A STUDY OF SECURITY, PRIVACY AND ACCEPTABILITY ASPECT OF AADHAAR

A Dissertation Submitted to Panjab University, Chandigarh for Award of Master of Philosophy in Social Sciences

Submitted by:

ASHOK KUMAR

Roll No-4415

Under the Supervision of

Dr. SURABHI PANDEY

INDIAN INSTITUTE OF PUBLIC ADMINISTRATION

NEW DELHI

2018-19

CERTIFICATE

I have pleasure to certify that the dissertation titled "A Study of Security, Privacy and Acceptability aspect of Aadhaar" is a bonafide research work carried out by Ashok Kumar under my guidance and supervision in IIPA. This dissertation is the result of his own research and to the best of my knowledge this has not been copied from any other research, dissertation or book.

This is being submitted to the Indian Institute of Public administration (IIPA), New Delhi for Master's Diploma in Public Administration in partial fulfilment of the requirement for the Advanced Professional Programme in Public Administration (APPPA) of the IIPA, New Delhi.

I recommend that the dissertation of Shri Ashok Kumar is worthy of consideration for the award of M.Phil degree of the Panjab University, Chandigarh.

(Dr Surabhi Pandey)

Supervisor

Indian Institute of Public Administration (IIPA)

I.P. State, Ring Road, New Delhi-1100012

ACKNOWLEDGEMENT

I express my sincere gratitude to my guide Dr Surabhi Pandey, who had extended her constant and invaluable support throughout my project. She had provided her assiduous continual contribution and supervision in all domain of the project since beginning. Without her guidance and encouragement, it would not have been possible to complete the dissertation with quality in such a limited time.

I am also thankful to my colleagues who shared their valuable thoughts regarding the multi aspect of Aadhaar's use and misuse. I also acknowledge the support of my colleagues and friends of 44th APPPA batch.

I express my thanks to UIDAI team at Headquarter New Delhi and its Regional offices and its Data center at Manesar who had extended their support to get the questionnaire feedback. I appreciate the cooperation extended by the officers of UIDAI who have provided necessary data and other relevant information.

I would like to acknowledge the contribution of officials from BSNL, MTNL, DoT, DTU and all the individuals who have helped me to complete the questionnaire which helped me to get primary data.

The staff of the APPPA office and the IIPA library deserve the special mention for their helping attitude. Lastly, I am also thankful to my family members who had cooperated all along while doing this course and completing the project.

Ashok Kumar

February 2019

PREFACE

The UIDAI is to issue unique Aadhaar number to all Indian residents to eliminate duplicate and fake identities which can be verified and authenticated in an easy, cost-effective way. It would not just help the government way down individuals but also make life extreme easier for citizens as they don't have need to submit multiple documents every time when they want a new. In Aadhaar Bill 2016, Aadhaar card was made mandatory for authentication purposes for many such Government scheme. In view of these, on the one side, Aadhaar is getting more popular and enrolment has crossed 1.22 billion as of July 2018 and is becoming the government's base for public welfare and citizen services scheme. However, on the other side, Media has been reporting the issues wrt privacy & security of Aadhaar data like leaking of data, misuse of data, deletion of data etc. Security and so Privacy concerns relating to the Aadhaar project has been the subject of much heated debate in recent past.

Therefore, it there is a need to study about the Aadhaar system in order to understand whether there is really some issue of Privacy & Security of Aadhaar or it is only a myth due to lack of awareness about the Aadhaar system. Accordingly a detail study has been conducted with the objectives a) to study a broad architecture and security systems network and datacenters of UIDAI in reference to security aspect of system; b) to study the access mode and methodology of UIDAI systems; c) to study about the issues related to data protection and Privacy of Aadhaar data; and d) to assess the awareness among public regarding Aadhaar system and issues related to Privacy & security in order to assess the overall acceptability among public.

The entire technology architecture behind Aadhaar is based on principles of openness, linear scalability, strong security, and most importantly vendor neutrality. The architecture has been structured to ensure clear data verification, authentication and deduplication, while ensuring a

high level of privacy and information security. Key technology components like 'Central ID Data Repository (CIDR)' for storing residents data, 'UID Servers' for enrolment and the authentication service, 'Biometric Sub-System' for enrolling as well as authenticating residents, 'Enrolment Client' to captures and validate demographic and biometric data, 'Network' to make all UID enrolment and authentication services online and 'Security Systems' to secures UIDAI systems from logical/physical attack. Authentication & E-KYC Services includes an online authentication platform to authorized institutions to validate identity of Aadhaar holders. Presently UIDAI offers two services through its online authentication platform namely a) Authentication and b) e-KYC. While "Authentication" service returns only a *Yes* or a *No* in response to an authentication attempt, e-KYC service returns entire demographic data including the address and photograph of the resident in case of successful match. However, it may be noted that no biometric data is returned under any circumstance. Authentication APIs are protected by a robust security framework consisting of encryption, digital signature, access control and audits to protect any unauthorized access or usage of authentication services.

This research is based on the study and analysis of the various secondary inputs available from different sources and discussion/ interview were conducted from UIDAI officials and experts of IT & Telecom Industry to understand the issues of security and Privacy. Accordingly, the qualitative approach of study has been adopted during research for assessing different issues related to security and Privacy of Aadhaar data. Further, in order to understand the opinion of public in respect of Aadhaar system vis-à-vis the issues of security and privacy of Aadhaar data, a Quantitative Approach of study was considered by taking survey from a diverse group with a sample size of 400 respondents.

It is found that the Aadhaar datacenter sites are of International Standards with proper security system. The CIDR database is not accessible from outside of Aadhaar network so it is secure from any cyber threats. Aadhaar data is encrypted using PKI-2048 and AES-256. The data are being collected on software provided by the UIDAI and encrypted to prevent leaks in transit. UIDAI follows the principle of privacy i.e. collection of limited personal information, no profiling and tracking information, release of information in the form of 'yes' or 'no' response and there is no convergence and linking of UIDAI information to other databases.

It is concluded from study that the data is always secured/encrypted i.e., at rest, in transit and in storage. There may not be issue of security and privacy on Aadhaar and there is no any issue in acceptability of Aadhaar also. However, due to lack of awareness about the Aadhaar systems, Principle and process adopted by UIDAI etc., people have some concerns.

Therefore, UIDAI needs to educate and inform to residents that Aadhaar system is fully safe & secure and UIDAI does not collect sensitive personal information such as religion, caste, community, income, health, financial details etc. UIDAI never does profiling and tracking of individuals. Open house session may be conducted to create awareness among the public regarding Aadhaar system. As security is a dynamic concept in rapidly changing internet domain, in addition to action for awareness, a "comprehensive Security Policy" covering all dimensions need to be implemented and reviewed at regular in defined interval.

ABBREVIATION

ABIS	Automated Biometric Identification System
ABPS	Aadhaar Payment Bridge System
AEA	Aadhaar Enabled Account
ANPP	Australia National Privacy Principles
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interfaces
ASA	Aadhaar Service Agency
AUA	Aadhaar User Agency
BPL	Below Poverty Line
BSNL	Bharat Sanchar Nigam Limited
CCTV	Closed-Circuit Television
CIDR	Central Identities Data Repository
CISF	Central Industrial Security Force
CSC	Common Service Centers
DBT	Direct Benefit Transfer
DCP	Deputy Commissioner of Police
DDSVP	Demographic Data Standards And. Verification Procedure.
DeITY	Department of Electronics and Information Technology

DOT	Department of Telecommunications
EPF	Employee Provident Fund
EU	European Union
FACTA	Foreign Tax Compliance Act
FIR	First Information Report
FTE	Failure to Enrol
GOI	Government of India
HAC	Message Authentication Cod
HMAC	Hash Based Message Authentication Code
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
ISO	International Organization for Standardization
IT	Information Technology
KSK	e-KYC Service Agency
KUA	e-KYC User Agency
KYC	Know Your Customers
MGNREGA	Mahatma Gandhi National Rural Employment Guarantee
MOU	Memorandum of Understanding
NCR	National Capital Region

NIC	Network Information Center
NPR	National Population Register
NSN	Nokia Siemens Networks
OECD	Organisation for Economic Co-Operation and Development
OTP	One Time Passwords
PAN	Permanent Account Number
PDS	Public Distribution System
PII	Personal Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act
PKI	Public Key Infrastructure
PMJDY	Prandhan Mantri Jan Dhan Yojana
PoA	Proof of Address
PoC	Proof of Concept
POI	Proof of Identity
SDK	Software Development Kit
SMS	Short Message Service
SRO	Self-Regulatory Organization
SSN	Social Security Number
STQC	Standardisation Testing and Quality Certification

TCS	Tata Consultancy Services
TEC	Telecommunication Engineering Center
TOTP	One-Time Temporary Password
TPDS	Targeted Public Distribution System
TRAI	Telecom Regulatory Authority of India
UID	Unique Identification Number
UIDAI	Unique Identification Authority of India
VID	Virtual ID
WAN	Wide Area Network

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES / GRAPHS

LIST OF ANNEXURES

CHAPTER 1

INTRODUCTION: AN OVERVIEW OF AADHAAR PROJECT AND BACKGROUND OF STUDY

1.1 An overview of UIDAI

Based on the recommendations of the Kargil Review Committee[1] regarding issue of "Multi-purpose National Identity" cards to villagers living in conflict zones, the concept of Aadhaar for all citizen was developed. The main motive to cover all citizen was to ensure the welfare of citizens by single identification document. The *Unique Identification Authority of India* (UIDAI) was constituted on 28 January 2009 for this purpose, as an attached office to the Planning Commission. The purpose of the UIDAI is to issue a unique identification number (UID) to all Indian residents that is

(a) robust enough to eliminate duplicate and fake identities, and

(b) can be verified and authenticated in an easy, cost-effective way.

Features of the UIDAI model[2] (UIDAI, 2010)

1.1.1 **The Unique Identification (UID) number is only identity:** The UIDAI's purview is limited to the issue of unique identification numbers linked to a person's demographic and biometric information. It only guarantees identity, not rights, benefits or entitlements.

1.1.2 **The UID proves identity, not citizenship:** All residents in the country can be issued a unique ID. The UID is proof of identity and does not confer citizenship.

1.1.3 **A pro-poor approach:** The UIDAI envisions full enrolment of residents, with a focus on enrolling all India's poor and underprivileged communities as well. The UID method of authentication also improve service delivery for the poor.

1.1.4 **Enrolment of residents with proper verification:** Existing identity databases in India are fraught with problems of fraud and duplicate/ghost beneficiaries. To prevent this from seeping into the UIDAI database, the UIDAI plans to enrol residents into its database with proper verification of their demographic and biometric information. This ensures that the data collected is clean from the start of the program.

However, much of the poor and underserved population lack identity documents and the UID may be the first form of identification they have access to. The UIDAI ensures that the Know Your Resident (KYR) standards don't become a barrier for enrolling the poor, and devised suitable procedures to ensure their inclusion without compromising the integrity of the data.

1.1.5 **A partnership model:** The UIDAI approach leverages the existing infrastructure of government and private agencies across India. The UIDAI is a regulatory authority managing a Central Identities Data Repository (CIDR), to issue UIDs, update resident information, and authenticate the identity of residents as required.

In addition, the UIDAI is partner with agencies such as central and state departments and private sector agencies who are 'Registrars' for the UIDAI. Registrars process UID applications and connect to the CIDR to de-duplicate resident information and receive UID numbers. These Registrars can either be enrollers, or appoint agencies as enrollers, who interface with people seeking UID numbers. The Authority has also become partner with service providers for authentication.

1.1.6 **Enrolment is not mandated:** The UIDAI approach is a demand-driven one, where the benefits and services that are linked to the UID ensured demand for the number. This will not however, preclude governments or Registrars from mandating enrolment.

1.1.7 **The UIDAI assign a number:** The UIDAI's role is limited to issuing the number. This number may be printed on the document/card that is issued by the Registrar.

1.1.8 **The number does not contain intelligence:** Loading intelligence into identity numbers makes them susceptible to fraud and theft. The UID is a random number.

1.1.9 **The UIDAI only collect basic information on the resident:** The UIDAI seek the following demographic and biometric information in order to issue a UID number:

- Name
- Date of birth/Age
- Gender
- Father's/Husband's/ Guardian's name and UID number (optional for adult residents)
- Mother's/ Wife's/ Guardian's name and UID number (optional for adult residents)
- Introducer's name and UID number (in case of lack of documents)
- Address
- All ten fingerprints, photograph and both iris scans

1.1.10 **Process to ensure no duplicates:** Registrars send the applicant's data to the CIDR for deduplication. The CIDR performs a search on key demographic fields and on the biometrics for each new enrolment, to ensure that no duplicates exist. The enrolment quality checking filters to ensure uniqueness are given as below in figure 1.1.

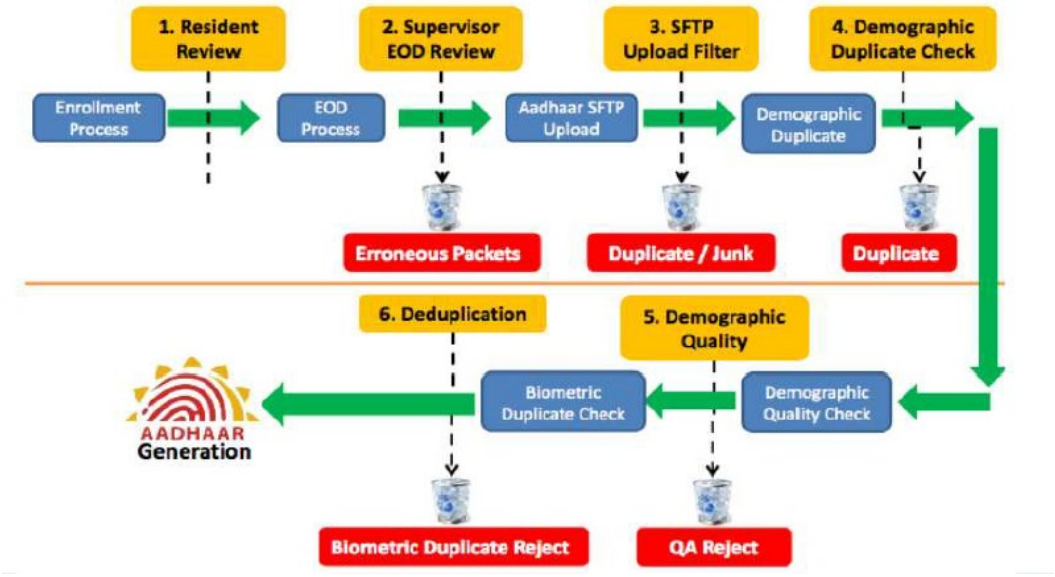


Figure-1.1: Enrolment Quality Check [1]

The incentives in the UID system are aligned towards a self-cleaning mechanism. The existing patchwork of multiple databases in India gives individuals the incentive to provide different personal information to different agencies. Since de-duplication in the UID system ensures that residents have only one chance to be in the database, most of individuals provide accurate data. This incentive become especially powerful as benefits and entitlements are linked to the UID.

1.1.11 **Online authentication:** The UIDAI offers a strong form of online authentication, where agencies can compare demographic and biometric information of the resident with the record stored in the central database. The Authority supports Registrars and agencies in adopting the UID authentication process and defines the infrastructure and processes they need.

[1] A presentation by a Technical expert of UIDAI, http://trai.gov.in/sites/default/files /presentations _&_cv/Day-3_25Aug2017/Session2_Digital%20world/Digital%20Identifiers_Ashok%20Kumar.pdf ,Date accessed: 10.02.2019

1.1.12 **The UIDAI does not share resident data:** The UIDAI envisions a balance between 'privacy and purpose' when it comes to the information it collects on residents. The agencies may store the information of residents they enrol if they are authorized to do so, but they do not have access to the information in the UID database. The UIDAI answers requests to authenticate identity only through a 'Yes' or 'No' response or e-KYC.

1.2 Technology overview of Aadhaar System[2]

1.2.1 Technology Architecture

The entire technology architecture behind Aadhaar is based on principles of openness, linear scalability, strong security, and most importantly vendor neutrality. The architecture has been structured to ensure clear data verification, authentication and deduplication, while ensuring a high level of privacy and information security. The technology followed the basic three features of Open architecture, scalability and security.

a) **Open architecture** – Building the Aadhaar system with true openness meant that they relied on open standards to ensure interoperability; the platform approach with open APIs made it possible for the ecosystem to build on top of Aadhaar APIs; vendor neutrality was ensured across the application components by using open and standard interfaces. The identity system was designed to work with any device, any form factor, and on any network.

b) **Design for scale**: The Aadhaar system has been designed to issue UIDs to all residents i.e. with initials for more than 1.3 billion identities and which will continue to grow as the resident population expands. Since every new enrollment requires biometric de-duplication across the entire system, every component needs to scale to very large volumes. This meant that the system needed to be able to handle hundreds of millions of transactions across

billions of records doing hundreds of trillions of biometric matches every day. In addition, all online services such as Aadhaar authentication, e-KYC services, and update services must work with high availability and sub-second performance. In order to achieve such massive scalability, the program established network and datacenter load balancing and a multi-location distributed architecture for horizontal scale.

c) **Data Security** – The security and privacy of one's data is a foundation of the Aadhaar system. The system uses 2048-bit PKI encryption and tamper detection using HMAC (is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key) in order to ensure that no one can decrypt and misuse the data. Resident data and raw biometrics are always kept encrypted, even within UIDAI data centers. In addition, the system does not keep track of any transactional data.

1.2.2 Key Technology Components

a) **CIDR**: The Central ID Data Repository is central database of all residents, containing the minimal set of fields sufficient to confirm identity. The federated set of databases belonging to the Registrars may contain additional information about the resident, and can use the resident's UID as the key.

b) **UID Servers**: This provides the enrolment and the authentication service. These services are available over the network for the various Registrars and their authenticating agencies to use. The backend servers need to be architected for the high demands of the 1:N biometric de-duplication as well as the large peak loads from authentication requests.

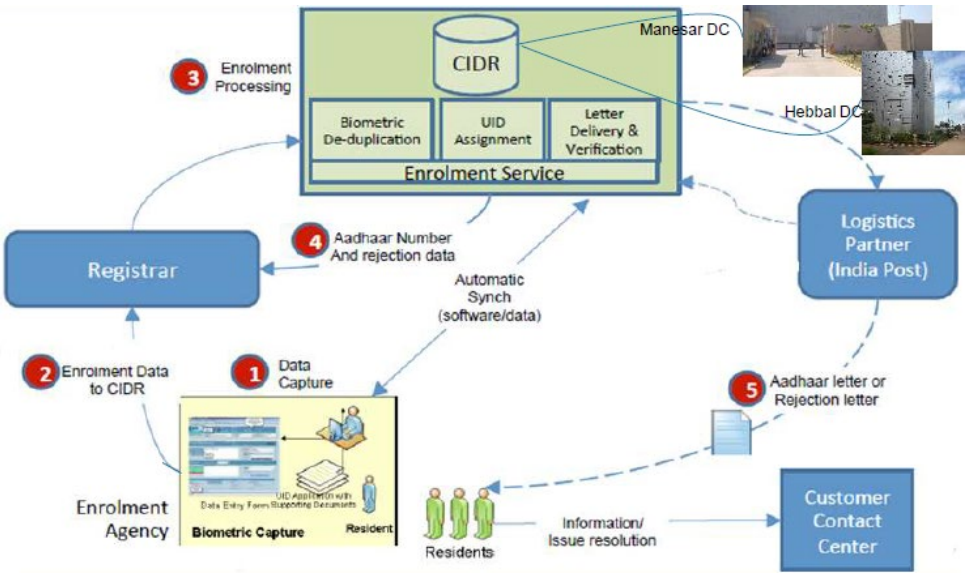


Figure-1.2: Aadhaar Enrolment Ecosystem [1]

c) **The Biometric sub-system:** It is central to the UID system for enrolling as well as authenticating residents. A multi-modal biometric solution is being used to achieve a high level of assurance. Innovative techniques of hashing, indexing, distributed processing, and in-memory databases using multiple-biometric modes has been employed to get acceptable performance.

d) **The Enrolment client:** It captures and validate demographic and biometric data. This client needs to work in an offline mode in the village setting when there is no internet connectivity, and upload batch files to the server for processing. Alternatively, the batch files can be physically transported to the CIDR for uploading. The client application need to be deployed on a standard enrolment workstation.

[1] A presentation by a Technical expert of UIDAI, http://trai.gov.in/sites/default/files /presentations _&_cv/Day-3_25Aug2017/Session2_Digital %20world/Digital%20Identifiers_Ashok%20Kumar.pdf , Date accessed: 10.02.2019

e) **The Network:** It is a critical aspect of the system, since all UID enrolment and authentication services are available online. UID services work over secure WAN networks, the vanilla internet or over wireless network.

f) **The Security design:** It secures all the above components from logical/physical attack. This includes.

- Server Security – firewall, intrusion prevention and detection systems (IPS, IDS)
- Network, Client Security – Encryption, PKI etc

g) **The Administration system** help administer the UIDAI's operations. This includes

- Account setup – creation/modification of Registrar, enrolling and authenticating agency accounts.
- Role based access control – Assign rights over UID resources based on role.
- Audit trailing – track every access to the UID system.
- Fraud detection – detect identity theft and cyber crimes using audit trails
- Reporting and Analytics – Visual decision support tools, Charting etc.

1.3 An overview of Authentication & E-KYC Services[2]

UIDAI offers an online authentication platform to authorized institutions to validate identity of Aadhaar holders. Presently two types of authentication services are offered by UIDAI namely *Authentication* and *E-KYC* which may be leveraged in the context of service delivery or other use cases. During the authentication process, the agency collects the Aadhaar number, along with other identity attributes (possibly including biometrics) and sends it to the CIDR for verification. The UIDAI responds with a Yes or No in the case of *Authentication* and entire demographic data

including address & photograph in the case of *E-KYC*, thus authenticating the identity of the individual.

Effectiveness of an authentication services lie in answering the following three questions:

a) **What you have**: Something the user uniquely has (e.g., a card, security token, mobile phone, tablet/laptop computer accessing email, etc.).

b) **What you know**: Something the user knows that is not public (e.g., a password, PIN, secret question, etc.). Demographic details such as date of birth may also be classified in this category although they are generally considered weak factors.

c) **Who you are**: Something the user individually is or does (e.g., fingerprint pattern, iris pattern, signature, handwriting, etc.). As explained in subsequent sections, Aadhaar authentication platform offers multiple modalities of authentication to answer the above questions for varying effectiveness.

1.3.1 Modalities of Authentication Services

Presently, UIDAI's authentication permits use of three modalities namely *demographic data*, *biometrics* & *OTP (One Time Password sent to registered mobile phone)* and combinations of the three for varying degrees of effectiveness. The diagram here depicts various modalities of authentication platform. Effectiveness of authentication can be ascertained with the number of modalities used in the process. As an example, an authentication performed with modalities viz. demographic data and biometrics will be more secure and fraud-resistant than a transaction performed with only demographic data as the modality. Similarly, an authentication performed with all modalities used together will be more secure than a transaction with up to two modalities. Among, the modalities, it can be appreciated that all transactions requiring biometric

modality are more secure than those not using it. This is primarily because biometric authentication requires presence of the Aadhaar holder and that it cannot be easily faked. Types of modalities are explained below:

- Demographic Authentication: In the case of demographic authentication, one or more demographic fields including address along with Aadhaar number are submitted to CIDR for authentication.
- Biometric Authentication: Biometric authentication requires submission of one or more fingerprint and iris biometric attributes along with Aadhaar number to CIDR for authentication
- OTP Authentication: Mobile number provided at the time of enrolment or during last data update becomes concerned Aadhaar holder's registered mobile number whereby the Aadhaar holder is presumed to be the owner of that mobile number. As part of OTP authentication, a one-time password is sent to the registered mobile of the resident undergoing authentication which is then fed back to complete the authentication process.
- Combination of Modalities: Authentications may be carried with combinations of the above three types of authentications for better effectiveness.

Figure 1.3: Authentication Services [1]

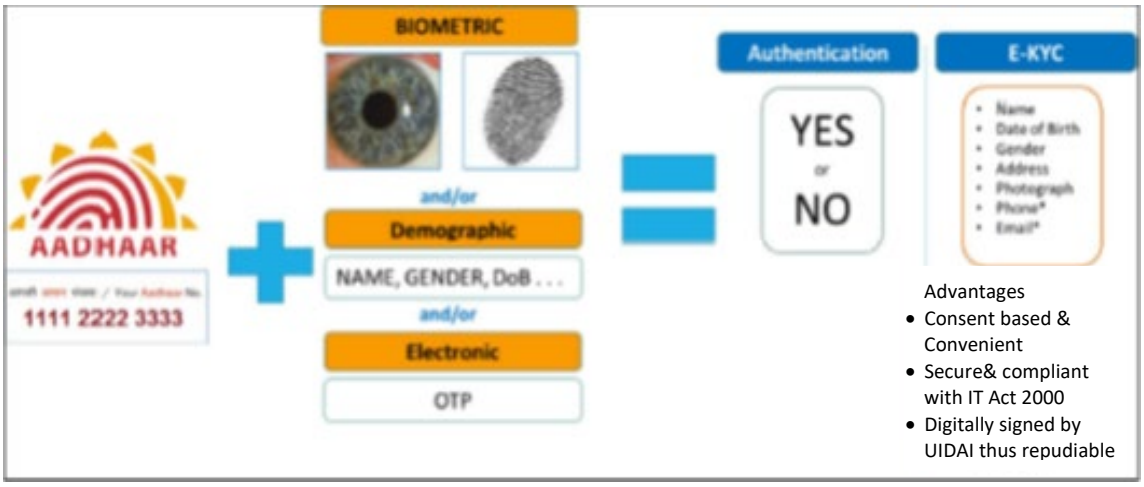
1.3.2 **Federated Authentication Model**

Aadhaar being voluntary in nature, UIDAI recommends federated authentication models whereby Aadhaar authentication is used only to strengthen existing authentication systems of the user agencies. UIDAI also views existing authentication systems to be more specific to the industry domain in which they are used therefore Aadhaar authentication which is global & generic in nature should only be used to strengthen existing authentication systems. Nonetheless, it is the prerogative of the user agency to either use Aadhaar authentication in federated model or standalone.

[1] UIDAI Strategy Overview, UIDAI HQ, New Delhi (2010)

1.3.3 **Authentication Services**

UIDAI offers two services through its online authentication platform namely a) Authentication and b) e-KYC. While "Authentication" service returns only a *Yes* or a *No* in response to an authentication attempt, e-KYC service returns entire demographic data including the address and photograph of the resident in case of successful match. However, it may be noted that no biometric data is returned under any circumstance. The schematic diagram below explains the two authentication services:



Figures 1.4: Aadhaar Authentication & e-KYC Services [1]

1.3.4 **Authentication Ecosystem**

Authentication ecosystem consists of UIDAI and its partner organizations comprising a) AUAs & KUAs are service providers or government entities who leverage Aadhaar authentication as part of their service delivery and b) ASAs & KSAs who provide AUAs & KUAs secure network connectivity to UIDAI's CIDR.

AUA: Aadhaar User Agency

ASA: Aadhaar Service Agency

[1] UIDAI Strategy Overview, UIDAI HQ, New Delhi (2010)

KUA: e-KYC User Agency

KSA: e-KYC Service Agency

UIDAI onboards each of the ecosystem partners through a detailed due-diligence and approval process in order to ensure that only qualified public & private sector entities are allowed access to authentication services and that there is a genuine need of the service. Terms of usage of platform are agreed through a Memorandum of Understanding which forms the basis of all the activities performed as part of the engagement. During the entire course of engagement, UIDAI holds the authority to discontinue access to any of the ecosystem partners if an evidence of inappropriate usage is detected or reported thus ensuring security of residents' data stored in CIDR.

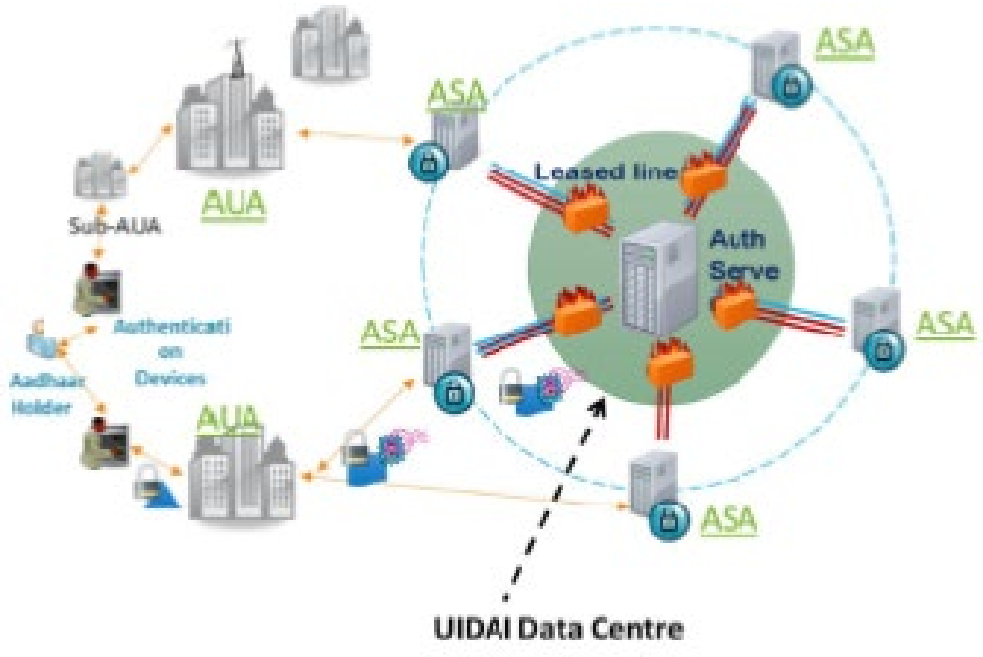


Figure 1.5: Aadhaar Authentication Ecosystem [1]

[1] UIDAI Strategy Overview, UIDAI HQ, New Delhi (2010)

1.3.5 **Authentication Infrastructure**

Keeping in view security of residents' data and high volume of transactions owing to huge population of the country, UIDAI has deployed a highly robust, secure and scalable authentication infrastructure. The infrastructure is designed to meet the following expectations:

- Multi datacenter for high availability and reliability even in the event of an outage at one datacenter

- Sub-second response to avoid introduction of unnecessary delays in applications leveraging Aadhaar authentication

- Fully load balanced to address the need of scalability and speed

- Linear scalability architecture through simple expansion of server farm for achieving higher scalability

- Support for 100 million transactions per day.

- Maintenance of detailed audit trail for future references

1.4 An Overview of Information Privacy & Security[2]

Aadhaar authentication services are architected in such a way that without residents' awareness and explicit consent authentication cannot be carried out. This is to ensure that no AUA or KUA misuses resident data for undue benefits. As per the terms of usage agreed with UIDAI through Memorandum of Understanding, each AUA & KUA is mandated to capture a physical consent of Aadhaar holders in the service delivery application or on paper before conducting authentication.

Apart from the above safeguard, authentication APIs are protected by a robust security framework consisting of encryption, digital signature, access control and audits to protect any unauthorized access or usage of authentication services. All the aspects are explained below:

1.4.1 **Personal Identifiable Information (PII)**: PII refers to data which can be used to uniquely identify a single individual. From the data collected by the UIDAI the following is classified in this manner:

Aadhaar Number- Unique 12 digit number issued to residents

Demographic data- All demographic data including address except Gender, Age & Year of Birth and components of address unless they are not combined with other PII fields

Biometric data- All biometric records are considered PII

Enrolment Records- Resident data including the biometrics

Data Change Records- Resident data. May include biometrics too

Authentication Records- Aadhaar number and one or more PII data While the demographic data that the UIDAI collects is already available with several agencies in the country – some of it is also available to the public (E.g., electoral rolls, railway reservation charts, telephone directories, etc.) - it is recognized as sensitive data within Aadhaar system and handled with due care. Similarly, the authentication records are designed to be sensitive to resident privacy concerns.

1.4.2 **Access Control**: Authentication services are accessible to the ecosystem partners only through APIs (Application Programming Interfaces) available over private leased lines which prevents direct access to any of the application servers or database servers.

Additionally, access to the APIs is available only to white-listed IP addresses of ecosystem partners which prevents any unauthorized access.

It may also be noted that the access given to ecosystem partners is time bound which is ensured through use of randomly generated license keys. All communications of ecosystem partners with UIDAI requires sharing of license key which has a limited validity. At the end of validity of license keys, the keys are renewed subject to validity and good standing of terms stated in Memorandum of Understanding.

1.4.3 **Encryption:** All the communication between AUA/ KUA applications and CIDR remains in encrypted form unless the authorized entity, whether UIDAI or ASA/KUA, decrypts the information. As per the design of Authentication service, all PII including demographic information and biometric data are encrypted with a randomly generated session key using AES-256 symmetric algorithm (AES/ECB/PKCS7Padding) after which the key itself is encrypted using 2048bit UIDAI public key using asymmetric algorithm (RSA/ECB/PKCS1 Padding). Such a design ensures that the resident data while in transit remains encrypted and cannot be viewed by a hacker or any unauthorized entity watching the data traffic.

1.4.4 **Digital Signature**: Design of authentication service mandates use of digital signature to sign every data packet when exchanged between the ecosystem partners. Such an arrangement ensures integrity of data packets and non-repudiation. Presently, UIDAI allows use of Class II and III digital signatures for the purpose issued by Certifying Authorities authorized by Controller of Certifying Authorities, Govt. of India, under IT Act.

1.4.5 **Audit Trails**: All authentication transactions performed by AUAs & KUAs are logged in CIDR for future reference, say in case of inquiries or disputes. Nonetheless, logged information is agnostic of the business process or the context of authentication. Such a safeguard has been built into the system to prevent all possibilities of snooping and profiling of Aadhaar holders. It may be deduced that the logged information is used only for resolution of technical issues which may be reported from the field either by ecosystem partners or Aadhaar holders.

1.4.6 **Data Retention & Usage**: Following table defines the period for which each type of data will be stored by UIDAI.

Table 1.1: Data Retention Policy[1]

Data Type	**Retention Period**
Aadhaar Number	Forever
Current Demographic data	Forever
Current Biometric Data	Forever
Enrolment Record and archived data update Records	Forever in archived form
Authentication Records	6 months in active audit and up to 7 years in archived storage
Transactions Aggregated records (no PII)	Forever
Master Data	Forever

UIDAI ensures through its strict security procedures that no PII data ever leaves the CIDR, except through an approved process, or with explicit resident consent.

[1] UIDAI Strategy Overview, UIDAI HQ, New Delhi (2010)

1.5 National Privacy Principles for Privacy Bill[3]

A Group of Experts was constituted under the chairpersonship of Justice A P Shah to identify key privacy issues and prepare a paper to facilitate in the formulation of Privacy bill while keeping in view the international landscape of privacy laws, global data flows and predominant privacy concerns with rapid technological advancements. Different geographies across the globe have defined their privacy requirements, articulating the requirements for the protection of the personal data and prevent harm to an individual whose data is at stake. The group of expert has gone through the privacy requirements as articulated by the OECD Privacy Guidelines, EU Data Protection Directives, APEC Privacy Framework, Canada PIPEDA (Personal Information Protection and Electronic Documents Act), and Australia ANPP (Australia National Privacy Principles). Privacy Principles such as Notice, Consent, Collection Limitation, Use Limitation, Access and Corrections, Security/Safeguards, and Openness cut across all these frameworks. The summary of recommendations of Justice Shah committee for the National Privacy Principles are as below-

1.5.1 **Principle 1: Notice**

A data controller shall give simple to understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them. Such notices should include:

a) During Collection

- What personal information is being collected;
- Purposes for which personal information is being collected;
- Uses of collected personal information;

- Whether or not personal information may be disclosed to third persons;
- Security safeguards established by the data controller in relation to the personal information;
- Processes available to data subjects to access and correct their own personal information;
- Contact details of the privacy officers and SRO ombudsmen for filing complaints.

b) Other Notices

- Data breaches must be notified to affected individuals and the commissioner when applicable.
- Individuals must be notified of any legal access to their personal information after the purposes of the access have been met.
- Individuals must be notified of changes in the data controller's privacy policy.
- Any other information deemed necessary by the appropriate authority in the interest of the privacy of data subjects.

1.5.2 **Principle 2: Choice and Consent**

A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information and take individual consent only after providing notice of its information practices. Only after consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in the case of authorized agencies. When provision of information is mandated by law, it should be in compliance with all other National Privacy Principles. Information collected on a mandatory basis should be anonymized within a

reasonable timeframe if published in public databases. As long as the additional transactions are performed within the purpose limitation, fresh consent will not be required.

The data subject shall, at any time while availing the services or otherwise, also have an option to withdraw his/her consent given earlier to the data controller. In such cases the data controller shall have the option not to provide goods or services for which the said information was sought if such information is necessary for providing the goods or services. In exceptional cases, where it is not possible to provide the service with choice and consent, then choice and consent should not be required.

1.5.3 **Principle 3: Collection Limitation**

A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.

1.5.4 **Principle 4: Purpose Limitation**

Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should be in compliance with the National Privacy Principles.

1.5.5 **Principle 5: Access and Correction**

Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data. Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.

1.5.6 **Principle 6: Disclosure of Information**

A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.

1.5.7 **Principle 7: Security**

A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks.

1.5.8 **Principle 8: Openness**

A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

1.5.9 **Principle 9: Accountability**

The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner.

1.5.10 **Use of Personal Identifiers**

The ubiquitous use of personal identifiers, like UID, PAN, and Passport, to complete transactions is taking place across India. As a result of this practice, centralized and decentralized databases that contain detailed records of individuals and their transactions are being converged by organizations and bodies on an adhoc basis. The amount and granularity of information that can be converged through the use of these personal identifiers makes it possible for comprehensive profiles to be created of individuals and track individuals across databases via their personal identifier. In India the use of personal identifiers across databases by third parties for tracing, convergence, or collation purposes is not addressed in the legislation that legally establishes the personal identifier [the UID Bill, Citizenship Act, the Passport Act, and the Indian Tax Act etc.] and is not addressed at the organizational or departmental level through policy. Thus, it is

unclear if access is taking place in accordance with laws in force, and what standards are in place to prevent the unauthorized disclosure/access/use of personal identifiers.

Therefore, it is not clear which organizations/bodies are legally collecting and storing personal identifiers, for what purposes, who is accessing data based on personal identifiers, how personal identifiers are being secured, how long personal identifiers are being retained, and if/how the personal identifiers are deleted. This creates a situation where governmental and private sector organizations can potentially access and use information directly or indirectly connected to, or generated by personal identifiers for multiple purposes without explicit authorization, and without the individual being aware or consenting to such access and use. The use of personal identifiers across databases should be in compliance with the National Privacy Principles.

1.6 Background of Study w.r.to Security and Privacy of Aadhaar

1.6.1 Media Reports on the issues of Security and Privacy of Aadhaar

Aadhaar's database has the records of over 1.22 billion registered users and is rapidly becoming the government's base for public welfare and citizen services scheme. As Aadhaar gained the currency of "proof of identity", most checkpoints like railways, airports and even protected areas have started using it as a source of identity.

Some incidence came to the limelight when a random blogger talked about how easy it is to access Aadhaar information with just a basic Google search. With the exponential growth in cybercrime, peoples are perceiving a threat to centralised database which may provide valuable information to wrong hands. This might lead to either illegal tracking of individuals or identification without consent. Another perception is that the sensitive financial information of individuals and companies may also be exposed through breaches of the UID database or internal collusion. Some of such media reports/website[7] are given below:

i) According to The Times of India[7]&[17], Maharashtra accepted that their 3 lakhs of Aadhaar data got lost with PAN. The incident happened when the IT Department were uploading the biometric information and PAN data to the UIDAI centralized server that is in Bangalore from Mumbai, due to the crash of hard disk. In fact the data were being uploaded and encrypted using strong algorithm, and when the Headquarters were downloading the data, they couldn't decrypt it. Therefore, many applicants, who complained about this, were asked to re-register for it. Later the State (Mumbai) IT department stated that the data belonged to people of Mumbai, and the lost data are being fully secured which can only be opened if you

have ‘keys and multi clues’. The State ensures that the data are safe but such type of issues has already raised serious concern.

ii) In a recent case, Sakshi Dhoni, wife of Indian cricketer MS Dhoni[7]&[18] tweeted to the Union of Law & Justice plus the Ministry of Electronics and IT about the Aadhaar data of MS Dhoni being leaked by the CSC e-Governance Services India Ltd. The CSC e-Governance Services India Ltd. had posted a photo of MS Dhoni fingerprint being scanned as well as the screenshot of the Aadhaar data of MS Dhoni. The shocking thing was that the Electronics and IT Minister also liked the tweet and retweeted the photo of MS Dhoni’s fingerprint being scanned by the CSC agency. Later the UIDAI took the strong step and blacklisted the CSC e-Governance Services India Ltd for next 10 years. In spite of all these rule and regulations sharing the information from a partner company raise the issue that whether any privacy is left and does this ensure that whether Aadhaar data is in the right hands or not.

iii) According to the sources of Indian Express[7]&[19], recently first time the NDA Government has admitted that the Aadhaar data had been leaked to the public domain. However, the government had been ignoring the fact that Aadhaar is a sensitive data and assuring us by saying that Aadhaar is fully secured and it can’t be breached easily. As the Aadhaar project has the largest database management the information loss or security breach to Aadhaar database can be a serious threat for India.

iv) Again, in a shocking incident, the information consisting names, addresses, Aadhaar numbers and bank accounts of more than a million beneficiaries of Jharkhand’s old age pension scheme, have been compromised by a programming error on a website maintained by the Jharkhand Directorate of Social Security[7]&[20]. It is to be noticed that the Jharkhand

government has over 1.6 million pensioners, 1.4 million of whom have seeded their bank accounts with their Aadhaar numbers to avail of direct bank transfers for their monthly pensions. As the information of all the citizens can be accessed freely by logging onto the website, this case raises the serious threats of linking Aadhaar card to various government functionalities.

v) In a similar case in Kerala[7]&[21], Aadhaar data of over 35 lakhs of pensioner has been leaked from the Kerala state pension department. All those 35 lakhs of pensioners had linked their Aadhaar number and bank account as required by the "direct benefit transfer" scheme. The service pension website had put up their names, addresses, phone numbers, bank account numbers, Aadhaar numbers and photographs for anyone to download in stark violation of the Aadhaar Act. Furthermore, the site also had the pension id used to draw information, and the data has been pulled from the website only after the news created a stir.

vi) In August 2018, Times of India news regarding Aadhaar data 'edited' to pilfer public distribution system in more than 43 districts at the time of transaction on Aadhaar based POS.

vii) In Chandigarh[7], food and supplies and consumer affairs department shared the UID numbers of number of people on their website. It was said that even ration cards of the person, Date of Birth, spouse name details were displayed on their public domain. In fact, Ministry of Water and Sanitation, which is considered as one arm of Swatch Bharat Mission too publicized the Aadhaar details of the citizens with details like Voter ID number, ration card number and their caste status. However due to various cases of data leaks from government domains, the central government has recently circulated a set of 27 do's and 9 don'ts on data handling and instructions to encrypt sensitive data with a legal consequences.

Further each department has been asked to review their public domain to check if there is any personal data on display, and to allot an official who must be responsible for Aadhaar data protection.

viii) According to The Times of India[7], there was an Aadhaar controversy in which the Aadhaar card were being considered invalid on the various factors. In this case a senior citizen got his Aadhaar card without any hassle or without any problem, but the problem aroused when he got the Aadhaar card mentioning the 'Year of Birth' instead of 'Date of Birth' which was considered as an invalid Aadhaar card. Later the Secretary of State (Mumbai) IT Department considered it to be valid as the senior citizens who were born before the year 1989, can use Year of Birth as they didn't have the provision for birth certificate at that time. Recently, Aadhaar has been made mandatory to be linked with PAN card, since then various cases of mismatching names on PAN card and Aadhaar card have also been reported. The main reason is that Aadhaar does not require to disclose the name of the citizen without initials where as the PAN requires the disclosure of full name with the initials. Due to this, many people are not able to link PAN with Aadhaar card. As per the finance act 2017, now Aadhaar is mandatory for applying a fresh PAN application and for filing Income Tax returns. Further government is also saying that the existing PAN would be cancelled if Aadhaar has not been linked with it; the reason is to control tax evasion and eliminate multiple PAN's. Therefore the linkage of Aadhaar to PAN is a good initiative but name of Aadhaar card has not paid much attention while implementing this project. Though such types of problems are occurring, it is to be noticed that Income Tax department made mandatory to link Aadhaar card with bank accounts by 30 April 2017 to self-certify them to comply with FACTA (**F**oreign **T**ax **C**ompliance **A**ct) regulations.

ix) According to Live mint[7], UIDAI filed a complaint on which Delhi police has lodged an FIR in which two different names enrolled with same biometric. The Deputy Director of UIDAI regional office in Pragati Maiden, Delhi told police that on March 18, a person named Raj Kishore Roy enrolled for Aadhaar and submitted his demographic and biometric details. However UIDAI found that on March 17, a person named Deben Roy enrolled for Aadhaar with same biometric information. This example also raises serious concerns. However later UIDAI lodged a complaint under Aadhar act as cheating by impersonation.

x) According to the report by Times of India[7], UIDAI filed a complaint with Delhi Police against Axis Bank Ltd., business correspondents Suvidhaa Info serve and ensign provider, eMudhra stating that they have attempted unauthorized identity theft by means of illegally storing of Aadhaar biometrics. It was found that 397 transactions were made with the same biometric between July 14, 2016 to February 19, 2017 in which 194 transactions were from Axis Bank, 112 from eMudhra and 91 through Suvidhaa Infoserve. The problem was detected when multiple transactions took place using the same biometric. The Axis Bank spokesperson told to livemint.com that it was the developer Suvidhaa, who carried out live-based Aadhaar Authentication and that goes against the government that claims that Aadhaar is not penetrable. UIDAI gave them the time till 27th of February 2017 to explain why they did this. However, UIDAI have banned the Aadhaar enabled system temporarily for the three firms i.e. Axis Bank Ltd. e-Mudhra and Suvindhaa Infoserve. Chapter VII Clause 35 of Aadhaar act 2016 states that “Whoever, with the intention of causing harm or mischief to an Aadhaar number holder, or with the intention of appropriating the identity of an Aadhaar number holder changes or attempts to change any demographic information or biometric information of an Aadhaar number holder by impersonating or attempting to

impersonate another person, dead or alive, real or imaginary, shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to a fine which may extend to ten thousand rupees".

xi) On February 2017, a FIR (**F**irst **I**nformation **R**eport) [7] was filed against an individual known to be Sameer Kochhar, who leads Gurgaon think tank Skoch Development Foundation. The complaint was filed for his article "Is a Deep State at work to Steal Digital India?, in which he mentioned the Aadhaar security vulnerability and included a video on how the Axis Bank fraud transactions case took place. The Authority Chief Executive responded it in Twitter by tweeting "The video is fake and asked Kochhar to stop spreading rumours". The DCP (**D**eputy **C**ommissioner of **P**olice) confirmed that "UIDAI has filed a police complaint against Kochhar regarding putting a fake video on an article in Google. Therefore, the a senior police official confirmed that the case filed by UIDAI was under section 37 of Aadhaar Act which states that, "Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorised under this Act or regulations made there under or in any agreement or arrangement entered into pursuant to the provisions of this Act, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both (Aadhaar Act 2016)".

In Budget 2017, Aadhaar was made mandatory for availing Permanent Account Number (PAN) cards and filing Income Tax Returns. This interlinking of Aadhaar with various utility platforms (banks, PANs, birth certificates, etc.) will facilitate interconnectedness by making a network of networks. That, in turn, would pave the way for more

accountability and transparency, although at the same time such a massive scale of digitisation and data centralisation may attract several threats and hence are crucial to outline.

1.6.2 **Supreme Court's Case references**

Aadhaar card is a major concern for the nation which led the Supreme Court of India interferes. The objective of this section is to present the findings of the court. On 20th November 2012, the legislative and the state knocked the door of Supreme Court of India where the court observes the arguments against National Identification Authority of India Bill 2010 which possibly overlaps the Article 73 of Constitution of India which states "Extent of the executive power of the Union, states that, Subject to the provisions of this Constitution, the executive power of the Union shall extend to the matters with respect to which Parliament has power to make laws and to the exercise of such rights, authority and jurisdiction as are exercisable by the Government of India by virtue of any treaty or agreement". On 23rd September 2013, the Supreme Court of India held by three-judge bench ordered that the Central Government cannot refuse to give subsidies to the person who does not possess an Aadhaar card. Therefore, court admitted that Aadhaar is voluntary but not mandatory. But in 2016, the Supreme Court of India[7] extended the use of Aadhaar Card to MGNREGA, pension schemes, EPF (**E**mployee **P**rovident **F**und) and PMJDY though Aadhaar was first only restricted to Cooking Gas subsidies and PDS distribution system.

It is to be noticed that in January 2017-March 2017 alone the government of India has made possession of an Aadhaar card mandatory for availing over 30 central schemes. On 27th March 2017[7], the court again reiterated that government cannot make Aadhaar mandatory for

welfare schemes. However, the court has not stopped the government to make Aadhaar mandatory for other schemes.

Later in 2017, Supreme Court of India[25] started hearing on a batch of petitions challenging Section 139AA of Income Tax Act which made mandatory linking of Aadhaar with IT Returns. Senior Advocate Aravind Datar argued that the Section 139AA of Income Tax Act is contrary to the orders of the Supreme Court, and further the section violates Article 14 and 19(1)(g) of the constitution of India. A similar type of petition was also filed by the former Kerala minister and CPI leader Binoy Viswam stating that section 139 AA(1) is 'illegal and subjective' and violates Article 14 and Article 21 of Constitution of India.

A five-judge bench, led by Chief Justice of India Dipak Misra, reserved its verdict in the case on May 10 after a 38-day hearing. On 26th September 2018[26], the Supreme Court pronounced that the Aadhaar programme is constitutionally valid. The court, in its Aadhaar verdict, however put in place a series of conditions with regards to the need for an Aadhaar number for certain services. Aadhaar cannot be made mandatory for opening bank accounts or for education, for example. An Aadhaar number however will be needed to file an income tax return.

CHAPTER 2

LITERATURE REVIEW

There is very limited literature available which dealt to understand the actual issue related with the privacy and security issues of Aadhaar. However, there are some papers, news articles etc. which have discussed some part of the issues

2.1 A study on Aadhaar[1] (Naveen, 2012-13)**:** A dissertation submitted to Panjab University Chandigarh at Indian Institute of Public Administration

2.1.1 This study has dealt with the objective of Aadhaar card, implementation strategy, Technology used in the card etc. This has focused on the advantages of Aadhaar like Government will have clear view of their population as it will eliminate the fake & duplicate identities due to proper information of demographic and biometric information. This will help Government to stop exchequer losses arising out of ghost identifications or duplication. It is very easy identity proof for residents as they can prove their identity Anywhere, Any time & Any mode (i.e. physical mode or electronic mode) by Aadhaar. This study established that it is beneficial for both residents as well as nation by way of providing benefits actual needy person in faster &effective manner and by avoiding the benefit to non-eligible beneficiaries.

2.1.2 However, the study has not covered the detail of security measures taken by UIDAI for datacentre and network. It has not covered the standard and procedures adopted by UIDAI for security of equipment and information stored in datacenter. It has also not included the measures taken for data protection and privacy of the Aadhaar data.

2.2 Privacy and Security of Aadhaar[4]: (Agrawal, Banerjee, & Sharma, 2014) A Computer Science Perspective, IIT Delhi

2.2.1 The study has discussed the Aadhaar authentication framework including various entities involved in authentication. This is based more on theoretical approach for general systems rather than practical approach with respect to the specific system of UIDAI. Further, it has taken an assumption of threats from internal employees and different agencies.

2.2.2 The security measures and standards being followed by UIDAI for their systems have not been considered in the study, the study seems more on general concept of security.

2.3 Survey Paper on UID System Management[6]: (Chauhan, Sharma, Geetanjali, & Verma, 2014).

2.3.1 It has covered different features inbuilt with Aadhaar. It has briefly covered procedure of UID system including recording process, authentication process like role based authentication etc. It is focused on the advantages/benefits of having Unique ID for the citizens and creating an ecosystem for Nation. It concerns that it may be harmful to the general public because all the data related to them is stored on computers and can be misused by hackers.

2.3.2 It has raised only apprehension of misuse of data without any concrete study on this aspect but not covered the privacy & security issue.

2.4 Rebooting India[5]: Nandan Nilekani & Viral Shah (2015), Penguin Books. PP(1-46)

2.4.1 It has covered the Aadhaar enrolment process along with the features of Aadhaar. it is mentioned that Unique ID is primary function, and it is universal, digital, secure

verification method for many applications/services e.g. Social Security scheme, subsidies, Govt services, e-KYC, Voting, effective administration, efficient & effective delivery of public services etc.. Aadhaar will be gamechanger for the Government in reducing the pilferage of subsidies by avoiding duplication and transferring money directly to the beneficiary's accounts.

2.4.2 Its basic focus on the relevance and importance of UID and this book has not the concern of Privacy and Security of Aadhaar.

2.5 Aadhaar Card: Challenges and Impact on Digital Transformation[7]: Raja Siddharth Raju, Sukhdev Singh, Kiran Khatter (2017)

2.5.1 This study has covered the advantages of Aadhaar for various Government schemes such as cooking gas subsidies, house allotment, school scholarship passport, e-lockers, bank accounts, PMJDY(Pradhan Mantri Jan Dhan Yojana), provident funds account, pensions, driving license, insurance policies loan waiver etc. It has covered how Aadhaar can play major role in improving the different systems like Railways Reservations system, ATM Security, Cloud based e-voting, Aadhaar e-KYC Services, Denture Identification, E-helth care, Municipal corporation, Aadhaar Pay, Airport system etc. for delivering services efficiently & effectively. Further, this study has shown concerns on-

a) Whether biometric technology is capable to the gigantic task of de-duplication.

b) There has been no cost benefit analysis or feasibility report of the project.

c) The purported benefits of the project in social sector e.g. PDS are largely illusive.

2.5.2 The study is more focused on its importance & advantages with the concerns on viability of such a large scale project. However, it has not discussed the issue of Privacy and Security.

2.6 A Failure to "Do No Harm"[8] – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.Pam Dixon (2017):

2.6.1 It has raised issues of privacy and security with respect to Aadhaar also based on protections measures on privacy and autonomy for general systems. It has mentioned that in Aadhaar deployment, technical deployment was done before the policy development regarding.

2.6.2 Wrt privacy and security, it has not discussed about the system & processes being used by UIDAI. The provisions w.r.t Privacy & security made in Aadhaar act & IT Acts 2004 has not been considered.

CHAPTER 3

STRATEGIES, METHODOLOGY AND RESEARCH DESIGN

3.1 Research Problem

The government of India has been forcing to link the Aadhaar with various government schemes such as cooking gas subsidies, bank accounts under PMJDY (Prandhan Mantri Jan Dhan Yojana), provident funds account, pensions, and filing income tax returns and many more. In fact, Aadhaar Bill (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) 2016 was passed as a Money Bill. In this bill, Aadhaar card was made mandatory for authentication purposes for many such Government scheme.

On the one side, Aadhaar is getting more popular and enrolment has crossed 1.22 billion as of July 2018, representing about 90% of the estimated population and is becoming the government's base for public welfare and citizen services scheme. However, on the other side, Media has been reporting the issues wrt privacy & security of Aadhaar data like leaking of data, misuse of data, deletion of data etc. as discussed earlier in Chapter-1 of this study.

With such news in media, the society starts pondering and becomes cautious and rethinking on acceptance of Aadhaar. Security and so Privacy concerns relating to the Aadhaar project have been the subject of much heated debate recently. The security of Aadhaar Systems and privacy of information of all residents are very important aspect of project.

Therefore there is a need to study about the Aadhaar system, its network, its process flow and access mode/privilege, data protection methods and provisions in Aadhaar Act-2016, IT Act 2000/ 2008 in order to understand whether there is really some issue of Privacy & Security of Aadhaar or it is only a myth due to lack of awareness about the Aadhaar system and provisions.

3.2 Research Objective and Research Questions

3.2.1 The research objectives are as below-

a) To study a broad architecture and security systems network and datacenters of UIDAI in reference to security aspect of system

b) To study the access mode and methodology of UIDAI systems and Aadhaar data

c) To study about the issues related to data protection and Privacy of Aadhaar data.

d) To assess the awareness among public regarding Aadhaar system and issues related to Privacy & security in order to assess the overall acceptability among public.

3.2.2 The broad research questions are as below-

a) What is broad architecture and systems for network and datacenters of UIDAI in reference to security aspect of system?

b) What is the access mode and methodology of UIDAI systems and Aadhaar data?

c) What are the issues related to data protection and Privacy of Aadhaar data?

d) How much public is aware regarding Aadhaar system and issues related to Privacy & security in order to assess the overall acceptability among public.

3.3 Research Strategy / Design

The different aspects of this research are based on the study and analysis of the various secondary inputs available from different sources. The security issues need a study of security policy and practices have been adopted by UIDAI and various other agencies involved in the different stages of Aadhaar. Further, for the privacy issues first, it needs to understand the different principle of privacy being adopted worldwide and in India within the ambit of laws and regulations of the Nation. Therefore, this requires a detailed study of documents and discussion/ interview of UIDAI officials to understand the issues of security and Privacy. Accordingly, the qualitative approach of study has been adopted during research for assessing different issues related to security and Privacy of Aadhaar data.

Further, in order to understand the opinion of public in respect of the importance of Aadhaar vis-à-vis the issues of security and privacy of Aadhaar data, a Quantitative Approach of study was considered by taking survey from population segment (representing a diverse group of target population for Aadhaar).

Accordingly, this research is based on both Qualitative and Quantitative in nature. The Quantitative Approach has been done based on the analysis of data received from response of Questionnaire set-B. The qualitative approach has been adopted in the analysis of Discussion & Interview with UIDAI officials keeping in view of the input observed from different reports and documents studied during the research.

3.4 Methods used for Data sources

The study is based on both primary data and secondary data. Being a part of study is technical understanding, the target population for survey has been different depending on the issue. The data collection has been done from different segment in Delhi/NCR area only due to paucity of time.

- **Secondary Data:** The sources of secondary data are the documents available in Public Domain and collected from UIDAI. Some of these sources are as below-
  - UIDAI Strategy Overview
  - Report of the Group of Experts on Privacy (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court)
  - A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Report of Committee of Experts under the Chairmanship of Justice B.N. Srikrishna)
  - Aadhaar act 2016
  - Review of Books, Journals and Published Articles
  - Reports Released by GOI and various other Organisations
  - Various news of Newspaper from websites
  - UIDAI website
- **Primary data**: Primary data have been collected from different sources as given below-
  - **Discussion and Interview**- Discussion cum Interview were held with the UIDAI officials at UIDAI Headquarter, Bangla Sahib Road, Behind Kali Mandir, Gole Market, New Delhi and UIDAI Regional Office, Ground Floor, Pragati Maidan Metro

Station, Pragati Maidan, New Delhi-110001 in order to understand the UIDAI network architecture and its component from various aspect of security and privacy of Aadhaar data. A sample of "open ended" questions were asked during interview is enclosed at Annexure-I.

- **Questionnaire mode**: The questions were prepared keeping in view of the basic objective of our study i.e. to study a broad architecture of network and datacenters of UIDAI in reference to security aspect of system, to study the process flow of Aadhaar data enrolment and its access mode from other agencies i.e. other than UIDAI, to study about the issues related to Privacy and security of Aadhaar data from public perspective and to assess the awareness among public regarding Aadhaar system and issues related to Privacy & security in order to assess the overall acceptability among public. Accordingly, there are two set of questionnaires for study focusing Security and Privacy aspect from different target of population.

  Questionnaire Set-A: One set of questionnaires covering various aspect specific to the UIDAI network architecture, its equipment and access mode to Registrar, Service Providers & users. This was focused for the security part of study of Aadhaar network. Being specific natures of questions, the response for this set of questionnaires was collected from UIDAI official and Registrar and Service providers to assess their opinion. It is given at Annexure-II.

  Questionnaire Set-B: The second set of questionnaires was general purpose for assessing the response of public covering from the different segment like IT departments, Telecom, Regulatory, IT professionals, Students, Lecturers, professors etc. It is given at Annexure-III.

3.5 Sample size and Target group for survey

Qualitative Analysis

Sample size: This study is based on the technical logic on security of Aadhaar data and network. Accordingly, a sample of 10 persons with technical background from different organization has been considered keeping in view of Creswell's (1998) recommendation for sample size of 5 – 25 for logical studies.

Target group:

- Discussion and Interview were conducted from officials at UIDAI, HQ responsible for Policy and Technical implementation and from officials at its Regional center, New Delhi.
- In order to understand opinion from other technical expert of Telecom & IT industry, discussion/interaction were conducted from official / executives of Telecommunication Engineering Center (TEC), Department of Telecommunications (DoT), Department of Electronics and Information Technology (DeITY), Telecom Regulatory Authority of India (TRAI), Bharat Sanchar Nigam Limited (BSNL), Nokia Siemens Networks (NSN) & Tata Consultancy Services (TCS) have been considered.

Quantitative Analysis:

Sample size: Following steps have been considered for sample size calculation-

a) **Population size:**

The population here referred are all residents of country as all need to be issued Aadhaar. However, here the target population are considered only those who are considered as middle class or above and well educated because they are only to be considered as raising security and privacy concerned with Aadhaar. It is assumed here that most of the middle class and lower class people are not raising any privacy concern in view of advantages they are getting with Aadhaar. This size of population can be considered approx. 1-5% of total population.

b) **Margin of Error**- In order to ensure that the answers of survey reflect the views of the population with minimum error, a 5% margin of error has been considered.

c) **Confidence Level-** A confidence level is the likelihood that the sample selected represent the population. In order to ensure that the sample considered shall reflect the population accurately, 95% confidence level has been used here.

d) Sample size: Considering the above margin of error and confidence level, the sample size has comes out to 384 which is rounded to 400.

Target group for Sample: In order to have IT departments, Telecom, Regulatory, IT professionals, Students, Lecturers, professors etc. The survey was through different mode i.e. email, social media, personal and friend/colleague. In order to have opinion from representative of different regions/area, the responses were collected with a more focus to metropolitan area i.e. Delhi/NCR region, Bengaluru, Hyderabad, Pune and other area like Lucknow, Allahabad and Varanasi.

3.6 Scope/Limitations

Complexity of System: In order to handle huge size of data requirement for complete population, huge number of transactions per unit time and security requirement, the data centers of UIDAI for storage as well as serves/network equipment are very complex.

Limitation of Access of Datacenter/System: The real security threat assessment requires detailed vulnerability assessment of each and every equipment from various aspects and which need access to various systems to make the comprehensive study. As per their security policy and guidelines, the UIDAI has not allowed me to access to their datacenter and various system / sub-system of UIDAI to do such study being the sensitive data.

Time Limitation: Further, there is limitation of time as well to make a detail and comprehensive study.

Therefore, study of security & Privacy aspect of Aadhaar is limited to the personal interaction with official of UIDAI and feedback from the field survey for overall acceptability of Aadhaar only.

CHAPTER 4

OBSERVATIONS, ANALYSIS AND FINDINGS

4.1 Responses of Discussion & Interview

4.1.1 Responses of Discussion & Interview with UIDAI Officials

In order to have understand and make more effective study, first discussion cum interview were held with the UIDAI officials with following set of open-ended questions.

i. What is their view on the physical security of the UIDAI datacenter?

Response: Keeping in view of physical security of Aadhaar data, the UIDAI main datacenter having Central Identities Data Repository (CIDR) at Manesar in Haryana for storing data of 1.9 billion Indians is having a boundary wall of 13-feet high and 5-feet wide. There are approx. 200surveillance cameras/CCTVs and over 150 CISF personnel guarding the data of Indian citizens constantly. Further, there is similar secondary datacentre in Bengaluru to meet any disaster situation. There is 24-hour security and apart from the CISF, there are two private security agencies also to support in security. There is a three-tier check before one even makes it to the entrance of the building. Any unauthorized access in campus is totally prohibited.

ii. Is there any system to manage building and to give access to building?

Response: Yes. There is different kind of management system to manage/ monitor the Building Management, Access Management, Security Management, other Infrastructure management etc. of datacenter. Every entry is recorded and properly log registers are maintained. There is different level of authorization to the access of different part/room of building. The access to different datacenter area is electronically controlled and allowed as per authorization role defined in the system and all such access are well captured in the system.

iii. How the Data Storage and Process are secure from cyber security threats?

Response: Storage of data in secured servers with limited access is one of the core mantras of cybersecurity. The UIDAI official told that Aadhaar data is stored and processed within its own datacentre. It also said that the data resides within its own secured servers. The chances of data breaches are manifold when servers are connected to the outside world via the Internet. However, data servers of UIDAI have no connection or link with the outside world through Internet, pen-drives, laptops or any other devices.

iv. What kind of security equipment have been deployed in the datacenter?

Response: The UIDAI data center is world class datacenter and have been deployed all kind of security equipment like Intrusion detection system, Intrusion Prevention System, Firewall etc. with state of art technology have been deployed. There are many more security equipment and applications have been deployed in the data center and UIDAI networks but due to security policy it can not be informed. However, rest assure that the UIDAI has put into place all the advanced technology to mitigate any kind of risk from electronic data breach.

v. How the Physical Protection of Data are ensured?

Response: To prevent any kind of breach, UIDAI ensures the physical protection of datacentre through robust testing of hardware. Hardware supplies are tested twice to identify and plug defects, if any. Moreover, the biometric image data captured during Aadhaar enrolment is not in the possession of the solutions provider or its employees. The biometric service provider needs to strictly conform with the Government's data security guidelines that are mentioned in the contract.

The apps running on the IT hardware of UIDAI are well-protected through intrusion and firewall prevention system. In other words, the Government has put into place advanced technology to mitigate risk of any physical or electronic data breach.

vi. What security practices are being followed by UIDAI?

Response: UIDAI constantly strengthens and reviews its infrastructure and ecosystems in line with the best international security practices and technological standards and has multi-layered security and privacy considerations built into the core strategy of Aadhaar

with three basic doctrines of **minimal information, optimal ignorance and federated database** which give higher level of security to the data.

vii. What kind of safety have been taken to prevent threat from the vendors of technology?

Response: The threat of a breach doesn't always necessarily arise from a hacker. Eventually, breaches can happen due to third-party involvement including private contractors, and vendors. To prevent leakage of sensitive data, the Aadhaar platform hinges largely on open-source technology. Deployment of propriety technology ensures the protection of data from private contractors and third-party vendors.

High-level of encryption is one of the fundamental pillars of data safety. Cybersecurity experts put a lot of emphasis on encryption to secure data from falling prey to cyber criminals. Aadhaar data is encrypted using PKI-2048 and AES-256. These are one of the most robust public key cryptography encryptions. Each enrolment data packet is stored in PKI encrypted form, ensuring that no system or person has access to these packets.

To add more security, each Aadhaar data has a built-in mechanism to detect any kind of tampering.

viii. What is your view on the performance and availability of service of UIDAI?

Response: The enrolment has crossed 1.22 billion as of July 2018, representing about 90% of the estimated population and the system may be handling millions of transaction per second. As of now there is no any major performance issue were reported which indicates that the system has been designed with scalability features to met the growth requirement. The availability of system has been defined with five 9 and to meet the disaster situation, a secondary datacentre with the similar set of system has been deployed in Bengaluru.

ix. Whether Aadhaar Privacy is a relay challenge for the Government?

Response: UIDAI has been ensuring all kind of security and following the privacy principles but of course with more than a billion people having enrolled for Aadhaar, its privacy remains one of the challenges for the Government as any minor lapse will further put question marks on the Government’s effort to streamline the KYC process with a single document across sectors and curb corruption.

While the Government is making every effort to secure Aadhar data, the onus also lies on the Aadhaar holder to protect one's personal information and biometrics. Due diligence on the part of the holder will go a long way in preventing misuse of his/her unique 12-digit number.

x. What are the Data protection and privacy measures taken by UIDAI?

Response: The UIDAI has the obligation to ensure the security and confidentiality of the data collected. The data are being collected on software provided by the UIDAI and encrypted to prevent leaks in transit. The UIDAI has a comprehensive security policy to ensure the safety and integrity of its data. There are security and storage protocols in place. UIDAI has published guidelines in this regard which is available on its website. Penalties for any security violation will be severe and include penalties for disclosing identity information. There will also be penal consequences for unauthorised access to CIDR – including hacking, and penalties for tampering with data in the CIDR.

xi. What are the privacy protections in place to protect the right to privacy of the resident?

Response: Protection of the individual and the safeguarding their information is inherent in the design of the UID project. From having a random number which does not reveal anything about the individual to other features listed below, the UID project keeps the interest of the resident at the core of its purpose and objectives.

- **Collecting limited information**: The UIDAI is collecting only basic data fields - Name, Date of Birth, Gender, Address, Parent/ Guardian's (name essential for children but not for others) photo, 10 finger prints and iris scan.
- **No profiling and tracking information collected**: The UIDAI policy bars it from collecting sensitive personal information such as religion, caste, community, class, ethnicity, income and health. The profiling of individuals is therefore not possible through the UID system.
- **Release of information – yes or no response**: The UIDAI will not reveal personal information in the Aadhaar database – the only response will be a 'yes' or 'no' to requests to verify an identity

- **Convergence and linking of UIDAI information to other databases**: The UID database is not linked to any other databases, or to information held in other databases. Its only purpose will be to verify a person's identity at the point of receiving a service, and that too with the consent of the Aadhaar number holder. The UID database will be guarded both physically and electronically by a few select individuals with high clearance. The data will be secured with the best encryption, and in a highly secure data vault. All access details will be properly logged.

xii. Who will have access to the UID database? How will the security of the database be ensured?

- Residents who have Aadhaar numbers will be entitled to access their own information stored in the UID database.
- CIDR operations will be follow strict access protocols to limit access to the database.
- The database itself will be secured against hacking and other forms of cyberattacks.

xiii. Any other suggestion to avoid misuse?

Response: There are many input regarding security, privacy and to keep safe Aadhaar data e.g. Locking of Biometric Details- To protect the potential misuse of biometrics, UIDAI has introduced a new security feature where one can lock his/her biometric data. With the help of Aadhaar biometric locking system, Aadhaar holders can lock and temporarily unlock their biometrics. They can do it from the official website of UIDAI. This feature ensures that no one can access biometrics of an Aadhaar holder without his/her consent.

Further, a set of questions along with responses (FAQ) was collected from UIDAI as enclosed at Annexure-4. This gives awareness to the Aadhaar system and information to keep safety precautions for keeping our Aadhaar safe.

4.1.2 Responses of Discussion/Interview with Technical Experts

a) **Comment of Experts from Telecommunication Engineering Center (TEC)/ Department of Telecommunications (DoT)**:

As a policy they cannot tell much about the equipment specific, but as per information all the equipment's like storage, servers, network equipment have been deployed in Aadhaar datacenter are international standard following latest technology/architecture. The standard equipment support the inbuilt redundancy as well as system have been designed with the requisite redundancy requirements. There is no doubt, the requisite security equipment have been deployed at Aadhaar datacentre as UIDAI has claimed repetitively that they are meeting all the security requirement and following the privacy policy as well. As per their opinion, there is no risk of Aadhaar data, rather being unique ID Aadhaar is an easy and useful in tracing the calls, which is really useful in curbing the security threat malicious call to nation.

b) Comment of Experts from Department of Electronics and Information Technology (DeITY):

The UIDAI data center is world class datacenter and have been deployed all kind of security equipment like Intrusion detection system, Intrusion Prevention System, Firewall etc. with state of art technology have been deployed. The Aadhaar datacenter is one of the largest datacenter in the world to handle a huge capacity of data for more than billions of residents. The processing capacity of datacenter also very huge for meeting millions of transactions per unit time. Accordingly, all the international standards of datacenter have been followed by UIDAI for its datacenter keeping in view of critical data of residents are stored in CIDR. UIDAI also keeps updating the security update as per requirement

and the guidelines issued by the IT department of Government of India as well. In their opinion, there may not be security and privacy issue on Aadhaar.

c) Comment of Experts from Telecom Regulatory Authority of India (TRAI):

In their opinion also, UIDAI datacentre is robust and foolproof as claimed by UIDAI many times. Further they mentioned that Protection of the individual information is integral part of UID project. A random number which does not reveal anything about the individual. The UID project keeps the interest of the resident at the core of its purpose therefore it collects limited information i.e Name, Date of Birth, Gender, Address, Parent/ Guardian's, photo, 10 finger prints and iris scan. The UIDAI policy bars it from collecting sensitive personal information such as religion, caste, community, class, ethnicity, income and health. The profiling of individuals is therefore not possible through the UID system. The UID database is not linked to any other databases, or to information held in other databases. UIDAI has proper guidelines and contractual obligations for their Registrar and Agencies to protect individual information. Further, they mentioned the case of their Chairman Dr R S Sharma where a false claim regarding hacking of his personal information.

d) Comment of Experts from Bharat Sanchar Nigam Limited (BSNL)

The comment of BSNL regarding datacentre is similar to that DOT/ DeITY. It is further told that UIDAI is following concept of virtual networking to restrict the access of CIDR from outside of UIDAI network in order to enhance the security. It is mentioned that overall Aadhaar datacentre is very good. However, UIDAI needs to educate the residents about their role to ensure their information secure and confidential. Further, security being a dynamic feature, it needs to be updated with the time by UIDAI.

Further, it is mentioned that Aadhaar is very easy toll for verification of identity for provision of telephone service.

e) Comment of Experts from Nokia Nokia Siemens Networks (NSN)/Tata Consultancy Services (TCS)

The technology and equipment deployed in Aadhaar datacenter is based on principles of openness, linear scalability, strong security and most importantly vendor neutrality. The technology architecture has been structured to ensure clear data verification, authentication and deduplication, while ensuring a high level of privacy and information security. The technology followed the basic three features of Open architecture, scalability and security. It was mentioned that the datacenter are being managed by reputed software companies i.e. HCL, Wipro and TCS who are well equipped to run the system with all the updated requirement for the system including security measures.

4.1.3 Aadhaar breach reports are misleading: UIDAI to court[1]

Hindustan newspaper[28] reported on dated 14 Feb 2019 that, in an affidavit filed before a bench of Justice S Ravindra Bhat and Justice Prateek Jalan, the UIDAI said **all reports of data breaches were misleading and false**.

The Unique Identification Authority of India (UIDAI) informed the Delhi high court on Thursday that its database — Central Identity Data Repository (CIDR) — had not been breached as existing security controls and protocols were "robust and capable of countering any such attempts or malicious designs of data breach or hacking".

[1] Aadhaar breach reports are misleading: UIDAI to court https://www.hindustantimes.com/india-news/aadhaar-breach-reports-are-misleading-uidai-to-court/story-CUnRdOBOoDz6Zxw6U3nmZL.html

"... the data is fully secured/encrypted at all times i.e., at rest, in transit and in storage. For further strengthening of security and privacy of data, security audits are conducted on regular basis, and all possible steps are taken to make the data safer and protected...," it said.

"... UIDAI has taken fool-proof measures to ensure end-to-end security of resident data, spanning from full encryption of resident data at the time of capture, tamper resistance, physical security, access control, network security, stringent audit mechanism, 24/7 monitoring and measures such as data partitioning and data encryption with UIDAI controlled data centres," the affidavit added. The reply comes on a plea by Kerala-based lawyer Shamnad Basheer who has alleged that there were several breaches of the Aadhaar system leading to leakage of personal information of individuals since January 2018. The plea contended that UIDAI and the Centre were liable to compensate people whose data were compromised.

4.2 Observations on Response of Questionnaire Set-A

In order to assess a basic security measures and to develop a confidence level, the response of UIDAI on a set of basic questions were taken and same is given below in Table4.1.

Table 4.1: Response of questionnaire Set-A

Sl No	Questions	Response
1.	Whether Aadhaar datacenter sites are following International standards of physical Access to the equipment and equipment's rooms? **YES / NO**	YES
2.	Whether datacenter of Aadhaar is meeting the requirement of Tier-IV standards (as per Uptime institute definition)? **YES / NO**	YES
3.	Whether UIDAI is following ISO 9000 - Quality System for its Aadhaar datacentre? **YES / NO**	YES

4.	Whether UIDAI is following ISO 14000 - Environmental Management System for its Aadhaar datacentre? **YES / NO**	YES
5.	Whether UIDAI is following ISO 27001 - Information Security for its Aadhaar datacentre? **YES / NO**	YES
6.	Whether UIDAI is following EN 50600-2(1) Building (2) Power distribution, (3) Environmental control, (4) Telecommunications cabling infrastructure, (5) Security systems and (6) Management and operational information systems for its Aadhaar datacentre? **YES / NO**	YES
7.	Whether Firewalls have been deployed in Aadhaar datacenter in order to strength the security of datacenter? **YES / NO**	YES
8.	Whether Intrusion Detection System (IDS) have been deployed in Aadhaar datacenter in order to strength the security of datacenter? **YES/NO**	YES
9.	Whether Intrusion Prevention System (IPS) have been deployed in Aadhaar datacenter in order to strength the security of datacenter? **YES/ NO**	YES
10.	Whether Policy, Signatures etc. of security equipment like Firewalls are being updated regularly to protect from latest security threats? **YES/NO**	YES
11.	Whether proper security policy like Access & Authorization policy, Password policy for different equipment have been implemented? **YES/NO**	YES
12.	Whether security policy like Access list (based on IP addresses, Port etc.), Filter list etc. have been implemented? **YES / NO**	YES
13.	Whether Server Hardening has been done in datacenter? **YES / NO**	YES
14.	Whether servers running frontend applications (which may be accessed from outside) and Servers running backend applications (which are being used in backend and accessed by internal server of datacenters only) are separate? **YES / NO**	YES
15.	Whether CIDR having Aadhaar data is accessible from outside of Aadhaar network? **YES / NO**	NO

16.	Whether the concept of zoning of network like Secure zone, demilitarized zone and open zone etc. has been implemented at Data center? **YES / NO**	YES
17.	Whether any Security Policy defining all security procedures & guidelines has been laid down for Aadhaar datacenter? **YES / NO**	YES
18.	Whether the security policy of Aadhaar datacenter are being updated by on Regular basis? **YES / NO**	YES
19.	Whether any Audit are being carried out for Security implementation and practices adopted by UIDAI ? **YES / NO**	YES
20.	Whether comprehensive measures of data security such as complete data backup & recovery, using data encryption while transferring files, enforcing the latest data privacy regulations and comprehensive monitoring of traffic are being followed? **YES / NO**	YES

Note- *Due to the security policy guidelines, UIDAI officials were not giving response to this questionnaire set, however, finally they gave an indicative information only instead of specific to any equipment/ system.*

4.3 Observations of Responses of Questionnaire Set-B:

The responses of this set of questionnaires was collected from 400 persons of different field and different region/area for assessing the public opinion on the issues/awareness related to the security, privacy and acceptability of Aadhaar data. The responses were collected from people studying/ working the field like IT professionals, Telecom, Regulatory, Advocate, Judiciary, Students, Lecturers, professors etc. The survey was through different mode i.e. email, online, personal and friend/colleague. The responses were collected from across the country, however, special focus in big cities/ metropolitan area i.e. Delhi/NCR region, Bengaluru, Hyderabad, Pune and other area like Lucknow, Allahabad and Varanasi. The summary of responses received during survey are given below in Table4.2.

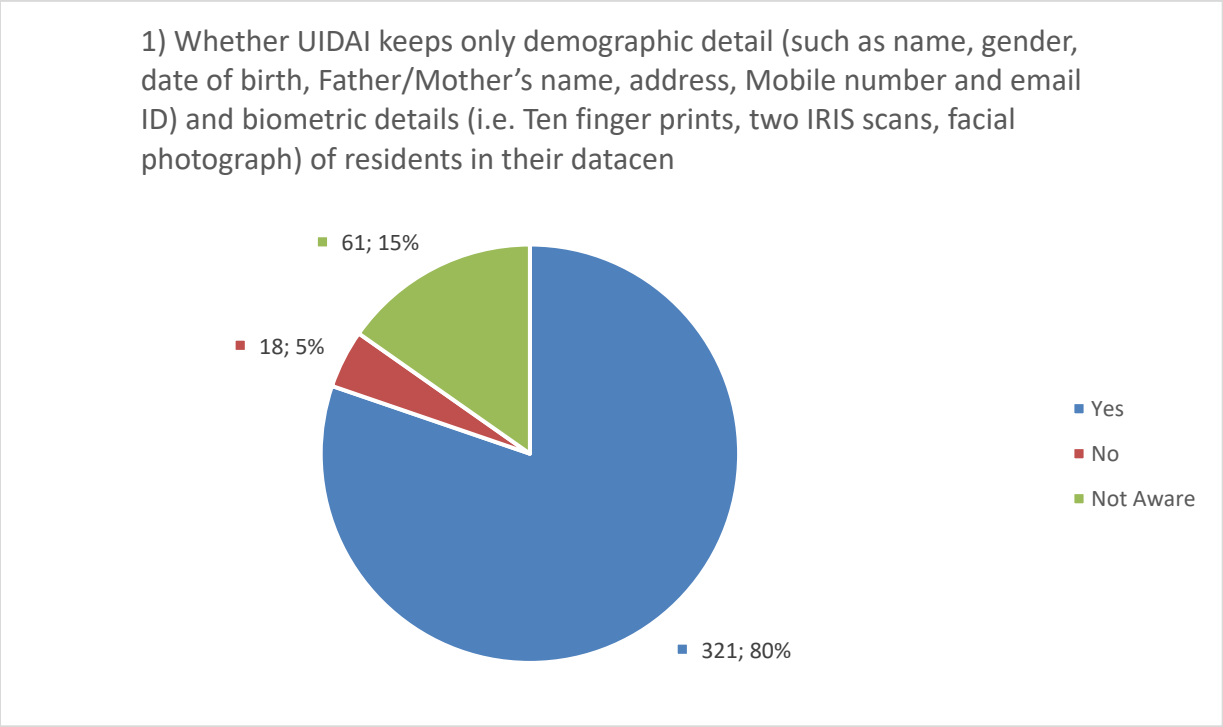
Table 4.2: Summary of responses of questionnaire set B

Sl No	Questions	Number of Responses			
		YES	NO	Not aware	Total
1.	Whether UIDAI keeps only demographic detail (such as name, gender, date of birth, Father/Mother's name, address, Mobile number and email ID) and biometric details (i.e. Ten finger prints, two IRIS scans, facial photograph) of residents in their datacentre?	321	18	61	400
2.	Whether UIDAI keeps other personal detail like health records, family, caste, religion, education, etc. in their datacentre?	14	324	62	400
3.	Whether UIDAI keeps the details of profession, business, property details financial, bank detail, PAN, shares, mutual funds, etc in their datacentre?	16	301	83	400
4.	Do you think UIDAI tracks our activities?	8	348	44	400
5.	Whether UIDAI receives or collects your bank, investments, insurance etc. details?	18	318	64	400
6.	Are you aware that the Aadhaar Act 2016 has been passed by Parliament?	392	0	8	400
7.	Are you aware that Section 32(3) of the Aadhaar Act 2016 prohibits UIDAI from controlling, collecting, keeping or maintaining any information about the purpose of authentication?	293	26	81	400
8.	Are you aware that Regulation 17(1)(a) of the Aadhaar (Authentication) Regulations 2016, strictly prohibits any requesting entity which includes mobile phone companies, banks etc from storing, sharing or publishing the finger-prints for any reason whatsoever?	293	26	81	400
9.	When you link your bank accounts, shares, mutual funds and your mobile phones with Aadhaar, will UIDAI get these information?	48	280	72	400
10.	Do you know that when you link your bank accounts, shares, mutual funds and your mobile phones with Aadhaar UIDAI only responds to the verification requests by replying either 'Yes' or 'No' and in few cases, if the verification answer is 'Yes', your basic KYC details (name, address, photo etc) available with UIDAI, are sent to the service provider for	319	34	47	400

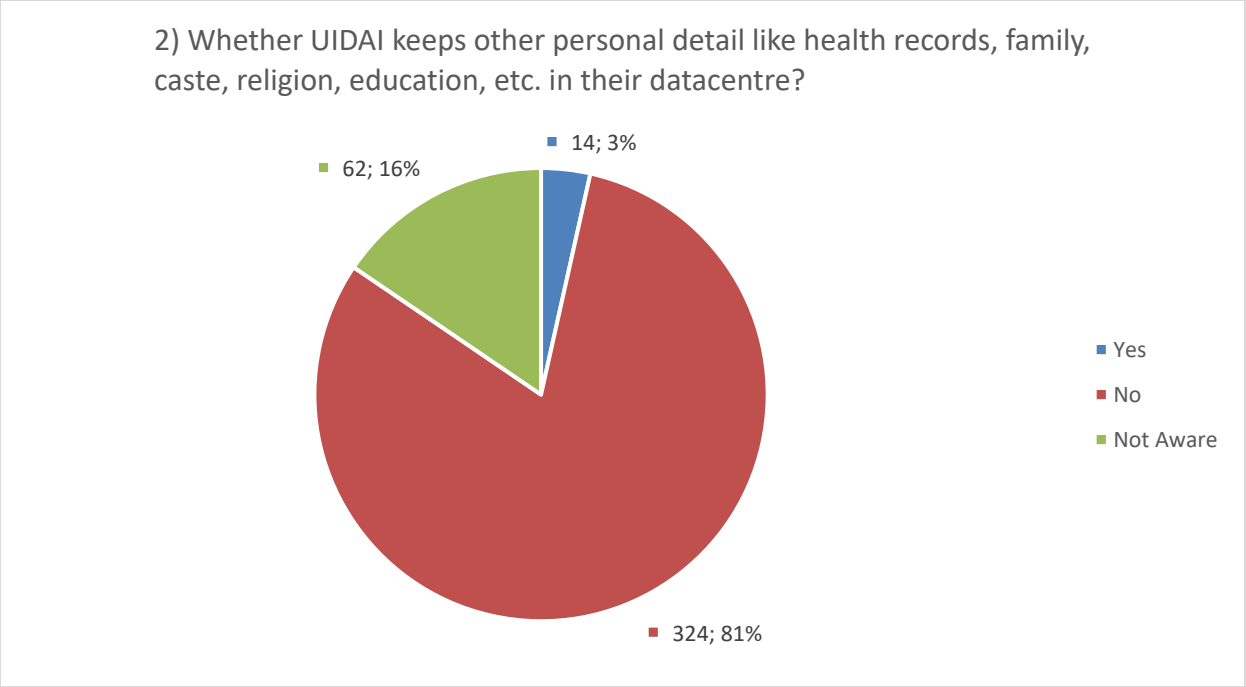
	authentication only.				
11.	Whether your Aadhaar data has been misused ever?	2	352	46	400
12.	Whether UIDAI data center storing Aadhaar data is robust?	292	17	91	400
13.	Whether UIDAI data center storing Aadhaar data is secure?	292	17	91	400
14.	Whether the linking/sharing of Aadhaar number with your bank accounts, shares, mutual funds and your mobile phones etc. has any threat to your privacy?	46	266	88	400
15.	Are you aware about the provision of Security and confidentiality of information and Restriction on Sharing information under Aadhaar Act 2016?	286	26	88	400
16.	Are you aware about the provision of Penalty & Punishment under Aadhaar Act 2016 for impersonation of Aadhaar data, disclosing Identity information, unauthorised access to the Central Identities Data Repository etc.?	286	26	88	400
17.	Whether Aadhaar is a threat to your privacy?	8	348	44	400
18.	Do you think Aadhaar is a unique identity for any resident?	392	0	8	400
19.	Do you think Aadhaar is robust enough to eliminate duplicate and fake identities?	350	6	44	400
20.	Do you think Aadhaar should be made mandatory for all residents of India?	393	7	0	400

4.4 Analysis of Responses:

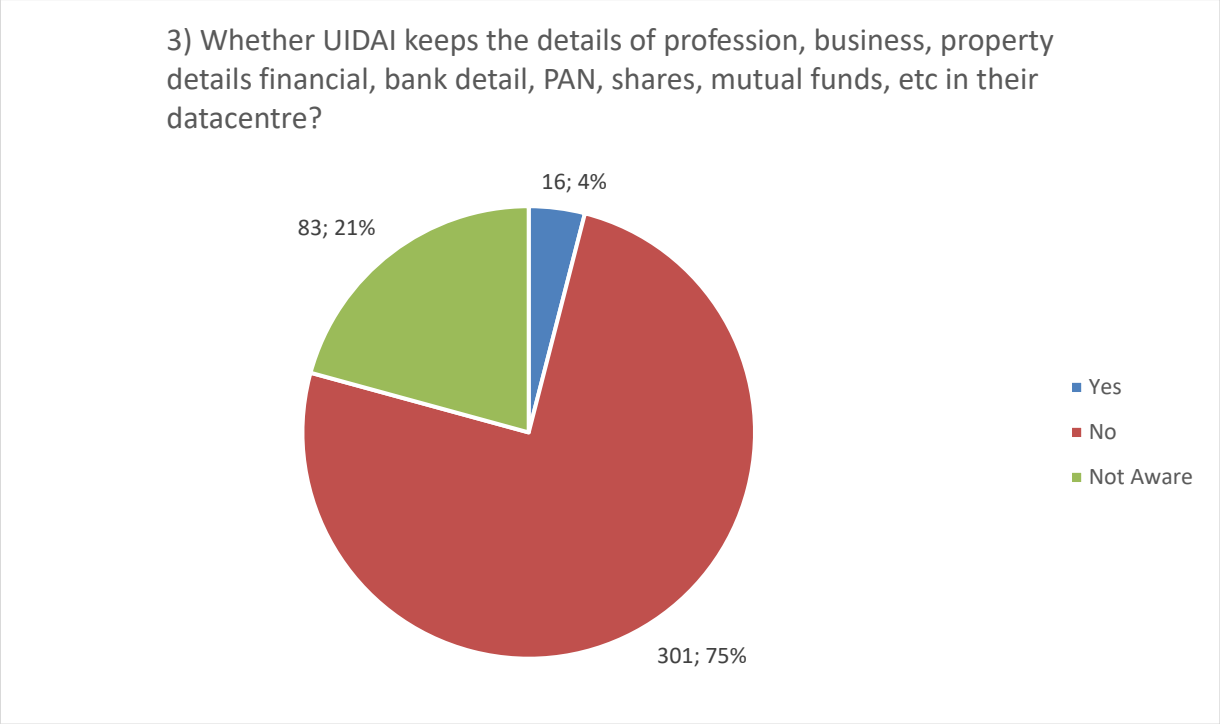
This survey was mainly focused to assess the awareness of the public regarding the information being collected by UIDAI for unique Aadhaar number following the Privacy principle of minimum data collection of each resident. Accordingly, first 3 question were framed. The response indicates that at least 20-25% (i.e. approx. one fourth to one fifth) people are not aware about what data are being collected and what are not collected. Further, 4-5% people think that their personal/sensitive data like health record, professional records, financial details, bank details etc. are being recorded in the UIDAI system. This may be the concern of some population and they may be advocating against the Aadhaar. The pictorial Pie graph for the first three response are given below – Graph 4.1 to Graph 4.3 respectively.



Graph 4.1: Pictorial Pie chart of response to question number 1 of set B



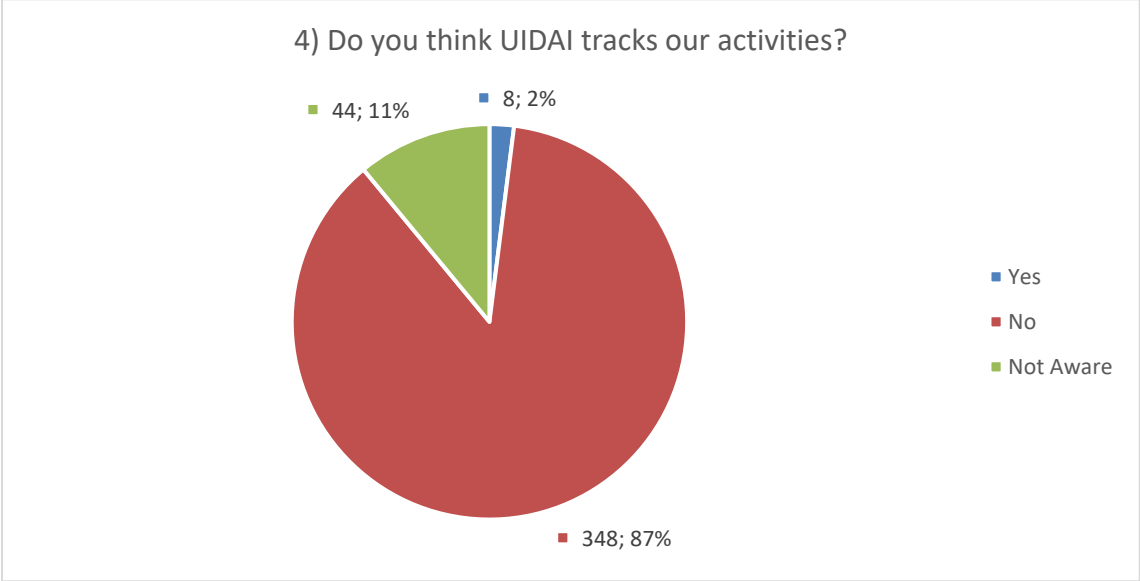
Graph 4.2: Pictorial Pie chart of response to question number 2 of set B



Graph 4.3: Pictorial Pie chart of response to question number 3 of set B

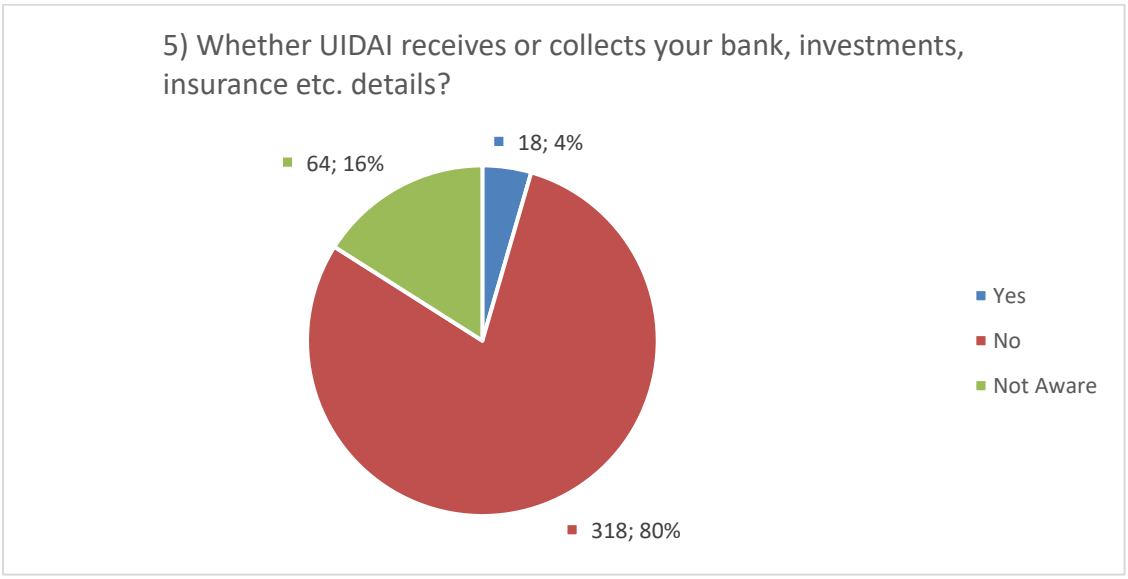
- It is important that more than only 2% respondent thinks that their activities are being tracked and 11% people are unaware. However, 87% people are aware that UIDAI does

not track their activity so this may be good for the system. The Pie graph for this response is given below in Graph 4.4.



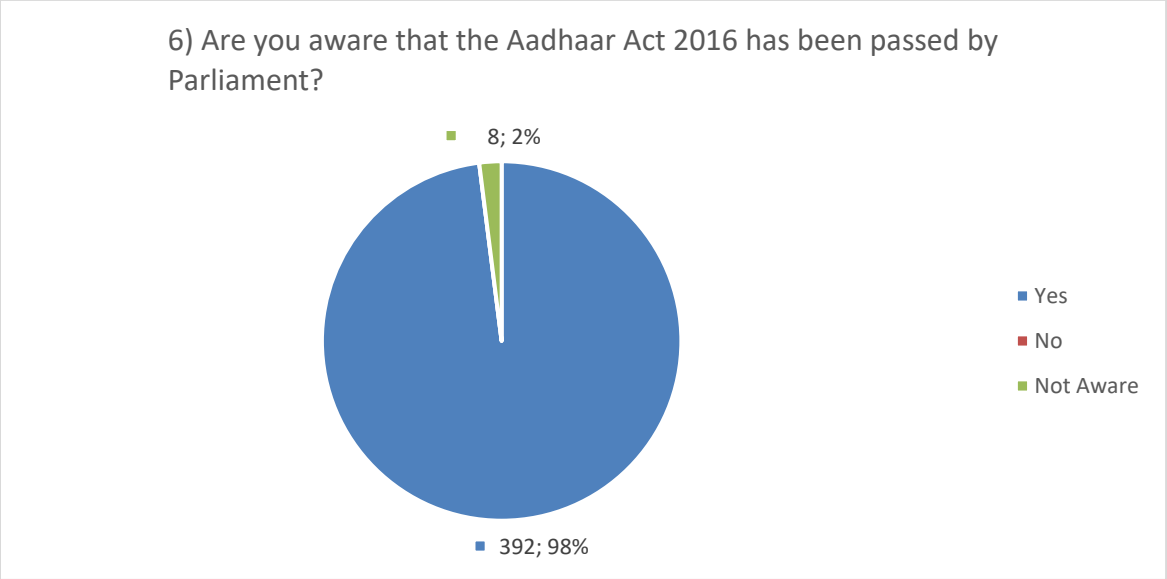
Graph 4.4: Pictorial Pie chart of response to question number 4 of set B

- Only 80% people are aware that UIDAI does not receive or collect their financial details, however, approx. 4% respondents think that UIDAI receives/ collects their financial details and 16% respondents are unaware. This may be deterrent to link Aadhaar with such institution. The Pie graph for this response is given below in Graph 4.5.



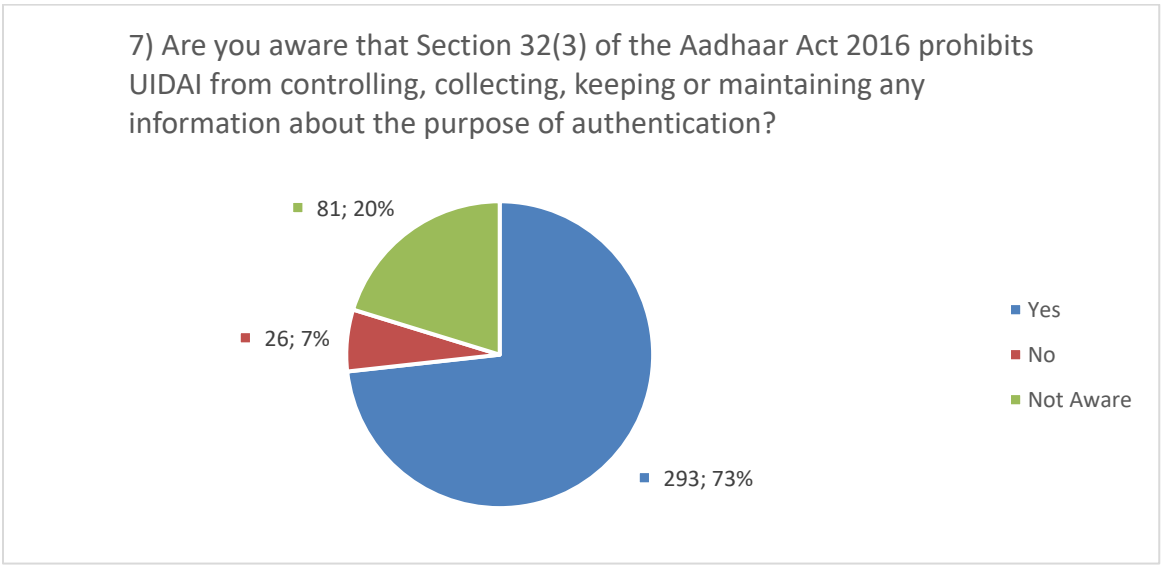
Graph 4.5: Pictorial Pie chart of response to question number 5 of set B

- The Pie graph for the response regarding Aadhaar Act 2016 is given below in Graph 4.6, shows that most of the respondents i.e. more than 98% are aware that Act has been passed.



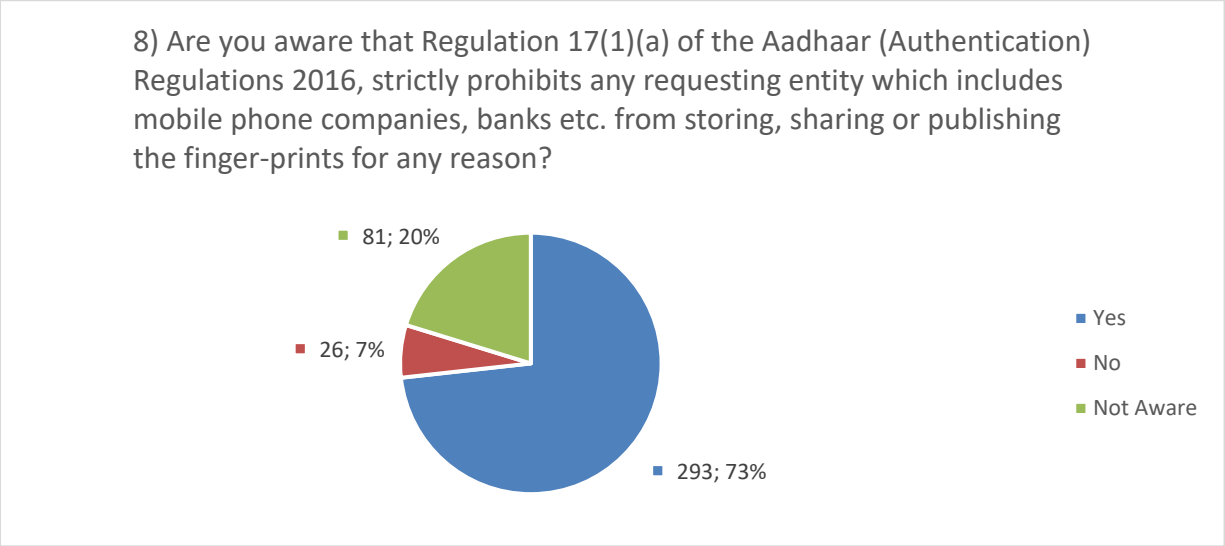
Graph 4.6: Pictorial Pie chart of response to question number 6 of set B

- It is important that more than 98% are aware that Aadhaar Act 2016 has been passed but only 73% respondent are aware about the provision of Section 32(3) of the Aadhaar Act 2016 which prohibits UIDAI from controlling, collecting, keeping or maintaining any information about the purpose of authentication. The Pie graph for this response is given below in Graph 4.7.



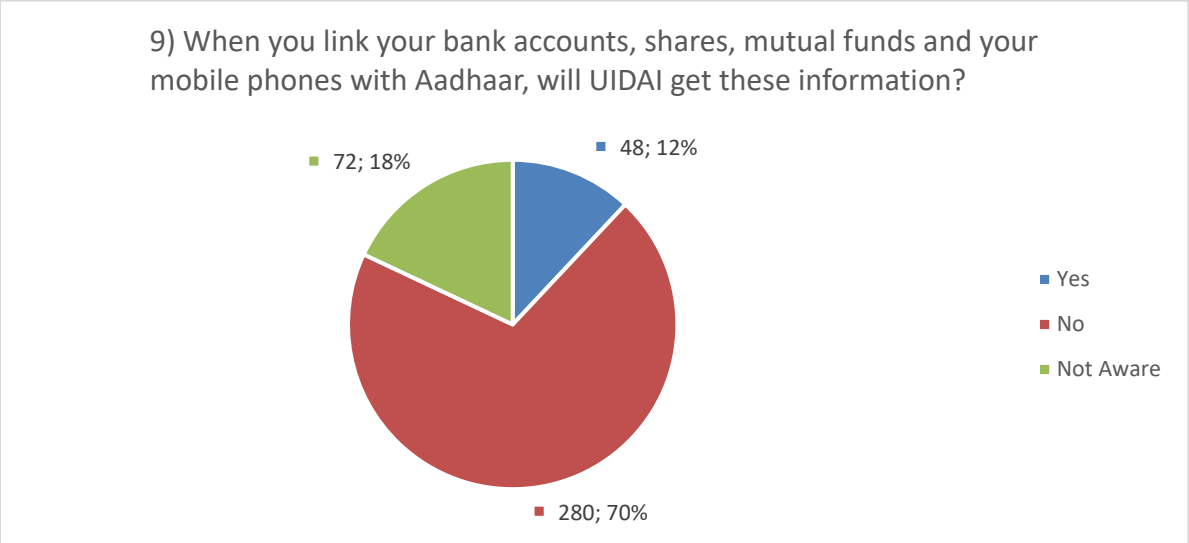
Graph 4.7: Pictorial Pie chart of response to question number 7 of set B

- It is observed that approx. 27% respondent are not aware about the Regulation 17(1)(a) of the Aadhaar (Authentication) Regulations 2016 which strictly prohibits any requesting entity which includes mobile phone companies, banks etc. from storing, sharing or publishing the finger-prints for any reason. The Pie graph for this response is given below in Graph 4.8.



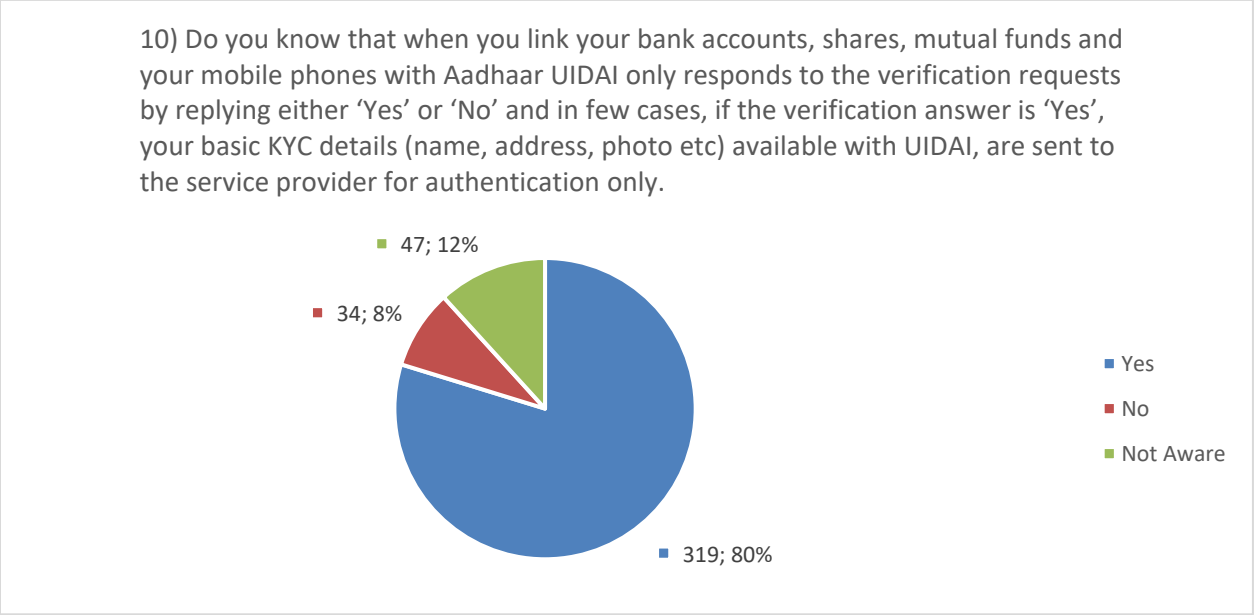
Graph 4.8: Pictorial Pie chart of response to question number 8 of set B

- Only 70% people are aware that UIDAI does not get information on linking of their bank accounts, shares, mobile phones etc. with Aadhaar, however, approx. 12% respondents think that UIDAI get their information and 18% respondents are unaware. This may be deterrent to link Aadhaar with such institution. The Pie graph for this response is given below in Graph 4.9.



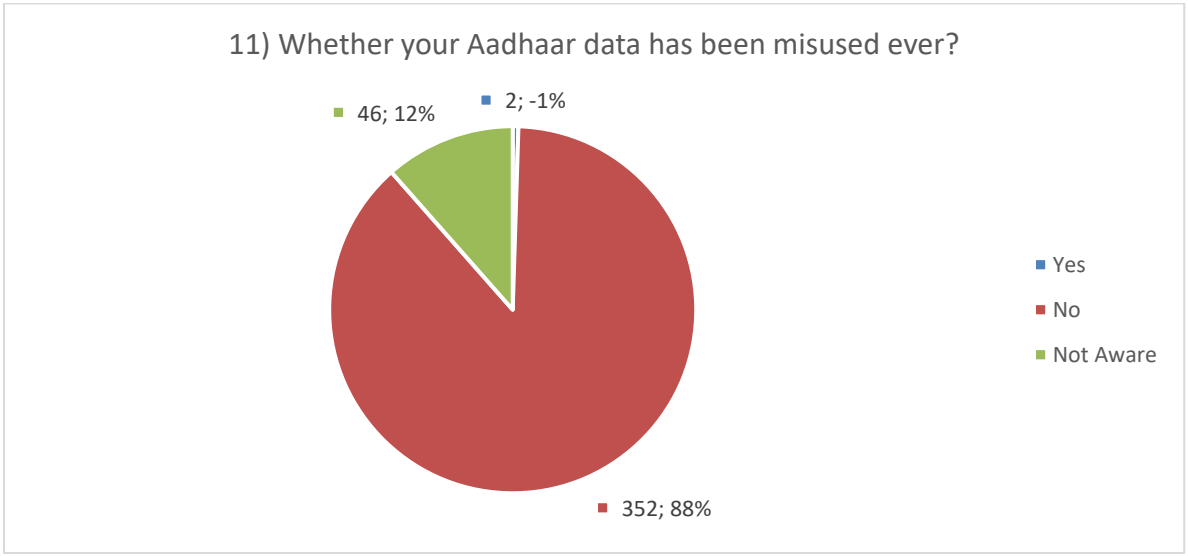
Graph 4.9: Pictorial Pie chart of response to question number 9 of set B

- Approx. 80% respondents are aware about the Authentication & KYC process for services, however, 20% respondents do not unaware. The Pie graph for this response is given below in Graph 4.10.



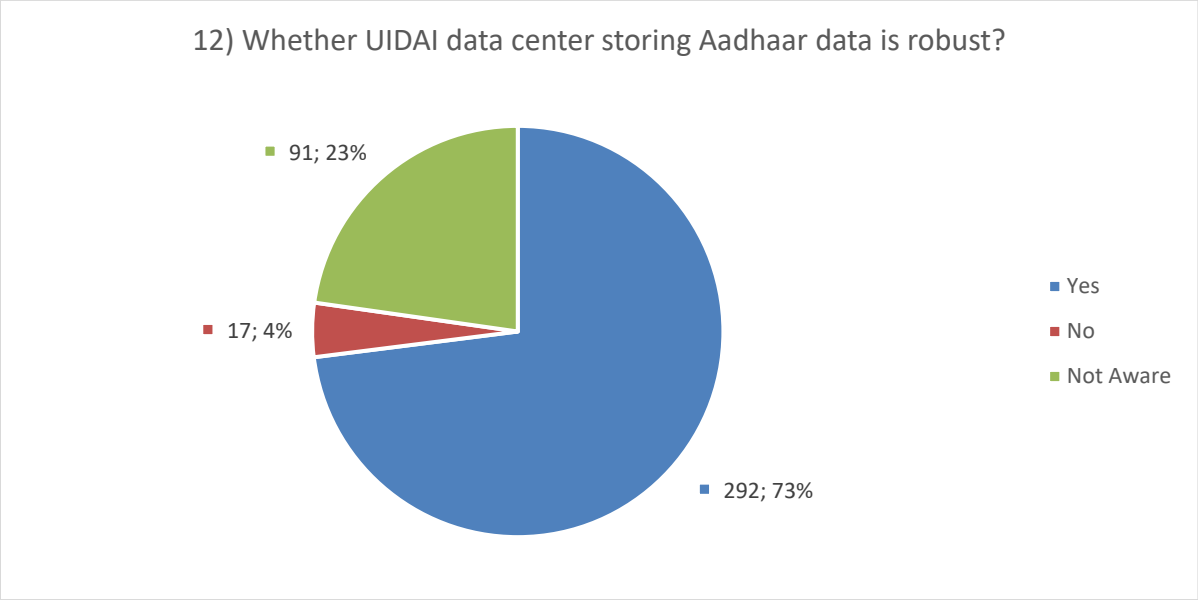
Graph 4.10: Pictorial Pie chart of response to question number 10 of set B

- One of the most important observation that approx. no one (less than 1%) mentioned that their Aadhaar is misused. 88% respondents mentioned that their Aadhaar never misused and 12% do not aware. The Pie graph for this response is given below in Graph 4.11.



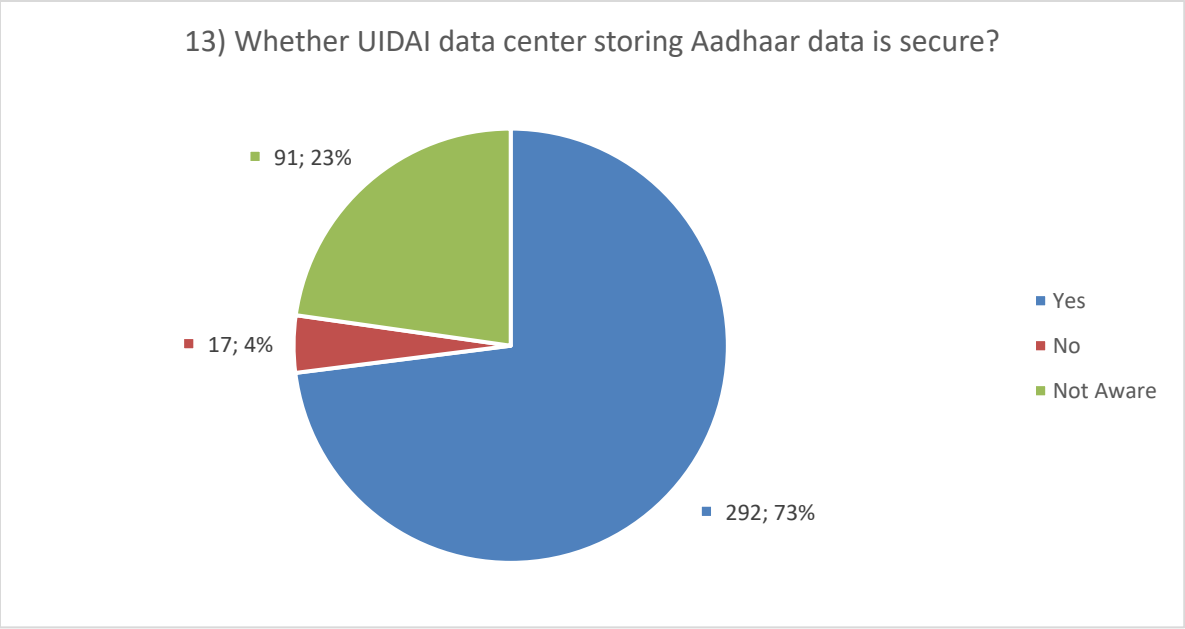
Graph 4.11: Pictorial Pie chart of response to question number 11 of set B

- More than 73% respondents agreed that Aadhaar datacenter is robust enough but 4% did not agree on same and 23% respondents are unaware. This indicates that people need to be taken into confidence that datacenter is foolproof. The response is given below in Graph 4.12.



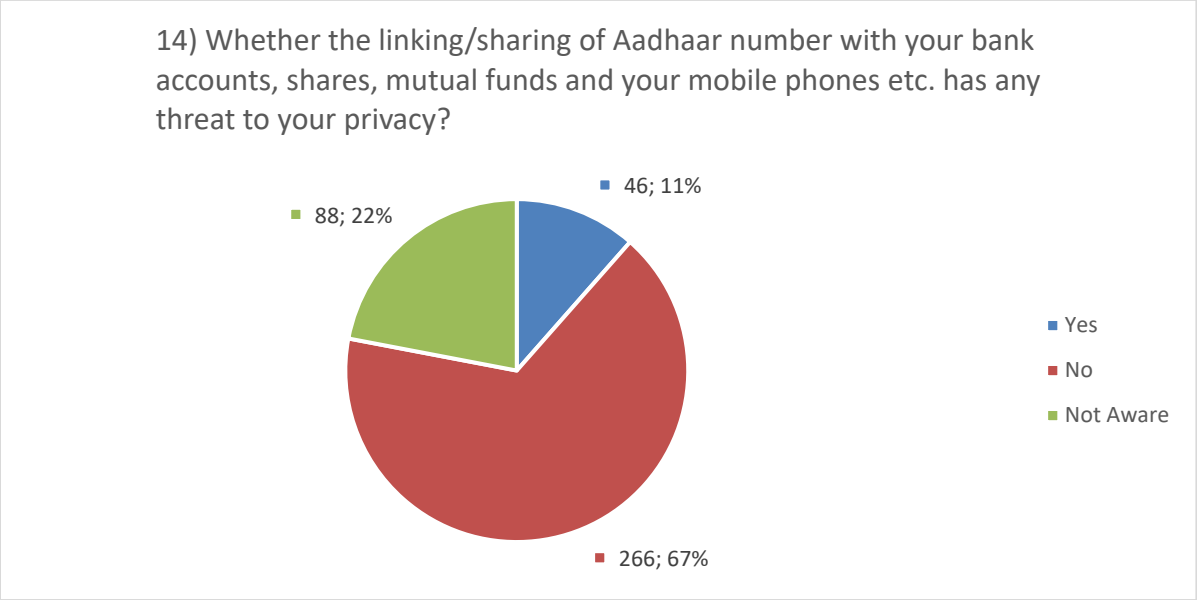
Graph 4.12: Pictorial Pie chart of response to question number 12 of set B

- Only 73% respondents agreed that Aadhaar datacenter is secure but 4% did not agree and 23% respondents are unaware security of datacenter. This indicates that people need to be taken into confidence that the datacenter is secure. The for response is given below in Graph 4.13.



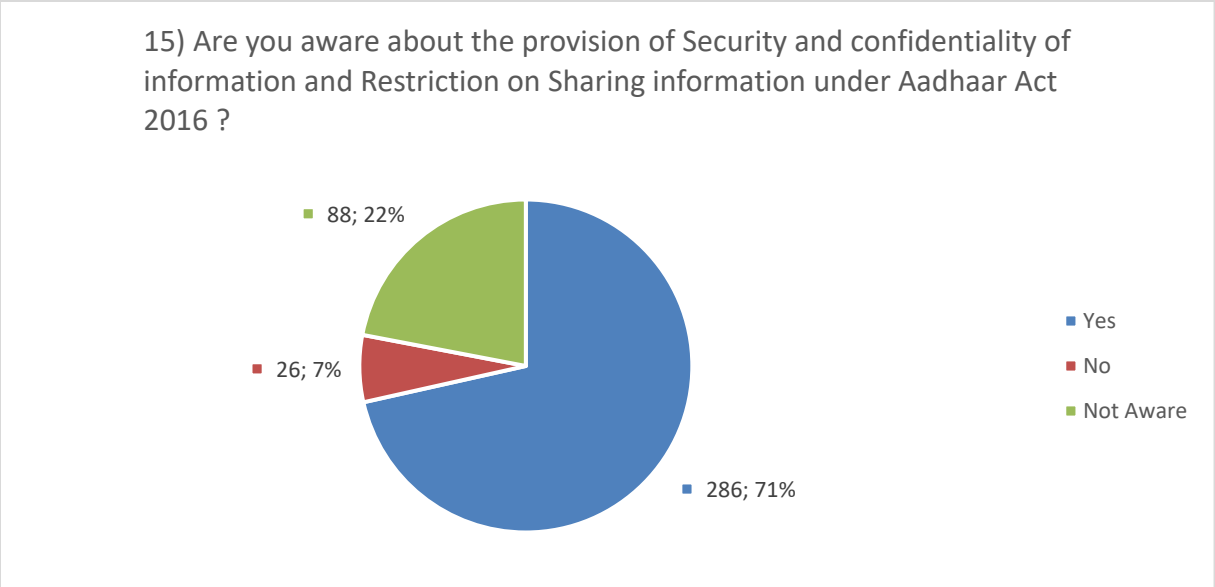
Graph 4.13: Pictorial Pie chart of response to question number 13 of set B

- Approx. 11% respondents think that linking/sharing of Aadhaar number with bank, shares, mobile phones etc. has threat to their privacy however, 67% respondents do not think so and 22% respondents are unaware. The Pie graph for this response is given below in Graph 4.14.



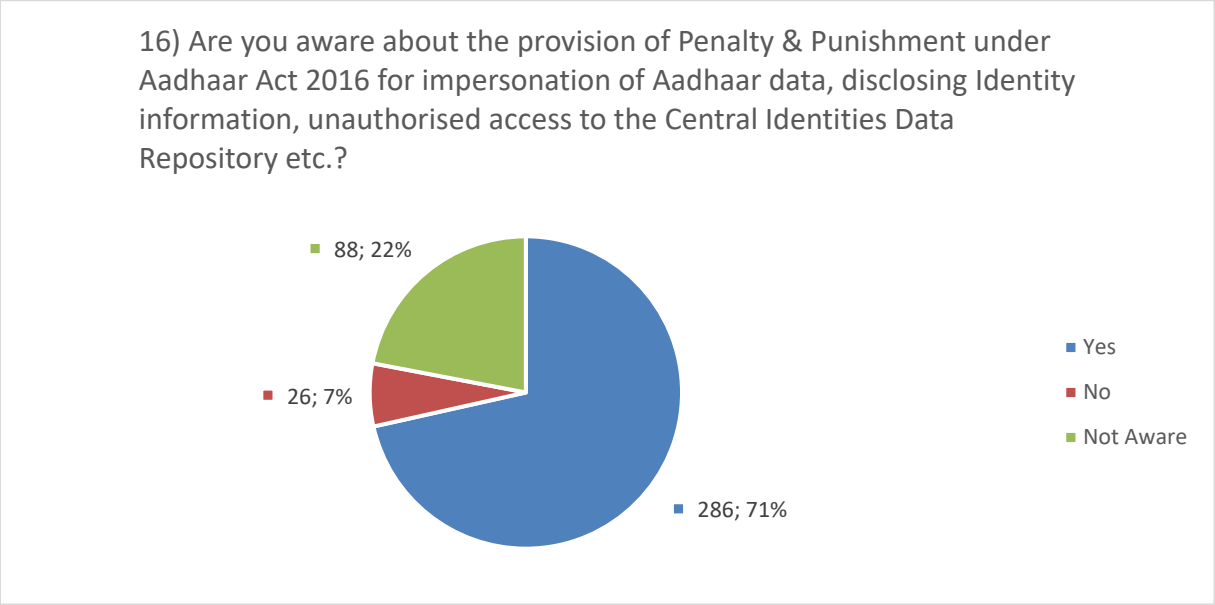
Graph 4.14: Pictorial Pie chart of response to question number 14 of set B

- It is observed that approx. 29% (22% & 7%) respondents are not aware about the provision of Security and confidentiality of information and Restriction on Sharing information under Aadhaar Act 2016. The Pie graph of response is given below in Graph 4.15.



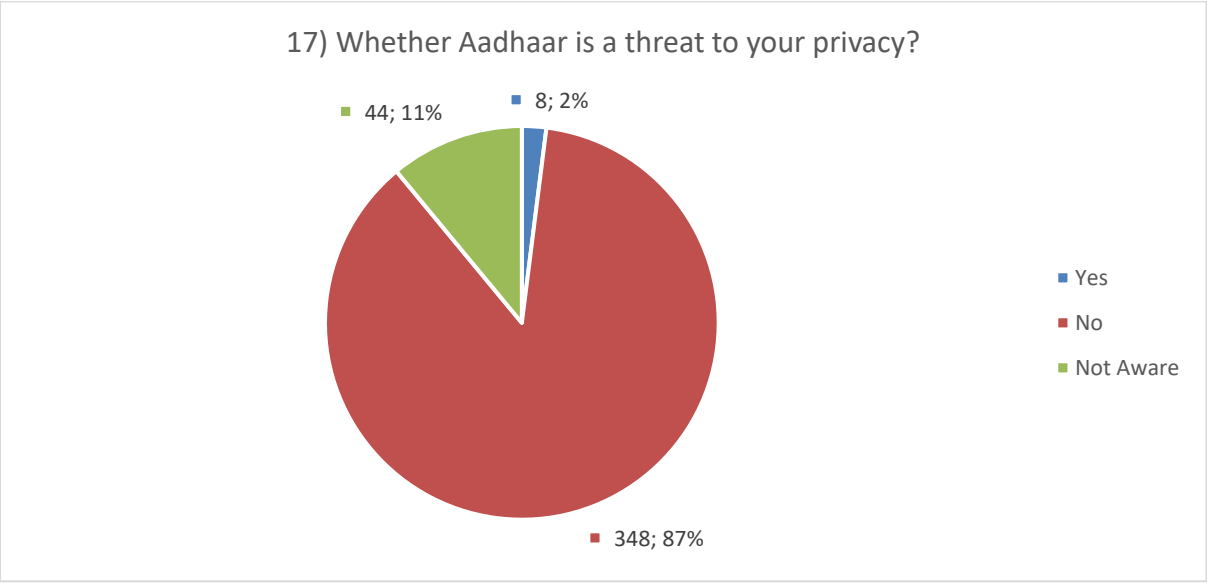
Graph 4.15: Pictorial Pie chart of response to question number 15 of set B

- Only 71% respondents are aware about the provision of Penalty & Punishment under Aadhaar Act 2016 for impersonation of Aadhaar data, disclosing Identity information, unauthorised access to the Central Identities Data Repository etc. and 29% are not aware. The Pie graph of response is given below in Graph 4.16.



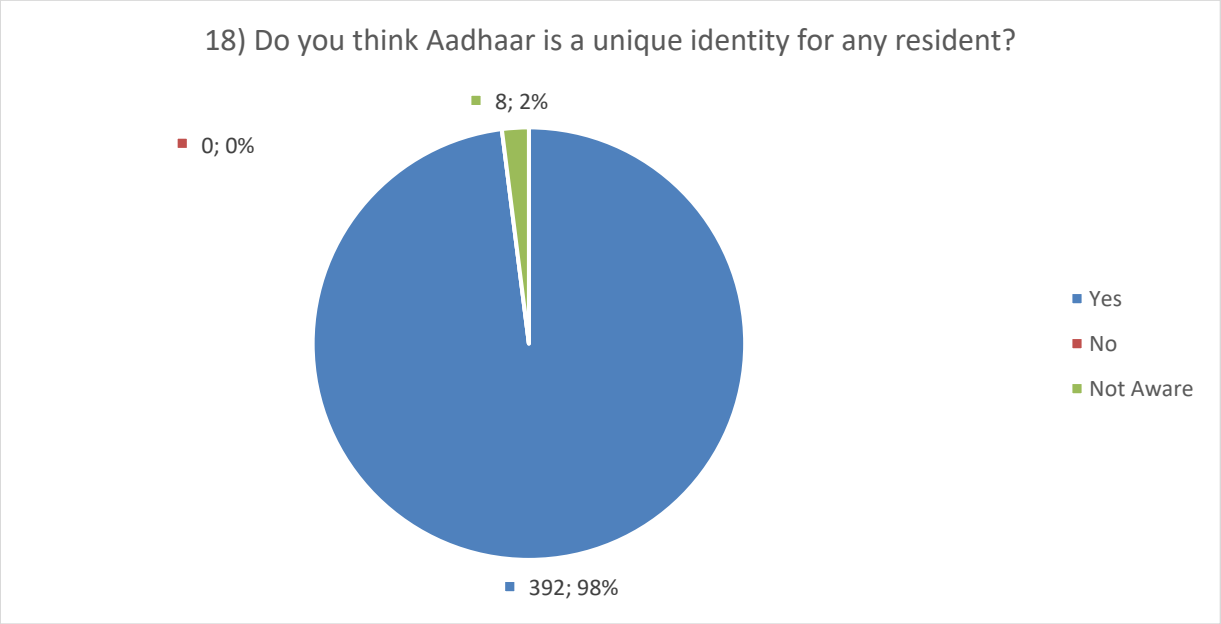
Graph 4.16: Pictorial Pie chart of response to question number 16 of set B

- Only 2% respondents agree that Aadhaar is a threat to privacy, however 87% did not agree and 11% are unaware about privacy. So, it can be taken that 98% respondents do not see Aadhaar as threat to privacy. The Pie graph of response is given below in Graph 4.17.



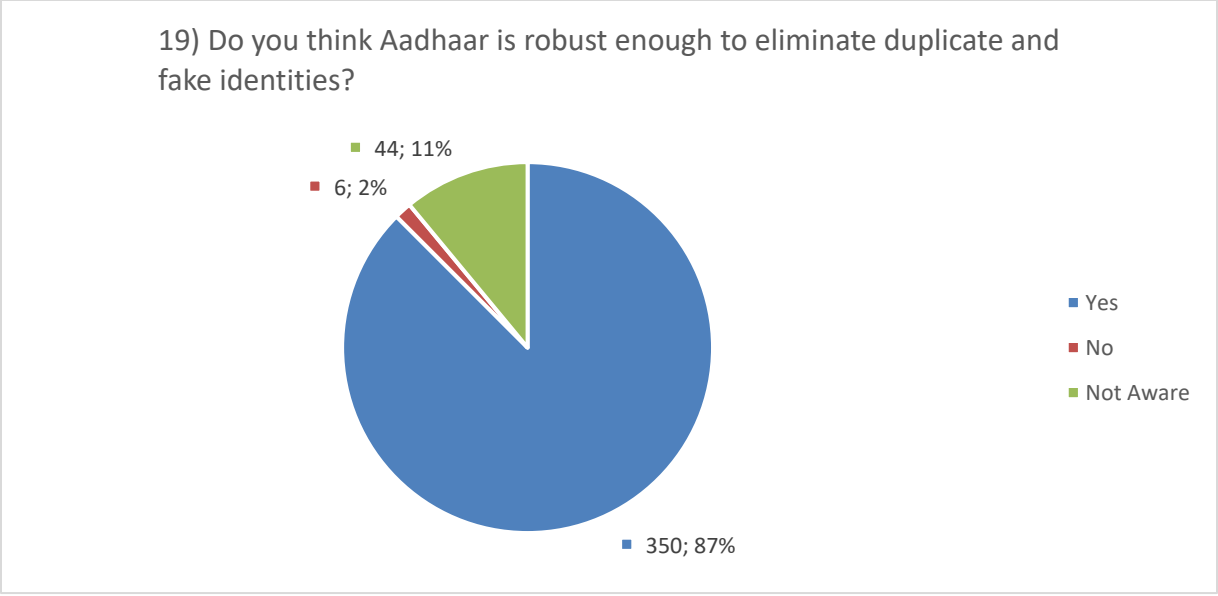
Graph 4.17: Pictorial Pie chart of response to question number 17 of set B

- 98% respondents opined that Aadhaar is Unique Identity of residents and no one disagree but 2% respondents are not aware about uniqueness. The Pie graph of response is given below in Graph 4.18.



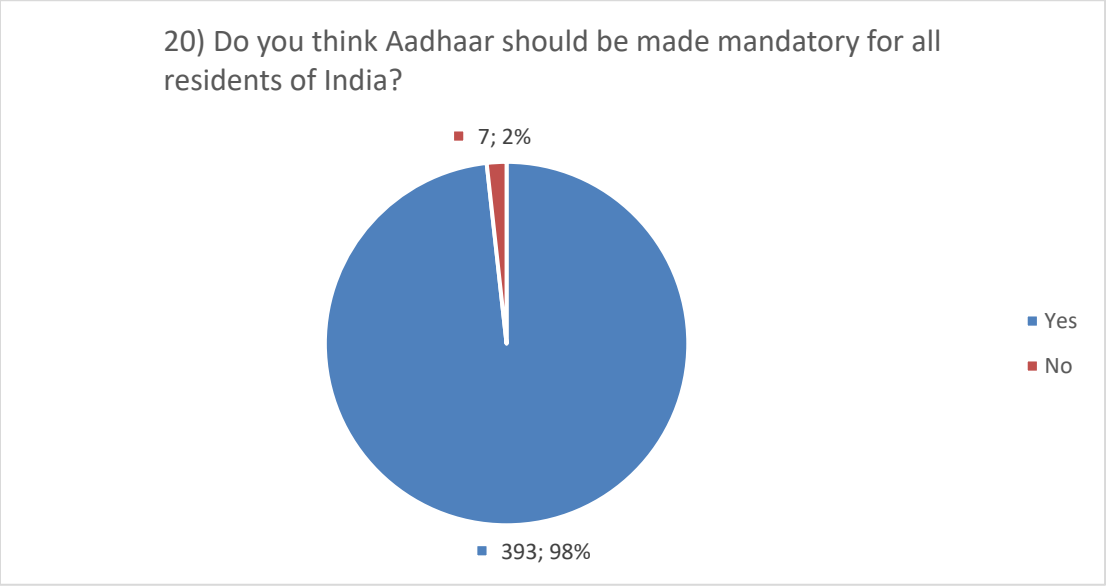
Graph 4.18: Pictorial Pie chart of response to question number 18 of set B

- 87% respondents agreed that Aadhaar is robust enough to eliminate duplicate and fake identities and only 2% do not agree with this. However, 11% said not aware. The Pie graph of response is given below in Graph 4.19.



Graph 4.19: Pictorial Pie chart of response to question number 19 of set B

- Most important observation is that nearly all 98% (except 2%) respondents agreed that Aadhaar should be made mandatory and only the 2% were disagree, this may be due to the observations of their concerns on the issues of linking of Aadhaar with service providers. The Pie graph of response is given below in Graph 4.20.



Graph 4.20: Pictorial Pie chart of response to question number 20 of set B

4.5 Observations and Findings

4.5.1 Based on the response of questionnaire set-A for assessment of standards and basic security measures, indicative observations may be given as below:

i. The Aadhaar datacenter sites are meeting the requirement of International standards of uptime, quality standards etc. It is also following Information security standards, Building, cabling etc.

ii. The datacenter follows the International standards of physical Access to the equipment and equipment's rooms.

iii. The security equipment like Firewalls, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) etc. have been deployed in Aadhaar datacenter in order to

strength the security of datacenter. Being security a dynamic phenomenon, the security measures are being updated regularly to protect from latest security threats.

iv. A security policy for Access & Authorization and Password policy for different equipment have been implemented.

v. The concept of zoning of network like Secure zone, demilitarized zone and open zone etc. has been implemented at Data center. Therefore, the CIDR is not accessible from outside of Aadhaar network.

vi. A Security Policy defining security procedures & guidelines has been laid down for Aadhaar datacenter and being updated by on Regular basis. Audit are also being carried to ensure the same.

4.5.2 Following are the key finding based on the discussion & Interview with UIDAI Officials-

Building Safety and Security: The UIDAI datacenter building having Central Identities Data Repository (CIDR) are meeting all the standards of strength, fire-resistant etc. requirement of international datacenter. The equipment and manpower have been deployed to meet the surveillance requirement of security challenge of Building. Further, there is similar secondary datacentre in Bengaluru to meet any disaster situation as well.

Access and Authorization: Datacenter is equipped with different kind of management **system** for Building Management, Access Management, Security Management, other Infrastructure management etc.. Unauthorised access are not allowed. The access to different datacenter area is electronically controlled and allowed as per authorization role defined in the system and all such access are well captured in the system.

Data Storage and Process: The chances of data breaches are manifold when servers are connected to the outside world via the Internet. However, CIDR of UIDAI have no connection or link with the outside world through Internet. Aadhaar data is stored and processed within its own datacentre.

Security equipment of the datacenter: The UIDAI data center is world class datacenter and all kind of security equipment like Intrusion detection system, Intrusion Prevention System, Firewall etc. with state of art technology have been deployed.

Physical Protection of Data: UIDAI ensures the physical protection of datacentre through robust testing of hardware. Hardware supplies are tested twice to identify and plug defects, if any. The biometric image data captured during Aadhaar enrolment is not in the possession of the solutions provider or its employees. The apps running on the IT hardware of UIDAI are well-protected through intrusion and firewall prevention system.

Security practices followed by UIDAI: UIDAI constantly strengthens and reviews its infrastructure and ecosystems in line with the best international security practices and technological standards and has multi-layered security and privacy considerations built into the core strategy of Aadhaar with three basic doctrines of minimal information, optimal ignorance and federated database which give higher level of security to the data.

Safety to prevent threat from the vendors of technology: To prevent leakage of sensitive data, the Aadhaar platform hinges largely on open-source technology. Deployment of propriety technology ensures the protection of data from private contractors and third-party vendors. Aadhaar data is encrypted using PKI-2048 and AES-256. These are one of the most robust public key cryptography encryptions. Each enrolment data packet is stored in PKI encrypted form, ensuring that no system or person

has access to these packets. Each Aadhaar data has a built-in mechanism to detect any kind of tampering.

Scalability, Performance and availability of System: The technology is based on principles of openness, linear scalability with five 9 availability features. As per UIDAI, no major performance issue has been observed while enrolment has crossed 1.22 billion.

Data protection and privacy measures: The UIDAI accepts obligation to ensure the security and confidentiality of the data collected. The data are being collected on software provided by the UIDAI and encrypted to prevent leaks in transit. The UIDAI has a security policy to ensure the safety and integrity of its data. There are security and storage protocols in place. Penalties for any security violation are severe and include penalties for disclosing identity information.

Protections of the right to privacy of the resident: In order to protect the interest of the resident, UIDAI follow the principle of privacy-

- **Collection of limited personal information:** The UIDAI is collecting only basic data fields - Name, Date of Birth, Gender, Address, Parent/ Guardian's (name essential for children but not for others) photo, 10 finger prints and iris scan.
- **No profiling and tracking information collected**: The UIDAI policy bars it from collecting sensitive personal information such as religion, caste, community, class, ethnicity, income and health. The profiling of individuals is therefore not possible through the UID system.

- **Release of information – yes or no response**: The UIDAI does not reveal personal information in the Aadhaar database; the only response is being given by 'yes' or 'no' to the requests to verify an identity.
- **Convergence and linking of UIDAI information to other databases**: The UID database is not linked to any other databases, or to information held in other databases. Its only purpose is to verify a person's identity at the point of receiving a service, and that too with the consent of the Aadhaar number holder. The data will be secured with the best encryption, and in a highly secure data vault.

Virtual ID (VID): VID is a temporary, revocable 16-digit random number mapped with the Aadhaar number. VID can be used in lieu of Aadhaar number whenever authentication or e-KYC services are performed. Authentication may be performed using VID in a manner similar to using Aadhaar number. It is not possible to derive Aadhaar number from VID.

Locking of Biometric Details- To protect the potential misuse of biometrics, UIDAI has introduced a new security feature where one can lock his/her biometric data. With the help of Aadhaar biometric locking system, Aadhaar holders can lock and temporarily unlock their biometrics. They can do it from the official website of UIDAI. This feature ensures that no one can access biometrics of an Aadhaar holder without his/her consent.

4.5.3 **Observations/Findings from Discussion & Interview with Technical Experts:** Following are the observation and finding experts from discussion with representatives of different organisations i.e. TEC, DOT, MeITY, BSNL, TRAI, NSN & TCS-

- Aadhaar datacenters are following international standards with latest technology/ architecture.

- The UIDAI data center is world class datacenter and all kind of security equipment like Intrusion detection system, Intrusion Prevention System, Firewall etc. have been deployed.
- All the international standards of datacenter have been followed by UIDAI for its datacenter keeping in view of critical data of residents are stored in CIDR.
- UIDAI is following the requisite security measures and Principle of Privacy.
- UIDAI datacentre is robust and foolproof. There may not be issue of security and privacy with Aadhaar data.

4.5.4 As per an affidavit filed by UIDAI[1] before a bench of Justice S Ravindra Bhat and Justice Prateek Jalan:

- All reports of data breaches were misleading and false.
- UIDAI database i.e. Central Identity Data Repository (CIDR) had not been breached as existing security controls and protocols were "robust and capable of countering any such attempts or malicious designs of data breach or hacking".
- The data is fully secured/encrypted at all times i.e., at rest, in transit and in storage.
- UIDAI has taken fool-proof measures to ensure end-to-end security of resident data, spanning from full encryption of resident data at the time of capture, tamper resistance, physical security, access control, network security, stringent audit mechanism, 24/7 monitoring and measures such as data partitioning and data encryption with UIDAI controlled data centres.

[1] Aadhaar breach reports are misleading: UIDAI to court https://www.hindustantimes.com/india-news/aadhaar-breach-reports-are-misleading-uidai-to-court/story-CUnRdOBOoDz6Zxw6U3nmZL.html

4.5.5 **Observations and Findings from survey Responses of Questionnaire Set-B:** The observations and findings are summarized as below-

- From the responses of all questions, it is observed that there is significant lack of awareness as the target segment have been selected from educated society even though there is minimum 10% (in some cases upto 25%) respondents have mentioned as "not aware" for most of the questions.
- The response indicates that at least 20-25% (i.e. approx. one fourth to one fifth) people are not aware about what data are being collected and what are not being collected by UIDAI. Further, 4-5% people think that their personal/sensitive data like health record, professional records, financial details, bank details etc. are being recorded in the UIDAI system. This may be the concern of some population.
- Approx. 20% respondent do not aware that UIDAI does not receive or collect their financial details so this may be deterrent to link Aadhaar with such institution. Similarly, 30% people are not aware that UIDAI does not get information on linking of their bank accounts, shares, mobile phones etc. with Aadhaar. This may be deterrent to link Aadhaar with such institution.
- It is good that more than 98% are aware that Aadhaar Act 2016 has been passed but a significant population, approx. 27% respondent are not aware about the provision of Section 32(3) of the Aadhaar Act 2016 which prohibits UIDAI from controlling, collecting, keeping or maintaining any information about the purpose of authentication.
- Similarly, approx. 27% respondent are not aware about the Regulation 17(1)(a) of the Aadhaar (Authentication) Regulations 2016 which strictly prohibits any requesting entity

which includes mobile phone companies, banks etc. from storing, sharing or publishing the finger-prints for any reason.

- Approx. 27% respondents are not aware that Aadhaar datacenter is robust enough and secure. This indicates that people need to be taken into confidence that datacenter is foolproof.
- It can be said that approx. 98% respondents agree that UIDAI does not track their activity and only 2% respondent thinks that their activities are being tracked.
- One of the most important observation that nearly all responses (except 2 out of 400) can be considered as their Aadhaar is never misused.
- It is observed that approx. 29% (22% & 7%) respondents are not aware about the provision of Security and confidentiality of information and Restriction on Sharing information under Aadhaar Act 2016. Similarly, they are also not aware about the provision of Penalty & Punishment under Aadhaar Act 2016 for impersonation of Aadhaar data, disclosing Identity information, unauthorised access to the Central Identities Data Repository etc..
- Only 2% respondents agree that Aadhaar is a threat to privacy, however 87% do not agree and 11% are unaware about privacy. However, it is important to note that Approx. 33% respondents are not aware that the linking/sharing of Aadhaar number with bank, shares, mobile phones etc. has no threat to their privacy.
- 98% respondents opined that Aadhaar is Unique Identity of residents and no one disagree but 2% respondents are not aware about uniqueness. But only, 87% respondents agreed

that Aadhaar is robust enough to eliminate duplicate and fake identities and 2% do not agree with this and 11% said not aware.

- Most important observation is that nearly all 98% (except 2%) respondents agreed regarding Aadhaar should be made mandatory for all residents of India. Only 2% disagree, this may be due to the issues of privacy observation while linking of Aadhaar with service providers and due to unawareness about provisions of Aadhaar Act and other Regulations and measures taken by UIDAI.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusions of study

5.1.1 Security and Privacy Aspect

i. The UIDAI datacenter building having Central Identities Data Repository (CIDR) are meeting international standards of strength, fire-resistant etc. requirement of international datacenter. The equipment and manpower have been deployed to meet the surveillance requirement of security challenges of infrastructure. Further, there is similar secondary datacentre in Bengaluru to meet any disaster situation as well. So, **it can be concluded that the Aadhaar data of residents stored in CIDR are physically safe including in disaster situations.**

ii. Datacenter is equipped with different kind of Management Systems for Building Management, Access Management, Security Management, other Infrastructure management etc.. Unauthorised access are not allowed. The access to different datacenter area is electronically controlled and allowed as per authorization role defined in the system and all such access are well captured in the system. This means the **Aadhaar data of residents are safe from any unauthorized access**.

iii. The UIDAI data center are having various kind of security equipment like Intrusion detection system, Intrusion Prevention System, Firewall etc. with state of art technology. A security policy like for Access & Authorization for different equipment have been implemented. This means the **Aadhaar datacenter are capable to mitigate different kind of cyber-attacks from external world.**

iv. The concept of zoning of network like Secure zone, demilitarized zone and open zone etc. has been implemented at Data center. CIDR of UIDAI have no connection or link with the outside world through Internet, pen-drives, laptops or any other devices. Therefore, the **CIDR is not accessible from outside of Aadhaar network so data stored in CIDR is secure from any kind of threats from internet world.**

v. A Security Policy defining security procedures & guidelines has been laid down for Aadhaar datacenter and being updated by on Regular basis. Audit are also being carried to ensure the same. However, information about the detail of security policy and audit policy could not be gathered, this may be due to their security policy.

vi. The UID database is not linked to any other databases of any service providers or anyone. Its only purpose will be to verify a person's identity at the point of receiving a service and that too with the consent of the Aadhaar number holder. This indicates that the **protection of data and privacy principle are being followed**.

vii. Aadhaar data is encrypted using PKI-2048 and AES-256. These are one of the most robust public key cryptography encryptions. Each enrolment data packet is stored in PKI encrypted form, ensuring that no system or person has access to these packets. Each Aadhaar data has a built-in mechanism to detect any kind of tampering. This indicates that **data is secure during transition period also.**

viii. The basic concept of security and confidentiality of the data collected have been followed by UIDAI. The data are being collected on software provided by the UIDAI and encrypted to prevent leaks in transit. There are security and storage protocols in place to ensure data security and privacy. This means that **data protection and privacy are ensured in storage and transition**.

ix. The UIDAI collects only basic data fields - Name, Date of Birth, Gender, Address, Parent/ Guardian's (name essential for children but not for others) photo, 10 finger prints and iris scan. The UIDAI does not collect sensitive personal information such as religion, caste, community, class, ethnicity, income, health, financial details etc.. The **profiling and tracking of individuals are not done by** UIDAI.

5.1.2 **Privacy and Acceptability**

i. It is noted from survey that **there is not much issue of privacy and acceptability**. However, due to **unawareness regarding the data being captured / stored by UIDAI**, there is concern among respondents regarding collection and storing of sensitive personal information such as religion, caste, community, income, health, financial details etc. by UIDAI.

ii. Due to lack of awareness, some people thinks that UIDAI does profiling of their data and tracking their activities while they perform any financial transactions etc.. However, people think if they do not link their Aadhaar with service providers (bank etc..) then no tracking is possible. This means that **there is no any issue of Privacy but there is some concern due to lack of awareness.**

iii. Nearly all the respondents opined that Aadhaar is Unique Identity of residents but due to lack of awareness, some people think that Aadhaar is not robust enough to eliminate duplicate and fake identities. Further, nearly all respondents agreed regarding Aadhaar should be made mandatory for all residents of India. This means that **there is no issue of acceptability however, there is need of more awareness about the UIDAI system**.

Summary of conclusion: UIDAI is following the requisite security measures and the Principles of Privacy. The data is fully secured/encrypted at all times i.e., at rest, in transit and in storage. There may not be issue of security and privacy on Aadhaar. There is no any issue in acceptability of Aadhaar also, however, due to lack of awareness about the UIDAI datacenter, Aadhaar Act 2016, Principle and process adopted by UIDAI etc., people have some concerns.

5.2 Recommendations

i. UIDAI needs to educate and inform to residents that Aadhaar system is fully safe and secure. The data protection and privacy of all residents enrolled in Aadhaar system have been ensured.

ii. UIDAI shall inform to larger public that UIDAI collects only basic data i.e. Name, Date of Birth, Gender, Address, Parent/Guardian's, photo, finger prints and iris scan. The UIDAI does not collect sensitive personal information such as religion, caste, community, income, health, financial details etc. The UIDAI never does profiling and tracking of individuals.

iii. The provisions of Aadhaar Act 2016 related to security, data protection, Privacy, provision of penalty etc. needs to be advertised in order to build confidence among common public and to deter person involved in wrong activities by any reason.

iv. The benefit of Aadhaar to every individual and advantages of Aadhaar to the Nation may be informed in order to motivate individuals for registering Aadhaar as well as linking with the different service providers.

v. Open house session may be conducted to create awareness among the public regarding foolproofness of the Aadhaar systems.

vi. The Service providers like Banks, Telecom service providers etc. may be asked to inform their customer that their data are neither being shared to UIDAI nor being collected by

UIDAI. The linking of their account with Aadhaar data will help them only in authentication only.

vii. Further, it is agreed that UIDAI database i.e. Central Identity Data Repository (CIDR) is "robust and capable of countering any malicious attempts of data breach or hacking" and UIDAI is following International Standard practices for maintaining their datacentre & networks. However, the issue of data security in internet domain is very vast and extremely complex, so it is very difficult to avoid and mitigate "always" from "all kind of security threats" being security is a dynamic concept in rapidly changing environment of internet domain. Any data leakage may lead to issue of privacy as well. Therefore, in addition to above action for awareness, following suggestions may be helpful in ongoing security measures:

a) A "**Comprehensive Security Policy**" may be prepared to provide guidelines and directions for the protection of UIDAI's systems against accidental or deliberate damage or destruction; with following core objective-
    - To prevent unauthorised disclosure of information stored or processed on UIDAI's systems (**Confidentiality**)
    - To prevent unauthorised accidental or deliberate alteration of data (**Integrity**)
    - To prevent unauthorised accidental or deliberate destruction or deletion of data necessary for operations (**Availability**)
b) The "C**omprehensive Security Policy"** needs to be reviewed at regular and defined interval say yearly.
c) The "C**omprehensive Security Policy"** shall include at least Physical and Environmental Security Policy, Security Organization Policy, Security Policy for each

of Critical equipment like CIDR, other servers, network equipment of datacenter, Incident Management Procedures, Emergency Procedures / Privileged Ids, Networks Security Policy, Audit policy.

d) Policy statement shall include the "Technical standards" and "Non-technical standards" each with minimum requirements of critical datacentre and good practices of international standards like ISO 9000 for Quality System, ISO 14000 for Environmental Management System, ISO 27001 for Information Security and EN 50600-2 standards for Building, Power distribution, Environmental control, Security systems and Management & operation of systems. Minimum Security requirements are specific security standards, which are essentially to be implemented to safeguard UIDAI's systems.

e) **Physical and Environmental Security Policy**: Aadhaar datacenters are secured from unauthorised access, damage or interference as per observation from input of UIDAI. However, Physical and Environmental Security Policy needs to be laid down so that Physical security measures must always be in place and audited accordingly to ensure the security and integrity of the Aadhaar Systems. It shall define the physical security standards and the environmental controls that will be followed in order to maintain a desired level of protection to the Systems.

f) **Security Policy for Critical Equipment**: A detailed security policy including various security measures, procedures for critical equipment like CIDR etc. need to be prepared, implemented. A clear security policy for equipment like Access & Authorization policy, Access list (based on IP addresses, Port etc.), Filter list, Password policy for different equipment need to be defined and implemented. In order to make security equipment

like Firewall, IDS, IPS etc. more effective, the policies defined on the security equipment shall be updated regularly for revised access lists, filter lists, new signatures etc. as per latest security requirement.

g) **Networks Security Policy**: Networks enable groups of users to share resources and communicate with each other effectively. Unfortunately, this often leads to a security threat to the system. Proper network management controls shall be established to protect networks from attacks by hackers / unauthorised users from within and outside. Network management controls include network protection controls on network servers, network operating systems, network services, login process and system and network logging.

   Network devices like routers, firewalls, switches and modems can increase the exposure to unauthorised access, if not configured properly. There are often situations, where network devices are set up with little or no centralised control or guidelines. This often leads to vulnerability in the network. The network devices must be secured with appropriate logical and physical access controls.

h) **Remote Access Policy**: Remote connections provide a potential for unauthorised access to sensitive information. Therefore, remote access to information must be based on an appropriate level of user identification and authentication. There are different types of authentication method, some of which provide a greater level of protection e.g. the methods based on the use of cryptographic techniques can provide strong authentication. An appropriate authentication method must be selected in order to ensure that unauthorised users do not compromise the security of the network services.

i) **Incident Management Procedures**: Incident management responsibilities and procedures shall be established to ensure quick, effective and orderly response to security incidents. This would help to avoid and minimize the damage from security incidents and malfunctions and help to monitor and learn from security incidents.

j) **Emergency Procedures / Privileged Ids:** The bypassing of normal access controls during emergency situations could affect the integrity of system and data. There could be loss of integrity of information and data due to application of inappropriate or unauthorised procedures in emergency situations. Therefore, a proper procedure for emergency shall be laid down.

k) Personnel Security Policy during Hiring, Transfer & Termination: Security responsibilities need be addressed at the time of commencement of employment and the engagement of a contractor. Security responsibilities shall also be included in job descriptions and contracts and monitored during an individual's employment. Potential recruits need to be adequately screened in order to ascertain the individual's suitability and reliability from a security point of view.

All employees, external contractors, and other third parties, who require access to UIDAI's systems, shall responsible for ensuring the security policies to be adhered. The protection of systems resources shall be a fundamental responsibility of all personnel.

l) **Audit Policy**: An audit policy shall be laid down to audit the datacenter/network and various processes in order to ensure proper implementation of security policies. There shall be clear "schedule" and "procedures" of audit for "network", "datacenter" and "processes" being followed. The audit shall be performed at a defined regular interval.

6 References/Bibliography

[1]. Kumar Naveen: A study on Aadhaar; A dissertation submitted to Panjab University Chandigarh at Indian Institute of Public Administration, 2012-13

[2]. UIDAI Strategy Overview, UIDAI HQ, New Delhi also available on UIDAI website (2010)

[3]. Report of the Group of Experts on Privacy (Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court), (2012)

[4]. Privacy and Security of Aadhaar: A Computer Science Perspective by Shweta Agrawal Subhashis Banerjee Subodh Sharma Computer Science and Engineering, IIT Delhi

[5]. Nandan Nilekani & Viral Shah, Rebooting India, Penguin Books. PP(1-46) (2015)

[6]. Swati Chauhan, Chetanshi Sharma, Geetanjali & Akshita Verma: Survey Paper on UID System Management; International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 3, No. 2, February 2014.

[7]. Raja Siddharth Raju, Sukhdev Singh, Kiran Khatter: Aadhaar Card: Challenges and Impact on Digital Transformation (2017)

[8]. Pam Dixon: A Failure to "Do No Harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.(2017)

[9]. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits And Services) Act, 2016 No. 18 of 2016

[10]. Compendium of Regulations, Circulars & Guidelines for (Authentication User Agency (Aua)/E-Kyc User Agency (Kua), Authentication Service Agency (ASA) and Biometric Device Provider) UIDAI Updated as on 6thDecember 2017

[11]. Draft Bill on right to privacy, Government of India, New Delhi (2011)

[12]. A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Report of Committee of Experts under the Chairmanship of Justice B.N. Srikrishna) (2018)

[13]. Ashok Kumar: A presentation by a Technical expert of UIDAI, http://trai.gov.in/sites/default/files/presentations_&_cv/Day-3_25Aug2017/Session2_Digital%20world/Digital%20Identifiers_Ashok%20Kumar.pdf , Date accessed: 10.02.2019

[14]. Data Security and Privacy, https://uidai.gov.in/my-aadhaar/about-your-aadhaar/security-in-

uidai-system.html , Date Accessed : 12.02.2019

[15]. Dass Rajanish, Unique Identification for Indians: A Divine Dream or A Miscalculated Heroism

[16]. Aadhaar Automated Biometric Indentification Subsystem Interface UIDAI 2009-10

[17]. Maharashtra loses data of 3 lakh UID cards. http://timesofindia.indiatimes.com/city/mumbai /Maharashtra-loses-data-of-3-lakh-UID-cards/articleshow/19687125.cms. Date accessed: 23/11/2018.

[18]. MS Dhoni's Aadhaar details leaked, wife Sakshi complains to Ravi Shankar Prasad. http://www.hindustantimes.com/cricket/ms-dhoni-s-personal-info-from-aadhar-card-form-leaked-wife-sakshi-complains/story-8M4B7ZabHIu8cAcWhKuIzH.html Date accessed: 29/11/2018

[19]. Government admits your Aadhaar data has been leaked. http://www.newindianexpress.com/nation/2017/mar/31/government-admits-your-aadhaar-data-has-been-leaked-1588027.html. Date accessed: 31/10/2018.

[20]. Details of over a million Aadhaar numbers published on Jharkhand govt website. http://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFlScg5Dn5neLyBzrkw1I.html. Date accessed: 29/11/2018.

[21]. Aadhaar leak: 35 lakh people in Kerala have their personal data breached. http://english.manoramaonline.com/news/kerala/2017/04/25/aadhaar-leak-people-kerala-personal-data-breached.html. Date accessed: 25/11/2018.

[22]. https://uidai.gov.in/images/recently_asked_ques_13012018.pdf , Date Accessed: 10.02.2019

[23]. https://uidai.gov.in/images/news/Judgement_26-Sep-2018.pdf, Date Accessed: 14.02.2019

[24]. Aadhaar data 'edited' to pilfer public distribution system https://timesofindia.indiatimes.com/city/lucknow/aadhaar-data-edited-to-pilfer-public-distribution-system-ration-in-up/articleshow/65547049.cms

[25]. Aadhaar mandatory for filing I-T returns, applying for PAN card. http://indiatoday.intoday.in/story/aadhaar-mandatory-for-filing-i-t-returns-pan-card/1/909530.html Date accessed: 21/11/2018.

[26]. SC verdict on Aadhaar(26/09/2018), https://www.thehindu.com/news/resources/article25048939.ece/binary/AadhaarVerdict.pdf date Accessed:15.01.2019

[27]. https://indianexpress.com/article/india/aadhaar-verdict-live-updates-supreme-court-judgment-today-5374587/ Date Accessed: 15.02.2019

[28]. Aadhaar breach reports are misleading: UIDAI to court (HT news date 14.02.2019) https://www.hindustantimes.com/india-news/aadhaar-breach-reports-are-misleading-uidai-to-court/story-CUnRdOBOoDz6Zxw6U3nmZL.html Access date 24.02.2019

Annexure-I

Open-ended questions for discussion and Interview

i. What is their view on the physical security of the UIDAI datacenter?

ii. Is there any system to manage building and to give access to building?

iii. How the Data Storage and Process are secure from cyber security threats?

iv. What kind of security equipment have been deployed in the datacenter?

v. How the Physical Protection of Data are ensured?

vi. What security practices are being followed by UIDAI?

vii. What kind of safety have been taken to prevent threat from the vendors of technology?

viii. What is your view on the performance and availability of service of UIDAI?

ix. Whether Aadhaar Privacy is a relay challenge for the Government?

x. What are the Data protection and privacy measures taken by UIDAI?

xi. What are the privacy protections in place to protect the right to privacy of the resident?

xii. Who will have access to the UID database? How will the security of the database be ensured?

xiii. Any other suggestion to avoid misuse?

Annexure-II

SET-A: Questionnaire for basic security measures of Aadhaar data

Dear Sir/Madam,

You are requested to answer the questionnaire given below. The questionnaire has been prepared for evaluating the security aspect of UIDAI datacenter and privacy aspect of Aadhaar data keeping in view of Government policy. You are requested to share your views for Aadhaar. Your responses would help us in improving perception of public with respect to privacy and security of their personnel data stored with UIDAI datacenter.

Thanks for your valuable comments and time.

1) Whether Aadhaar datacenter sites are following International standards of physical Access to the equipment and equipment's rooms?

   A. Yes

   B. No

2) Whether datacenter of Aadhaar is meeting the requirement of Tier-IV standards (as per Uptime institute definition)?

   A. Yes

   B. No

3) Whether UIDAI is following ISO 9000 - Quality System for its Aadhaar datacentre?

   A. Yes

   B. No

4) Whether UIDAI is following ISO 14000 - Environmental Management System for its Aadhaar datacentre?

   A. Yes

   B. No

5) Whether UIDAI is following ISO 27001 - Information Security for its Aadhaar datacentre?

   A. Yes

   B. No

6) Whether UIDAI is following EN 50600-2(1) Building (2) Power distribution, (3) Environmental control, (4) Telecommunications cabling infrastructure, (5) Security systems and (6) Management and operational information systems for its Aadhaar datacentre?

   A. Yes

   B. No

7) Whether Firewalls have been deployed in each of the Aadhaar datacenter in order to strength the security of datacenter?

   A. Yes

   B. No

8) Whether Intrusion Detection System (IDS) have been deployed in each of the Aadhaar datacenter in order to strength the security of datacenter?

   A. Yes

   B. No

9) Whether Intrusion Prevention System (IPS) have been deployed in each of the Aadhaar datacenter in order to strength the security of datacenter?

   A. Yes

   B. No

10) Whether Policy, Signatures etc. of security equipment like Firewalls are being updated regularly in order to protect from latest security threats?

   A. Yes

   B. No

11) Whether proper security policy like equipment access & authorization policy, password policy for different equipment have been implemented?

A. Yes

B. No

12) Whether security policy like access list (based on IP addresses, Port etc.), filter list etc. has been implemented and being updated at regular interval?

A. Yes

B. No

13) Whether server hardening has been done in datacenter?

C. Yes

D. No

14) Whether servers running frontend applications (which may be accessed from outside) and Servers running backend applications (which are being used in backend and accessed by internal server of datacenters only) are separate?

A. Yes

B. No

15) Whether Aadhaar data are stored in the backend servers and access from outside Aadhaar network are allowed in order to strengthen security of data?

A. Yes

B. No

16) Whether the concept of zoning of network like Secure zone, demilitarized zone and open zone etc. has been implemented at Data center?

A. Yes

B. No

17) Whether any security policy has been laid down for Aadhaar datacenter by UIDAI?

A. Yes

B. No

18) Whether the security policy of Aadhaar datacenter are being followed properly?

A. Yes

B. No

19) Whether the security policy of Aadhaar datacenter are being updated by UIDAI?

A. Yes

B. No

20) Whether security audit of Aadhaar datacenter are being carried out?

A. Yes

B. No

21) Whether comprehensive measures of data security such as complete data backup & recovery, using data encryption while transferring files, enforcing the latest data privacy regulations and comprehensive monitoring of traffic are being followed?

A. Yes

B. No

Annexure-III

SET-B: Questionnaire for the Aadhaar holders

Dear Sir/Madam,

You are requested to answer the questionnaire given below. The questionnaire has been prepared for evaluating the awareness about the Aadhaar data, UIDAI network and Government policy. You are requested to share your views for Aadhaar.

Thanks for your valuable comments and time.

1) Whether UIDAI keeps only demographic detail (such as name, gender, date of birth, Father/Mother's name, address, Mobile number and email ID) and biometric details (i.e. Ten finger prints, two IRIS scans, facial photograph) of residents in their datacentre?
   A. Yes
   B. No
   C. Not aware
2) Whether UIDAI keeps other personal detail like health records, family, caste, religion, education, etc. in their datacentre?
   A. Yes
   B. No
   C. Not aware
3) Whether UIDAI keeps the details of profession, business, property details financial, bank detail, PAN, shares, mutual funds, etc in their datacentre?
   A. Yes
   B. No
   C. Not aware
4) Do you think UIDAI tracks our activities?
   A. Yes
   B. No

C. Not aware

5) Whether UIDAI receives or collects your bank, investments, insurance etc. details?

   A. Yes

   B. No

   C. Not aware

6) Are you aware that the Aadhaar Act 2016 has been passed by Parliament?

   A. Yes

   B. No

   C. Not aware

7) Are you aware that Section 32(3) of the Aadhaar Act 2016 prohibits UIDAI from controlling, collecting, keeping or maintaining any information about the purpose of authentication?

   A. Yes

   B. No

   C. Not aware

8) Are you aware that Regulation 17(1)(a) of the Aadhaar (Authentication) Regulations 2016, strictly prohibits any requesting entity which includes mobile phone companies, banks etc from storing, sharing or publishing the finger-prints for any reason whatsoever?

   A. Yes

   B. No

   C. Not aware

9) When you link your bank accounts, shares, mutual funds and your mobile phones with Aadhaar, will UIDAI get these information?

   A. Yes

   B. No

   C. Not aware

10) Do you know that when you link your bank accounts, shares, mutual funds and your mobile phones with Aadhaar UIDAI only responds to the verification requests by replying either 'Yes' or 'No' and in few cases, if the verification answer is 'Yes', your basic KYC details (name, address, photo etc) available with UIDAI, are sent to the service provider for authentication only.

    A. Yes

    B. No

    C. Not aware

11) Whether your Aadhaar data has been misused ever?

    A. Yes

    B. No

    C. Not aware

12) Whether UIDAI data center storing Aadhaar data is robust?

    A. Yes

    B. No

    C. Not aware

13) Whether UIDAI data center storing Aadhaar data is secure?

    A. Yes

    B. No

    C. Not aware

14) Whether the linking/sharing of Aadhaar number with your bank accounts, shares, mutual funds and your mobile phones etc. has any threat to your privacy?

    A. Yes

    B. No

    C. Not aware

15) Are you aware about the provision of Security and confidentiality of information and Restriction on Sharing information under Aadhaar Act 2016 ?

A. Yes

B. No

C. Not aware

16) Are you aware about the provision of Penalty & Punishment under Aadhaar Act 2016 for impersonation of Aadhaar data, disclosing Identity information, unauthorised access to the Central Identities Data Repository etc.?

A. Yes

B. No

C. Not aware

17) Whether Aadhaar is a threat to your privacy?

A. Yes

B. No

C. Not aware

18) Do you think Aadhaar is a unique identity for any resident?

A. Yes

B. No

C. Not aware

19) Do you think Aadhaar is robust enough to eliminate duplicate and fake identities?

A. Yes

B. No

C. Not aware

20) Do you think Aadhaar should be made mandatory for all residents of India?

A. Yes

B. No

Annexure-IV

Inputs/Responses/FAQs Collected from UIDAI

1. What is Virtual ID (VID)?

   VID is a temporary, revocable 16-digit random number mapped with the Aadhaar number. VID can be used in lieu of Aadhaar number whenever authentication or e-KYC services are performed. Authentication may be performed using VID in a manner similar to using Aadhaar number. It is not possible to derive Aadhaar number from VID.

2. How does a resident obtain VID?

   VID can be generated only by the Aadhaar number holder. They can also replace (generate a new VID) their VID from time to time after UIDAI set minimum validity period (currently set as 1 day, i.e. a new VID be generated after 00:00 hrs on the next day) . At any given time only one VID will be valid for an Aadhaar number. UIDAI will provide various options to Aadhaar number holders to generate their VID, retrieve their VID in case they forget, and replace their VID with a new number. These options will be made available via UIDAI's resident portal, eAadhaar download, Aadhaar Enrolment centre, mAadhaar mobile application etc. Presently, VID generation facility is available on UIDAI's resident portal. Whenever required, VID will be sent to residents via SMS on registered mobile number.

3. Can anyone else generate VID for me?

   No other entity like AUA/KUA can generate VID on behalf of Aadhaar number holder.

4. What if an Aadhaar number holder forgets VID? Can he/she obtain again?

   Yes, UIDAI will provide multiple ways to generate new and/or retrieve current VID. These options will be made available via UIDAI's resident portal, eAadhaar, Aadhaar Enrolment centre, mAadhaar mobile application etc. Presently, VID generation facility is available on UIDAI's resident portal. Whenever required, VID number will be sent to residents via SMS on registered mobile number.

5. Can VID be used for OTP or biometrics or demographics authentication?

Yes. VID can be used in lieu of Aadhaar number in Authentication API input. Various entities will update their Aadhaar authentication application by 01.06.2018 to accept VID as an input for authentication.

6. In case of VID, do I need to provide consent for authentication?

   Yes, Aadhaar number holder consent is necessary for VID based authentication. Agency is required to inform the Aadhaar number holder the purpose for authentication and collect explicit consent for performing authentication.

7. Can an agency store VID?

   No. Since VID is temporary and can be changed by the Aadhaar number holder, storing VID has no value. Agencies should not store VID in any database or logs.

8. Will re-generation of VID lead to the same VID or a different VID?

   After the minimum validity period (currently set as 1 day), on Aadhaar number holder requests regeneration, a new VID will be generated and the previous VID will be deactivated. In case resident opts for retrieval of VID, the last active VID will be sent to the Aadhaar number holder.

9. What is the expiry period of VID?

   At this time there is no expiry period defined for VID. VID will be valid till the time a new VID is generated by the Aadhaar number holder.

10. What are biometric locking /Unlocking?

    This feature is to secure biometric authentication by locking biometrics data of the resident. Biometric remains locked till the Aadhaar Holder chose to either unlock it (which is temporary) or Disable the Locking system.

11. How resident can lock their Biometrics?

    - Open your profile
    - Click on the top RHS corner.
    - Select Biometric Settings.
    - To lock biometrics select check box ‘Enable Biometric Lock’.

- To save your selection, click on Tick Mark on top RHS.
- An OTP will be generated and auto-filled and biometrics will be locked.
- The Biometric will be locked permanently till unlocked.

12. What is Temporary and Permanent Biometric un-Locking?

    Resident can unlock Biometrics in 2 ways

    - Temporary Unlock – Unlocked valid for 10 minutes
    - Permanent Unlock – Unlocked Permanently

    Note: In order to permanently unlock Biometrics it takes 6 hours, so might be resident will not be able to Authenticate for next 6 hours.

13. How resident can unlock their Biometrics?

    - Open your profile
    - Click on the top RHS corner.
    - Select Biometric Settings.
    - To unlock biometrics select check box 'Enable Biometric Lock'.
    - To save your selection, click on Tick Mark on top RHS.
    - An OTP will be generated and auto-filled and biometrics will be locked.
    - The Biometric will be un-locked permanently till unlocked.

    Note: In order to permanently unlock Biometrics it takes 6 hours, so might be resident will not be able to Authenticate for next 6 hours.

14. How to configure mAadhaar?

    - Download mAadhaar android mobile application
    - Create new resident profile.
    - Navigate to TOTP page view, your TOTP should be visible and is valid for 30 seconds.

15. Where can m-Aadhaar be used?

m-Aadhaar is accepted as proof of identity for undertaking journey in any reserved class in Indian Railways.

16. What is TOTP?

    - It is an one-time temporary password (OTP), that is generated by an algorithm and valid only for 30 seconds. Because of this time variable characteristic, it is called TOTP.
    - TOTP is 8 digit long numeric strings.
    - TOTP is personal to the resident and is uniquely generated every 30 seconds for each resident separately.
    - With time-based OTP, the TOTP validation server and token generation app(like mAadhaar) use their respective system times to generate OTPs. The TOTP algorithm assumes that the system times are synchronized.

17. How resident can create profile in mAadhaar app?

    - Enter 12 digit Aadhaar Number or scan your Aadhaar card
    - Ensure that your mobile connection is active and that the mobile number is same as that available with UIDAI as your registered mobile number.
    - After providing the mandatory inputs press the button 'Verify', available at the bottom of the screen. After pressing 'Verify' button do not navigate away from the screen
    - If details provided by you are found to be correct then application will receive OTP and will read OTP automatically from the phone.

18. Can mAadhaar app work offline?

    mAadhaar needs to be connected and download data from UIDAI. So ensure that internet connectivity is available on your phone.

19. Why to use TOTP?

    TOTPs avoid a number of shortcomings that are associated with traditional SMS based OTP. The most important shortcoming that is addressed by TOTPs is that resident will not be

dependent on mobile network for SMS delivery. Generating and sending OTP requires users to go through a completely unrelated workflow.

20. Why my profile on mAadhaar gets inactive when have changed to new phone with registered mobile number?

    One Aadhaar profile can be active on only one device at a time. If you create profile on another device by inserting the SIM in another device, the previous profile would become inactive and would be deleted from older device whenever any operation is attempted from that device.

21. Is it compulsory to have registered mobile number to use m-Aadhaar?

    Yes, it is compulsory to have registered Mobile Number.OTP will be shared and auto-filled via registered mobile number in mAadhaar app. In case you're mobile number is not registered with Aadhaar visit the nearest Aadhaar Enrolment/Update Centre.

22. What is Masked Aadhaar?

    Mask Aadhaar option allows you to mask your Aadhaar number in your downloaded Aadhaar.

23. What happens if some fraudster who obtains a copy of my Aadhaar card and tries to open a bank account in my name without my knowledge. Will I not be harmed?

    One must keep in mind that a bank account cannot be opened merely on the presentation or submission of a physical Aadhaar card or its photocopy. Under the PML Rules and RBI circulars, to open a bank account, the bank is required to do biometric or OTP authentication and other due diligence before accepting Aadhaar for banking transaction or KYC. So no one can open a bank account in your name without your verification through biometric/OTP etc. If however, a bank account is opened by accepting Aadhaar without biometric or OTP authentication and other verification, then the bank will be held responsible for any loss. An Aadhaar holder cannot be held responsible for bank's fault. It is just like if some fraudster opens a bank account by presenting someone else's Voter card/Ration card, it is the bank that would be held responsible not the voter or ration card holder. Till date no Aadhaar holder has suffered any financial loss on account of such misuse.

24. I gave my Aadhaar card to a service provider for proving my identity. Can anyone harm me by knowing and misusing my Aadhaar number?

    No. Just, by knowing your Aadhaar number, no one can harm you. It's just like any other identity document such as passport, voter ID, PAN card, ration card, driving license, etc., that you have been using freely for decades with service providers. Aadhaar identity, instead, is instantly verifiable and hence more trusted. Also, as per the Aadhaar Act 2016, the Aadhaar card is required to be verified by fingerprint, iris scan, OTP authentication, and QR code. Hence, it is near impossible to impersonate you if you use Aadhaar to prove your identity. People have been freely giving other identity documents such as passport, voter ID, PAN card, ration card, driving license, etc. But did they stop using these documents for the fear that somebody would use them to impersonate? No! They continue using them and if any fraud happens, the law enforcement agencies handle them as per law. The same logic will apply to Aadhaar. In fact, Aadhaar is more secure than many other identity documents, because unlike other IDs, Aadhaar is instantly verifiable through biometric and OTP authentication and QR code. Further, under the Aadhaar Act, 2016 stringent penalties, including fines and imprisonment are provided whenever a person misuses your Aadhaar number or tries to cause any harm to you.

25. There are many agencies that simply accept physical copy of Aadhaar and do not carry out any biometric or OTP authentication or verification. Is this a good practice?

    Aadhaar is to be accepted as a proof of identity only after proper authentication under the Aadhaar Act. Also, UIDAI strongly recommends that if authentication facility is not available, the verification of Aadhaar should be done offline through QR code available on the physical Aadhaar copy. If any agency does not follow these best practices, then that agency will be fully responsible for situations or losses arising out of possible misuse or impersonation. An Aadhaar holder is not responsible for the wrongful act of or by any agency.

26. Can a fraudster withdraw money from my Aadhaar linked bank account if he knows my Aadhaar number or has my Aadhaar card? Has any Aadhaar holder suffered any financial or other loss or identity theft on account of impersonation or misuse?

Just like by merely knowing your bank account number, one cannot withdraw money from your account, similarly by merely knowing your Aadhaar number, no one can withdraw money from Aadhaar linked bank account. As in bank for withdrawing money, your signature, debit card, PIN, OTP, etc., is required, similarly for withdrawing money from your Aadhaar linked bank account through Aadhaar, your fingerprint, IRIS or OTP sent to your Aadhaar registered mobile will be required. No Aadhaar holder has suffered any financial or other loss or identity theft on account of any said misuse or attempted impersonation of Aadhaar. Notably, everyday more than 3 crore Authentications are carried out on the Aadhaar platform. In the last eight years, so far more than 2,182 crore authentications (till 31st July 2018) have been successfully done. UIDAI keeps upgrading and reviewing its security systems and safety mechanisms to make Aadhaar more secure and more useable. There has not been a single instance of biometric data breach from Aadhaar database. Therefore, people should freely use and give Aadhaar to prove their identity as and when required.

27. Does linking my bank account, PAN, and other services with Aadhaar make me vulnerable?

No. As your bank information is not shared by the bank with anyone else, no one can have information about your bank account just by knowing your Aadhaar number. Also, UIDAI or any entity for that matter would not have any information about your bank account. For example, you give your mobile number at various places and to various authorities such as bank, passport authorities, income tax departments, etc. Would the telecom company have access to your bank information, income tax returns, etc.? Obviously no! Similarly, when you provide Aadhaar number to various service providers, your detail remains with the respective service providers and no single entity including the Government or UIDAI will have access to your personal information spread across various service providers.

28. Why am I asked to verify Bank account, Demat account, PAN and various other services with Aadhaar?

When you link your bank account, demat account, mutual fund account, PAN, etc., with Aadhaar, you secure yourself because no one can impersonate you to avail these services. Often the fraudsters carry out transactions and transfer money from someone else's account to their accounts and go untraced as they generally submit their fake identities to the bank

while opening their accounts. They operate bank accounts in fictitious names/companies and run shell companies' accounts to carry out money laundering or stash black money. Therefore, when all the bank accounts are verified with Aadhaar then it would not be possible for these unscrupulous elements to go untraced and banking as a whole would become more safe and secure as the identity of each bank account holders is established uniquely beyond doubt through eKYC. As of now 96 crore bank accounts out of total 110 crore accounts have been linked to Aadhaar.

At the same time, you also contribute to serve the vital national interests by making the system rid of bogus, fakes and duplicates who could misuse IDs to evade taxes, siphon off public money, etc. Through use of Aadhaar and other process improvements, the Government has been able to weed out more than 6 crore fakes, duplicates and ghosts beneficiaries and save more than Rs. 90,000 crore of public money. Also, ghost and shell entities and companies used to be created for tax evasion, money laundering, terror financing, etc. Verification of identity through Aadhaar has helped curb these practices. Similarly, use of Aadhaar has checked unscrupulous elements that used to resort to impersonation in various examination and tests for college admission and jobs, etc., and thereby denying the genuine candidates of their rightful dues. There are number of other areas where verification of identity through Aadhaar has brought in fairness and transparency in the system.

29. Recently, UIDAI has issued an advisory asking people not to share their Aadhaar number openly in the public domain especially on Social Media or other public platforms. Does this mean that I should not use Aadhaar freely?

You should use your Aadhaar without any hesitation for proving your identity and doing transactions, just like you use your bank account number, PAN card, debit card, credit card, etc., wherever required. What UIDAI has advised is that Aadhaar card should be freely used for proving identity and doing transactions, but should not be put on public platforms like Twitter, Facebook, etc. People give their debit card or credit card details or cheque (which has bank account number) when they purchase goods, or pay school fee, water, electricity, telephone and other utility bills, etc. Similarly, you can freely use your Aadhaar to establish

your identity as and when required without any fear. While using Aadhaar, you should do the same level of due diligence as you do in case of other ID cards – not more, not less.

30. If Aadhaar has to be freely used for proving identity and it is safe to do so, then why has UIDAI advised people not to put up their Aadhaar number in Social Media or public domain?

    You use PAN card, debit card, credit card, bank cheques wherever required. But do you put these details openly on internet and social media such as Facebook, Twitter, etc.? Obviously no! You do not put such personal details unnecessarily in public domain so that there is no unwarranted invasion attempt on your privacy. The same logic needs to be applied in case of uses of Aadhaar.

31. How will the grievances of the resident be addressed?

    The UIDAI will set up a Contact Centre to manage all queries and grievances and serve as a single point of contact for the organization. The details of the Contact Centre will be published on the website as and when enrolment begins. The users of this system are expected to be residents, registrars and enrolment agencies. Any resident seeking enrolment is given a printed acknowledgement form with an Enrolment Number, that enables the resident to make queries about her/his enrolment status through any communication channel of the contact centre. Each enrolment agency will be given a unique code that will also enable faster and pointed access to the Contact Centre that includes a technical helpdesk.

32. Can a resident opt out of Aadhaar?

    The resident has the option in the first instance not to enrol for Aadhaar at all. Aadhaar is a service delivery tool, and not designed for any other purpose. Aadhaar being unique to every resident, is non-transferable. If the resident does not wish to use the Aadhaar, it will remain dormant, as the use is based on the physical presence and biometric authentication of the person. However, currently, there is no provision to opt out of the Aadhaar database, but it must be again said here that except for the resident, his Aadhaar cannot be used by any other person.

33. Can the resident's data be purged from Aadhaar database?

    As is the case with the other services availed from the government, there is no provision for purging the data of the resident from the database once he has obtained his Aadhaar. The data is also required as it is used for de-duplication of every new entrant in the database against all the existing records to establish the uniqueness of the resident. Only after this process is completed that the Aadhaar is assigned.

34. What are the possible criminal penalties envisaged against the fraud or unauthorized access to data?

    Following are the possible criminal penalties in the Bill:

    - Impersonation by providing false demographic or biometric information is an offence – imprisonment for 3 years and a fine of Rs. 10,000.
    - Appropriating the identity of an Aadhaar number holder by changing or attempting to change the demographic and biometric information of an Aadhaar number holder is an offence - imprisonment for 3 years and a fine of Rs. 10,000.
    - Pretending to be an agency authorized to collect Identity information of a resident is an offence – imprisonment for 3 years and a fine of Rs. 10,000 for a person, and Rs. 1 lakh for a company.
    - Intentionally transmitting information collected during enrolment and authentication to an unauthorized person is an offence – imprisonment for 3 years and a fine of Rs. 10,000 for a person, and Rs. 1lakh for a company.
    - Unauthorized access to the central identities data repository (CIDR) and hacking is an offence – imprisonment for 3 years and a fine of Rs. 1 crore.
    - Tampering with the central identities data repository is an offence – imprisonment for 3 years and a fine of Rs. 10,000.
    - Providing biometrics that is not one's own is an offence – imprisonment for 3 years and of Rs. 10,000.