Digital Identity Evaluation Framework for Social Welfare

Umar Bashir Mir, Arpan Kumar Kar, Manmohan Prasad Gupta

Digital Identity Evaluation Framework for Social Welfare

Umar Bashir Mir[1] [0000-0002-6768-801X], Arpan Kumar Kar[2], and Manmohan Prasad Gupta[3]

[1, 2, 3] Information Systems area, Indian Institute of Technology Delhi, New Delhi, India
[1]mirumar.iitd@gmail.com

Abstract. Identification systems are vital in improving efficiency and enabling innovation for public and private-sector services, such as greater efficiency in the delivery of social safety nets and facilitating the development of digital economies. With all these benefits along with the rapid improvement in the technology has led many countries to adopt a new foundational digital identity system (DIS) or retrofit the existing paper-based identity system especially in the developing economies. Apart from all these benefits, DISs has also been criticized for issues related to the security, privacy, surveillance and exclusion of people from various services they are entitled to. Considering the significant impact of DIS on the people, it is necessary to have an evaluation framework that could help understand the suitability of a DIS in a particular context. In this study, we propose a conceptual evaluation framework specifically for DISs based on the processes followed, regulations and technologies employed.

Keywords: Digital Identity, Aadhaar, E-Governance, Technology Assessment.

1 Introduction

Digital identity (DI) is the digital counterpart to a real identity. Identity in general is comprised of various data points mingled with unique characteristics of an individual. Trustworthy digital identification is the cornerstone for a secure and sustainable digital economy. The primary purpose of identification system is to authenticate and authorize a person seeking access to a particular service. In digital space, designated bodies that provide any service – Service Providers (SP), utilise digital identification system to prevent fraudulent service access. From the public sector perspective, it is believed that digital identity system has a positive impact on the adoption of e-Government services. DISs enables people to prove they are who they say they are – authentication, which is must while opting for services provided by public or private institutions. The digitisation wave across the globe has made DI a necessity and has opened a new horizon for the development and empowerment of people. In pursuit of solving one set of problems using technological solutions often gives birth to another set of challenges. For example IoT based systems are believed to have compromised the privacy of an individual [1] which is the basic right of a person [2].

It is important to understand that it is very difficult if not impossible for an individual to control their DI themselves considering the time and expertise it requires. There is a need of robust and consistent DIS that possesses high utility and scalability value for both public and governments. There is a lack of trust between government and people and that has resulted in various grievances and complaints about DISs. In US, Social Security Number (SSN) has been a de facto DI however there has been growing concerns about its effectiveness to deal with identity related frauds. Stakeholders have realised there is a need of better identity systems; that has better privacy and security measures; is convenient; and is trusted by users and service providers [3]. In UK national ID was seen as threat to user privacy and had to be scrapped because of the protests from public [4]. India's digital identity –Aadhaar, is world largest DIS in terms of the number of enrolments. Apart from all the benefits it has facilitated in terms of financial inclusion, public distribution system (PDS), employment and distribution of government subsidies, Aadhaar has been criticised for its effectiveness in preventing leakages in various government schemes [5]. Ideal DIS does not exist, almost all the existing DISs have been criticized for one reason or the other. We can broadly categorise these concerns into following categories: consent, surveillance, data localisation, data security, data control etc. [6]. Developing and implementing an identity system is a costly affair and requires lot of resources [7]. To avoid losses at later stages, it is advisable to evaluate identity systems for its effectiveness from a context specific view beforehand. The motivation of this study is the growing criticism of identity systems [8], [9].

All these issues have affected trust aspect of DISs which in turn is affecting the adoption of DISs. There is a need to have a mechanism to evaluate DIS beforehand that could be utilised by the people as well as governments to evaluate best suitable DIS for a particular context [7]. This study is positioned in this direction. In this study we propose an evaluation framework specifically meant for evaluating DISs. To the best of our knowledge we did not find any study that has developed a framework specifically for evaluating DISs based on processes, regulations and technologies employed. DISs have distinct characteristics and purpose as compared to generic IS or e-Government projects in terms of cost, time, utility and implementation, and hence requires a context specific evaluation approach [8].There is a need to mitigate risks in DISs [10].

This study is grounded on the Technology Landscape for Digital Identification work of World Bank Group which analyses the relevance and effectiveness of various technologies in solving potential problems associated with user identification and authentication phenomena [11]. Needless to mention that technology is not the only factor that determines the effectiveness and adoption of massive e-government schemes like DIS [12]. In an attempt to minimise the possible damage beforehand this study attempts to develop a framework that will enable concerned authorities to evaluate a DIS. Precisely, the study focuses on the following aspects:

- Firstly, a comprehensive framework for evaluating DISs is proposed
- Next, the proposed framework is used for comparative analysis of four DISs

The remaining sections are organized as follows : Literature specific to DISs and assessment frameworks is described in section 2. Section 3 describes the methodology adopted followed by findings in section 4. In section 5, discussion surrounding implications of this paper is presented and finally limitation and future research directions are explained in section 6

2 Literature

Electronic governance in general has garnered lot of traction in the last decade. E-Governance is an umbrella domain that includes different other research areas. Assessment of e-governance projects has been conducted either before implementation or after implementation of the project. E-governance schemes affect diverse dimensions of the society via highly complex mechanisms. Broadly, impact ranges from socio-political, socio-economic, environmental and socio-technical aspects of the society. The identification and analysis of these effects is critical when evaluating large highly complex e-government projects especially when public is involved. Evaluation is defined as the assessment of projects worth by focusing on its design, implementation and impact [13]. Subsequently, the evaluation of DIS should take into consideration: the technology employed; utility; resources required; citizen rights; and safety measures [2]. In the context of this study we have reviewed literature specific to the assessment of information technology and e-government projects.

Literature indicates that IT and e-governance act as important components for the development and change in society. The assessment of such schemes has been confined to basic instruments that could be manipulated easily [14]. Primarily researchers have focused on evaluation process and it is not always clear that what aspects of the scheme should be evaluated. Some of the assessment studies have focused on the pre and post implementation assessment of project [15]. Just knowing the changes brought by a project is not sufficient. What is more impactful is to understand what components of the project are responsible for which part of the change[16]. A comprehensive evaluation plan is required to understand the linkage between the project components and the outcome.

In [17], authors have studied the significance of interoperability in the adoption of e-government IS and identified risk management, collaboration and coordination and technical expertise as major factors that impact interoperability aspect of IS like e-government websites. Another limitation is that most of e-government systems primarily focus on the government side objectives and neglecting public aspiration by generalising highly context sensitive systems [18]. This marks another reason why a context specific assessment mechanism is required to evaluate a DIS that has significant impact on socio-political, socio-economic and cultural dimensions of the nation.
In [19] authors have evaluated digital identity systems mainly from the privacy perspective. Further, the impact of privacy on the adoption is studied with the help of a comparative analysis of four national digital identity systems. There are multiple reasons why large projects fail e.g. gaps in design and reality, unclear focus, quality of content, necessary skills, execution, regulatory issues, technical issues, lack of feed-

back and proper communication procedures [20]. A framework presented by World Bank in its recently published report on the technology landscape of DIS highlights the highs and lows of possible technologies that could be employed in a DIS [11]. The proposed assessment framework assesses each identification technology like biometrics, cards, protocols etc. based on six major parameters which in turn has multiple sub-parameters under each parameter. While it enables practitioners and stakeholders to evaluate available technological alternatives for identification, it does not asses non-technical parameters of identification that are equally vital for a successful DIS. In another study [10], a framework for evaluating digital identity is proposed that evaluates DIS based on its usage. The main focus of the framework is confined to the utility side of an identity system only which is just one of the many aspects of DIS. There is need of a comprehensive mechanism that would cover all the primary building blocks of DIS like technological, managerial, usage, legal and socio-political for evaluation. This article is an attempt to fill this gap. In this article, we propose a framework explicitly for evaluating DIS by taking diverse set of factors into consideration. This framework could be useful in getting first-hand experience of how strong a DIS is and will enable concerned authorities like policymakers, law makers and technology providers to align their DIS execution and implementation accordingly

3 Methodology

We did an extensive literature review of various secondary data sources that includes research publications related to DIS and impact assessment of IS and e-Government projects from Scopus database. Scopus is one of the largest abstracts and citation repository which is being used extensively by the research community across domains. Relevant articles were selected based on the abstract and conclusion of papers which resulted in 89 articles. In some of the cases we read introduction and discussion section also to be able to clearly identify the relevance of the paper in the context of this study. Further, the corpus was narrowed down to 36 articles based on the quality of conference and publishing journal and by removing redundant articles. Apart from research articles, we also considered white papers published by World Economic Forum (WEF), United Nations (UN), National Institutes of Standards and Technology, World Bank, and official reports issued by various governments including India, Estonia, US and UK to build support and identify list of evaluation parameters for this study.

3.1 DIS Evaluation Framework

Understanding the lifecycle of a DIS enables designers, implementers, and policy developers grasp the processes followed and technologies involved in provisioning the credentials that enable identification and authorization of an individual. For example from technological perspective – iris based systems are still in its early stage where as fingerprint recognition is fairly mature and have seen wide adoption already. Based on the technologies implemented and processes followed in a DIS, we have

proposed a framework as shown in Table 1 below. Each major parameter is evaluated based on specific factors. The evaluation parameters are presented below:

Biometrics. Biometric recognition uses an individual's unique physiological and behavioural attributes to identify and authenticate his or her identity. Physiological features include elements related to the shape or composition of the body, such as iris patterns, finger-prints ridges, and facial characteristics. Examples of behavioural attributes include gait, signature, keystroke patterns, and mouse usage.

Table 1. Comparative Analysis using DIS Evaluation Framework

DI Parameters	Reference	Factors	Scale	Aadhaar	Estonia	SSN	UK
Biometrics	[21][8]	Physiological	Desirable	✓	✓		✓
		Behavioural	Desirable				
Governance Structure	[22]	Public	Desirable	✓		✓	✓
		Private	Least Desirable				
		PPP	Desirable		✓		
Purpose	[23][24]	Foundational	Desirable	✓	✓		✓
		Functional	Less Desirable			✓	
Instrument Type	[7][22]	Card/paper	Least Desirable			✓	✓
		Number	Desirable	✓			
		Chip	Desirable		✓		
Identity provider	[25][26]	Government	Desirable	✓	✓	✓	✓
		Third-party	Less Desirable				
Scalability	[27][28]	One time	Less Desirable			✓	✓
		Future-proofing	Desirable	✓	✓		
Type of Identity system	[29]	Platform	Desirable	✓	✓		✓
		Software Product	Least Desirable			✓	
ID Architecture	[7]	Centralized	Less Desirable	✓		✓	✓
		Decentralize	Desirable		✓		
Verification mechanism	[30]	Technology-assisted	Desirable	✓	✓	✓	✓
		Human dependence	Least Desirable				
Enrolment	[27][31]	Fully Automatic	Desirable				
		Semi-Automatic	Less Desirable	✓	✓		✓
		Manual	Least Desirable			✓	

Data localisation	[45][46]	Access control	Desirable		✓		✓
		Consent	Desirable		✓		✓
Relying parties	[29]	Both public and private	Desirable	✓	✓	✓	✓
		Either public or private	Less Desirable				
Adoption	[3]	Voluntarily	Desirable	✓			✓
		Mandatory	Less Desirable		✓	✓	
Eligibility	[27][34]	For all	Desirable	✓			
		Age limit	Less Desirable		✓	✓	✓
		Category limit	Least Desirable				
Interoperability	[7][28]	At national level	Desirable		✓		
		At state/region level	Less Desirable	✓		✓	✓
Accountability	[19][35]	User side	Desirable		✓		
		Management side	Desirable		✓	✓	
Redressal mechanism	[26]	Online	Desirable	✓	✓	✓	✓
		Offline	Less Desirable				
Reusability of ID	[24]		Desirable				
Utility in online and offline space	[27][26]	-	Desirable	✓	✓	✓	✓
General Data Protection Regulation (GDPR) adherence	[29]	-	Desirable		✓		✓

Governance structure. Governance structure depicts the powerhouse of DIS. Majority of the national identity systems are governed by the government of that particular country. However, there is a possibility that government can outsource some functionalities of the DIS management to third-party. In general, DIS could be governed by either government or by a government-approved private entity or by PPP model.

Purpose. Most of the countries have some type of DIS that is tightly coupled with some specific services and are serving an only particular section of the society. Such systems are widely known as functional systems. According to World Bank report, 18% of the developing nations have identity system that is used only for identification, 55% have identity system that is tailored for a particular accessing service like voting, subsidies, banking etc. and only 3% have an identity system that can be uti-

lized to access a variety of online as well as offline services –Foundational systems [36].

Instrument Type. It could be a certificate, object, or a data structure that guarantees the identity of an individual via an authentication and authorization process. Digitization has revolutionized the means of verifying the legitimacy of an individual. It has significantly impacted the way proof of identity is realized. Traditional systems were based on paper-based identity instruments which were replaced by ID cards and chips. Recent technological innovations like cloud computing and blockchain have further transformed hardware-based ID instruments into software-based, e.g. numbers. Each type of ID instrument has its benefits and challenges and hence makes it an important factor in a novel DIS.

Identity provider. Identity provider (IdP) is the heart of a DIS. It is an entity that is responsible for managing and issuing identity to an individual. IdP could be the government itself or a single specific department that works under the guidelines of government or fully independent third-party entity with its own set of rules. IdP is responsible for collecting user data like biometrics, and demographic details and links it to a unique ID which is issued to the user.

Relying parties. Relying party (RP), also known as the service provider, is an entity that provides some services to users based on their credentials. It relies on another entity for user identification before providing access to a particular service. The information exchange between RP and IdP depends on the type of Identity management model adopted. The relation between RP and IdP could be one-to-one (traditional), one-to-many (centralized), or many-to-many (federated).

Scalability. Scalability is important from the view point of technology and backend processing. It is well known that Algorithms do not always scale gracefully. Since DIS is supposed to generate identities for large population (using biometrics for ensuring uniqueness) .It is important to know if algorithms used for this process will scale up or not. Therefore, scalability, of technology and processes used to process the data and generate these unique IDs is a critical parameter in DIS.

Type of Identity system. DIS could be implemented either as a software application system or as a platform. Massive software application systems are complex and tedious to manage but require little network connectivity whereas platform is heavily dependent on network connectivity among large number of commodity devices. It is comparatively easy to secure software application system which requires less information sharing as compared to platform in which information is shared among nodes extensively.

ID Architecture. A technical framework that covers the processes of creating, managing and application of DIs is referred to as Identity and Access Management (IAM). IAM can be broadly classified into two categories: centralized and decentralized. Centralized systems were most common in the initial days of IAM wherein IAM was developed, owned, and controlled by a single organization. Centralized systems store all user credentials in a single large database which is queried during authentication and authorization processes. Decentralized systems, on the other hand, have user data scattered on multiple devices that are in sync and is usually used by multiple institutions.

Verification Mechanism. Verification of user credentials is the first step in accessing services. It has three levels; in the lowest level, the only photograph is checked whereas in highest level biometric data is also included and in some cases additional information like One-Time Password (OTP) or answer to the security question is also provided during verification process. The process of verification could happen in two ways. One where some level of human intervention is necessary to complete the verification process, second where human intervention is both minimal and not mandatory to complete the verification process.

Data Localization. In recent times, the physical location of the database in which user data is stored has become one of the hot debatable topics because of the growing concerns towards surveillance and information war among countries. On one side, cloud storage has reduced the burden of having developing infrastructure from scratch, and on the other side, it has been questioned for data leakage and data control. Governing bodies prefer full possession and control on its citizen data, and demand data is stored within the physical boundaries of the countries.

Enrolment. Users provided their credentials to enrolment agency that is responsible for recording data in the most accurate form so as to avoid any incomplete or duplicate entry in the system. Depending on the type of data recorded defines the necessary requirements from technological perspective. For example capturing biometric data requires sophisticated devices with high precision whereas recording demographic details could be done manually. Reliability of enrolment system has a significant impact on the overall efficiency of the DIS.

Adoption. Adoption is the stage where a particular technology is selected for use by an individual or an organization.The rate of adoption depends on whether DI has been made mandatory by the authorities, or it is voluntarily adopted by an individual. From the control-flow perspective, mandatory systems follow the top-to-bottom approach, whereas bottom-up is followed in voluntary systems. Adoption rate could be higher in mandatory systems, but that does not guarantee high usage. It is the public value of DIS that will drive its usage, and each individual values DIS differently based on their attitude and needs.

Eligibility. Developing an identity system is a highly complex political process. All the functional identity systems developed until now are based on some criteria. There could be multiple reasons for restricting identity to a particular section only. The most commonly found example is of voter ID that is issued only after attaining a particular age, e.g. in India, voter ID is issued if a person is above 18 years. Most of the existing Identity systems signify the eligibility and entitlements a particular user is entitled to with the help of user identity.

Interoperability. Extending utility of DI beyond today's confined range of services to a wider range of services that spans domains and sectors is highly dependent on the interoperability support. User access different types of services from private and public entities which means they may have to deal with a different set of incompatible systems that require user identity in different forms. Standardized DI that could be used across geographies and sectors will reduce the burden of keeping and managing service-specific identities.

Accountability. Success of DIS is dependent on the level of trust people have in it and accountability is one of the significant factor in building trust. Further, accountability has impact on other dimensions of DIS also like transparency, adoption, satisfaction and privacy of DIS. Personal details of an individual is extremely important and must be guarded from all forms of violations so as to ensure security and privacy. Entities that process user data should be held accountable for any misuse of data and should be penalised depending on the severity level of misuse [37].

Redressal Mechanism. Grievance Redressal is a common mechanism in the service sector. User can report grievances that can originate from various processes like information sharing, access and service consumption, the accuracy of user data, availability etc. It enables an individual to register a complaint or seek an update on the already submitted complaint. Effective Grievance Redressal mechanism enables agencies to be more transparent and responsive to their users. Complaints could be made either using online web-portal or by directly submitting it to the department.

Reusability of ID. Reusability in identity systems is relatively a new concept. Although most of the existing DIS did not focus on the reusability aspect of DIS, initially, this attitude is changing fast, considering its significant impact on the speed and cost of onboarding new users. According to a survey, some institutions spend around $500 million per year to onboard new users and $60 million in financial institutions alone.

Utility in Online and Offline Space. Internet penetration has increased exponentially in the last decade or so, which has resulted in the tremendous growth of online service delivery. Identity is a must for conducting any transaction, and it becomes even more important in case of online transactions –faceless transactions. One of the major drawbacks in traditional identities is that they lack support for interoperability and that hampers its utility in online space.

GDPR adherence. Data breaches happen, and data gets compromised. To protect citizens' data from being violated European Union has passed a law in 2016 –GDPR. Its adherence is mandatory for companies that deal with EU citizen data. Although it does not apply to all the countries, all the companies that process EU citizen data need to follow it. It is the most versatile data protection law taking into account user consent, data anonymization, data breach update, and safe data flow across borders. Adherence to GDPR or similar regulations must be mandatory for DIS so that protection of user data is ensured.

3.2 Evaluation Scale

Proposed DI Evaluation Framework uses a three-point scale of "desirable", "less desirable" and "least desirable" to rate the significance of each factor. "Desirable" depicts that a particular factor is crucial, and its presence in DIS should be given utmost priority. "Less desirable" factors were common in traditional identity systems and were the reason behind some of the lacunas in those identity systems. Inclusion of such factors should be considered when no better alternative is available. Moreover, such factors are highly context-sensitive, and decisions regarding its inclusion should

be made accordingly. “Least desirable” factors bring more hardship than benefits. Inclusion of such factors should be avoided in the best possible way.

4 Findings

The study uses national digital identity schemes of four countries as a case study for evaluation. Many countries have evaluated or implemented national identity programs in the past. Some implemented successfully, whereas few had to withdraw because of strong protests from the public. It is worthwhile to note that digital identity systems have raised strong concerns regarding privacy, security, governance mechanism and inclusion or exclusion of people from various schemes. National identity systems evaluated in this study are briefly explained below.

4.1 India –Aadhaar

Aadhaar is considered as the world largest digital identity system based on the number of enrolments which is more than 1 billion. It is a random 12 digit unique number assigned to each resident of India. It is coupled with the biometric and demographic details of an individual. It is linked across sectors including banking, healthcare, education and telecom. It is governed by the government of India and is utilized in both public and private sector for user authentication. Apart from its all promising benefits, it has been criticized for various reasons which are mainly related to the technological issues, privacy issues and monitoring issues.

4.2 Estonia

Estonia is considered to have the most advanced e-governance platform in the world. Estonian digital identity could be owned via three means: Chip-based ID card, Mobile-ID SIM card, and application-based Smart-ID. People use the ID card to avail services like healthcare, banking, travelling and shopping on a routine basis. There are approximately 600 and 2,400 e-services being offered to the citizens and businesses respectively. In 2017 around 750,000 national ID’s got compromised because of a technical glitch that enabled to infer private key from users public key.

4.3 Social Security Number

Social Security Number is a 9-digit number issued by Social Security Administration to permanent and working residents of U.S. SSN is not a conventional digital identity as its primary purpose was to keep a check on taxes. Over the time it has been used for identification of an individual in the private and public sector and has become a de facto national identity of U.S. As per a report, the US has lost around $16.8 billion to identity fraud cases in 2017 and saw a 44.7% increase in data breaches. Further, reports suggest that the use of SSN as an identifier should be stopped in both the private and public sector, and a new age digital identity system should be developed [3].

4.4 UK

UK's national ID cards linked an individual's personal identification documents, and travel documents with National Identity Register. In 2011, national identity, along with its associated register, was scrapped because of public protest against it [4]. There were many reasons for the failure of national ID, which includes scalability, lack of support for interoperability, and lack of communication between public institutions and industry regarding technical aspects of the scheme[23].

We tested our proposed DI evaluation framework based on the comparative analysis of four national identity systems. The results of the study are shown in Table 1 above.

5 Discussion

With multiple technologies available, an evaluation framework can help designers, implementers, and policy developers to compare available technological alternatives, gaining a sense of how systems work, what are the strong and weak aspects in the system and how they might be useful for a particular use-case. Such mechanisms could help mitigate potential risks that could impact DIS negatively [10] and facilitate the development of better identity system [3]. Identity systems of various countries including China, UK, US, and India, have been questioned for various issues which also includes violations in security and privacy of user data. Having an identity system is not enough rather having the right identity system for a particular context is what is desirable, but there are basic minimum criteria that every identity system must meet. Apart from supporting interoperability, it will also facilitate in building trust in the system. The study is in line with the growing concerns related to identity systems and helps to understand it in a better way from process and technology relational perspective [8], [23].

Comparative analysis of four identity systems depicts the relative strengths and weakness of each identity system. ID systems that possess better data localization and interoperability support are found to be more desirable. It could be justified because of the growing concerns regarding data security and privacy issues [36] that has made people serious about their personal data. Initially, national-level interoperability was desired as the majority of the population was mostly confined within the geographical boundaries of a country. As international travelling has become more convenient and cheaper, people travelling across borders in pursuit of better growth opportunities have also increased considerably. This could be another reason why ID systems with support for international interoperability are desirable considering its potential to make international travel convenient. Type of ID system is another important factor that impacts the adoption of an ID system. Most of the traditional ID systems were centralized and software-based systems that used to suffer from issues like bugs, software crash and natural calamities which could be avoided to a great extent in platform-based systems. Platform-based ID systems are easy to maintain and scale and is another crucial factor that should be taken into consideration while evaluating an ID system. ID systems are mostly driven by public entities and may lack domain-specific technical expertise. Incorporating specialized private entities for such tasks could improve the effectiveness and efficiency of design, development and implementation

of the ID system. From the comparative analysis, we can see high scored Estonia's ID system, which is considered as the world's most advanced systems is based on PPP model. Instrument type is another crucial factor and is dependent on the target population. Number based ID is preferred over chip-based ID systems for larger populations. Aadhaar is a number based ID that is presently the largest ID system in the world with more than 1 billion enrolments [8]. Also, number-based ID systems reduce the overall cost of an ID system. Voluntary adoption faces little resistance from the people, and by increasing the utility value of ID could have a positive impact on the adoption and acceptance. Aadhaar is the best example that increased adoption rate by making it voluntary and increasing utility value of the ID system. However, voluntary systems may not always achieve desired goals considering the reluctance, and digital divide among masses towards technological changes and hence require contextual considerations. Accountability upon intentional or unintentional misuse of user data should be clearly defined along with the penalty. This will enable conflict resolution in case of any data violations. Regarding international regulations about data security, GDPR is the most advanced one and has been made mandatory by the UK government for processing its citizen data within and outside the country for smooth transactions.

The study contributes to two aspects: 1) it enables concerned authorities to focus on the critical aspects of an ID system in advance that will further help in utilizing effective processes and technologies for robust and successful ID system; 2) the framework could be used in the preliminary analysis by the policymakers and evaluators for comparing the various ID systems. It could also be utilized in the feasibility phase of the ID development for an initial set of recommendations.

6 Conclusion

In this article, we identified 21 important parameters from the secondary data sources that primarily included research articles, official reports, and white papers. The findings from the comparative analysis of four DIS highlight the significance of each parameter in accordance with the best available identity system of Estonia. Parameters like governance structure, ID architecture type, data localization, interoperability, accountability, blockchain support and adherence to GDPR play a pivotal role in evaluating any DIS. In case of developing a new DIS, DIS evaluation framework could be helpful in identifying avoidable losses by dropping obsolete technologies, and inefficient processes beforehand from the proposed system. For existing DIS, it can play a vital role in deciding the success or failure reasons of the system that could act as a feedback for policymakers and DIS developers in the future. The primary limitation of this study is the type of data source –secondary in this case, from which parameters are identified. Directions for future research are to enrich the proposed DIS evaluation framework by incorporating primary data source for analysis and test the proposed framework on more DISs for better insights.

References

[1] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, “Privacy in the Internet of Things: threats and challenges,” *Secur. Commun. Networks*, vol. 7, no. 12, pp. 2728–2742, Dec. 2014.

[2] United Nations, “Universal Declaration of Human Rights,” *United Nations*, 1948. [Online]. Available: https://www.un.org/en/universal-declaration-human-rights/.

[3] The Better Identity Coalition, “Better Identity in America: A Blueprint for Policymakers,” 2018.

[4] A. Travis, “ID cards scheme to be scrapped within 100 days,” *The Guardian Weekly*, 2010.

[5] R. Khera, “The Aadhaar debate,” *Contrib. to Indian Sociol.*, vol. 52, no. 3, pp. 336–342, Oct. 2018.

[6] P. Dixon, “A Failure to Do No Harm – India ’ s Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U . S .,” *Health Technol. (Berl).*, 2017.

[7] U. B. Mir, A. K. Kar, Y. K. Dwivedi, M. P. Gupta, and R. S. Sharma, “Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India,” *Gov. Inf. Q.*, vol. 37, no. 2, p. 101442, 2020.

[8] U. B. Mir, A. K. Kar, M. P. Gupta, and R. S. Sharma, “Prioritizing Digital Identity Goals – The Case Study of Aadhaar in India,” in *Digital Transformation for a Sustainable Society in the 21st Century*, 2019, pp. 489–501.

[9] J. K. Pinto and S. J. Mantel, “The causes of project failure,” *IEEE Trans. Eng. Manag.*, vol. 37, no. 4, pp. 269–276, 1990.

[10] V. Bhandari, S. Trikanad, and A. Sinha, “Governing ID: A Framework for Evaluation of Digital Identity,” 2020.

[11] World Bank, “Technology Landscape for Digital Identification,” 2018.

[12] U. B. Mir, S. Sharma, A. K. Kar, and M. P. Gupta, “Critical success factors for integrating artificial intelligence and robotics,” *Digit. Policy, Regul. Gov.* , no. March, 2020.

[13] World Bank Group, “ICT for greater development impact-information and communication tech-nology.,” 2012.

[14] R. Howitt, “Theoretical foundations.,” in *New Directions in Social Impact Assessment*, F. Vanclay and A. M. Esteves, Eds. EdwardElgar, 2011, pp. 3–19.

[15] R. Heeks and M. Alemayehu, “Impact Assessment of ICT-for-Development Projects: A Compendium of Approaches,” *SSRN Electron. J.*, 2009.

[16] C. Pade-Khene and D. Sewry, “Proposed stages of a rural ICT comprehensive evaluation framework in ICT for rural development projects,” in *Proceedings of the South African Institute of Computer Scientists and Information Technologists Conference on Knowledge, Innovation and Leadership in a Diverse, Multidisciplinary Environment - SAICSIT ’11*, 2011, p. 326.

[17] N. Van Thanh, H. Yoon, and J. Hwang, “A study on the factors affect to technological adoption of e-Government Information System interoperability in Vietnam,” *Int. Technol. Manag. Rev.*, vol. 7, no. 2, p. 125, 2018.

[18] I. Zahran, H. Al-Nuaim, M. Rutter, and D. Benyon, “A Critical Analysis of e-

Government Evaluation Models at National and Local Municipal Levels," *Electron. J. e-Government*, vol. 13, no. 1, pp. 28–48, 2015.

[19] A. Khatchatourov, M. Laurent, and C. Levallois-Barth, "Privacy in Digital Identity Systems: Models, Assessment, and User Adoption," in *Electronic Government*, 2015, pp. 273–290.

[20] L. Anthopoulos, C. G. Reddick, I. Giannakidou, and N. Mavridis, "Why e-government projects fail? An analysis of the Healthcare.gov website," *Gov. Inf. Q.*, vol. 33, no. 1, pp. 161–173, Jan. 2016.

[21] S. Thorat and V. Bhilare, "Comparative Study of Indian UID Aadhar and other Biometric Identification Techniques in Different Countries," *Int. J. Curr. Trends Eng. Res.*, vol. 2, no. 6, pp. 62–72, 2016.

[22] A. M. Al-Khouri, "Digital identity: Transforming GCC economies," *Innov. Manag. Policy Pract.*, vol. 16, no. 2, pp. 184–194, 2014.

[23] McAfee, "Modernizing the Social Security Number," 2018.

[24] "A frictionless future for identity management; A practical solution for Australia's digital identity challenge," no. December, 2016.

[25] M. Laurent and S. Bouzefrane, *Digital Identity Management*. 2015.

[26] E. K. U. Jacobsen, "Unique Identification : Inclusion and surveillance in the Indian biometric assemblage," 2012.

[27] UIDAI, "UIDAI Strategy Overview Creating a Unique Identity Number for Every Resident in India," pp. 1–45, 2010.

[28] F. Zelazny, "The Evolution of India ' s UID Program Lessons Learned and Implications for Other Developing Countries CGD Policy Paper 008," no. August, 2012.

[29] A. I. Segovia, D. / Álvaro, and M. Enríquez, "Digital Identity: the current state of affairs Digital Identity: bthe current state of affairs," 2018.

[30] A. Okumura, S. Komeiji, M. Sakaguchi, M. Tabuchi, and H. Hattori, "Identity Verification Using Face Recognition for Artificial-Intelligence Electronic Forms with Speech Interaction," in *HCI for Cybersecurity, Privacy and Trust*, 2019, pp. 52–66.

[31] A. Venkatanarayanan, "Aadhaar enrolment costs," *Medium Corporation*, 2018. [Online]. Available: https://medium.com/karana/aadhaar-enrolment-costs-bc17f0d30018. [Accessed: 04-Jul-2019].

[32] J. Selby, "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?," *Int. J. Law Inf. Technol.*, vol. 25, no. 3, pp. 213–232, 2017.

[33] B. Mahammadbakhsh, E. Fathiazar, A. Hobbi, and M. Ghodratpour, "Globalization and local and global identities among Iranian students," *Int. J. Intercult. Relations*, vol. 36, no. 1, pp. 14–21, 2012.

[34] WorldBank, "Global ID Coverage by the Numbers : Insights from the ID4D-Findex Survey," vol. 15, no. Id, pp. 15–18, 2017.

[35] S. Graham and D. Wood, "Digitizing surveillance: categorization, space, inequality," *Crit. Soc. policy*, vol. 23, no. 2, pp. 227–248, 2003.

[36] BankWorld, *World Development Report 2016: Digital Dividends*. The World Bank, 2016.

[37] A. Knight and S. Saxby, "Identity crisis: Global challenges of identity protection in a

networked world," *Comput. Law Secur. Rev.*, vol. 30, no. 6, pp. 617–632, 2014.