Realizing Digital Identity in Government: Prioritizing design and implementation objectives for Aadhaar in India

Umar Bashir Mir
Ph. D., Student
Indian Institute of Technology Delhi, New Delhi
National Capital Territory of Delhi, India
Email: umarmir123@gmail.com

Arpan K. Kar
Associate Professor
Indian Institute of Technology Delhi, New Delhi
National Capital Territory of Delhi, India
Email: arpan_kar@yahoo.co.in

Yogesh K. Dwivedi
Professor
Swansea University, UK
Email: y.k.dwivedi@swansea.ac.uk

M. P. Gupta
Professor
Indian Institute of Technology Delhi, New Delhi
National Capital Territory of Delhi, India
Email: mpgupta@iitd.ac.in

R.S Sharma
Chairman
Telecom Regulatory Authority of India (TRAI), New Delhi
National Capital Territory of Delhi, India
Email: cp@trai.gov.in

Abstract: With the increasing levels of digital transformation, focus on digital identities of individuals is increasingly getting prominence. It is the information captured as part of the identity surrounding the citizens which decides what services and products one is entitled to and can access. At present, there are still around 1.1 billion people in the world without any official identity. To address this concern, United Nations through its 16th Sustainable Development Goals (SDGs) recommended governments to provide their citizens with unique identities by 2030. India's Aadhaar is one significant step in this direction as it has already reached over 1 billion enrolments in India. However establishing a national digital identity program successfully requires expertise, time, and huge financial commitments. This paper takes Aadhaar as a case study and uses Design Theory (DT) and Critical Success Factor theory (CSF) as a theoretical lens and attempts to evaluate design and execution choices made during the tenure of the project. The study also identifies and prioritizes primary goals of Aadhaar based on the secondary data, expert opinion through a Focus Group Discussion (FGD) and subsequently systematic prioritization using mixed research methodologies. The expert opinion from the FGD was analyzed using the Best-Worst method (BWM), followed by the Total Interpretive Structural Modeling (TISM) method and Matrix of Cross Impact Multiplications Applied to Classification (MICMAC) analysis. The study identified uniqueness, security and privacy as the top priority goals in an identity system and is 11 times more crucial than scalability which is identified to be of lesser priority. These findings from this study could be considered as a reference for other countries that aim to develop and implement digital identity for its citizens.

Keywords: Digital Identity, Aadhaar, Design Theory, e-Governance, Critical Success Factor, Best-Worst, TISM

1. Introduction

Identity is a multi-faceted concept, and defines an individual uniquely. It is comprised of those attributes that makes an entity unique and distinguishable from others (Olson, 2015). (Ben Ayed, 2014) also defined identity as a set of qualities and characteristics, by which an entity can be defined, distinguished and recognized in comparison to other entities. With a focus on context, International Telecommunication Union (ITU) has defined identity as a set of one or more attributes that distinguish a particular entity within a context (ITU-T, 2010). The International Organization for Standardization (ISO) defines digital identity as "item inside or outside an information and communication system, such as a person, an organization, a device, a subsystem, or a group of such items that has a recognizably distinct existence." (ISO, 2011). Further, World Economic Forum (WEF) defined digital identity as "collection of individual attributes that describe an entity and determine the transactions in which that entity can participate" (Mcwaters, 2016).

India became the first nation with a population exceeding 1 billion citizens to implement digital identity for all its citizens. With a population of 1.3 billion (Bank, 2016), India is second most populous country in the world. For such a country to roll out a program like Aadhaar, which is world's largest digital identity program as of July 2019, by Unique Identification Authority of India (UIDAI) in itself is a big challenge considering various practical challenges like high illiteracy rate (26% as per 2011 census), diverse cultures, political beliefs, varied demographics and many more. The primary purpose of Aadhaar – Unique Identification and Online Authentication, is achieved by the technological advancements in biometrics (Gelb & Clark, 2013). Aadhaar is a combination of 12-digit random number (Barnwal, 2015) tightly coupled with biometric details of an individual like a photograph, fingerprints, iris and demographic information like age, date of birth, gender and address. India has issued Aadhaar cards to more than 1 billion residents after initial launch

(Dixon, 2017). As of February 2019, more than 1.2 billion people have already been issued Aadhaar numbers (UIDAI, 2019) and hence it surpasses the US's biometric project called VISIT, which was earlier considered to be the world's largest biometric project (Epstein, 2008). This current study is much needed for giving a roadmap for implementation of digital identity considering the recent recommendations by United Nations in its 16th SDG that each individual should be provided a legal identity by 2030 (UN, 2016). One of the driving motivation for this study is that at a global level, despite the focus brought out in the 16th SDG of the UN, 24% of the developing countries do not have any form of digital identity system, and among others only 3% of the countries have foundational identity system that could be used in both online and offline domains (BankWorld, 2016; Segovia, Álvaro, & Enríquez, 2018). Countries that do not possess any national identity scheme could use this roadmap such that the desired objectives of identity for all is achieved in a timely and cost-efficient manner. For meeting such an objective, this study is useful for benchmarking design and execution objectives of digital identity programs, considering its developmental cost, reach and the technologies used.

E-government projects fail because of the multiple reasons (Aladwani, 2016; Anthopoulos, Reddick, Giannakidou, & Mavridis, 2016; Elkadi, 2013). One of the main reasons for the failure of e-government projects is the divergent interests and differences in the stakeholder expectations from the project (Sivamalai, 2013). Further, Sivamalai using Social Construction of Technology (SCOT) framework studied how different stakeholders perceive Aadhaar differently and how the analysis of design decisions before implementation could solve this problem. The present study takes it forward from there and evaluates the design and implementation decisions made during the tenure of the project such that the risks of the possible project failure could be mitigated. This study makes an attempt to breakdown the complexity of developing a digital identity system like Aadhaar in a way that it becomes easier for others to follow the process and develop a biometric based digital identity system based on their requirements.

To understand the implementation of Aadhaar, an in-depth analysis of Aadhaar from planning to implementation phase is required. The selection of over-arching goals for Aadhaar and multiple criteria associated with each goal can be considered as a MCDM problem because each goal is dependent on multiple factors/criteria that need to be taken care of right from the planning phase. From theoretical perspective this study uses CSF and DT to study overarching goals and their design and executions choices respectively. Both the theories have been used extensively in the e-government literature e.g. (Rana, Dwivedi, & Williams, 2013) used CSF to identify challenges and barriers of e-government adoption, (Akhtar Shareef, Kumar, Kumar, & Dwivedi, 2014) identified ability to use and assurance to use as the critical factors in the adoption of electronic government, (Shah, Braganza, & Morabito, 2007) identified organizational factors critical to e-business, and (Bergeron & Bégin, 1989) highlighted the use of CSF in evaluating information systems. Similarly, extant research literature about DT is nicely covered (Agogué & Kazakçi, 2014). Studies have proposed DT for market surveillance (Li, Sun, Chen, Fung, & Wang, 2015), digital platforms supporting online communities (Spagnoletti, Paolo, Resca, & Lee, 2015), and for developing policy alternatives (Pluchinotta, Kazakçi, Giordano, & Tsoukiàs, 2019). Some of general utility areas of DT are design and development of policies (Esfahlan & Valilai, 2019; Howlett, 2014; May, P.J, 2003; Mintrom & Luetjens, 2016) and decision making (Le Masson, Hatchuel, Le Glatin, & Weil, 2019).

This study attempts to address following research questions:

- What are the overarching design and implementation goals of India’s digital identity – Aadhaar?

- How can we establish the priority among these overarching design and implementation goals?
- What are the influencing factors that made it possible to design, develop and implement such a large scale biometric digital identity program?

To answer these questions, a MCDM method, namely the Best-Worst MCDM method has been adopted for evaluating the experts' feedback gathered from a multi-stakeholder workshop. All these experts were identified from the government and private sector having direct and senior role in the implementation of Aadhaar. Inputs from experts are analyzed and transformed into the list of weighted criteria based on their significance corresponding to the primary goals of Aadhaar. This prioritization will be helpful in forming an implementation and risk assessment roadmap for large projects similar to Aadhaar and can enhance the probability of a project to be successful. It can also increase the transparency, acceptance and utility of a particular project. Further, two well established methodologies, TISM and MICMAC analysis are used to verify the BWM results.

The remaining sections are organized as follows: Section 2 describes the unique identification concept primarily from biometrics perspective, including its functional utility, technical architecture and process flow. Section 3 presents Aadhaar as a digital identity case study. Section 4 discusses about the research gaps in the domain and contribution made. The theoretical lens for this study is covered in section 5. Section 6 introduces the focus group followed by data analysis part of the study using BWM for prioritization. Verification of BWM output using TISM and MICMAC is covered in section 7 and finally, discussions about the theoretical and practical contribution of this paper along with the future research directions are explained in section 8.

2. Literature Review

This section is subdivided into three sub-sections. The first subsection focuses on the utility of biometrics for citizens from a functional perspective. The second sub-section explores the technical architecture for such a solution and process mechanism for biometrics in practice is explained in the third sub-section.

2.1 Biometrics for Citizens – The Functional Utility

Biometrics could be used for identity recognition based on various biological traits like voice, iris, face, fingerprints, palm, DNA, ear, retina or behavioral characteristics like handwriting, signature and body movements, also called gait (Hoang & Caudill, 2012) Among all; fingerprints are the oldest biometrics in use. Traditionally, fingerprints were used in ink and paper documents for legal purposes. In the recent past, DNA as biometric has also gained much interest among researchers. However, any biological or behavioral trait can be used as biometric characteristics as long as it agrees to the criteria shown in Table 1.

Table 1: Biometric selection criteria

Criteria	Description
Universal	Every individual should have the particular biometric attribute. The attribute must be scarcely lost to accidents or health related illness.
Unique	Biometric attribute should be different for each individual. Attribute should possess distinct properties such that one individual could be distinguished from other.
Permanent	Attribute should remain unchanged indefinitely. It should be constant over the period of time and should not be subjected to any major change.
Recordable	Once captured, biometric attribute should be storable such that it becomes easy to handle and perform operations on it.

Based on the unique features of biometrics, biometrics based technologies have a wide scope of applications like logical or physical security (Hodeghatta & Nayak, 2014), surveillance (Bouchrika, 2017), healthcare (Marohn, 2006), law enforcement (A K Jain, Ross, & Prabhakar, 2004), time and attendance (Fenu, Marras, & Boratto, 2018), and electronic signatures (Nunno, 2000). These studies highlighted that the design and execution goals of any digital identity should address universality, distinctiveness, permanence, collectability, performance, acceptability and circumvention.

2.2 Biometrics for Citizens – The Technical Architecture

It is found that researchers started publishing about biometric systems from 1960's. In the year 1963, Mitchell Trauring published his work on fingerprint matching on automated biometric recognition (Trauring, 1963). After that, other biometrics have been used in various automated biometric systems like voice (Pruzansky, 1963), signature and Hand geometry (Mauceri A.J, 1965) and iris (Daugman, 1993) systems were also developed subsequently.

Biometric systems have evolved over a period and have improved considerably regarding performance, accuracy, and usability. Any new biometric technology is evaluated against the benchmark set by National Institute of Standards and Technology (NIST) before it can be made available for commercialization. NIST evaluation process is very complex and takes into consideration various test conditions before finalizing the results (NIST, 2013). The detailed explanation of these test conditions adopted by NIST is beyond the scope of this paper. However, a few important parameters that Digital Identity Systems (DIS) use globally has been illustrated in appendix section A.1. Some of the state-of-the-art biometric technologies can achieve greater accuracy (Phillips, Flynn, & Bowyer, 2017). An overview of the comparison of various biometric identifiers based on their application and design goals is illustrated in Table 2.

Table 2: Important factors in biometric identity of citizens, extended from A. K. Jain et al., (2004)

Biometric Identifier	DNA	Ear	Face	Facial Thermogram	Finger-print	Gait	Hand geometry	Hand vein	Iris	Keystroke	Odor	Palmprint	Retina	Signature	Voice
Universality	H	M	H	H	M	M	M	M	H	L	H	M	H	L	M
Distinctiveness	H	M	L	H	H	L	M	M	H	L	H	H	H	L	L

Permanence	H	H	M	L	H	L	M	M	H	L	H	H	M	L	L
Collectability	L	M	H	H	M	H	H	M	M	M	L	M	L	H	M
Performance	H	M	L	M	H	L	M	M	H	L	L	H	H	L	L
Acceptability	L	H	H	H	M	H	M	M	L	M	M	M	L	H	H
Circumvention	L	M	H	L	M	M	M	L	L	M	L	M	L	H	H
Inbuilt security	H	M	M	H	M	M	M	H	H	L	L	M	H	L	M
Processing cost	H	M	L	M	L	H	M	H	H	L	M	M	H	L	L
Convenience	L	M	H	M	H	L	M	L	L	H	M	M	L	H	H
Robustness	H	M	H	M	L	L	L	H	H	L	M	M	H	L	L
Utility	L	L	H	M	H	M	M	L	H	M	L	M	H	H	M

Where H = High, M = Medium, and L = Low labels are based on the authors perception.

2.3 Biometrics for Citizens – Process Flow

The National Science and Technology Council provides the following overview of biometric system components: “A typical biometric system comprises of five integrated components: A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template. A data storage component keeps information with which new biometric templates will be compared to. A matching algorithm compares the new biometric template to one or more templates maintained in data storage. Finally, a decision process (either automated or human-assisted) uses the results from the matching component to make a system level decision.

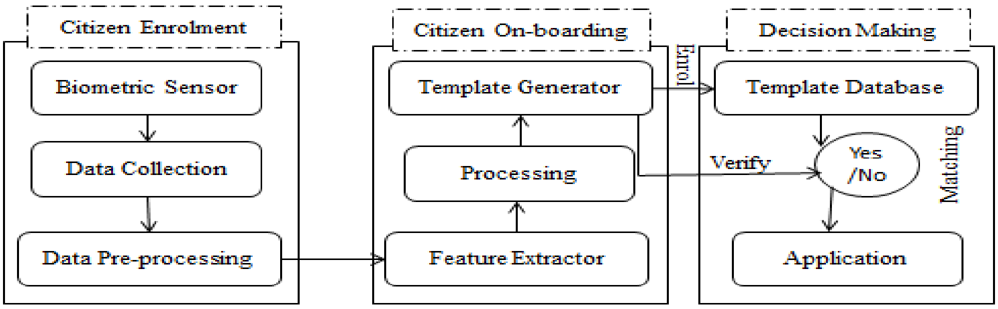

Fig. 1. Process blueprint for the verification process through a biometric system

Fig 1 illustrates a process flow of a typical biometric system and categorizes processes into three stages, citizen enrolment, citizen on-boarding and decision making. Citizen enrolment is the first stage where in data is collected from the citizens and made ready for further processing by cleaning and filtering data from noise. In the second stage biometric templates are generated after feature extraction and in the final stage these templates are permanently stored in the database for decision making.

Classification of authentication systems can be done based on what an individual has (e.g., tokens, smart cards), what the individual knows (e.g., PIN, passwords) and what the individual comprises of (e.g., iris, fingerprints). As per Census 2011 there are about 104 million elderly people aged above 60 years who often forget access credentials and is expected to grow to 173 million by 2026 (GOI, 2016). Also such users often share their credentials to others to access the services, due to which two factor authentication systems became popular (Singh, Cabraal, Demosthenous, Astbrink, & Furlong, 2007). Similarly, biometric systems could also get compromised, as demonstrated by Professor Tsutomu Matsumoto at Electric Imaging 2002 conference. He developed a fake finger with gelatin and used a simple digital camera and a computer to fool a biometric device 80% of the time (BBC News, 2002). However, with recent advancements in biometrics technology can detect fakes by considering factors like sweat pores, conduction properties and finger on contorts the surface of a biometric scanner (Anil & Sharathchandra, 2001).

It is important to note that biometric-based systems are not entirely foolproof (Pagnin & Mitrokotsa, 2017). Even though biometric technology has come a long way in the last five decades, it still has challenges and issues that are not sufficiently addressed yet (Bálint & Bucko, 2013; Chandra & Calderon, 2005; Anil K. Jain, Nandakumar, & Ross, 2016; Uludag, Pankanti, Prabhakar, & Jain, 2004). Resolving biometric technology issues in it-self is a separate research area, and researchers are actively working in this field (Abate, Marcialis, Poh, & Sansone, 2019; Arutyunov & Natkin, 2010; Baichoo et al., 2018; P.Down & J.Sands, 2004).

3. Aadhaar – The Indian Case Study

In 2009, Government of India came up with a proposal to provide every citizen of India a Unique Identification which can be used to provide benefits of various government schemes to desirable citizen directly. Considering the fact that India is the second most populous country in the world it was extremely vital to use some technology which can effectively and efficiently serve the purpose. With continuous improvement in accuracy and reliability of biometric technology, it was one of the best options available for identifying people uniquely. The primary purpose for rolling out Aadhaar was (a) to ensure proper utilization of government subsidies (b) to provide a unique identity to every citizen of India which can be accepted as identity and address proof throughout India (c) to tackle illegal immigrants (Dass, 2011; Ronald, Elizabeth, Noopur, & Neil, 2017; Zelazny, 2012). Technological architecture of UIDAI is shown in Fig 2. For the implementation of Aadhaar, it was very vital to have a mechanism that can deal with duplicates, be time efficient, scalable and should be feasible to integrate with other existing systems like Public Distribution Systems (PDS). The government took a transformational decision to implement AADHAAR which is based on the demographic and biometric details of a person. To decide which biometrics to use, a Biometric Committee was constituted which presented its report (Zelazny, 2012) to UIDAI. Finally, demographic details, photograph, fingerprints of 10 fingers, and iris of both eyes were included as necessary data inputs for the issuance of unique Aadhaar number (UIDAI, 2009). Rolling out an identity system which could suffice such a heterogeneous population was a big challenge for UIDAI. Aadhaar was launched with the intention to provide legal identity to the residents of the country so that they could avail various welfare benefits which they were denied earlier because of the lack of official identity documents. In addition to that, it was also intended to reduce corruption, reduce intermediation and agency costs, avoid identity related frauds and most importantly to increase participation of people in various government sponsored welfare schemes.

It can be observed from the Table 2 that no single biometric technique can out-perform others in all factors and hence a combination of biometric technologies is required based on the importance of each factor in a particular application. As a pre-study to establish the feasibility of Aadhaar, we performed a first-hand check of the methods of digital identity, as illustrated in Table 2. Our exploratory study indicated that biometrics used in Aadhaar - Photograph, Finger-print, and Iris, complement each other in all factors. It indicates that Aadhaar has required biometrics in place to deal with de-duplication, scalability, and uniqueness of its Central ID Repository.

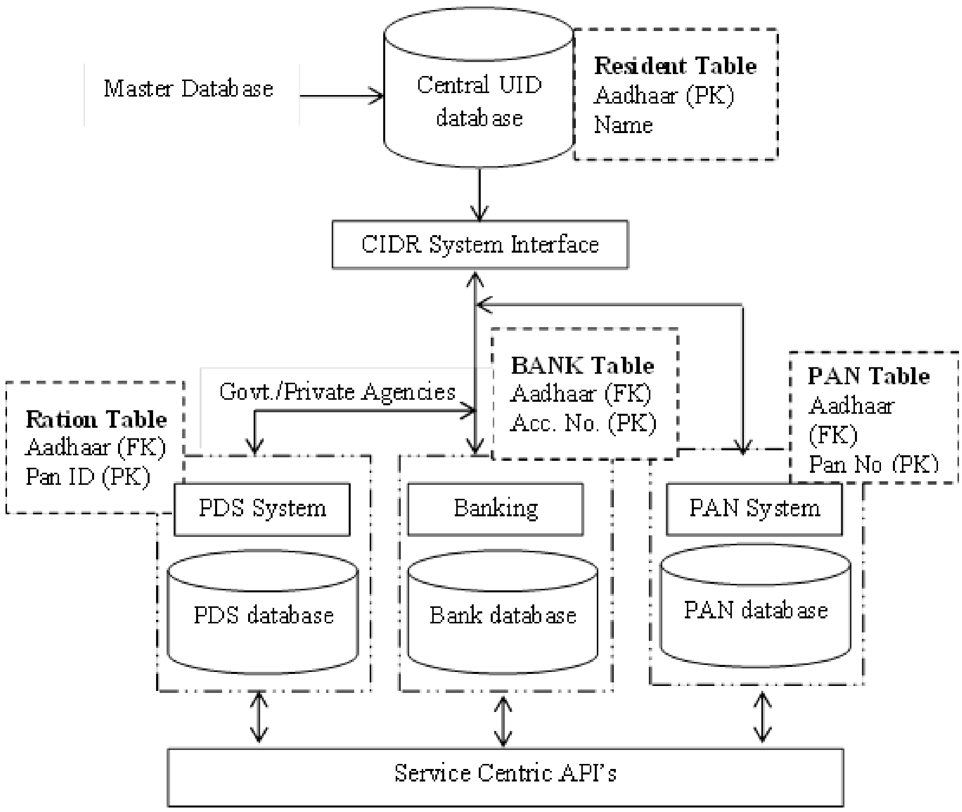

Fig. 2. Technology Architecture of Aadhaar (Adapted from UIDAI, 2010)

Where, FK = Foreign Key, PK = Primary Key, PDS = Public Distribution System, POS = Point of Sale, RDPR = Rural Development and Panchayath Raj, and PAN = Permanent Account Number

India is the only country with such a large scale for national identification of its citizens (exceeding 1 billion) through Aadhaar. As of February 2019, more than 1.2 billion citizens out of 1.3 billion have enrolled under Aadhaar (UIDAI, 2019). Notably, India is not the only country to implement national identification program, some of the other countries as shown in Table A.1 have similar identification programs like Aadhaar although their purpose varies.

4. Research objectives

The utility, design and governance of digital identity system is an emerging area of research which has not been studied much (McKinsey, 2019). Development, governance and implementation of e-ID for public e-service delivery is quite challenging and requires a lot coordination (Melin, Axelsson, & Söderström, 2016). Some Journals have published special issues specifically for electronic identity and eGovernment related research covering the multi-dimensional perspectives of e-IDs and its challenges and applications (Gal & Whitley, 2011; Irani et al., 2016; Meier & Terán, 2019; Whitley, Gal, & Kjaergaard, 2014). In (Lentner & Parycek, 2016), authors have examined different legislative approaches adopted in four European countries with focus on identification and authentication in customer-to-government eGovernment services, similarly, (Seltsikas & O'Keefe, 2010) studied challenges faced by stakeholder in developing, implementing and maintaining trusted e-IDs, (Hedström, Karlsson, & Söderström, 2016) identified usability, attitude, behavior and privacy concerns as primary challenges in implementing eID in healthcare.

To the best of our knowledge, there is no such study found in the literature which has tried to prioritize the attributes of any biometric identity project like Aadhaar and their interdependence with each goal. Majority of the research on Aadhaar explores the application side of it, e.g., electronic voting, payment systems, continuous verification of online exams, financial inclusion, healthcare sector and in government welfare schemes. Therefore, the motivation for this research is to analyze Aadhaar project from design and implementation perspective thoroughly. This study deals with three main objectives:

- To identify overarching goals of Aadhaar and their significance in a biometric based digital identity system.
- To identify design and execution goals of Aadhaar corresponding to each overarching goal and their significance and inter-linkages with respect to goals.
- To establish how these goals are linked to each other in meeting the overarching objectives of the project.

This study contributes to three perspectives. First, it prioritizes the attributes of Aadhaar for each goal based on the expert opinion. It gives us an opportunity to uncover how Aadhaar project was approached during its incremental implementation phase which led to its successful implementation. This study could act as a reference for implementation of similar large size biometric programs in future.

Second, methodologically, we also attempt to demonstrate the application of the BWM method on a real world, highly complex group decision-making problem. This study could be used as a valuable case for the validation of BWM on real-world decision problems involving more than a single decision maker. Further, the results of BWM is again verified by TISM and MICMAC methodologies for identifying consistency in results. The case study highlights how such an approach can be effectively used for prioritization and decision making, for complex problems involving multiple factors.

Thirdly, from theoretical perspective, DT for digital identity system is integrated with CSF for a better understanding of digital identity systems. Both these theories are well explained in the literature as mentioned in the introduction section and in the section for theory development.

5. Theoretical lens

Theories like Deferred Action Theory (DAT), systems theory, and stakeholder theory are options available that could have been used in this study, but DT is chosen over others because DT is more suitable for this study as elaborated subsequently.

DAT is relatively new as compared to DT. The basic building blocks of DAT are planned action, emergence, and deferred action (Schneberger, 2012). It helps to discover the impact of emergence on the company and system design (Patel, 2007). DAT is suitable for conceptualizing systems that are operating in a dynamic neighborhood and thereby causing systems and organizations to be emergent (Patel & Hackney, 2010). DAT is relevant and could have been used in this study as the primary theoretical lens but DT is preferred over DAT because the researchers across specializations have widely accepted the former one when stable systems are planned. Moreover, this study analyses an existing systems rather than conceptualizing a new non-existent system and the possibility to evaluate a product and its development process followed makes DT a better choice.

In similar lines, systems theory is used to explore a complex set of interacting elements in a system (Daniël F M Strauss, 2002; Von Bertalanffy, 1956). Systems theory and its variants have been widely applied in various research areas like personality development (Millová & Blatný, 2015), motivational development (M.E. Schneider, 2001; Marianne E. Schneider, 2015), organizational behaviour management (Ludwig, 2015), healthcare (Champion, Kuziemsky, Affleck, & Alvarez, 2019; Clacy, Goode, Sharman, Lovell, & Salmon, 2019), governance (Timoshenko, Kuruppu, Badshah, & Ambalangodage, 2020; Zahra Mansoor & Williams, 2018), and marketing (Mele, Pels, & Polese, 2010). Systems theory does not provide a sophisticated mechanism to identify the problems that designers may encounter (Buchanan, 2019). The theory is based on the assumption that a system is composed of the entities that interact with one another, which in turn depicts a system as a self-regulating entity. The focus of this study is to analyze the development and implementation of Aadhaar which is not the main focus of systems theory and this does not make systems theory a best choice for this study as compared to DT.

Further, Stakeholder Theory (ST) is a proven and widely applied theory in various areas of research for focusing on groups which are vital to the survival of the organization (Freeman, 1999; Stieb, 2009; Schneberger, 2012; Singh, Kar, & Ilavarsana, 2017). The significance of stakeholders in e-governance research has been extensively acknowledged in the literature (Knol, Janssen, & Sol, 2015; Brooks, Janssen, & Papazafeiropoulou, 2018; Janssen & Estevez, 2013; Singh et al., 2017). ST is relevant in the context of this study and could be used as a central theoretical lens, but because the main focus of this study is to analyze the design and implementation process of Aadhaar explicitly, we have strictly restricted our analysis to single stakeholder category that is primarily responsible for the development and implementation of Aadhaar. While extending this study, we will be taking multiple stakeholders into consideration like citizens, NGOs, and other public and private sector participants.

This study attempts to validate the Aadhaar biometric identity system through the lens of DT. DT is often applied to both processes and/or products (Gregor & Jones, 2007). In this research we have used the lens of information systems DT (Walls, Widmeyer, & El Sawy, 1992) as a baseline for analyzing the project of Aadhaar system.

5.1 Design Theory

DT is a widely accepted and implemented theory (Hatchuel et al., 2016). DT focuses on the importance of early stakeholder engagement (Liedtka, King, & Bennett, 2013). It evaluates and examines design as a concept and enables us to verify if the product and the process followed to develop this product, satisfies the fundamentals of the DT.

DT has been defined through multiple lenses like prescriptive by (Walls et al., 1992), practical by (Goldkuhl, 2004), principle based by (Markus, Majchrzak, & Gasser, 2002) ,basis for action by (Gregor & Jones, 2007) and dualist construct by (Simon, 1996; Walls et al., 1992). Walls divided DT for information systems into two major components "Design Product" and "Design Process" and defined DT for information systems as "a prescriptive theory based on theoretical underpinnings which says how a design process can be carried out in a way which is both effective and feasible".

In this study we have applied DT to analyze the process of developing a digital identity system in India. Purpose of understanding and breaking down the whole developmental process of Aadhaar using the DT is to validate the approach adopted which in turn will be beneficial for the countries that might consider Aadhaar as a reference to build their own similar biometric identity system. We use DT to provide an explanatory view of an already implemented digital identity system –Aadhaar. Theoretical approach stresses upon "why" and "how" aspects of the system components. Meta-requirements justifies why a particular goal is important and meta-design explains how to achieve a particular goal with the help of design and execution choices. Components of digital identity DT using CSFs are shown in Fig 4.

5.2 Identification of CSFs of digital identity system

Identification of vital parameters in Aadhaar system is studied through CSF theory approach. Data was collected from the existing academic research articles, official reports from UIDAI, news articles, and from experts who were directly involved with the Aadhaar project right from the beginning. Focus was to cover all the preliminary goals of Aadhaar no matter how latent they are (refer Table A.2 in appendix for details).

Critical success factors theory: Our research is rightly placed within the theory of CSF. CSF theory is defined as "the limited number of areas in which results if they are satisfactory will ensure successful competitive performance for the organization". CSFs were originally defined by (Boynton & Zmud, 1984) as “those few things that must go well to ensure success”. For any large project, the most tedious and challenging tasks are to take right decisions at right time, without taking any risk for granted. The implementation of CSF theory enables to facilitate stakeholders to focus on the significant factors that could lead to achieve a desired goal successfully (Bai & Sarkis, 2013). Thus any initiative taken by an organization must ensure that the performance of critical factors remains high or else there is a possibility that the target goals of an organization may not be achieved.

We conducted a comprehensive literature review of various secondary data and research papers related to digital identity across economies from the Scopus database. Apart from research articles, we also considered official reports from government especially UIDAI and news articles published by some of the leading online news portals. A total of forty preliminary goals were identified that are refined regrouped, renamed and classified into fourteen generic themes out of which nine were selected as CSFs (these form the Meta-requirements) by experts (see Table A.2). Initial classification was done by the authors based on their experience and understanding of literature and classified forty preliminary goals into fourteen themes. Out of fourteen themes, nine were selected by experts after building consensus for the same in three iterations. The final nine accepted labels are shown in Table A.2 in appendix section, and are used for further analysis and address our first research objective i.e. to identify CSFs of Aadhaar. The overall research roadmap is shown in Fig. 3 below.

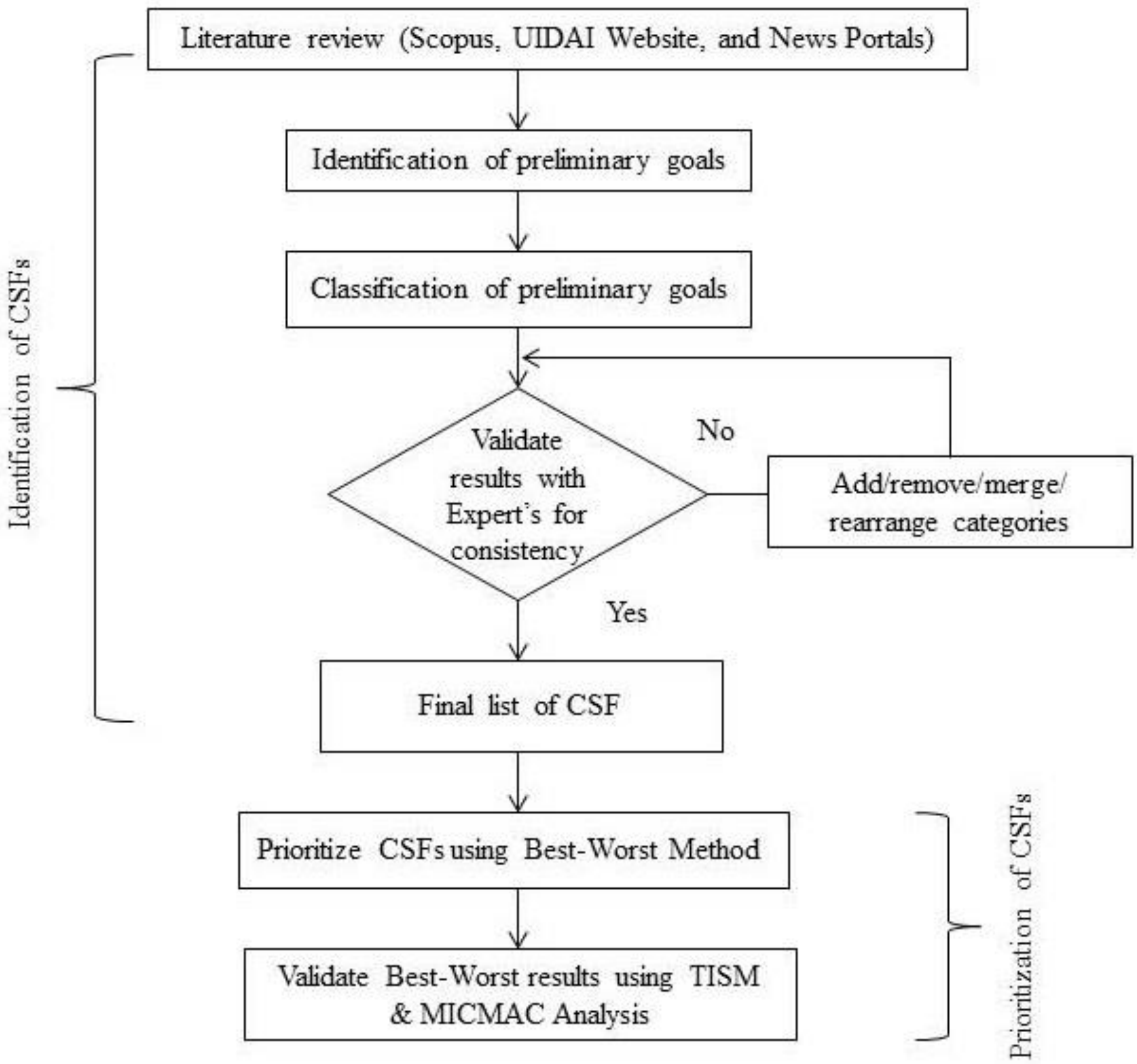

Fig. 3. Research roadmap to identify CSFs of Aadhaar

5.3 Meta-Requirements of digital identity system derived from CSFs

It identifies the list of goals on which theory is applied. For the identification of goals literature review is done that resulted into an extensive list of objectives which was then refined i.e. duplicates were removed, similar ones were combined, and loosely related ones were dropped from the final list based on expert opinion. From the initial forty preliminary objectives, nine goals were shortlisted using CSF theory. These nine goals form meta-requirements for this study.

5.4 Design Method of digital identity system

Design method in this case is a composition of two sub-processes, identification of design choices and execution choices. It was observed that some of the design choices are related to multiple meta-requirements but vary in degree of significance. Dependence of design and execution choices on each meta-requirement is shown in Table A.8 in appendix section. The design and execution choices focus on three aspects of implementation i.e., operational part focusing on the "how" aspect of fulfilling meta-requirements, technological part focusing on the set of technologies needed in the system and social aspect focusing on the societal parameters that play a vital role in the acceptance and effectiveness of the system.

Design choices: Corresponding to nine meta-requirements identified, a total of 17 design choices were made during the tenure of Aadhaar system. The set of design choices were identified from the extensive literature review and verified by the experts before processing it further in the study. Design choices ensure that corresponding to each meta-requirement, a set foundational design criteria are fulfilled.

Execution Choices: Corresponding to 9 meta-requirements identified, a total of 23 execution choices were identified in a similar manner as meta-requirements. It is observed that some of the choices are common in design and execution choices of meta-design (see Table A.8 in appendix). The relation between design and execution choices is many-to-many.

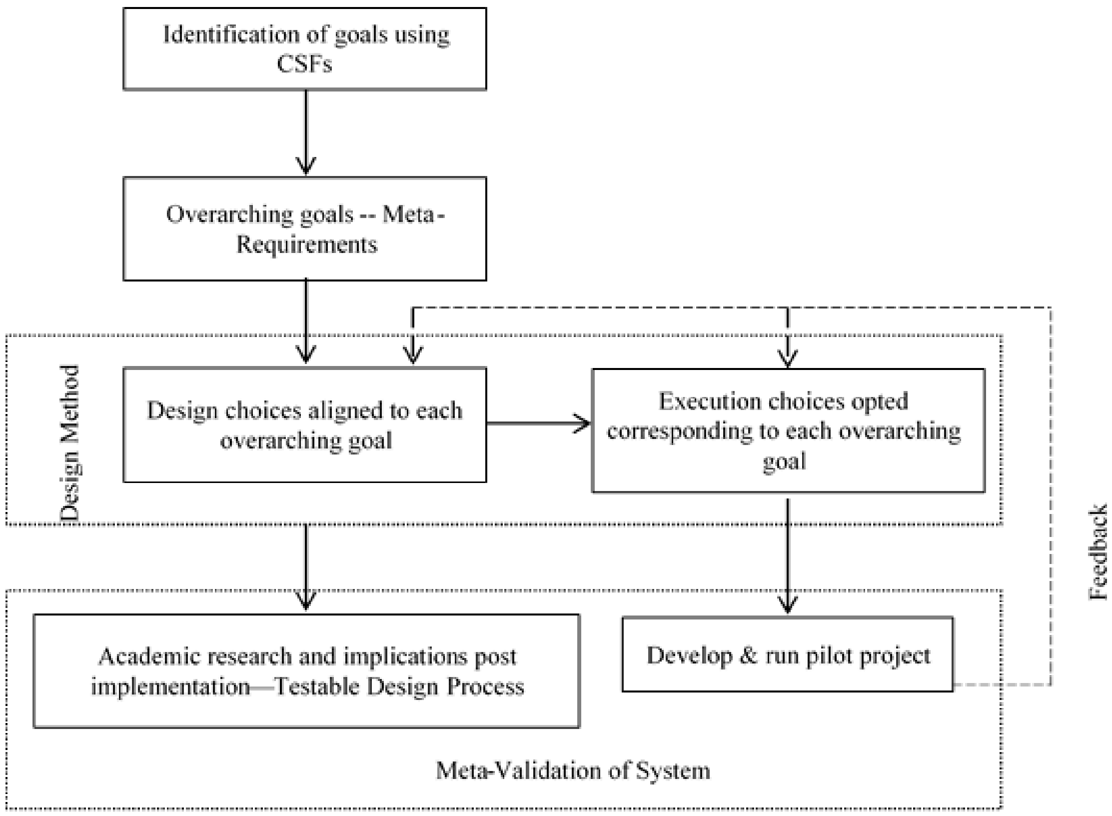

Fig. 4. Components of Digital Identity DT Using CSFs

5.5 Meta-validation of system

Aadhaar digital identity system is tested in two phases. Based on the meta-requirements and meta-design, UIDAI in 2010 conducted a proof-of-concept study in the three states of India i.e. Bihar, Karnataka, and Andhra Pradesh. This helped in identifying the lacunas in the initial version of the scheme. The gaps identified in critical areas like workflow, policy, and system design were addressed in the modified version of scheme and then launched in other parts of the country with corrective measures in place (Zelazny, 2012). Prototyping is considered as a good low-cost tool to gain design information in the early part of design process (HALL, 2001). Another signal depicting successful implementation of Aadhaar could be that more than 20 countries are keen to implement Aadhaar and its underlining technology for its citizens (OECD, 2018). We tried to summarize impact of Aadhaar corresponding to its goals and understand if intended goals of Aadhaar are being achieved in practice or not. Evidences suggest that goals are being achieved to a larger extent but there are some cases were progress is still slow. List of evidences corresponding to each goal are shown in Table 3 and provides a birds-eye-view about the accomplishments of Aadhaar. It tries to explain the impact of each goal in practice.

Table 3: Validation of Aadhaar

Goal	**Validation check**
Building it as a platform	Linking 252 welfare schemes; distributed compute platforms; serving billions of requests daily; data sharded across multiple databases
Future-proofing of technology	Use of open-source technology; open APIs for linking services; Aadhaar number is blocked on the death of the holder;
Data Security and privacy	Option to generate Virtual ID via Aadhaar; limited access to stored personal information; No option to download data; 2048 bit encryption with 256 bit hash
Scalability	Use of open standards; supports large scaling of enrolments and authentications;
Inclusion	99% Coverage; 0.14% failure to enroll; started face ID for enrollment
Uniqueness of IDS	Random number; necessary inclusion of Iris demonstrated with proof-of-concept
Cost Optimisation	less than 100 Indian Rupees per person
Speed	Time required to enroll a single person is approximately 3 minutes; 1 to 4 million enrolments a day; demand based allocation of manpower for enrollment
Resident Convenience	36000 enrolment station operated by 83 agencies via 400 registrars across 32 states and union territories; started face ID for enrollment; home delivery of Aadhaar via speed post in less than 30 days;

Another approach used for meta-validation of the system is by analyzing the research literature on Aadhaar. We searched for “Aadhaar” keyword on Scopus which is the largest peer-reviewed database. Only journal articles were taken into consideration and a total of 76 articles were retrieved out of which 38 articles were found relevant for the study. Authors classified 38 articles manually into three categories based on whether article is in support (17 studies), against (15 studies) or neutral (6 studies) towards the Aadhaar project.

6. Research Methodology

This study adopted focus group methodology to identify the confidence levels between the over-all objectives, design, and execution of Aadhaar project as it is cost effective (Morgan, 1996) and time efficient (Caroline Tynan & Drayton, 1988) in case of in-depth information retrieval about a particular topic is needed. FGD is very useful when there is not much research literature available on a particular topic (Krueger & Casey, 1994), which holds true for this study. Focus group methodology also known as group interviews is a well-known interactive and systematic technique for receiving the opinion of experts on particular issues. It has been used in the various domains like supply chain management (Lambert & Enz, 2017), smart city selection (Kumar, Singh, & Gupta, 2018), business communication (Hartman, 2004), information systems (Burgess, 2010), and logistics (Coule, 2013; O.Nyumba, Wilson, Derrick, & Mukherjee, 2018). FGD is an amalgamation of people from similar backgrounds or experiences together to discuss a particular topic. It falls under the qualitative research category where questions are asked based on the perception, beliefs, opinions or ideas. All members of FGD are free to talk with each other and have discussion based communication. Typically the number of people in a group varies from 6 to 12 people (Wilkinson, 1998). This whole discussion is led by an interviewer specifically called moderator who is responsible for directing the overall discussion.

In this study, an eight-member focus group was formed, each related to Aadhaar project directly and having more than fifteen years of experience in developing and implementing eGovernment projects. The eight experts ranging from senior management professionals, Indian Administrative Service Officers, Deputy-Directors and Secretaries were directly involved in identifying the CSFs of Aadhaar. Identified factors were filtered and validated by the experts, and the final list of CSFs was selected based on the consensus of all the experts.

Details of the focus group members are shown in appendix section A.2**.** Since it was not feasible to arrange a face-to-face meeting with all the group members (many of who were very senior government officials) at a particular location because of their geographical dispersal, a tele-conferencing focused group discussion was conducted. Finally, documents were collated by the authors after consensus was achieved, and results were analyzed using the BWM Method.

5.1 Data Analysis

MCDM Methods

Since this study is based on the evaluation of multiple criteria's for making a final decision, we should use some MCDM method. There have been various MCDM methods applied in the literature (Triantaphyllou, 2013) (Wang, Chen, & Richards, 2018) (Kubler, Robert, Neumaier, Umbrich, & Le, 2018). MCDM allows us to evaluate numerous criteria with varying weights. From the literature, we found multiple MCDM methods being proposed and their applicability in various sectors. Each MCDM method has its own advantages and disadvantages. In Table A.3 we tried to summarize some of the commonly used MCDM methods which could also have been used in our study. We mainly focused on preferred application area, advantages and disadvantages of a particular MCDM method.

Prioritization Approach - Best-Worst Method (BWM)

Many MCDM methods are available among those we choose recently developed MCDM know as Best-Worst Method (Rezaei, 2015, 2016). The reason to choose BWM is because it produces more consistent results, requires fewer data points, does not rely on complete pairwise comparison matrix like AHP and has sophisticated pairwise comparison procedure (Rezaei, 2015). It is also believed by the decision makers that, BWM is very close to how they actually process and make decisions in real life scenario. Because of its simplicity and capability to produce consistent results, this method has been used in many problems like identification of factors that influence standard dominance in business to government data exchange (Kaa, Janssen, & Rezaei, 2018), supplier classification (Torabi, Giahi, & Sahebjamnia, 2016), risk assessment (Torabi et al., 2016) innovation management (Gupta & Barua, 2016) supply chain management (Badri Ahmadi, Kusi-Sarpong, & Rezaei, 2017; Wan

Ahmad, Rezaei, Sadaghiani, & Tavasszy, 2017) , logistics performance measurement (Rezaei, Roekel, & Tavasszy, 2018), measurement of research and development performance (Salimi & Rezaei, 2018), and scientific output evaluation (Gupta & Barua, 2016).

Based on the academic literature and official government reports published by UIDAI from time to time, (Ronald et al., 2017; UIDAI, 2010; Zelazny, 2012) a list of nine over-arching goals were identified. Inputs provided by the focus group were evaluated against these goals. The complete list of identified goals is shown is Table 4 and explained in detail in appendix section A.2.

Table 4: Identification of Goals

Goal	**Definition/description**	**Supporting References**
Uniqueness	Signifies that an identifier is unique in the database. De-duplication achieved by using multiple attributes. Enables one-to-one association between identifier and individual.	(Laurent & Bouzefrane, 2015; UIDAI, 2010)
Inclusion	Every resident of the country has to have one Aadhaar number.	(Jacobsen, 2012; Sharma, 2016; UIDAI, 2010)
Convenience	Getting Aadhaar should be easy in terms of enrolment, collection and modification of details for beneficiary.	(UIDAI, 2010)
Cost-optimization	To reduce the overall costs of Aadhaar project such that it is economically feasible for both government and residents.	(Ronald et al., 2017; Sharma, 2016)
Speed	To ensure coverage of target beneficiaries in a limited time frame.	(UIDAI, 2010)
Scalability	To utilize such technologies and algorithms which are scalable and can keep up with the continuous new enrolments in Aadhaar.	(UIDAI, 2010; Zelazny, 2012)
Platform Development	To develop Aadhaar as a technology platform that can provide yes/no answer such that it could be used in number of different domains.	(Dass, 2011; Ronald et al., 2017)
Technology Adaptation	To adopt to information and communication technologies which have lesser chances of becoming obsolete in near future.	(Zelazny, 2012)
Security and Privacy	The data of 1.2 billion Indian residents is stored and hence the criticality of information security and privacy	(Agrawal, Banerjee, & Sharma, 2017; UIDAI, 2010)

7. Results

In this study, multiple criteria which are vital for each goal were identified and BWM is applied to compute weights of these criteria. Prioritization is done at two stages, first corresponding to each goal its design and execution choices are prioritized which depicts the importance of each criterion and second nine identified goals of Aadhaar are prioritized to develop a final hierarchy of goals based on their significance making it easier to follow and replicate. It will help in taking up the most important goal and then, based on their priority order of design and execution choices could be followed to ensure success in implementation. Next, as an example, we have shown implementation of BWM on design choices of uniqueness goal in appendix section A.3. Similarly prioritization of each criteria for each goal is computed which depicts the relative importance of a particular criteria in achieving a particular goal. Detailed results for remaining goals are added in the appendix section A.2.

In addition to prioritizing criteria for each identified goal, we have attempted to prioritize the over-arching goals of Aadhaar. Here also BW method is used for prioritizing these goals. From the Table 5 below it could be observed that out of nine goals Uniqueness has the highest priority followed by Data Security and Privacy, Resident Convenience, Cost-optimization, Speed, Inclusion, Building it as a platform, Future-proofing, and Scalability. This prioritization could help in resource/budget allocation for each goal based on its importance for designing similar biometric identification programs.

Table 5: Prioritization Summary of Goals of Aadhaar

Goal	**Weight**	**Priority**	**#Design Criteria**	**CR of Design Criteria**	**#Execution Criteria**	**CR of Execution Criteria**
Uniqueness of IDS	0.294	1	3	0.090	5	0.001
Inclusion	0.059	6	3	0.134	4	0.150
Resident Convenience	0.119	3	8	0.075	6	0.070
Cost Optimisation	0.089	4	9	0.046	10	0.06

Speed	0.071	5	3	0.135	9	0.064
Scalability	0.025	9	1	_	4	0.091
Building it as a platform	0.051	7	1	_	6	0.084
Future-proofing of technology	0.044	8	1	_	5	0.071
Data Security and privacy	0.179	2	8	0.05	7	0.079

Where, CR is consistency ratio

Further to verify our results, we used TISM Methodology for analyzing the relationship among the goals; and MICMAC analysis to identify the driving and dependent power of each goal. Idea is to check if computed priorities of goals are also supported by TISM and MICMAC analysis or not. To keep it less textual we have used shorter labels for goals and assigned code to each goal for computation as shown in Table A.4 in appendix.

6.1 TISM/ISM

Total Interpretive Structural Modeling originated from Interpretive Structural Modeling – a process which is employed to transform unclear and ambiguous mental models into clear visible models (Sushil, 2012). TISM tries to address the limitation of ISM by answering one basic question of "why". TISM and ISM has been widely used, (Kumar et al., 2018) used it for choosing a city for smart city project, for food logistics (Shankar, Gupta, & Pathak, 2018), (Shibin, Gunasekaran, & Dubey, 2017) used for explaining sustainable supply chain performance, (Shukla & Mattar, 2019) used it to identify barriers in application of Bigdata analytics based sustainable auditing system . In this study, it is used to prioritize the goals of Aadhaar.

We have implemented TISM methodology elaborated by (Sushil, 2012) and (V. Jain & Raj, 2015). The first phase in TISM is to identify and define elements whose priorities' are to be identified. Second, contextual relationships among factors are identified via pair-wise comparisons. Third, interpretive logic – knowledge base is developed and each pair-wise comparison is interpreted based on directional relations that operate in a given context by answering interpretive query "A is of higher priority than B. All detailed matrix computations are not shown in this paper as the purpose of applying TISM is to compare the results with BWM.

In the next step, paired comparisons in the interpretive logic—knowledge base (see Table A.9) are translated into initial reachability matrix. If the entry in knowledge base is "Y" then corresponding cell in the reachability matrix is marked 1 or else 0. Once initial reachability matrix is developed it is checked for transitivity property and finally converted into final reachability matrix (Dubey & Ali, 2014; Sushil & Sushil, 2005). Transitivity property means if p helps q and q helps r, then p helps r also. The final reachability matrix is shown in Table A.5 in appendix.

Next, factors are arranged into hierarchical form based on their ranking. Reachability set (RS) and antecedent set (AS) corresponding to each factor is computed as shown in Table A.6. Corresponding to each factor, intersection set (IS) is computed between RS and AS. During iteration process if RS and IS are same for any factor then that factor is kept in the top level of hierarchy. In the subsequent iterations, factors with levels assigned are removed from the partition matrix and whole process is repeated for remaining factors. This iteration process is continued till all factors are assigned a level (Warfield, 1974) and (Sushil, 2012). After portioning is completed, canonical matrix is developed as shown is Table A.7 in appendix**.** In our case it took six iterations to determine the level of each element. The final partition matrix is shown in Table 6 below.

Table 6: Final Partitioning Matrix

Element	Reachability	Antecedents	Inters-	Levels
F1	{F1,F2,F4}	{F1,F3,F5,F6,F7,F8,F9}	{F1}	II
F2	{F2}	{F1,F2,F3,F5,F6,F7,F8,F9}	{F2}	I
F3	{F1,F2,F3,F4,F5,F7,F8,F9}	{F3,F6}	{F3}	V
F4	{F4}	{F1,F3,F4,F5,F6,F7,F8,F9}	{F4}	I
F5	{F1,F2,F4,F5}	{ F3,F5,F6,F7,F8,F9}	{F5}	III

F6	{F1,F2,F3,F4,F5,F6,F7,F8,F9}	{F6}	{F6}	VI
F7	{F1,F2,F4,F5,F7}	{F3,F6,F7}	{F7}	IV
F8	{F1,F2,F4,F5,F8}	{F3,F6,F8}	{F8}	IV
F9	{F1,F2,F4,F5,F9}	{F3,F6,F9}	{F9}	IV

Once final partitioning matrix is generated, it is converted into graphical TISM hierarchy model as shown in Fig 5. The TISM model indicates the prioritization and arrangement of factors based on their significance level through a systematic computation. It could be seen from the hierarchy model that uniqueness is the most significant goal followed by security and privacy (bottom level of the hierarchy means most significant whereas top most level means least significant). Speed, cost and convenience are at the same level which depicts they are of same importance followed by less significant one, inclusion which is rated higher than platform. The final level of TISM model is shared by two least significant goals i.e. future-proofing and scalability.

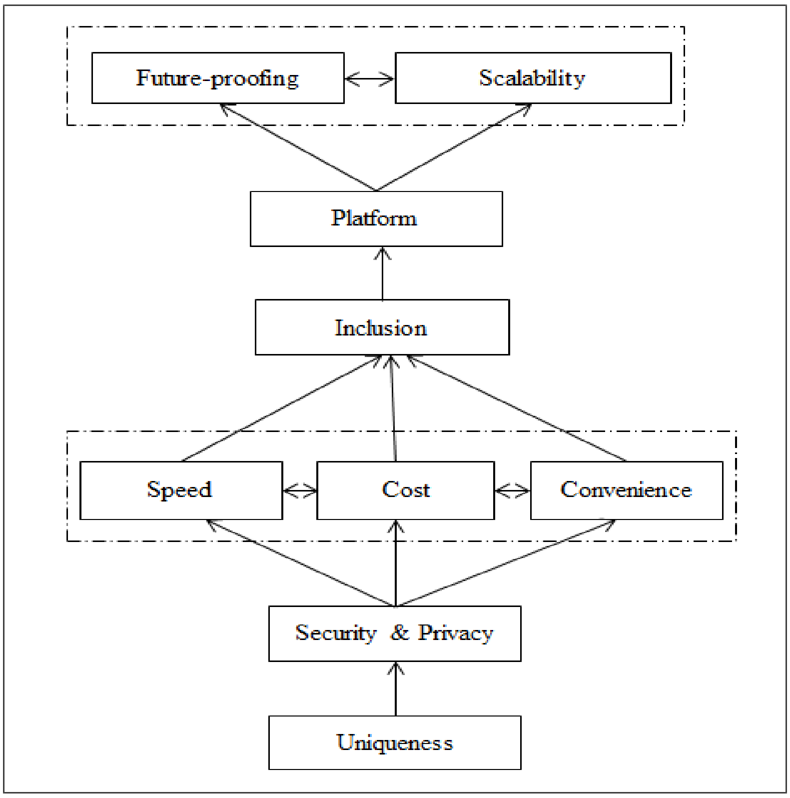

Fig. 5: TISM Hierarchy Model

When we compare results of TISM with BWM results (see Table 7), it is found that both results complement each other and are very similar. This similarity of results between BWM and TISM methodology further validates the output of this research.

Table 7: Comparison of Prioritization based on BWM and TISM

Goal	Significance in BWM		Significance in TISM		Comparison
	Rank	Weight	Rank	Level	
Uniqueness	1	0.294	1	6	Strongly Agree
Security and Privacy	2	0.179	2	5	Strongly Agree
Cost	4	0.089	3	4	Agree
Speed	5	0.071	3	4	Agree
Convenience	3	0.119	3	4	Strongly Agree
Inclusion	6	0.059	4	3	Strongly Agree
Platform	7	0.051	5	2	Strongly Agree
Future-proofing	8	0.044	6	1	Agree
Scalability	9	0.025	6	1	Strongly Agree

6.2 MICMAC

MICMAC was evolved by Duperrin and Godet in 1973 (Hu, H.-Y, Chui, S.-I, Yen, 2009). Based on the output of ISM methodology, it categorizes list of factors into four quadrants i.e. drivers, linkages, dependents and autonomous. Each quadrant classifies factors based on their position, which is identified by the driving and dependence power of a particular factor. MICMAC and its variants have been used to solve different problems like identifying barriers of mobile-commerce adoption in small and medium enterprises (Rana, Barnard, Baabdullah, & Rees, 2019), identification of CSF for reusable plastic packing (Gardas, Raut, & Narkhede, 2019), categorization of critical infrastructure sectors in India (Narain, Gupta, & Ojha, 2014), analysis of obstructions in the reduction of agri-food supply chain in India (Gokarn & Kuthambalayan, 2017), identification of reasons behind changing project management offices (Bredillet, Tywoniak, & Tootoonchy, 2018) etc.

We used MICMAC methodology to analyze the hierarchical relationship among factors based on their driving and dependence power. Nine factors were categorized into three categories. It was observed that F6 (Uniqueness) and F3 (Security and Privacy) possess higher driving power and F1 (Platform), F2 (Future-proofing), and F5 (Inclusion) possess higher dependent power whereas F7 (Cost), F8 (Speed) and F9 (Convenience) form linkages with somewhat balanced driving and dependent power.

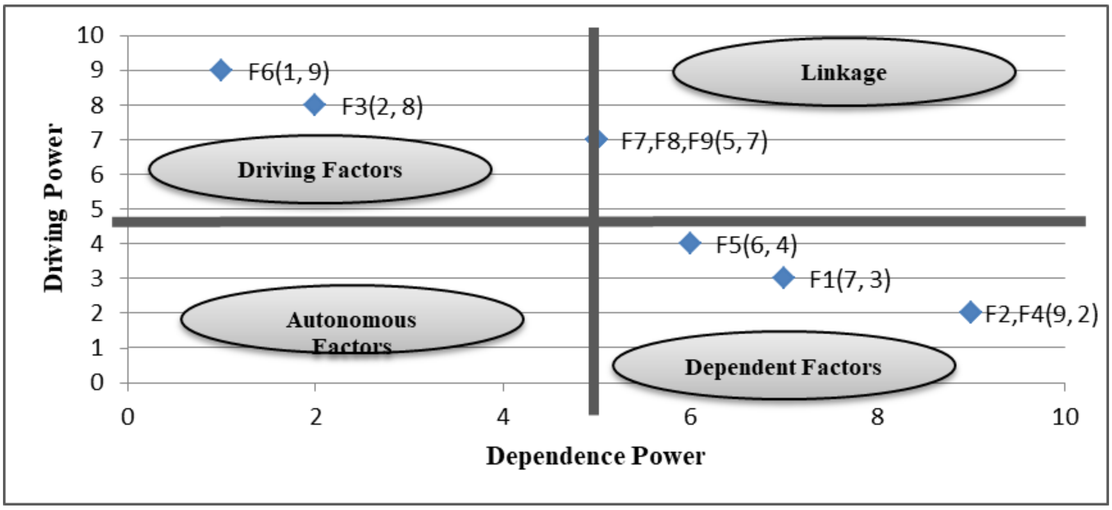

Fig. 6: MICMAC Analysis of Aadhaar Goals

Where, F1 is Platform; F2 is Future-proofing; F3 is Security and Privacy; F4 is Scalability; F5 is Inclusion; F6 is Uniqueness; F7 is Cost; F8 is Speed and F9 is Convenience

Cluster classification scatter diagram is developed based on the output of MICMAC analysis. It differentiates between the set of goals based on their significance. From the Fig 6 above, group of clusters is formed based on the driving and dependence strength of a particular goal.

Highest ranked goals in BW and TISM form driving factor category, and lowest ranked goals form dependent factor category in MICMAC analysis whereas remaining goals form linkage category. This way, MICMAC analysis also verifies the consistency, correctness and significance of goals as computed in BWM and TISM methodologies.

8. Discussion

The success of any Biometric Identification Systems is related to the biometrics employed in that system and how well they are performing. Purpose of the biometric system varies based on its application, e.g., Security, Education, Sports, Healthcare, Human identification, Government, Law enforcement, Banking, Manufacturing (Ilie-Zudor, Kemény, van

Blommestein, Monostori, & van der Meulen, 2011). In the literature section, the study on biometrics has been done based on (i) Functional utility (ii) Technical architecture and (iii) its process flow. In the recent past, many countries have thought of having a unique identification identity for its citizens for providing benefits to its citizens directly, some countries have already implemented, and some are starting now. Considering the complexity involved in terms of budget allocation, manpower required, technological requirement, and policy development in implementing a large-scale biometric identification program for citizen identification at country level, a stringent action plan is needed to avoid any unnecessary risks that might occur in the tenure of the project which could result in substantial losses. To the best of our knowledge, we did not find any study in the literature related to the prioritization of design and execution choices made during the development of any biometric identification system.

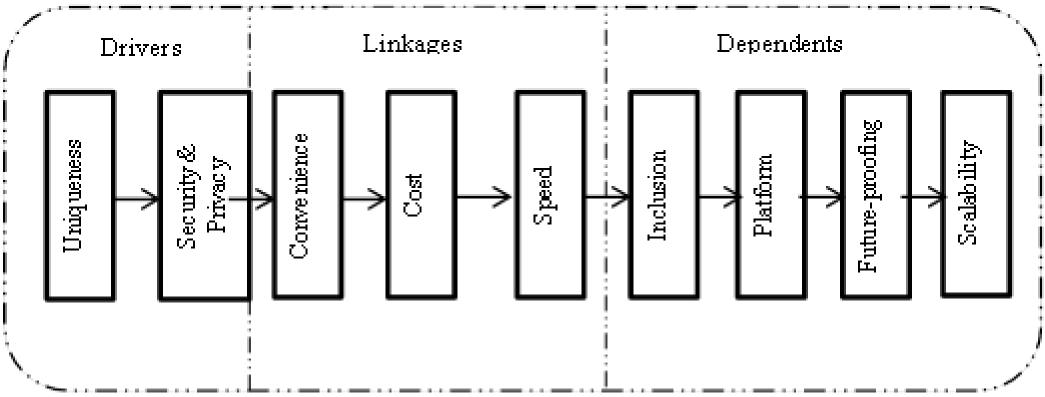

Fig. 7: Prioritization and Classification of Goals

Fig 7 illustrates the final prioritization and classification hierarchy of digital identity goals. High priority goals are labeled as drivers and less priority goals are labeled as dependents whereas goals under linkage label have medium priorities. This prioritization could be very helpful when implementing a biometric identification system from scratch as it depicts what goals should be taken up first and what goals could be taken up in the later stages of the project development.

8.1 Implications for theory

This study contributes to the theory on digital identity in a sense that it uses combination of two theories to explain the phenomena of designing and developing a digital identity system. This is for the first time that CSF and DT has been used together to explain the design and development process of any digital identity system. The adoption of guidelines for developing a digital identity system is always a good practice. Considering the implementation and developmental cost of a typical digital ID scheme which is around £100-250 million (Identity, 2018), in case of Aadhaar the total cost of Aadhaar project is INR 60,000 – 70,000 crores (McKinsey, 2010; Venkatanarayanan, 2018), it is essential to evaluate each decision beforehand with utmost importance such that no significant setbacks occur afterwards. Having a sophisticated digital ID scheme in place could save £5-10 billion by reducing identity-related fraud and improving operational efficiency (Identity, 2018). E-government schemes are complex and involve different actors, ambitions and perspectives (Larsson & Grönlund, 2014). E-government schemes have multiple stakeholders, and it is vital to give due diligence to their needs and aspirations right from the initial stages of the project development such that the probability of project failure is minimized. Studies to evaluate the significance of decisions taken during the design, development and implementation phases with focus on stakeholder aspirations is said to have high impact in the field of information and communication technology development. This study contributes to understanding the overall developmental process of e-government projects. It adds to the Social Construction of Technology (SCOT) study on Aadhaar (Sivamalai, 2013), that tries to explain how perception of different stakeholders vary about Aadhaar based on the SCOT framework. The result of this study not only supports the concept of stakeholder involvement during e-governance project development but also suggests that the development and implementation of project should be guided by the priorities of CSFs of that particular project. The results of this study are also consistent with the previous research that highlighted that confidentiality must be enforced over enrolment (this study found security and privacy as second most important goal) (Belanche-gracia, Casaló-ariño, & Pérez-rueda, 2015; Mali & Avila-Maravilla, 2018).

Failure of UK's National ID could be considered as a validity check for this research. One of the primary reasons for scarping this project was its cost (Travis, 2010). UK government spent around £4.5 billion from July 2002 to February 2010 on NID and had spent £250 million on developing it. The price of a single ID card was £30 which was considered too expensive. The significance of cost has been detrimental for National ID and this significance is reflected in our research as well as cost is the fourth most important goal for an identity system. Our study strengthens the understanding surrounding the factors which impact the outcome of such digital identity projects, even in developed economies.

Considering the digital identity as domain, no such study was found from the literature which has prioritized the goals of Aadhaar and decisions taken during design and development of Aadhaar system. With a focus on identifying linkages among goals of Aadhaar and multiple decisions evaluated during the design and implementation of the Aadhaar system, this study is unique in its own way.

The study is unique for its methodological contributions as well. From the research methodology point of view, the main contribution of this study is the combination and application of three different methodologies i.e. BWM, TISM and MICMAC, on a single large scale project and to analyze the process and factors taken into consideration for decision making in such a massive and critical national project. Also, the knowledge obtained through the method and technique implemented for collecting data may be helpful in other studies on analyzing large scale government initiatives. The integrated usage of three different methodologies also ensures higher rigor in the methodology which brings more confidence on the reliability and validity of the outcome.

Overall findings from three different methods reveal that in an identity scheme uniqueness of an entity and privacy and security of individual's data is of utmost importance and is the main driving factors of the whole scheme. The inclusion of entire population, building identity project as a platform rather than a single standalone system, making project capable of withholding dynamic technological innovations and a mechanism to scale project as and when needed are those objectives which are vital in an identity system but could be taken up in later stages of the project development. These four objectives are highly dependent on drivers and linkages, and hence it is logical to focus on drivers and linkages first as shown in prioritization hierarchy diagram. Linkages which comprise of cost, speed and convenience act as intermediaries between drivers and dependent factors and have higher priority than dependents. Based on the results we recommend to follow priority order however in case of linkages, three objectives, i.e. cost, speed and convenience could be shuffled if situation demands for it.

8.2 Implications for practice

Aadhaar has received much attention across the globe ever since UN recommended to provide the legal identity for all in its SDG 16 (UNGA, 2016). Aadhaar being a massive biometric project at present with more than 1.2 billion Aadhaar numbers issued, it has become a system which other countries may contemplate replication while implementing a biometric digital identity system. To start any such critical mega-project requires a lot of planning while focusing on budget estimation, implementation policy, and development plan and to identify various types of risks associated with the project at each stage. For developing nations, it may not be feasible to reinvent the wheel and conduct this analysis because of time, budget and expertise constraints. This research is intended to contribute in this space by bringing out both design and implementation factors for public policy makers of future digital identity systems. It will act as a reference for all those nations who are working on UN's SDG 16 for providing legal identity to all its individuals. It will be helpful in taking up a biometric identification program in a systematic manner by giving specific attention to high priority tasks. It will help concerned nations to save significant amount of time and money which otherwise would have been mandatory for conducting a pre-launch analysis. It will also enable governments to identify different types of risks associated at various stages of program and will allow them to have mitigation measures thereby increasing chances of having a successful, efficient project in place. In this study, we have shown how important each criterion is for accomplishing a particular goal. We also found how priority of same criterion varies among different goals. Further, we also illustrated through a case study on Aadhaar how BWM could be used in real-world complex decision-making problems.

9. Conclusion

We conclude our study of prioritizing goals of Aadhaar by verifying our results with the help of two more methodologies- TISM and MICMAC analysis. Original prioritization results are also supported by both TISM and MICMAC results which further strengthen our findings. Digital identities, in general, have the capacity for both bliss and misery. A well planned digital identity system, having necessary measures in place that can address issues like security, privacy, inclusion and citizen empowerment could unfold remarkable economic values. In this work, we conducted a detailed study to identify the primary goals that are must for any biometric identification system. India's biometric identification program- Aadhaar has been used as a case study and has been analyzed from the perspective of DT in this study. After prioritizing design goals of Aadhaar using Best-Worst Method and verified using TISM and MICMAC, it was observed that three clusters of goals were formed. All three clusters are critical for any biometric identification program but with varying priorities. First cluster (i.e. drivers) has the highest priority and must be dealt on priority in the initial stages of the program, second cluster (i.e. linkages) is the second most significant one and could be taken right after the first cluster, and third cluster (i.e. dependents) which has comparatively less priority as compared to drivers and linkages and could be taken up in the later stages of the program development. This study also tests the application of BWM method on a real-world complex problem for evaluating the opinion of focus group members.

Since this research is limited to only one case study –Aadhaar, we do not claim priorities of goals as an absolute one. We hope to inspire researchers across the world to conduct similar studies on other national biometric identity projects and develop a universal prioritization hierarchy. Future research direction is to verify the prioritized goals on some more existing biometric identification system and use the results of prioritization in designing the real-world biometric identification system. Also, security and privacy have emerged as the second most crucial goal in this study. However, frequent complaints related to the security and privacy of Aadhaar highlights that something is still lacking. This gap could be another exciting area to explore.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References:

Abate, A. F., Marcialis, G. L., Poh, N., & Sansone, C. (2019). Introduction to the special issue on robustness, security and regulation aspects in current biometric systems (RSRA-BS). *Pattern Recognition Letters*, *126*, 1–2. https://doi.org/10.1016/j.patrec.2019.07.004

Agogué, M., & Kazakçi, A. (2014). 10 Years of C–K Theory: A Survey on the Academic and Industrial Impacts of a Design Theory. In *An Anthology of Theories and Models of*

Design (pp. 219–235). London: Springer London. https://doi.org/10.1007/978-1-4471-6338-1_11

Agrawal, S., Banerjee, S., & Sharma, S. (2017). Privacy and Security of Aadhaar : A Computer Science Perspective, *52*(37), 1–23.

Akhtar Shareef, M., Kumar, V., Kumar, U., & Dwivedi, Y. (2014). Factors affecting citizen adoption of transactional electronic government. *Journal of Enterprise Information Management*, *27*(4), 385–401. https://doi.org/10.1108/JEIM-12-2012-0084

Aladwani, A. M. (2016). Corruption as a source of e-Government projects failure in developing countries: A theoretical exposition. *International Journal of Information Management*, *36*(1), 105–112. https://doi.org/10.1016/j.ijinfomgt.2015.10.005

Anil, K. J., & Sharathchandra, P. (2001). A Touch of Money. *IEEE Spectrum*, *4123*(March), 1–9.

Anthopoulos, L., Reddick, C. G., Giannakidou, I., & Mavridis, N. (2016). Why e-government projects fail? An analysis of the Healthcare.gov website. *Government Information Quarterly*, *33*(1), 161–173. https://doi.org/10.1016/j.giq.2015.07.003

Arutyunov, V. V., & Natkin, N. S. (2010). Comparative analysis of biometric systems for information protection. *Scientific and Technical Information Processing*, *37*(2), 87–93. https://doi.org/10.3103/S0147688210020012

Badri Ahmadi, H., Kusi-Sarpong, S., & Rezaei, J. (2017). Assessing the social sustainability of supply chains using Best Worst Method. *Resources, Conservation and Recycling*, *126*, 99–106. https://doi.org/https://doi.org/10.1016/j.resconrec.2017.07.020

Bai, C., & Sarkis, J. (2013). A grey-based DEMATEL model for evaluating business process management critical success factors. *International Journal of Production Economics*, *146*(1), 281–292. https://doi.org/10.1016/j.ijpe.2013.07.011

Baichoo, S., Heenaye-Mamode Khan, M., Bissessur, P., Pavaday, N., Boodoo-Jahangeer, N.,

& Purmah, N. R. (2018). Legal and ethical considerations of biometric identity card: Case for Mauritius. *Computer Law & Security Review*, *34*(6), 1333–1341. https://doi.org/10.1016/j.clsr.2018.08.010

Bálint, T., & Bucko, J. (2013). Comparative Analysis of Handwritten, Biometric and Digital Signature. *International Review of Social Sciences and Humanities*, *4*(2).

Bank, W. (2016). Population of India. Retrieved from https://data.worldbank.org/indicator/SP.POP.TOTL

BankWorld. (2016). *World Development Report 2016: Digital Dividends*. The World Bank. https://doi.org/10.1596/978-1-4648-0671-1

Barnwal, P. (2015). Curbing Leakage in Public Programs with Direct Benefit Transfers Evidence from India ' s Fuel Subsidies and Black Markets. *Working Paper*, (November 2014).

BBC News. (2002). Doubt cast on fingerprint security. Retrieved December 20, 2017, from http://news.bbc.co.uk/2/hi/science/nature/1991517.stm

Belanche-gracia, D., Casaló-ariño, L. V, & Pérez-rueda, A. (2015). Determinants of multi-service smartcard success for smart cities development : A study based on citizens ' privacy and security perceptions. *Government Information Quarterly*, *32*(2), 154–163. https://doi.org/10.1016/j.giq.2014.12.004

Ben Ayed, G. (2014). *Architecting User-Centric Privacy-as-a-Set-of-Services*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-08231-8

Bergeron, F., & Bégin, C. (1989). The Use of Critical Success Factors in Evaluation of Information Systems: A Case Study. *Journal of Management Information Systems*, *5*(4), 111–124. https://doi.org/10.1080/07421222.1989.11517842

Bouchrika, I. (2017). A Survey of Using Biometrics for Smart Visual Surveillance: Gait Recognition. In *Surveillance in Action* (pp. 3–23). Springer. Retrieved from https://link.springer.com/chapter/10.1007/978-3-319-68533-5_1

Boynton, A., & Zmud, R. (1984). An Assessment of Critical Success Factors. *Sloan Management Review*, *25*(4), 17.

Bredillet, C., Tywoniak, S., & Tootoonchy, M. (2018). ScienceDirect Why and how do project management of fi ces change ? A structural analysis approach. *International Journal of Project Management*, *36*(5), 744–761. https://doi.org/10.1016/j.ijproman.2018.04.001

Buchanan, R. (2019). Systems Thinking and Design Thinking: The Search for Principles in the World We Are Making. *She Ji: The Journal of Design, Economics, and Innovation*, *5*(2), 85–104. https://doi.org/10.1016/j.sheji.2019.04.001

Burgess, S. (2010). The Use of Focus Groups in Information Systems Research. *The International Journal of Interdisciplinary Social Sciences: Annual Review*, *5*(2), 57–68. https://doi.org/10.18848/1833-1882/CGP/v05i02/51567

Caroline Tynan, A., & Drayton, J. L. (1988). CONDUCTING FOCUS GROUPS — A GUIDE FOR FIRST-TIME USERS. *Marketing Intelligence & Planning*, *6*(1), 5–9. https://doi.org/10.1108/eb045757

Chandra, A., & Calderon, T. (2005). Challenges and Constraints to the Diffusion of Biometrics in Information Systems. In *Communications of the ACM* (p. 48).

Coule, T. (2013). Theories of knowledge and focus groups in organization and management research. *Qualitative Research in Organizations and Management: An International Journal*, *8*(2), 148–162. https://doi.org/10.1108/QROM-09-2011-1006

Dass, R. (2011). Unique Identification for Indians: A Divine Dream or a Miscalculated Heroism?, *36*(1), 1–14. https://doi.org/10.1177/0256090920110101

Daugman, J. G. (1993). High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *15*(11), 1148–1161. https://doi.org/10.1109/34.244676

Dixon, P. (2017). 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 and Technology*. https://doi.org/10.1007/s12553-017-0202-6

Dubey, R., & Ali, S. S. (2014). Identification of flexible manufacturing system dimensions and their interrelationship using total interpretive structural modelling and fuzzy MICMAC analysis. *Global Journal of Flexible Systems Management*, *15*(2), 131–143. https://doi.org/10.1007/s40171-014-0058-9

Elkadi, H. (2013). Success and failure factors for e-government projects: A case from Egypt. *Egyptian Informatics Journal*, *14*(2), 165–173. https://doi.org/10.1016/j.eij.2013.06.002

Epstein, C. (2008). Embodying Risk:Using Biometrics To Protect the Borders. In *Risk and the War on Terror* (pp. 178–193). Routledge. Retrieved from https://www.academia.edu/2420067/_Embodying_Risk_Using_Biometrics_to_Protect_the_Borders_in_L_Amoore_and_M_de_Goede_ed._2008_Risk_and_the_War_on_Terror_Routledge_London

Esfahlan, E. H., & Valilai, O. F. (2019). A Knowledge Oriented Framework to Enable New Service Development Using Axiomatic Design Theory: Focusing on Hotel Business Models. In *2019 15th Iran International Industrial Engineering Conference (IIIEC)* (pp. 267–273). IEEE. https://doi.org/10.1109/IIIEC.2019.8720620

Fenu, G., Marras, M., & Boratto, L. (2018). A multi-biometric system for continuous student authentication in e-learning platforms. *Pattern Recognition Letters*, *113*, 83–92. https://doi.org/10.1016/j.patrec.2017.03.027

Gal, U., & Whitley, E. A. (2011). Special Issue on Information Systems, Identity and Identification. *European Journal of Information Systems (EJIS)*, *1*(1), 1–2.

Gardas, B. B., Raut, R. D., & Narkhede, B. (2019). Identifying critical success factors to facilitate reusable plastic packaging towards sustainable supply chain management. *Journal of Environmental Management*, *236*(January), 81–92. https://doi.org/10.1016/j.jenvman.2019.01.113

Gelb, A., & Clark, J. (2013). Performance Lessons from India ' s Universal Identification Program CGD Policy Paper 020 May 2013, (May).

GOI. (2016). *Elderly in India*. Retrieved from http://mospi.nic.in/sites/default/files/publication_reports/ElderlyinIndia_2016.pdf

Gokarn, S., & Kuthambalayan, T. S. (2017). Analysis of challenges inhibiting the reduction of waste in food supply chain. *Journal of Cleaner Production, 168*, 595–604. https://doi.org/10.1016/j.jclepro.2017.09.028

Goldkuhl, G. (2004). Design Theories in Information Systems – A Need for Multi-Grounding. *Journal of Information Technology Theory and Application (JITTA)*, *6*(2), 59–72. Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1127&context=jitta

Gregor, S., & Jones, D. (2007). The Anatomy of a Design Theory. *Journal of the Association for Information Systems*, *8*(5), 312–335. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.232.743&rep=rep1&type=pdf

Gupta, H., & Barua, M. K. (2016). Identifying enablers of technological innovation for Indian MSMEs using best–worst multi criteria decision making method. *Technological Forecasting and Social Change*, *107*, 69–79. https://doi.org/https://doi.org/10.1016/j.techfore.2016.03.028

HALL, R. R. (2001). Prototyping for usability of new technology. *International Journal of Human-Computer Studies*, *55*(4), 485–501. https://doi.org/10.1006/ijhc.2001.0478

Hartman, J. (2004). Using Focus Groups to Conduct Business Communication Research. *Journal of Business Communication*, *41*(4), 402–410.

https://doi.org/10.1177/0021943604267775

Hedström, K., Karlsson, F., & Söderström, F. (2016). Challenges of introducing a professional eID card within health care. *Transforming Government: People, Process and Policy*, *10*(1), 26–46. https://doi.org/10.1108/TG-10-2013-0044

Hoang, B., & Caudill, A. (2012). Biometrics. *IEEE Emerging Technology Portal*, 1–3.

Hodeghatta, U., & Nayak, R. (2014). Physical Security and Biometrics. In *The InfoSec Handbook* (pp. 293–306). SpringerLink. https://doi.org/https://doi.org/10.1007/978-1-4302-6383-8_14

Howlett, M. (2014). From the 'old' to the 'new' policy design: design thinking beyond markets and collaborative governance. *Policy Sciences*, *47*(3), 187–207. https://doi.org/10.1007/s11077-014-9199-0

Hu, H.-Y, Chui, S.-I, Yen, T.-M. (2009). Modified IPA for order-winner criteria improvement: A MICMAC approach. *Journal of Applied Sciences*, *9*(21), 3792–3803.

Identity, I. (2018). Digital Identity in the UK : The cost of doing nothing, (April).

Ilie-Zudor, E., Kemény, Z., van Blommestein, F., Monostori, L., & van der Meulen, A. (2011). A survey of applications and requirements of unique identification systems and RFID techniques. *Computers in Industry*, *62*(3), 227–252. https://doi.org/10.1016/j.compind.2010.10.004

Irani, Z., Kamal, M., Axelsson, U. M., Karin, Wihlborg, E., & Janssen, M. (2016). Editorial. *Transforming Government: People, Process and Policy*, *10*(1), 2–7. https://doi.org/10.1108/TG-01-2016-0009

ISO. (2011). Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts. Retrieved from https://www.iso.org/standard/57914.html

ITU-T. (2010). X.1252 - Baseline identity management terms and definitions. *Itu-T X-Series*

Recommendations Data Networks, Open System Communications and Security, ITU-T X.1252 (04/2010).

Jacobsen, E. K. U. (2012). Unique Identification : Inclusion and surveillance in the Indian biometric assemblage. https://doi.org/10.1177/0967010612458336

Jain, A K, Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 4–20. https://doi.org/10.1109/TCSVT.2003.818349

Jain, Anil K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, *79*, 80–105. https://doi.org/10.1016/j.patrec.2015.12.013

Jain, V., & Raj, T. (2015). Modeling and analysis of FMS flexibility factors by TISM and fuzzy MICMAC. *International Journal of Systems Assurance Engineering and Management*, *6*(3), 350–371. https://doi.org/10.1007/s13198-015-0368-0

Kaa, G. Van De, Janssen, M., & Rezaei, J. (2018). Technological Forecasting & Social Change Standards battles for business-to-government data exchange : Identifying success factors for standard dominance using the Best Worst Method. *Technological Forecasting & Social Change*, *137*(July), 182–189. https://doi.org/10.1016/j.techfore.2018.07.041

Krueger, R., & Casey, M. (1994). *Focus Groups: A Practical Guide for Applied Research*. Sage Publications.

Kubler, S., Robert, J., Neumaier, S., Umbrich, J., & Le, Y. (2018). Comparison of metadata quality in open data portals using the Analytic Hierarchy Process. *Government Information Quarterly*, *35*(1), 13–29. https://doi.org/10.1016/j.giq.2017.11.003

Kumar, H., Singh, M. K., & Gupta, M. P. (2018). A policy framework for city eligibility analysis: TISM and fuzzy MICMAC-weighted approach to select a city for smart city transformation in India. *Land Use Policy*, *82*(February 2018), 375–390. https://doi.org/10.1016/j.landusepol.2018.12.025

Lambert, D. M., & Enz, M. G. (2017). Issues in Supply Chain Management: Progress and potential. *Industrial Marketing Management, 62*, 1–16. https://doi.org/10.1016/j.indmarman.2016.12.002

Larsson, H., & Grönlund, Å. (2014). Future-oriented eGovernance : The sustainability concept in eGov research , and ways forward. *Government Information Quarterly*, *31*(1), 137–149. https://doi.org/10.1016/j.giq.2013.07.004

Laurent, M., & Bouzefrane, S. (2015). *Digital Identity Management*. *ISTE Press and Elsevier*. https://doi.org/10.1007/978-3-319-08231-8

Le Masson, P., Hatchuel, A., Le Glatin, M., & Weil, B. (2019). Designing Decisions in the Unknown: A Generative Model. *European Management Review*, *16*(2), 471–490. https://doi.org/10.1111/emre.12289

Lentner, G. M., & Parycek, P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study. *Transforming Government: People, Process and Policy*, *10*(1), 8–25. https://doi.org/10.1108/TG-11-2013-0047

Li, X., Sun, S. X., Chen, K., Fung, T., & Wang, H. (2015). Design Theory for Market Surveillance Systems. *Journal of Management Information Systems*, *32*(2), 278–313. https://doi.org/10.1080/07421222.2015.1063312

Mali, N. V., & Avila-Maravilla, M. A. (2018). Convergence or Conflict? *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance - ICEGOV '18*, 443–448. https://doi.org/10.1145/3209415.3209487

Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A Design Theory for Systems That Support Emergent Knowledge Processes. *MIS Quarterly*, *26*(3), 179–212. Retrieved from https://www.jstor.org/stable/pdf/4132330.pdf

Marohn, D. (2006). Biometrics in healthcare. *Biometric Technology Today*, *14*(9), 9–11. https://doi.org/https://doi.org/10.1016/S0969-4765(06)70592-6

Mauceri A.J. (1965). *Feasibility Study Of Personnel Identification By Signature Verification.* Retrieved from http://www.dtic.mil/docs/citations/AD0617615

May, P.J. (2003). Policy design and implementation. In *Handbook of public administration* (p. 233).

McKinsey. (2010). *Inclusive growth and financial security*. Retrieved from http://ccmrm.org/wp-content/uploads/2015/05/McKinsey-2010-inclusive-growth-report.pdf

McKinsey. (2019). *Digital Identification : A Key To Inclusive Growth*. Retrieved from https://www.mckinsey.com/~/media/mckinsey/featured insights/innovation/the value of digital id for the global economy and society/mgi-digital-identification-a-key-to-inclusive-growth.ashx

Mcwaters, R. J. (2016). A Blueprint for Digital Identity The Role of Financial Institutions in Building Digital Identity. *World Economic Forum, Future of Financial Services Series*, (August), 1–108. Retrieved from http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

Meier, A., & Terán, L. (2019). Special Issue on eGovernment Research, Management, and Innovation.

Melin, U., Axelsson, K., & Söderström, F. (2016). Managing the development of e-ID in a public e-service context. *Transforming Government: People, Process and Policy*, *10*(1), 72–98. https://doi.org/10.1108/TG-11-2013-0046

Mintrom, M., & Luetjens, J. (2016). Design Thinking in Policymaking Processes: Opportunities and Challenges. *Australian Journal of Public Administration*, *75*(3), 391–

402. https://doi.org/10.1111/1467-8500.12211

Morgan, D. (1996). Focus Groups. *Annual Review of Sociology*, *22*, 129–152.

Narain, A., Gupta, M. P., & Ojha, A. (2014). Identifying critical infrastructure sectors and their dependencies : An Indian scenario. *International Journal of Critical Infrastructure Protection*, *7*(2), 71–85. https://doi.org/10.1016/j.ijcip.2014.04.003

NIST. (2013). Standards for Biometric Technologies. Retrieved July 21, 2019, from https://www.nist.gov/speech-testimony/standards-biometric-technologies

Nunno, R. M. (2000). Electronic Signatures : Technology Developments and Legislative Issues. *RterlyGovernment Information Qua*, *17*(4), 395–401.

O.Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). The use of focus group discussion methodology: Insights from two decades of application in conservation. *Methods in Ecology and Evolution*, *9*(1), 20–32. https://doi.org/10.1111/2041-210X.12860

OECD. (2018). *Case Study-Aadhaar*. Retrieved from https://www.oecd.org/gov/innovative-government/India-case-study-UAE-report-2018.pdf

Olson, E. (2015). Personal Identity. In *Stanford Encyclopedia of Philosophy*. Retrieved from https://plato.stanford.edu/entries/identity-personal/

P.Down, M., & J.Sands, R. (2004). Biometrics: An Overview of the Technology,Challenges and Control Considerations. *Information Systems Control Journal*, *4*(11–4).

Pagnin, E., & Mitrokotsa, A. (2017). Privacy-Preserving Biometric Authentication: Challenges and Directions. *Security and Communication Networks*, *2017*, 1–9. https://doi.org/10.1155/2017/7129505

Phillips, P. J., Flynn, P. J., & Bowyer, K. W. (2017). Lessons from collecting a million biometric samples. *Image and Vision Computing*, *58*(Supplement C), 96–107. https://doi.org/https://doi.org/10.1016/j.imavis.2016.08.004

Pluchinotta, I., Kazakçi, A. O., Giordano, R., & Tsoukiàs, A. (2019). Design Theory for Generating Alternatives in Public Decision Making Processes. *Group Decision and Negotiation*, *28*(2), 341–375. https://doi.org/10.1007/s10726-018-09610-5

Pruzansky, S. (1963). Pattern-Matching Procedure for Automatic Talker Recognition. *The Journal of the Acoustical Society of America*, *35*(3), 354–358. https://doi.org/10.1121/1.1918467

Rana, N. P., Barnard, D. J., Baabdullah, A. M. A., & Rees, D. (2019). International Journal of Information Management Exploring barriers of m-commerce adoption in SMEs in the UK : Developing a framework using ISM. *International Journal of Information Management*, *44*(June 2018), 141–153. https://doi.org/10.1016/j.ijinfomgt.2018.10.009

Rana, N. P., Dwivedi, Y. K., & Williams, M. D. (2013). Analysing challenges, barriers and CSF of egov adoption. *Transforming Government: People, Process and Policy*, *7*(2), 177–198. https://doi.org/10.1108/17506161311325350

Rezaei, J., Roekel, W. S. Van, & Tavasszy, L. (2018). Measuring the relative importance of the logistics performance index indicators using Best Worst Method. *Transport Policy*, *68*(March), 158–169. https://doi.org/10.1016/j.tranpol.2018.05.007

Ronald, A., Elizabeth, S. B., Noopur, S., & Neil, S. B. (2017). *State of aadhaar report 2016-17*.

Salimi, N., & Rezaei, J. (2018). Evaluating firms' R&D performance using best worst method. *Evaluation and Program Planning*, *66*(September 2017), 147–155. https://doi.org/10.1016/j.evalprogplan.2017.10.002

Segovia, A. I., Álvaro, D., & Enríquez, M. (2018). *Digital Identity : the current state of affairs*. *BBVA research*.

Seltsikas, P., & O'Keefe, R. M. (2010). Expectations and outcomes in electronic identity management: the role of trust and public value. *European Journal of Information*

Systems, *19*(1), 93–103. https://doi.org/10.1057/ejis.2009.51

Shah, M. H., Braganza, A., & Morabito, V. (2007). A survey of critical success factors in e-Banking: an organisational perspective. *European Journal of Information Systems*, *16*(4), 511–524. https://doi.org/10.1057/palgrave.ejis.3000693

Shankar, R., Gupta, R., & Pathak, D. K. (2018). Modeling critical success factors of traceability for food logistics. *Transportation Research Part E*, *119*(August 2017), 205–222. https://doi.org/10.1016/j.tre.2018.03.006

Sharma, R. S. (2016). UIDAI ' s Public Policy Innovations, (176), 1–19.

Shibin, K. T., Gunasekaran, A., & Dubey, R. (2017). Explaining sustainable supply chain performance using a total interpretive structural modeling approach. *Sustainable Production and Consumption*, *12*(July), 104–118. https://doi.org/10.1016/j.spc.2017.06.003

Shukla, M., & Mattar, L. (2019). Computers & Industrial Engineering Next generation smart sustainable auditing systems using Big Data Analytics : Understanding the interaction of critical barriers. *Computers & Industrial Engineering*, *128*(May 2018), 1015–1026. https://doi.org/10.1016/j.cie.2018.04.055

Simon, H. A. (1996). *The Sciences of the Artificial* (Third edit). London: MIT Press. Retrieved from https://monoskop.org/images/9/9c/Simon_Herbert_A_The_Sciences_of_the_Artificial_3rd_ed.pdf

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., & Furlong, M. (2007). Password sharing: implications for security design on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '07* (p. 895). New York, New York, USA: ACM Press. https://doi.org/10.1145/1240624.1240759

Sivamalai, L. (2013). Using the lens of "social construction of technology" to understand the design and implementation of aadhaar (UID) project. *IFIP Advances in Information and Communication Technology*, *402*, 633–638. https://doi.org/10.1007/978-3-642-38862-0_45

Spagnoletti, Paolo, Resca, A., & Lee, G. (2015). A design theory for digital platforms supporting online communities: a multiple case study. *Journal of Information Technology*, *30*(4), 364–380.

Sushil. (2012). Interpreting the interpretive structural model. *Global Journal of Flexible Systems Management*, *13*(2), 87–106. https://doi.org/10.1007/S40171-012-0008-3

Sushil, & Sushil. (2005). Interpretive Matrix: A Tool to Aid Interpretation of Management and Social Research. *Global Journal of Flexible Systems Management*, *6*(2), 27–30.

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, *89*, 201–218. https://doi.org/https://doi.org/10.1016/j.ssci.2016.06.015

Trauring, M. (1963). Automatic comparison of finger-ridge patterns. https://doi.org/10.1038/197938a0

Travis, A. (2010). ID cards scheme to be scrapped within 100 days. *The Guardian Weekly*. Retrieved from https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards

Triantaphyllou, E. (2013). *Multi-criteria Decision Making Methods: A Comparative Study* (Vol. 44). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4757-3157-6

UIDAI. (2009). *Biometrics Design Standards For UID Applications*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.189.2453&rep=rep1&type=pdf

UIDAI. (2010). UIDAI Strategy Overview Creating a Unique Identity Number for Every Resident in India, 1–45. Retrieved from http://eprints.cscsarchive.org/367/1/Strategy_Overveiw-001.pdf

UIDAI. (2019). Aadhaar Dashboard. Retrieved February 3, 2019, from https://uidai.gov.in/aadhaar_dashboard/

Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, *92*(6), 948–960. https://doi.org/10.1109/JPROC.2004.827372

UN. (2016). SDG. Retrieved February 8, 2019, from https://www.un.org/sustainabledevelopment/peace-justice/

UNGA. (2016). SDG. Retrieved from https://www.un.org/development/desa/disabilities/envision2030-goal16.html

Venkatanarayanan, A. (2018). Aadhaar enrolment costs. Retrieved July 4, 2019, from https://medium.com/karana/aadhaar-enrolment-costs-bc17f0d30018

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. *Information Systems Research*, *3*(1), 36–59. https://doi.org/10.1287/isre.3.1.36

Wan Ahmad, W. N. K., Rezaei, J., Sadaghiani, S., & Tavasszy, L. A. (2017). Evaluation of the external forces affecting the sustainability of oil and gas supply chain using Best Worst Method. *Journal of Cleaner Production*, *153*, 242–252. https://doi.org/https://doi.org/10.1016/j.jclepro.2017.03.166

Wang, D., Chen, C., & Richards, D. (2018). A prioritization-based analysis of local open government data portals : A case study of Chinese province-level governments. *Government Information Quarterly*, *35*(4), 644–656. https://doi.org/10.1016/j.giq.2018.10.006

Warfield, J. N. (1974). Developing Subsystem Matrices in Structural Modeling. *IEEE Transactions on Systems, Man and Cybernetics*, *SMC-4*(1), 74–80.

https://doi.org/10.1109/TSMC.1974.5408523

Whitley, E. A., Gal, U., & Kjaergaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems*, *23*(1), 17–35. https://doi.org/10.1057/ejis.2013.34

Wilkinson, S. (1998). Focus group methodology: a review. *International Journal of Social Research Methodology*, *1*(3), 181–203. https://doi.org/10.1080/13645579.1998.10846874

Zelazny, F. (2012). The Evolution of India ' s UID Program Lessons Learned and Implications for Other Developing Countries CGD Policy Paper 008, (August).