الأمور التشريعية والأخلاقية والقانونية، خاصةً مخاوف الخصوصية وحماية البيانات، نشر هذه الأنظمة

تهدف هذه الدراسة إلى وصف مفهوم الهوية الرقمية الوطنية وتأثيرها على التحول الرقمي، وتقييم توافقها مع الأجندات الرقمية. تتناول مشكلة الدراسة التحديات في تنفيذ الهوية الرقمية الوطنية، بما في ذلك الخصوصية وحماية البيانات والتشريعات والبنية التحتية التكنولوجية. من خلال مراجعة أدبيات منهجية، توضح هذه الورقة أسباب تنفيذ أنظمة الهوية الرقمية الوطنية وتقدم رؤى حول الفوائد والقيود المحتملة كجزء من أجندة التحول الرقمي للدولة

الكلمات الدالة: أنظمة التعريف الرقمي، الهوية الرقمية الوطنية، أنظمة الهوية البيومترية، التحول الرقمي، أنظمة إدارة الهوية

(1) كلية الآداب والعلوم الإنسانية والاجتماعية - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)
U20102623@Sharjah.ac.ae

(2) كلية الحوسبة والمعلوماتية - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)

(3) كلية الحوسبة والمعلوماتية - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)

(4) كلية إدارة الأعمال - جامعة الشارقة (الشارقة - الإمارات العربية المتحدة)