

INDAIN GOVERNMENT PERFORMANCE EVALUATON BY NATIONAL IDENTIFICATION SYSTEM

Dr. Neelu Jhala¹, Dr. Nisha Tanwar²

^{1,2}Assistant Professor, Faculty of Science, Bhupal Nobles' University, Udaipur, India.

ABSTRACT

In India, currently there are at least 18 documents that are recognized as acceptable proofs of identity. The range from the passport, the ration card, the voting card, each of these identities use as a specific function, and none act as one comprehensive national identifier. Identification is essential to the effective functioning of a Government polices, and for the movements of individuals in the formal structures of a country. State Governments use identification to assess populations for the delivery of services, and to monitor populations within its borders. Identification system provides governments with the ability to assess population. The expansive nature of identification technologies provides governments with the ability to gather, retain, combine, track and to share personal information easily. In recent years there has been an increase in privacy concerns surrounding identification schemes, as citizens worry that governments are reaching too deeply into their personal lives, and using identification for invasive purposes. In this paper we study about the security and process satisfaction of the users of the Unique identity of the Indians.

Keywords: Government, populations, Unique identity

1. INTRODUCTION

Government programs have their own database of beneficiaries that are not digitized.. Delivering public services efficiently and providing financial inclusion to the poor in partnership with the private sector depends on accurate identification and authentication of citizens and residents. Government programs must have the capacity to cross-reference databases and information[3,5].

Technological innovations have opened up new possibilities for governments to develop comprehensive identity management systems that link peoples' identities through their entire life from birth certificate driver's license, to marriage certificate, voter registration and aadhaar card.

Governments in developing countries are expected to carry out many of the same functions that richer countries are capable of performing; these functions include "providing universal access to healthcare and education, implementing know your customer (KYC) rules for financial institutions, and administering a wide variety of transfer programs." [1,4]

Table 1- National Identity Of Some Country In The World

Country	Official Name of National ID Program	Type of National ID Program	Mandatory Enrollment	Year of Launch	Status of Program
Bangladesh	National Identity Card (NID)	Government Issued National ID	Not specified	2007	Operational and in use/actively enrolling
China	Second Generation Resident Identity Card	Government Issued National ID	Yes	2003	Operational and in use
Egypt	National Identity Card (Current) Personal Verification Card	Government Issued National ID	Yes	Not specified	Operational and in use/actively enrolling
India	Aadhaar	Government Issued National ID	No	2008	Operational in and use/actively enrolling
Nepal	National Identity	Government Issued	No	2009	Planned

	Card (NID)	NationalID			
Sri Lanka	National Identity Card (NIC)/e-NIC	Government Issued National ID	Yes	2014	Operationaland in use
Thailand	National Identity Card/National ID Card/Smart ID Card	Government Issued National ID	Not specified	2005	Operationaland in use

Source: Giné, X. (n.d.). Use of biometric technology in developing countries. World Bank. Retrieved from

<http://siteresources.worldbank.org/DEC/Resources/Policy_paper-biometrics.pdf>

IDENTITY DOCUMENT POLICIES OF INDIA

When identity legislation is created without privacy in mind, it leads to allow unwarranted access by authorities to personally identifying information, it also permits the over collection of data and personal information to be used apart from the scope of identification without redressal mechanisms in place. Other privacy concerns related to identity include identity theft, impersonation, fraud, and inaccurate or incomplete information in the database[3,6,7].

With the increasing use of technology in government it is important to ensure that when e-government projects are implemented, they adopt integrated schemes to maintain privacy safeguards prior to collecting and using data[2]. The Indian government's growing practice in collecting, managing and retaining personal data without adequate privacy protection in place, pose a wide range of privacy concerns such as data mining, profiling, function creep, and inappropriate use of data.

In India, Unique Identification Authority of India (UIDAI) is responsible for provide Unique Identity Code to Indians. More than 95% of our residents already have 'Aadhaar'. Aadhaar is the most widely available, secure, and reliable form of personal identification in the country, and many other new uses of the infrastructure will be possible in the future[7].

2. OBJECTIVE

The present study is an attempt to evaluate performance of this National Identification System and possible additions and improvements to make it a single identity for all Indian throughout the country. The objective of this research paper is to find the access security satisfaction of the UID Users and to find the easiness and compliances of process and procedures standard for all UID users. We collect the data from 406 UID user I random manner. Initially the null hypothesis is assumed that the users are satisfied with the security and processor procedure of the UID.

3. DATA ANALYSIS

The figure of gathered responses of 406 users. t-test test is performed on the gathered data to test the hypothesis the proper test to inspect the hypothesis.

We collect the data about the security prospective of the UID by knowing that on one can access someone else's UID details without registered details.

Table 2: Security prospective of UID

Options	Frequency	Percent	CumulativePercent
Strongly Disagree	16	4.0	4.0
Disagree	26	6.4	10.4
Neutral	66	16.3	26.7
Agree	112	27.7	54.3
Strongly Agree	185	45.7	100.0
Total	405	100.0	

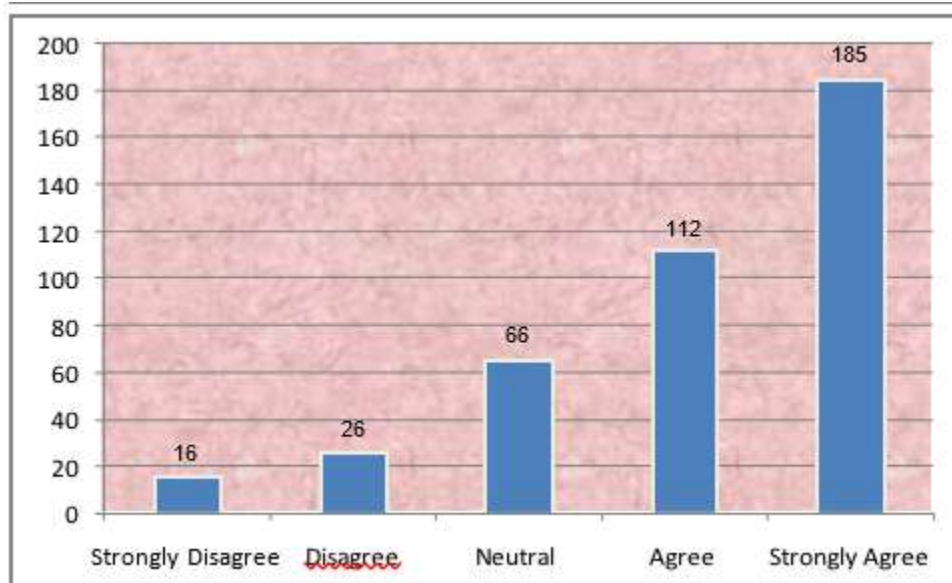


Fig. 1

Table 2 showing responses about **security** while accessing someone else's UID details.

Out of total 405, 16 respondents (4.0 percent) were strongly disagreed, another 26 respondents (6.4 percent) were disagreed, 66 respondents (16.3 percent) were neutral, 112 respondents (27.7 percent) were agreed and maximum 185 respondents (45.7 percent) were strongly agreed. It is clear that majority of people were agreed that they can't access someone else's UID details without registered details.

Secondly we collect the data about the process and procedures are standard for all UID users.

Table 3: Compliance about

Options	Frequency	Percent	CumulativePercent
Strongly Disagree	30	7.4	7.4
Disagree	23	5.7	13.1
Neutral	39	9.6	22.7
Agree	104	25.7	48.4
Strongly Agree	209	51.6	100.0
Total	405	100.0	

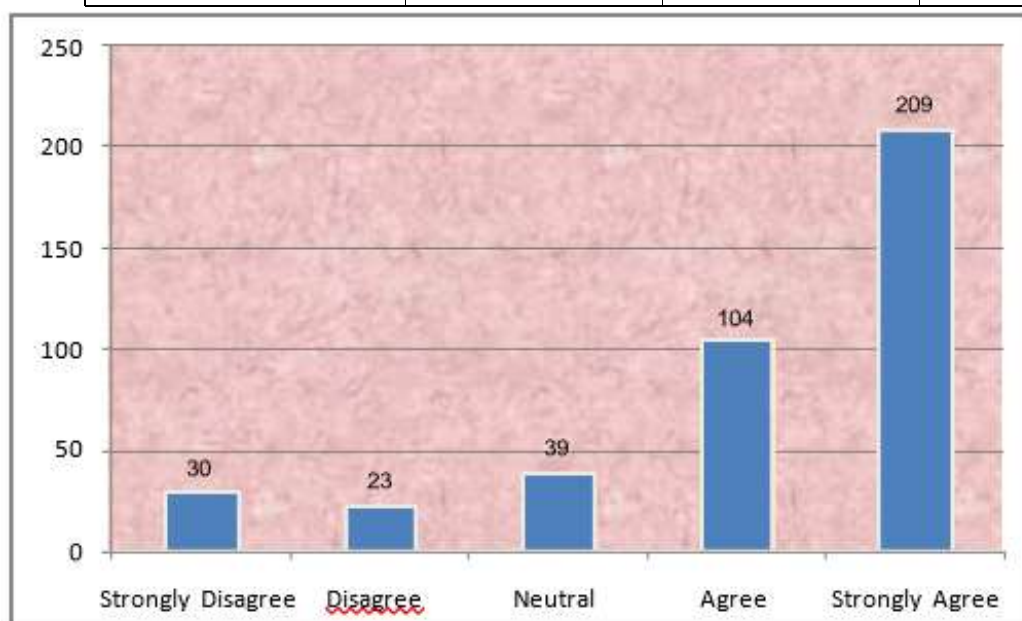


Fig. 2

Out of total 405, 30 respondents (7.4 percent) were strongly disagreed, 23 respondents (5.7 percent) were disagreed, 39 respondents (9.6 percent) were neutral, 104 respondents (25.7 percent) were agreed and maximum 209 respondents (51.6 percent) were strongly agreed. It is clear that majority of people were agreed that process and procedures are standard for all UID users.

Table 4: One Sample Test (Performance of National Identification System)

	t	df	Sig. (2-tailed)	Result
(i) satisfaction for security of Aadhaar information	16.311	404	.614	H ₀ accepted
(ii) process and procedure are standard for uses of UID	10.513	404	.934	H ₀ accepted

Table 4 shows that for all three questions, significance value remained higher than 0.05 (5% level of significance) for each i.e., $p > 0.05$ and **null hypothesis H₀ is accepted** for (i) and (ii). Hence, it is concluded that there is no significant difference according to satisfaction level of various demographic categories in performance of the National Identification System.

Conclusion

From this analysis, it is clear that although there is some unsatisfaction between a fraction of population but overall, according to majority of population, the National Identification System is performing as expected. This satisfaction level of the user increases the success of the Indian government's different policies in the development of the state and nation. A successful UID system makes a good governance.

4. REFERENCES

- [1] Ankita Rajpoot, Ved Prakash Kumar, Kusum Arunachalam and Sargam Singh Rasaily (2021), National bird, Indian peafowl (*Pavo cristatus*): Using DNA technology for species identification from degraded sample from Uttarakhand, India, *Forensic Science International: Animals and Environments*, Vol.1, November 2021, 100004.
- [2] Evan Marcus and Hal Stern (2019): Blueprints for High Availability: Designing Resilient Distributed Systems, John Wiley & Sons, ISBN0-471-35601-8.
- [3] Helena Machado, Rafaela Granja and António Amorim (2022), Ethical challenges of merging criminal identification and civil identification within the Prüm system, *Forensic Science International: Genetics*, Vol.57, March 2022, 102660.
- [4] Leonid B. Sokolinsky (2021), BSF: A parallel computation model for scalability estimation of iterative numerical algorithms on cluster computing systems, *Journal of Parallel and Distributed Computing*, Vol. 149, March 2021, 193-206.
- [5] Pradeep Javangula, Kourosh Modarre, Paresh Shenoy, Yi Liu and Aran Nayebi (2017), Efficient Hybrid Algorithms for Computing Clusters Overlap, *Procedia Computer Science*, Vol. 108, 2017, 1050-1059.
- [6] Ramaswamy, Parameshwari (September 2011). "Understanding the UID Aadhaar project and IT's role in its success", *Computer Weekly*, retrieved 24 April 2016.
- [7] Sridhar Raj S., Munaga V.N.K. Prasad and Ramadoss Balakrishnan (2022), Spatio-Temporal association rule based deep annotation-free clustering (STAR-DAC) for unsupervised person re-identification, *Pattern Recognition*, Vol.122, February 2022, 108287.