TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance

Abdul Salam Mohammed

PRIVACY AND SECURITY RISKS WITH AADHAR CARD: STUDY OF MEDIA DISCOURSES ON REPORTING VARIOUS THIRD-PARTY DATA BREACHES

Master's thesis
Programme: Technology Governance and Digital Transformation

Supervisor: Shobhit Shakya, PhD

Tallinn 2022

I hereby declare that I have compiled the thesis independently and all works, important standpoints and data by other authors have been properly referenced and the same paper has not been previously presented for grading.
The document length is 15,151 words from the introduction to the end of conclusion.

Abdul Salam Mohammed ……
(Signature, date)
Student code: 194319HAGM
Student e-mail address: amoham@ttu.ee

Supervisor: Shobhit Shakya, PhD:
The paper conforms to requirements in force

……
(Signature, date)

Chairman of the Defence Committee:
Permitted to the defence
……
(Name, signature, date)

TABLE OF CONTENTS

ABSTRACT

The study aims to measure the role of media in reporting third-party breaches of Aadhar cards. This study focuses on addressing the issues in critical discourse analysis. This analysis evaluates the issues based on text and discourse practices. Qualitative analysis uses to measure the third-party data breaches of Aadhar cards. Aadhar card breaches are classified into four themes: data leakages, privacy issues, security breaches, and data protection & privacy measures. Data leakages create intentional and unintentional threats. Most of the third-party company threats are intentional only. Intentional threats are in the form of improper encryption of Aadhar information in websites & apps or an online gateway platform. A relatively small number of unintentional threats finds due to improper encryption and publish information on websites and environmental hazards. Next, privacy issues arise due to misuse of personal information and unauthorized access to information. These issues are giving political benefits and financial benefits to the attackers. Security issues arise owing to data theft, sabotage, and social engineering, but Indian residents are more prone to data theft. So, actions like physical access control, personal data protection, creating a new password, legal actions, data removal, shutting down websites and apps, and debar the third-party to use the information to protect the Aadhar information from the third-party parties. Finally, the study concludes that data breaches of Aadhar information of the third-party prevail more in India. UIDAI should take action to protect the Aadhar ecosystem. Such action can diminish data breaches to happen soon.

Keywords: Aadhar card, privacy issues, security issues, data breaches and third parties

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

UIDAI	Unique Identification Authority of India
PDS	Public Distribution Systems
ID	Identification
CIDR	Central Identities Data Repository
ASA	Authentication Service Agency
LPG	Liquefied Petroleum Gas
UID	Unique Identification Number
PKI	Public Key Infrastructure
AUA/KUA	Authentication/e-KYC User Agency Agreement

INTRODUCTION

Not lot gap, Indian residents, more often than not, found difficulty in providing identity via cards. There is no single identity card available for residents in India. Residents have to submit different cards like ration cards, voter cards, PAN, and passports to prove their identification in the country, creating redundant information or fake identification (Sharma 2011). To resolve the issue, the Government of India developed a multipurpose national identity card – the Aadhar card. The main intention of the card was to offer services to people under a single identification document (Tyagi et al. 2018). Aadhar card benefits weaker section people to avail welfare schemes transparently (Singh 2021).

Aadhaar is a twelve-digit number that acts as a unique identifier for Indian citizens (Tyagi et al. 2018) which the Government of India issues (Madan n.d; Gupta et al. 2018). The Aadhaar card system is the world largest database having a subscriber of 1.2 billion people in 2018 (Singh 2021; Anand 2021). The key goal of implementing the Aadhaar card is to make error-free identities for Indian citizens (Gupta et al. 2018). The card can direct the Indian citizen to utilize various services like LPG, banks, etc. Even though the card offers numerous benefits to Indian residents, security and privacy issues are associated with the card (Raju et al. 2017). Security issues of digital identity cards are information privacy, unauthorised use of personal information, human errors, centralisation of database storing, decryption of data and theft and loss of cards (Kee et al. 2012; Alkhurayyif 2013). Privacy concerns identify individuals without consent, surveillance, and tracking people (Agarwal et al. 2017). Considering the issues from the previous studies, this study measures the security and privacy issues of Aadhar cards.

Research problem: Third-party breachers of Aadhar information are high and lead people to face the risk of financial frauds and threats (Aggarwal 2018). Nearly 1036 million Indian residents enrolled in the system. There is no proper security for the Aadhar information of Indian residents. Media news reported that improper security of the third parties leads to leakage of Aadhar information. Apart from threats, leakages and information vulnerabilities may create security and privacy issues. The most commonly cited literature issue for data breaches is the loss of privacy

of Aadhar information (Johari 2016; Drèze 2016; Yadav 2016). Other threats are data breaches, information loss, implementation loopholes, and lack of awareness of security threats (ibid). The problem of security issues (Easy access to databases, duplicate cards, publishing of Aadhaar information on government websites) is a known concern (firstpost.com 2018). Despite security issues, Personification, manipulation, financial fraud, theft activities are some of the privacy issues of Aadhar (Gupta et al. 2018; Meta, 2016). An identical problem is similarly highlighted by experienced Christopher (2018): third parties exhibit the Aadhar information from the UIDAI database, leading to security and privacy issues. Unlike security and privacy issues concerning the card's technology, the problem of third-party data breaches of Aadhar cards is still largely unsolvable as these concern broader awareness amongst various stakeholders and other participants. So, this study focuses on this particular aspect of the security concerns and tries to explore the context through analysis of media discourses.

Research questions:

1) What are the key privacy and security issues related to the Aadhaar card?
    a. How common are third-party related issues?
2) What are the dominant perspectives towards third-party related security and privacy issues of Aadhar cards as reflected in mainstream media reports?

The thesis is structured into five chapters as follows:

Chapter 1: Introduction

The researcher introduces the concept of the Aadhar Card in India and its benefits to different stakeholders such as the nation's citizens, the government, the business industry, and privacy and security issues.

Chapter 2: Review of Literature

In this chapter, the researcher will present the summary of published research works of others on Aadhar card, features, benefits, architecture, technology components, privacy and security at the Aadhaar system, third-party breaches, challenges of third-party breaches, privacy concerns, and security breaches of the Aadhar card information.

Chapter 3: Research Methodology

Under this section, the researcher covers research strategy, unit of analysis, sample, sampling procedure, data collection method, sample size, and tools used for the analysis.

Chapter 4: Data Analysis & Research Findings

The researcher analyses the collected information in a tabular format and exhibits the outcome in figures. Also, the section shows the summary of the findings.

Chapter 5: Conclusion

The researcher concludes the research work by quantifying the hypothesis of the role of media in reporting data breaches through third-party sources.

1. LITERATURE REVIEW

1.1. Aadhar card

The word “Aadhaar” originates from the Sanskrit language. Aadhar represents a foundation or base (UIDAI 2015). It was designed to identify the citizens of India. It contains the biometric information of Indians and their demographic data (Anusha, Rajkumar 2017).

Source: digitalindia.gov.in

1.1.1. Features of Aadhar card

Using the Aadhaar card offer five prerequisites that offer advantages to Indians (UIDAI, n.d.).

The first feature is the distinctive of the card. Aadhar cards offer biometric information and demographic information. It eliminates the probability of duplicate information from the users. It considers being the uniqueness of the Aadhaar card. Once the user registers their details for Aadhar, it stores in the UIDAI database. If a person tries to enroll it again, it rejects the information and matches it with the present one in the record. Hence, it makes to identify the individual distinctively.

The second feature is availability. Aadhar information is in computerized form. Anyone can access the information from anywhere in India. It shows a nationwide portability benefit for Indian citizens. It is particularly helpful for the people who move around (or) travel places.

The third feature is based on randomized numbers. Numbers are generated for an individual on a random basis. Individuals who want to enroll their demographic data have to enclose biometric information. It did not ask for caste, religion, income, and health.

The fourth feature is centrally managed architecture. UID architecture is scalable. Individual information is stored and managed centrally, making the information updation or authenticated easily done from anywhere. The architecture has the potential of handling 100 million authentications per day (ibid).

The fifth feature is eased access to information through technology. Aadhar card information does not sit on a single computer or any hardware; also, it is not managed by any vendors. This is possible due to open-source technologies (Pali et al. 2020).

1.1.2. Benefits of Aadhar card

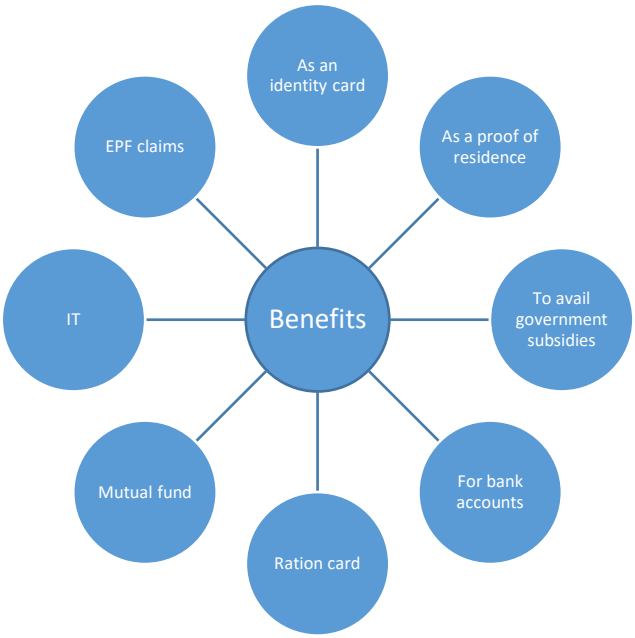

Figure 1. Benefits of Aadhaar card

Source: Author illustration

Indian people who have Aadhaar cards can enjoy the below-stated benefits given by the government (vikaspedia, n.d). Utilising Aadhar cards is receiving subsidies from the government for LPG and ration cards. Aadhar card acts as proof of evidence for opening a bank account at zero balance. This card reduces the time taken for the verification process of Indians to get a passport. It acts as the best platform to manage Indian resident's records and helps reduce fraud voters. It helps identify the genuine and precise people who apply to avail pension from the respective department. The most important use of the Aadhar card can easily integrate the particular residents to avail the government benefits. Such integration diminishes the take-ups in the place of fraudulent activities. Nowadays, Indian banks ask for an Aadhar card from Indian customers who make financial transactions above Rs.50,000 (ET 2017). So, it is clear that the Aadhar card plays an important role in availing government and banks' benefits.

Later acquiring the knowledge of benefits, the applications of the Aadhar card describes in detail. According to Raju *et al.* (2017), ten applications of Aadhar card lists below

- Acquiring a passport
- Opening a new bank account
- Acquiring a digital life certificate
- Enrolling in Jan Dhan yojana
- Availing PF and LPG subsidy
- Making railway reservations
- Enhancing ATM security and E-voting system
- Aadhar E-KYC services

1.2. Aadhar card model and Technology overview

Aadhar model: Aadhaar authentication and verify the system has the following entities:

1) Unique identification authority of India (UIDAI);
2) Authentication user agency (AUA);
3) Authentication service agency (ASA);
4) Users;
5) Point of sale;
6) Enrolment station.

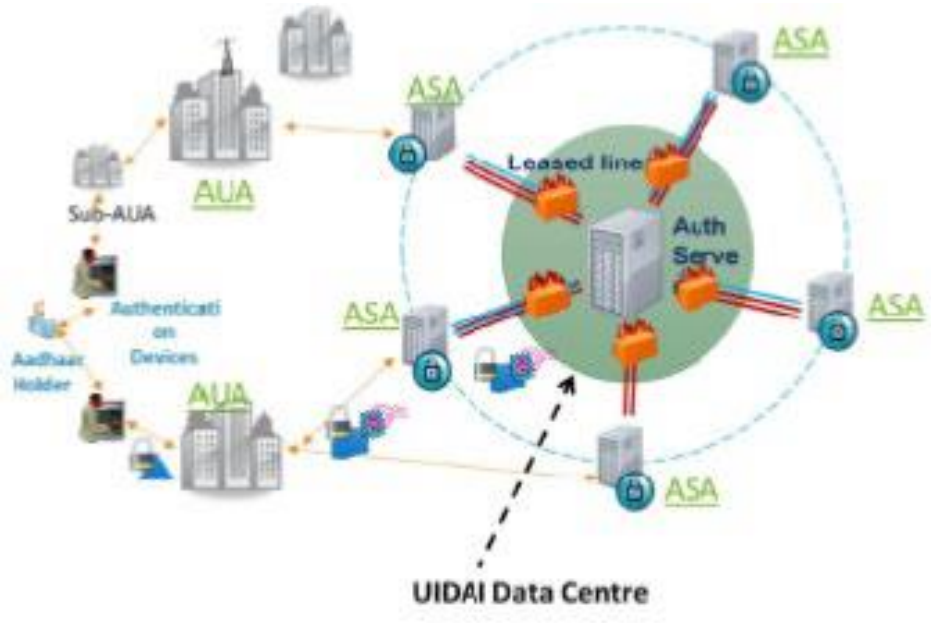

Figure 2. Aadhaar model

Source: UIDAI (2010)

1.2.1. Technology components

CIDR: Central ID data repository is the central database to store all the information (demographic and biometric). It asks for the minimum set of information to confirm identity. CIDR database may contain additional information relating to the resident. The resident is asking for a key to use data from the CIDR database (India, 2010).

UIDR: UIDR servers use to take enrolment and authentication data. It is available across the network. State government registrars and their authentication agencies can utilize the information.

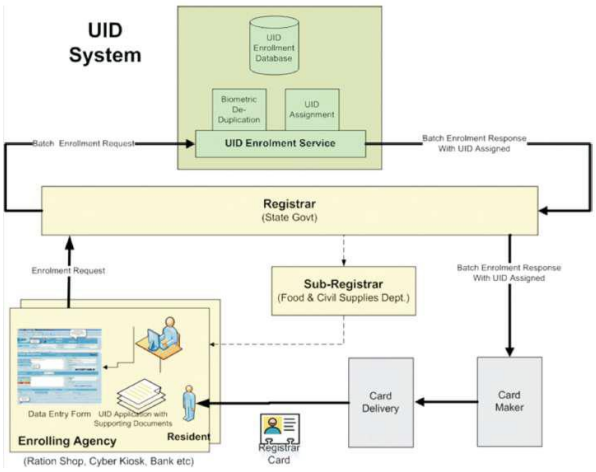

Figure 3. UID system

Source: Sharma (2011)

Backend servers are there to load data from the authentication requests. Backend servers are N biometric de-duplication, biometric sub-system, enrolment client application, network, and infrastructure. All the servers have high demand. Authentication requests were made to avoid biometric de-duplication from the wide peak data. First is de-duplication, which is the most computing-intensive operation of the UID system. It demands a state of an art robust technological solution in getting an acceptable performance. The second is the biometric sub-system, considered a central system for enrolling and authenticating residents' information. A specific multi-modal biometric solution setup to accomplish high accuracy and quality of data. The enrollment client application is the third server that captures and validates information (demographic and biometric data) at the specific enrolling sites. The network is the fourth server to make authentication and enrollment to be available online. Fifth is infrastructure security which contains components (server security, intrusion prevention, network, and client security) from external or physical attacks (Sharma 2011). All the above-stated architecture is illustrated with the help of the below diagram.

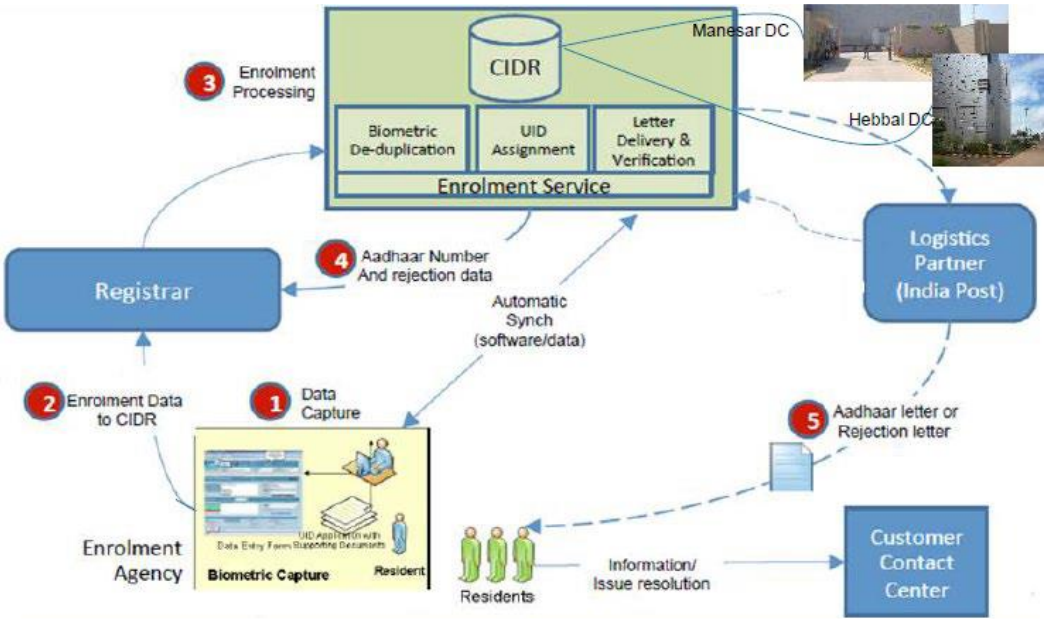

Figure 4. CIDR

Source: Kumar (2019)

Biometric sub-system: It is also used to enroll and authenticate residents. A multi-modal biometric solution sues to accomplish a high level of assurance. Innovative techniques like hashing, distributed processing, indexing, and in-memory databases were adopted to achieve acceptable performance (UIDAI, 2015).

Enrollment client: The enrollment client must capture and validate the information (biometric and demographic). It needs to work in both online and offline mode. For offline mode, there is no need for internet connectivity to upload files for processing. On the other hand, batch files can be transported to the CIDR for uploading the information. The client application prerequisite brings into effective action through a standard enrollment workstation (Justice, 2008).

Security design: The primary responsibility of security design is to safeguard the above components from physical or external attacks. Server security is used for intrusion prevention and detection system. Network security is made through encryption and PKI.

Administrative system: It administers account setup, role-based access control, audit trailing, fraud detection, and reporting & analysis through UIDAI operations (Kumar 2019; Government press, 2003).

1.2.2. Privacy and Security considerations of the Aadhar system

Aadhar system is developed to avoid misuse of resident data for their benefit. As per terms of usage stated in UIDAI through a memorandum of understanding, each AUA & KUA is given authority to capture the physical consent of Aadhar holders in the service delivery applications. It should be done on paper before being involved in authentication. Also, authentication API safeguard the information through encryption, access control, digital sign, audit to safeguard information from unauthorized access or using authentication services to enrich the security framework for the system. Personally identifiable information, access control, digital sign, encryption, audit trail, data retention usage to safeguard the resident information.

Data retention and usage: All the information stored in UIDIA is illustrated in the below figure:

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

Figure 5. Data retention and usage
Source: Ghangare and Ranade (2018)

With the strict procedures, no information ever leaves CIDR. Information leaves the consent only with the resident consent.

But the Ghangare and Ranade (2018) mentioned that the Aadhaar system faces the loss of privacy, security leakages that affect individual privacy. Madan (n.d) discussed that the architecture did not protect individual data against insider leaks, and hence it may lead to a higher degree of risk towards privacy. Privacy and security issues were serious in the Aadhar system (Agrawal et al., 2017). Privacy concerns from inside attacks or insider leaks are primarily seen in the present Aadhaar system (Tyagi et al., 2018). Data leakages at the application, network, and storage level is a prior breach of privacy concerns for the Aadhaar system (Shekhar 2018). A recent study pinpointed that third-party leakages and identity theft were the common breaches in the Aadhar system (Pali et al., 2020). A detailed description of third-party breaches of the Aadhaar card is described below.

Security breaches arise in the form of virus or unauthorized access, denial of service, sabotage, website defacement, and theft of proprietary information (Gordon et al. 2015). Some well-known security threats are data loss, phishing, botnet pose serious threats to data and software and server threats (Agrawal et al. 2017; Popović, Hocenski 2010). These security threats are either raised

internally or externally (Agrawal et al. 2017). A particular concern of security breaches in the Aadhaar card is data infringement, deliberate leakages of individual privacy information, and policy paralysis (Ghangare, Ranade 2018).

In the blog, Vidyut (2018) reported that the Aadhar number of 1.6 million pensioners and their demographic data was breached. Together with these, two million pregnant women's personal details were leaked by the government offices. Nearly two hundred and ten government websites made Aadhar information circulating public on the internet (Tech2 2018).

In addition to these, 130 to 135 million Aadhar numbers and one hundred million bank account details were disclosed by four government portals (Sinha, Kodali 2017). These leakages of information made by government officials had no legal action or financial compensation offered to the victims. Such breaches raise issues like the absence of security training to government officials, absence of defined data security policies, system vulnerabilities with Aadhar and its integrated API network, and external threats from hackers exploiting the system vulnerabilities (Vidyut 2018). Aadhar holds the data of more than 1.2 billion people. This huge data is a target for cyberattacks. If there is a compromise made on data storage, then UIDAI is responsible for the security practices of the Aadhar database. Instead of addressing the socio-technical lens risks, UIDAI criticizes technical safeguards (UIDAI 2019). The particular criticism proved in some recent studies that security issues are the major concern in the Aadhar database (Anand 2021; Agrawal et al. 2017; Tyagi et al. 2018).

Anand (2021) elaborates on the security and privacy issues of Aadhar information. Privacy issues were found in design and enrolment. Security concerns were the scale of security lapses, data leakage of confidential information, absence of training of government officials, system vulnerability with Aadhaar, external cyber security threats, and hackers vulnerabilities. After determining the issues, the study suggests improving the present system can enhance the Aadhar ecosystem. Also, offering education about risk, mitigation strategies can improve the transparency in the system.

Jain (2019) discusses that internal problems and leaks, vulnerability as an alternative for photo ID, legal problems, and privacy issues were the challenges of the Aadhaar card.

Later determining the studies relating to a third-party, Aadhaar card and data breaches, the following table represent the information in tabular format.

Table 1. Studies related to third-party breaches and Aadhar card

Author name	**Objectives**	**Research method**	**description**
Agrawal *et al.* 2017	"Discussing the major concerns of privacy issues of Aadhar card"	Qualitative method	Aadhaar card
Anand 2021	"Elaborating the security and privacy issues of Aadhar information"	Qualitative method	Aadhaar card
Banerjee, Sharma 2019	"Identifying privacy concerns of Aadhar cards like data theft, identification without consent using data, illegal tracking of information and absence of virtual identities information."	Qualitative method	Aadhaar card
Bergström 2015	"Discussing the misuse of information, unauthorised secondary usage and improper data access of Aadhar."	Qualitative method	Aadhaar card
Cheng *et al.* 2017	"Recognizing the data leak threats, incidents and how to prevent and detect using detection techniques"	Qualitative method	Third-party breaches
Datta *et al.* 2020	"Empirically investigate the security and privacy issues of Aadhar cards. Identify its threats and issues"	Qualitative method	Aadhaar card
Furnell *et al.* 2020	"Discuss the threats, attacks and cybercrime of data breaches"	Qualitative method	Third-party breaches
Ghangare, Ranade 2018	"To investigate the privacy issues of Aadhar information."	Qualitative method	Aadhaar card
Gordon *et al.* 2005	"Discussing the security breaches of Aadhar card"	Qualitative method	Aadhaar card
Hassanzadeh *et al.* 2021	"Exploring the data breaches on the internet"	Qualitative method	Third-party breaches
Jain 2019	"Legal and privacy issues of Aadhar card"	Qualitative method	Aadhaar card
Opderbeck 2015	"Discussing the cyber security and data breaches of the third-party"	Qualitative method	Third-party breaches
Popović, Hocenski 2010	"Discussing the security issues and challenges of cloud engineering"	Qualitative method	Aadhaar card
Saleem, Naveed 2020	"Describing data breach methods"	Qualitative method	Third-party breaches
Shekhar 2018	"Discussing privacy and security issues of the Aadhaar card"	Qualitative method	Aadhaar card
Tyagi *et al.* 2018	"To investigate the privacy and security issues of Aadhaar technology perspective"	Qualitative method	Aadhaar card

Source: Author Illustration

From these studies, it is clear that third-party data breaches are high in Aadhar cards. Some of the cases are reported in various news articles. Christopher (2018) stated that Aadhar data leaks of sensitive information were made by one of the state-owned utility In other cases, one of the Bangalore-based technomancy leaked the personal information of 0.5 million users of Aadhar card (Singh 2021). According to Times of India report, Telangana State Forensic Science Laboratory identified that IT Grids Private Limited made data breaches of voter ID and Aadhar card (Tech2 2018; Vudali 2019). These cases reveal information about the third-party data breaches of the Aadhar card.

Third-party breaches are data stolen from a third-party system. Third-party uses vendor system to access and steal the data stored in the respective system (Fasulo 2017). Such breaches are much more pervasive and costly than others (Opderbeck 2015). Furnell et al., (2020) discussed that the breaches involved attack, abuse, and cybercrime. Abuse is of undesirable utilization of technology which affects breach and the breach cost. An attack is a deliberate unlawful action that brings about a breach or physical action against another party. Cybercrime is the illegal use of technology and procedures preceded by unauthorized breaches. The relationship of all three breaches illustrates in the diagram.

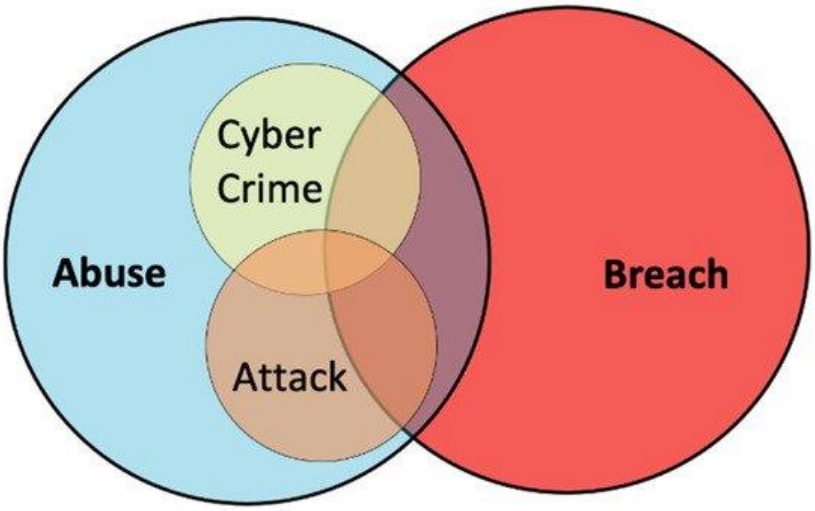

Figure 6. Third-party data breaches
Source: Furnell et al., (2020)

As per the Ponemon Institute survey, 59% of respondents had an experience of a data breach through a third-party (Ponemon Institute 2019). Such data breaches have been common and raised a broad concern recently (Hassanzadeh et al., 2021). Goddijn and Koun (2021) reported that eight billion public data records were exposed to data breaches globally. These breaches were made due

to negligence, poor password, absence of security measures, vulnerability, and hackers (Hassanzadeh et al., 2021).

1.2.3. Third-party data breaches in Aadhar card

Logix (2018) reported that data breaches in Aadhar cards increased in recent years. It is because of storing biometric and demographic information on local machines. These machines are the primary reason for massive data leaks of the Aadhar card.

Another incident came into the light that data breaches of personal information of almost 5 million users leaked apparently. Such information includes Aadhar number of beneficiaries, personal beneficiary details, family information and their respective mobile numbers.

Christopher (2018) stated that UIDAI secured the Aadhaar database, and there were no breaches of data that emerged from the system. As stated by UIDAI, the Aadhar database is safe and secure. But the leakages of information observe from third-party sites. Such sites have API access to the database. So, they are involved in abusing the data of millions of people.

In the article, Jain and Gill (2021) pinpointed the CSC BHIM website of over seven million records found in Israeli cybersecurity. The details of individual names, date of birth, ID numbers could give a chance to hackers to make illegal access to accounts of BHIM users. It affected millions of people in India because the availability of information could be preceded by engaging in fraud, theft, and more.

1.3. Challenges of third-party data breaches

Third-party data breaches are the more obvious and most important security and privacy problems (Saleem, Naveed 2020). These third-party steal the million or even billions of records of a public database. Such looting of data poses dire privacy issues, publicly revealing the sensitive data to intentionally ill people and making it available on the web (ibid). These ways of data breaches acquire the sensitive and valuable information that preceded to face the risk of loss or theft of information (Cheng et al., 2017). All the possible ways of looting challenges describe in detail.

1.3.1. Data leakage

Data breaches may result in misuse or leakage of highly confidential data (Sundareswaran 2018). Data leakages are mainly caused by internal information breaches and external information breaches, either inadvertently or intentionally leaking sensitive information. Data leakages may be done by insider or outsider threats. Insider threats are espionage, accidental sharing of information, transmitting without proper encryption and more. External threats are caused by hackers, malware, social engineering, and virus (Cheng et al., 2017). The classification of data leakages of parties illustrates in the below figure.

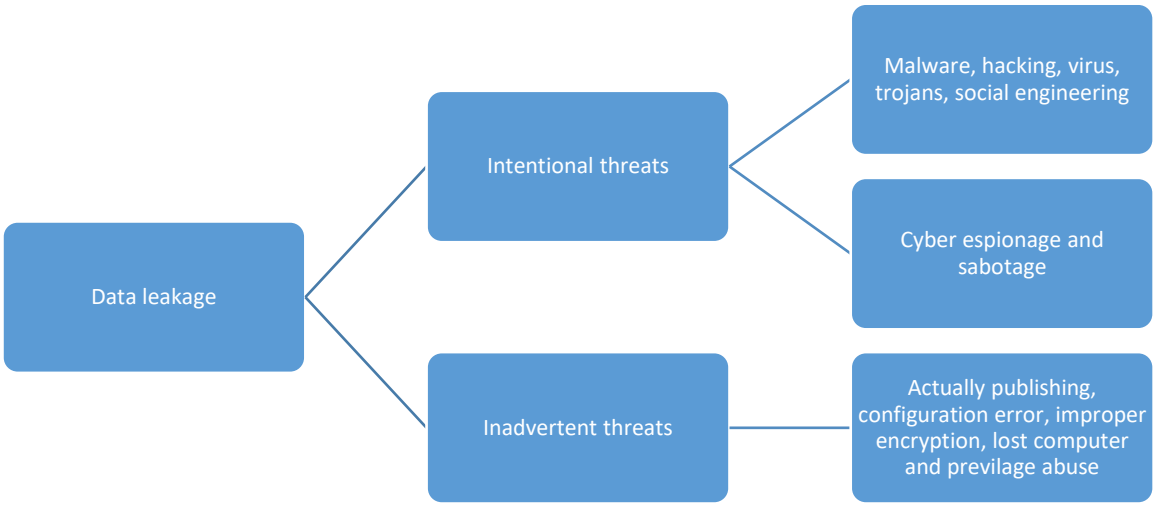

Figure 7. Data Leakage

Source: Author illustration

1.3.2. Privacy concerns of Aadhar card

Misuse of personal information, external unauthorized secondary usage and improper access of data (Bergström 2015). Sharma (n.d) discussed that there were three privacy and security issues of the Aadhaar card. The first concern is the identification of an individual through a global Aadhaar number without their consent. The second concern is to identify and authenticate an individual's biometric and demographic information without their consent. The third concern is surveillance and tracking the people through a centralized database.

Raju et al. (2017) discussed the privacy concerns of the Aadhaar card. The author pinpointed that the major privacy concerns were an individual can find out and authorize biometric data without

revealing Aadhaar numbers and demographic information. An individual can track people with legal permission from the government, mass surveillance and extract data from either internal attacks or external hacks

As per Banerjee and Sharma (2019), the privacy concerns of Aadhar cards are identified theft, identification without consent using Aadhar data, correlation of identities across domains, illegal tracking of individual data and lack of virtual identities.

The first concern is identified theft. Aadhar card is endangered to bring in biometric information illegally. There is a chance of leakage of information from the central Aadhaar repository. It may lead to risk. Also, it may lead to engaging in fraudulent activities. It primarily owes to not maintaining biometrics in a secret way which adds to the risk (Viswanath 2017; Khaira 2018).

A second concern is Aadhar card identification without any consent from the card holder. There is a chance of accessing biometrics to find out the people without getting the department's prior approval (Banerjee and Sharma, 2019).

The third concern is an association of identities over domains. It may be possible in tracking individual personal information over multiple domains of services through their global Aadhaar Id. Global Aadhaar ID is valid over domains. Hence, illegal tracking of information may lead to identifying information without prior knowledge of an individual (Banerjee and Sharma, 2019).

The fourth concern is the illegal tracking of individual information. There is a chance of tracking the individual information without proper authorization. Also, any person can be easily put under surveillance using data from the Aadhaar database or authentication requesting agencies databases without consent. Such information can provide information like location, time and context of authentications and services availed without recording the purpose of authentication. Authentication without proper authorization may put users face a serious risk of fraud even though Aadhar KYC is for one purpose that can be used for another (Viswanath 2017). Privacy by design is not accomplished through self-imposed blindness.

The other concern is that Aadhaar information can be readily available in just a google search. Such availability may offer valuable information to the criminals. The best example for unauthorized access is UIDAI temporarily about Aadhar payments by respective banks. Some of

the banks are Axis banks, Suvidhaa Infoserve, and eMudhra indulge in unauthorized access and impersonation of Aadhar biometrics (Tyagi et al., 2018).

Lack of virtual identities: Aadhaar is retrofitted in a limited form. It may create more privacy concerns. The absence of data usage policy and regulatory oversight worsen the concern (Agrawal et al., 2017). Privacy concerns will remain without a proper consent and limitation framework and a regulatory access control architecture. Such inadequate protection may lead to utilizing information in an unprecedented way (Sikri, 2018; Khera, 2019; Drèze 2016).

Later determining the various privacy issues, the Aadhaar card is stuck to possible loss of privacy. Recent studies have pinpointed that privacy concerns related to the Aadhaar card are the recently criticized topic in India (Agrawal et al., 2017; Ghangare, Ranade 2018; Tyagi et al., 2018; Datta et al., 2020).

Agrawal et al., (2017) discuss the concerns of weak privacy that existed for Aadhar cards. Aadhar system was unsafe because technological and legal flaws made a breach of privacy. So, the study investigated the privacy and security issues from the technological perspective. Privacy issues were in identification without consent, illegal tracking and insider attacks. Security issues were raised through untrusted networks and clients. Assessment of issues preceded finding out the flaws (lack of infrastructure, design problems) in the Aadhar system. Setting up a strong legal framework can resolve the data breaches made in Aadhaar.

2. THEORETICAL BACKGROUND OF THE STUDY

Mass media discourse is represented as the spoken or written interactions on a broadcast platform. In these interactions, discourses are oriented towards analysing readers, listeners, or viewers of social issues. Generally, discourses orient with the recipients, but they do not take instant responses to the producer of the discourses. Even though technology dominates the media no chances of getting instant responses to social issues. The written and listening discourse aligns with readership and viewing audience, respectively. Media discourse is a public, and manufactured & on-record form of interaction. The crucial aspect of media discourse is considering how this has been done at an ideological level. The most significant aspect of media discourse is preoccupied with critical ways, and it is termed critical discourse analysis. Critical discourse analysis is a structure for analysing the social issues in mass media discourse (Anitasari 2018). Critical discourse theory focuses on endeavouring in recognising social issues (Van Dijk et al. 2016). The other author stated that language plays a key role in constituting and transmitting knowledge in social issues (Lucke 1996). Critical discourse analysis is particular about social and political conditions in linguistic form. In theory, language uses in representing the speaker belief, ideas and position of issues. Such theory makes a significant contribution to social and political analysis and focuses on the structure of text and talk. The key aim of the analysis is to describe the relationship between text and interactions. Secondly, interpreting the configuration of practices is how and why social practices transformed the way they are (Rogers et al. 2005).

Critical discourse analysis can unite and determine the association between text, discourse practices, and the larger social context based on the above two (McGregor 2003). Such application of theory is qualitative because it expresses oneself with the help of words (ibid). Similar methods were adopted in the previous studies (Cross et al. 2019; Guasti, Mansfeldová 2015; Wojtkowski et al. 2020). A detailed description of studies mentions below:

Wojtkowski et al. (2020) focused on measuring media discourse on privacy issues through discourse analysis. The key objective of using the analysis was tracking the discourse on privacy.

Such privacy was measured in four aspects: relational, contextual, participatory and technology. These four aspects are used in this study to determine the tackle of creating the privacy policies. Such aspects are measured with the help of the critical discourse study approach in inductive analysis. In addition, quantitative and qualitative content analysis captured the character of privacy, dimensions and agents. The samples were picked out; data were gathered through websites, political magazines, and news portals. Content analysis reveals that most media discourses were a contextual dimension of privacy. Media discourse on privacy is associated with legal and formal aspects of privacy but not popularised in the European Union. Such issues were discussed in daily newspapers and online portals. Exhibiting the information to the public was monopolised owing to journalists and experts of the respective fields.

Guasti and Mansfeldová (2015) investigated media debates on security issues using discourse analysis. Such issues were measured in qualitative media analysis. The study findings reveal that media was an important resource for discussing security issues. The first risk was Iran nuclear programme was threatening the western world. The second risk was the deployment of technologies in cyber warfare. The third was a nuclear catastrophe. All these risks addressed the emotions had an impact on attitudes.

Arifin and Lennerfors (2021) focused on investigating the media coverage in Indonesia through critical discourse analysis. Such analysis found that gender issues, privacy, security, ethical issues were the most common issues in media coverage. These issues discussed did not have any real critical problem, but foreign media highly influenced discursive practices.

Cross et al. (2019) mentioned that data breaches of Ashley Madison were discussed. Such discussions were made through qualitative analysis. Data were gathered through an online database, and the assessment of information revealed that the exposed personal information created an emerging tension in the case. Victims of data breaches relied on the perceived immorality of the website and their actions in subscribing rather than focusing on the data breach.

Fornaciari (2014) discussed the privacy issues using frame theory in the study. This theory undertook support from critical discourse analysis. The author had explored one hundred and thirty articles from 2000 to 2012 to capture the economics of privacy developed during the period. CDA helps identify the four frames, namely confusion & absence of transparency, justification & private interests, the commodification of interest and law and self-regulation. The study findings indicate

that the absence of control, inappropriate flows created privacy issues. So, the outcome exhibits the media frames reflecting public opinion related to privacy issues.

Aripova and Bashmakova (2019) mentions in the study that online privacy issues discourse in news reports were investigated. The author supported critical discourse analysis to find out the issues. The findings of the study show that internet customers integrated with universal values and rights. But some misuse values could lead many internet companies to violate privacy laws.

Later describing the individual assessment of studies, all the studies and their important description are presented in the below table.

Table 1. Studies related to theoretical background

Author name	Objectives	Method	Results
Wojtkowski *et al.* (2020)	To focus on measuring media discourse on privacy issues through discourse analysis	Qualitative	Content analysis reveals that most media discourses were a contextual dimension of privacy. Media discourse on privacy is associated with legal and formal aspects of privacy but not popularised in the European Union.
Guasti and Mansfeldová (2015)	To investigate the media debates on security issues using discourse analysis	Qualitative	Media was an important resource for discussing security issues.
Arifin and Lennerfors (2021)	To investigate the media coverage in Indonesia	Critical discourse analysis	Gender issues, privacy, security, ethical issues were the most common issues in media coverage.
Cross *et al.* (2019)	"data breaches of Ashley Madison were discussed."	Qualitative	Victims of data breaches relied on the perceived immorality of the website and their actions in subscribing rather than focusing on the data breach itself.
Fornaciari (2014)	To discuss the privacy issues using frame theory	Qualitative	The study findings indicate that the absence of control, inappropriate flows created privacy issues. So, the outcome exhibits the media frames reflecting public opinion related to privacy issues.
Aripova, Bashmakova (2019)	To investigate the online privacy issues discourse in news reports	Critical discourse analysis	The findings of the study show that internet customers integrated with universal values and rights. But some misuse values could lead many internet companies to violate privacy laws.

Source: Author Illustratio

3. RESEARCH METHODOLOGY

Media articles highlighted the poor security of third-party portals leaking the information of Aadhar cards. These leakages may lead to Personification, manipulation and engagement of attackers in financial fraud and theft activities. Some of the previous research typically only investigated the security and privacy issues of Aadhar breaches. There is a lack of studies on measuring security and privacy issues through third-party data breaches. From the assessment of literature studies, this study finds that a limited method exists for measuring Aadhaar breaches through a third-party. (Agrawal et al. 2017; Ghangare, Ranade 2018; Tyagi et al. 2018; Datta et al. 2020). So, there is a need to measure the issues and identify the deep insights of third-party data breaches in qualitative research methods. The researcher explains how to carry out the research study to accomplish the objectives in this study. The study presents a unit of analysis, sampling, research methods, data collection methods, and tools to achieve the objective. A fuller discussion of the methodology provides in the subsequent section.

Unit of analysis: In this study, the unit of analysis is the activities of third-party data breaches of Aadhaar information.

Sampling: The sampling of study determines based on two-step. In the first step, the researcher identifies a relevant context of third-party data breaches of Aadhaar. Secondly, the study picks out the most relevant articles for detailed study. Convenience sampling refers to the elements which are available at the moment (Sedgwick 2013). Convenience sampling encounters for studying the third-party Aadhar breaches where materials are easily available in the newspaper websites. The advantages of using the sampling are that it is less costly and readily available than others sampling procedures. Together, it is efficient and simple to implement in the study. Contrary to the merits, lack of generalizability leads to bias and can be applied to the participant group.

Research methods: The source of evidence is media articles, and the researcher gains insights through qualitative research methods. The primary aids of using the methods are producing the

experiences and interpreting the meaning to the third-party Aadhar breaches of their actions. Such methods help to accomplish deeper insights into issues. In contrast to the merits, leaving out sensitivities and the absence of generalisations were the demerits of qualitative research methods.

Data collection: The source of data collection for this research is secondary data or the publicly available information on the media platforms, mainly from the National media, Newspapers and Journals, etc., to name a few: INDIA TODAY, THE WIRE, NDTV, and HINDUSTAN TIMES. The data is mostly collected from the National level media. The Newspapers operated at the National and local levels to find more about the state news on the security breaches.

The shortlisting of the Media houses was done carefully by looking at the research done on the most viewed and awarded media sources from 2017-2021. The articles considered for this study are taken only from the media sources, which are largely viewed by the people in India and whom people trust and rely upon news (Report, 2021). There are plenty of articles supporting the security and privacy issues of the Aadhar card. But the researcher shortlisted the articles based on keywords "third-party data breaches", "security", and "privacy" issues of Aadhar in India. Among the wide collection of articles, 35 media articles from the past five years about the data breaches with Aadhar cards have been found relevant and tabulated for this study.

To summarize the past empirical literature and provide a comprehensive understanding of the study topic, a broader research review method: the 'Integrative Review' method (Synder 2019), is used to understand and analyze the information gathered from these secondary sources. The significance of using the method in this study is that it gives knowledge about the current topic because it focuses on identifying, investigating and synthesising the articles to recognise the analysed phenomenon.

3.1. Tools used for data analysis

Qualitative analysis of word frequency, word cloud map and thematic analysis considered. All the analysis is conducted with NVivo software's help in this study. The researcher collects the articles from the respective sites, import the article to Nvivo, conduct the word frequency and world cloud analysis. In the thematic analysis, the researcher gets consistent support from the literature studies to define the appropriate theme for this study. A detailed description of the tools mentions below.

1) **Word frequency:** It indicates the most frequently used words in the news articles, indicating the news article perspective (Feng, Behar-Horenstein 2019). The advantage of using the technique is to avoid meaningless news articles relating to the study. Second, it helps to identify the patterns, maintain analytic integrity and decrease the bias of overweighing the articles (Halpern 1984; Lincoln, Guba 1985; Onwuegbuzie, Leech 2007; Sandelowski 2001). In this analysis, the tools help identify the highest attraction words in the news articles.
2) **Word Cloud map:** It is a commonly used visualizing text data (Tessem et al. 2015). It gives structure to the information, indicating what is important. It is a tool to support information (Rivadeneira et al. 2007; Hearst, Rosner 2008; Wilson et al. 2012). The advantage of using the tool is that the centralized words attract the users (Sinclair, Cardew-Hall 2008). In the present analysis, the word cloud uses to exhibit the commonly used words relating to third-party breaches of Aadhar cards.
3) **Thematic analysis:** Thematic Analysis (TA) to analyze the qualitative data collected from the sources, identify a greater number of cross-references and identify common patterns or themes. This analysis offers flexibility for starting the data analysis during the data collection process with no association of the data or information collected with the result of the process itself. More importantly, Thematic Analysis (TA) helps link different opinions and compare with the data collected (Alhojailan 2012).

4. DATA ANALYSIS

In this study, the thematic analysis applies to determine the constellations of themes present in the collected dataset. This analysis analyses the dataset more closely to identify the specific pattern of the theme found in the data. The study uses thematic analysis because the dataset is easily accessible, flexible and applicable for a wide range of third-party breaches on Aadhar cards. So, the detailed description of the analysis presents in the subsequent section.

4.1. Collection of the Media articles

The collected News/media articles from the various sources (mentioned in the previous section) related to the data breaches of Aadhar card from "private", "government/state government/departments", "external hacks" to analyse, can be represented in the graph below:

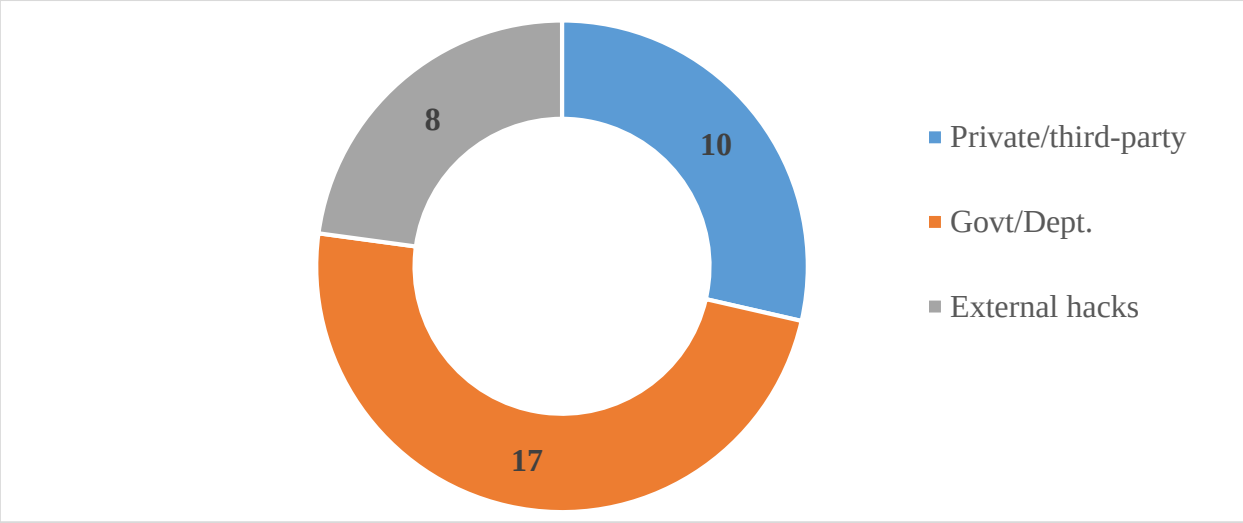

Figure 8: Media articles

Source: Author Illustration

4.2. Word frequency for Aadhar security issues where actions taken

Word frequency emphasises the importance of individual words related to security issues. In this study, assessment of selected articles reveal that the top used words in articles are "Aadhar",

"details", "government", "security", "breach", "database", "leaked" and "claims. From the articles, it is clear that government takes action for data leakages of Aadhar details. The least used words in the articles are "disclosing", "vulnerable" and "authentication", indicating that disclosing the action takes for Aadhar information vulnerability is genuine.

Figure 9. Privilege abuse word cloud

Source: Author Illustration

4.3. Thematic analysis

Thematic analysis suits to find out the specific pattern of third-party breaches of Aadhar found in the newspaper article. The most appropriate data for third-party breaches are newspaper data. The study collects information from various sources. Such sources help find out the four themes for third-party data breaches of Aadhaar information. One of four themes is data leakages, privacy issues, security breaches and data protection &privacy measures. The theme describes in detail in the following section.

Figure 10. Third-party data breaches

Source: Author illustration

4.3.1. Theme 1: Data Leakages

In the technological era, data is everything. Leakages of data may create a concern for people. Such leakages may be made internally (intentional threats) or externally (accidental threats). Issues related to both kinds of leakages were particularly identified with the help of newspaper articles. The detailed description of data leakages is present below:

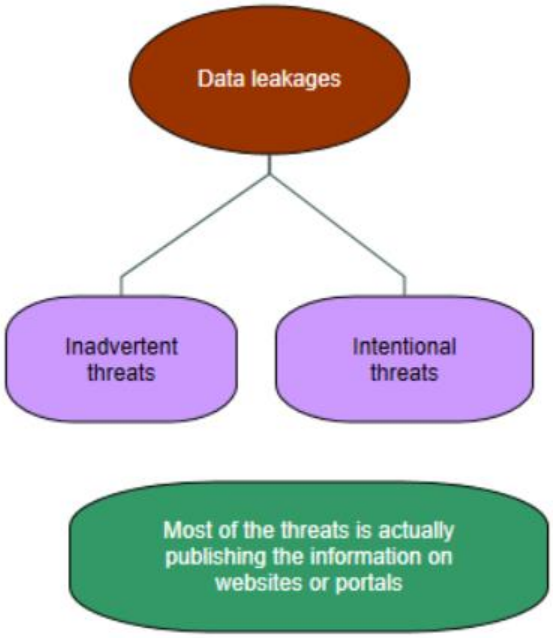

Figure 11. Data Leakages

Source: Author illustration

Intentional threats:

Another reported problem identifies from the article that two million users' information (address and Aadhar numbers) have been breached. Such breaches cited in Pratap (2021) that *"Millions of Airtel numbers may have been part of a recent leak that reportedly saw telephone numbers alongside personal details like address, city, Aadhaar card number, and gender details being up for sale on the web."*

Soni (2019) stated that data leakages of sensitive information of PAN & Aadhaar cards, passport size photos, income tax details and many more documents

IT Grid company acquires the data from central identities data repository and State Resident Datahub. Such a repository is responsible for holding a database of Aadhaar users. But the company illegally obtained the data from the repository and misused it for their purpose. Such

observation *is cited in the Vudali (2019) that "data recovered by the Telangana police from the premises of IT Grids (India) Pvt Ltd, on* ***suspicion of breach of voter ID and Aadhaar data".***

So, it makes clear that three articles showing the intentional data threats of third-party companies breach the Aadhar information from the central repository of UIDAI.

Inadvertent threats:

Such threats arise either from former employees or unauthorized access of operators or business partners. This study classified inadvertent threats into three sub-themes: improper encryption, environmental hazards, and publishing on websites.

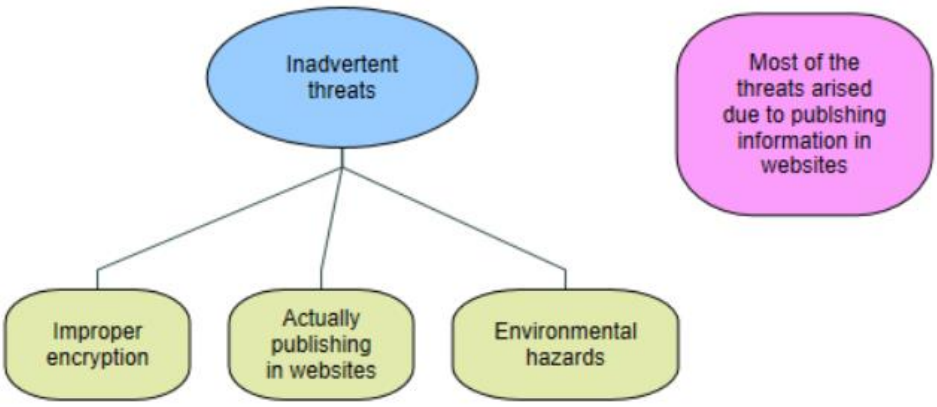

Figure 12. Inadvertent threats

Source: Author illustration

Sub-theme 1: Environmental hazards

The CSC BHIM breach is stored in unsecured data storage. This storage may lead to the exposure of valuable information vulnerable to threats and attacks. *Sifty (2020) stated that "The cybersecurity researcher's claim that 409 GB of data was stored on an unsecured Amazon Web Services (AWS) S3 bucket exposing records from February 2019."*

One of the third parties breached 0.1 million IDs of Indian Nationals on the dark internet. Such information leakage made the third parties involved in nefarious activities like thefts, scams and corporate espionage. *Sabarwal (2020) mentioned that "Over 1 lakh scanned copies of Indians' national IDs, including Aadhaar, PAN card and passport, have been put on the dark web for sale."*

It observes that vulnerable data storage and third-party breaches in the dark internet are the major reasons for accidental threats of Aadhar information.

Sub-theme 2: Improper encryption

Data leakage of 6.7 million subscribers of Indane gas can see on websites and apps. Such leakage includes subscriber Aadhaar number, name, address and ID of the particular dealer. Accessing the publicly available information from the vulnerable platform makes the public feel that the data is not secure. *Mukherjee (2019) cited that "UIDAI hasn't given out an official statement regarding the alleged leak. UIDAI's system isn't as secure as the agency assures from time to time."*

Anonymous seller created an online gateway through which Aadhar information including name, postal code, address, photo, email and phone number. Illegally the third-party breaches the Aadhar information through agents. *Babu (2018) reported that an agent representing "anonymous sellers over WhatsApp" created an online gateway through which she could log in to the Aadhaar portal, "and instantly get all particulars that an individual may have submitted to the UIDAI, including name, address, postal code, photo, phone number and email."*

From the observation of another article, the researcher observes that 3.5 million users' personal and payment information have been breached. These data breaches are phone numbers, email, passwords, bank accounts and credit card details. *Gurung (2011) cited that "The data breach includes 36,099,759 files, besides the 8.2 TB data compromising 99,224,559 user phone numbers, email, hashed passwords, addresses, bank accounts and card details."*

Out of three articles, two articles stated that vulnerabilities were raised through a third-party. It may be either websites or through an online gateway.

Sub-theme 3: Publishing

Publicly uploaded the details of Andhra Pradesh government beneficiaries of mobile number, village division, caste and Aadhar number. These breaches the data of thousands of farmers. *Soni (2019) pinpointed that the "Andhra Pradesh government exposed Aadhaar data of thousands of its state farmers."*

Government websites displayed the beneficiaries' name, addresses, UIDAI numbers. There is no prior information on publishing data breaches of beneficiaries in the respective government sites. More than 210 websites indulged in such breach activities. *PTI (2017) cited that "More than 200 central and state government websites publicly displayed details such as names and addresses of some Aadhaar beneficiaries, the Unique Identification Authority of India has said."*

Data leakage of one million users published in MNREGA MIS portal. It was represented in the article that *"The major website which was leaking 10,96,41,502 Aadhaar numbers was mnrega MIS portal" (Kodali 2017).*

Kerala university was discovered to be leaking research scholar info. On April 30, 2017, it was reported (SFLC 2017).

As per the onmanorama (2017), more than three million pensioners' details, bank details, and Aadhaar numbers were published on pensioner's websites (Sethi et al., 2017). Breaches came to light that more than 1.5 million pensioners' Aadhar number and their bank transfers are available on the Jharkhand government websites.

Data breach of Aadhaar card numbers, PAN numbers and biometric details in a data bundle of seven million customers have been breached. Such breaches may potentially lead to a high risk of theft, fraud, abuse, and cybercriminal. *Jain and Gill (2020) demonstrated that "The CSC BHIM data breach includes extremely sensitive information like Aadhaar details with complete scans of the Aadhaar cards, biometric details, addresses, date of birth and more.".* "The sheer volume of sensitive, private data exposed, along with UPI IDs, document scans, and more, makes this breach deeply concerning,"

Chandigarh's food supplies and consumer department shared Aadhaar information, ration card numbers, date of birth and more on their websites (ExpressNews 2017). Such details were accessed through a third-party, and they breached the data of people in Chandigarh.

Wirestaff (2018) stated data leakage of unsecured application interfaced operated by state-run utility service provider. The third-party breached the Aadhaar holder's name, information connected to the services and bank details. *Wirestaff (2018) reported that "data leak on a system run by a state-owned utility company can allow anyone to download private information on all Aadhaar holders, exposing their names… and information about services they are connected to, such as their bank details".*

Specifically, three Andhra Pradesh government websites reveal the number of children and adults Aadhaar. *NDTV (2018) Cited that "A Hyderabad-based cyber security researcher found three different portals of the Andhra Pradesh government disclosing Aadhaar numbers of 90 lakh adults and 70 lakh children in the last seven days"*.

From the observation, it is clear that most Aadhar information breaches were made in publishing the information on respective government websites.

4.3.2. Theme 2: Privacy issues

Breach of Aadhaar information is made in two ways: Misuse of personal information and unauthorized access. Such information describes in the subsequent section. The theme of privacy issues illustrates in the below diagram.

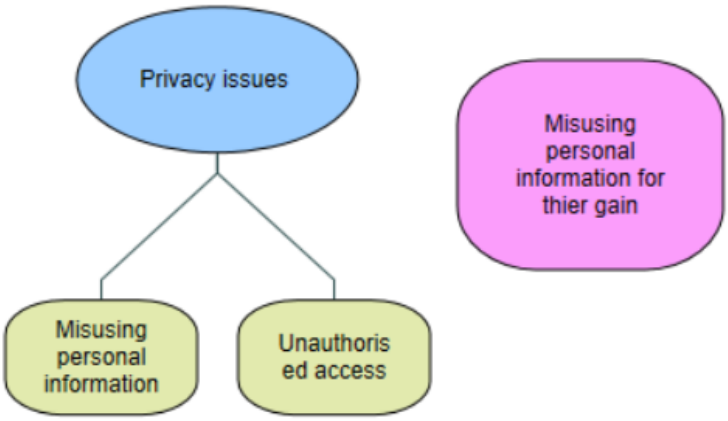

Figure 13. Privacy issues

Source: Author illustration

Misusing personal information:

One of the articles pinpointed that the ruling party misused the Aadhar information for their gain. *Scrollstaff (2021) cited that "Being the ruling party at the centre, BJP has misused its seat of power and indulged in identity theft, clearly in breach of the fiduciary duty it owes towards its subjects, i.e., the general public".*

The other article stated that attackers misuse the student database to acquire money from the respective parents. *TimesNowDigital (2020) reported that he "claimed the caller asking him to pay an amount of INR 10,000 as a one-time payment to get his child admission in Sainik School."*

Unauthorized access:

Jharkhand government followed a web-based attendance system, but there are no security protections for the system. So, anyone can access web pages with the personal details of state government employees. These systems offer government worker names, designation, photos, phone numbers and Aadhaar numbers.

From the observation, it is clear that misusing Aadhaar information is either political or financial gain.

4.3.3. Theme 3: Security issues

The security issues were measured in three themes: Data theft, sabotage and social engineering. All the information presents in detail in the below section.

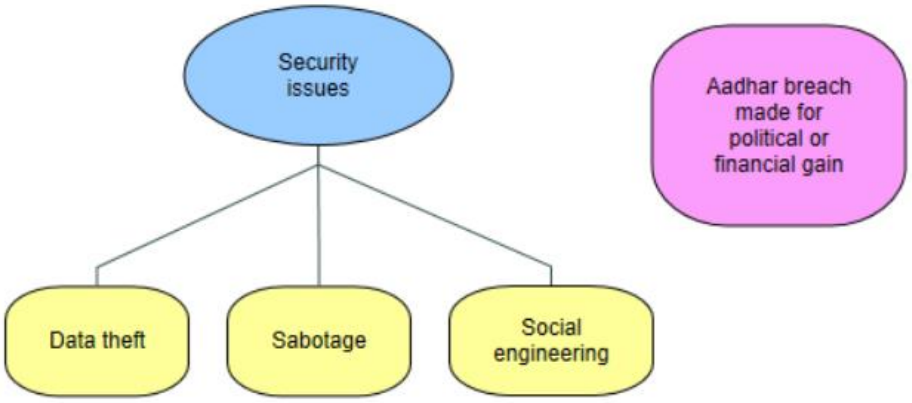

Figure 14. Security issues
Source: Author illustration

Data theft:

Hackers bypass the protocol, gain access to more than twenty thousand details of Aadhaar information. *UIDAI (2019) cited that" Aadhaar card details." These cards can be found on the internet. They are not on the UIDAI server. Everything is public, no hack is required,"*

Hackers reveal the TRAI chief personal details, PAN, alternative phone number, email ID and WhatsApp profile picture. ***"****The tweet was sent as a reply to one @kingslyj's post at around 1.45 pm. By 6 pm, however, French security expert and Aadhaar critic, who goes by the nickname Elliot Alderson, in* ***a series of tweets,*** *had revealed the mobile number linked to the Aadhaar number. Soon, Sharma's PAN number, alternative phone number, email ID, the phone he was using, his WhatsApp profile pic and some other sensitive data was out in the open". (Ganjoo 2018)*

Data stolen of 500 million guests' account information, email address, and encrypted password from Quora system. In addition to these, public content & actions and non-public content &actions are also affected by data breaches (Ganjoo 2018).

Sabotage:

The company (IT Grid) developed a structure similar to UIDAI, a breach of data of 78 million Indians from the respective two states (Andhra Pradesh and Telangana). These companies steal the information of Aadhar data, demographic, biometric information

The article cited the investigation that "As per the investigation, it was discovered that the structure and size of the database held by IT Grids were similar to what was owned by the Unique Identification Authority of India (UIDAI)."

TimesNow (2021) article observes that the confidential information of mobile numbers linked to the Aadhaar card has been leaked. An intentional ill person is misusing Aadhaar information to boost the electoral campaign of Puducherry. Such information is *reported that "one of the political parties has been accused of misusing Aadhaar data to boost election campaigns through bulk SMSes to Aadhaar-linked numbers in Puducherry."*

Petitioner stated that they received calls from an unknown number stating the petitioner's name, booth and constituency without revealing information to anyone. The petitioner was shocked to get SMS and phone calls from the number linked to the Aadhaar card. So, it is clear that there is no safe and secure Aadhaar card information UIDAI. Such insecure availability of information preceded the third-party to gain access to information and do whatever they like.

Scrollstaff (2021) cited that "Being the ruling party at the centre, BJP has misused its seat of power and indulged in identity theft, clearly in breach of the fiduciary duty it owes towards its subjects, i.e., the general public".

Hackers leaked the Saini school admission database; parents received a call from the anonymous person to pay money for the school admission. *TimesNowDigital (2020) reported that the article "claimed the caller asking him to pay an amount of INR 10,000 as a one-time payment to get his child admission in Sainik School."*

Social engineering:

The Aadhaar app is available in the google play store, and the app might allow the attackers to access the demographic data of Indian residents from the Aadhar database.

4.3.4. Theme 4: Data protection and privacy measures

Data leakage of Aadhar information through the third-party has been high recently. Such data leakage is controlled through provable guarantees that data is not used for any purpose. Similar protection measures are made in restricting and controlling data leakage through physical access control, personal data protection, creating a new password, legal actions, data removal, shutting down of websites and apps, and debar the third-party to use the information. Such themes represent the data protection and privacy measures, and the detailed description of the theme is given below.

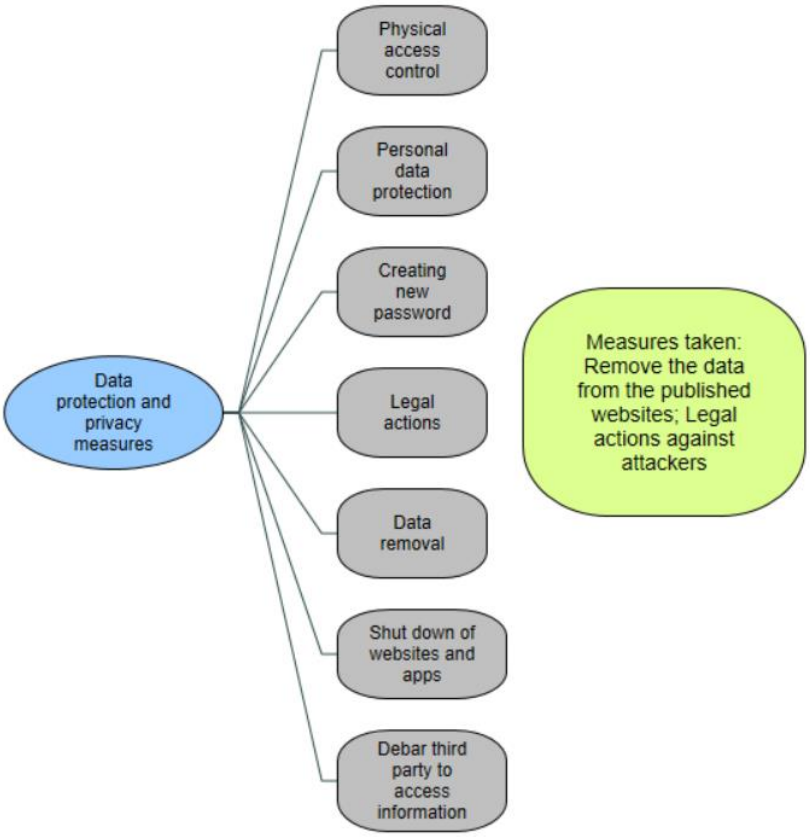

Figure 15. Data protection and privacy measures

Source: Author illustration

Physical access control:

"The RERA (Real Estate Regulatory Authority) website is currently inaccessible, and the insecure link is also deactivated". The article has cited that "the Gujarat RERA website is currently inaccessible on September 20 morning. Also, the download link shared by Elliot cannot be accessed anymore". So, it is clear that one article pinpointing physical access control is the privacy measures adopted by the Gujarat RERA website.

Personal data protection:

Jharkhand state government manages the infrastructure of Aadhar card for the whole nation. This might be the case where the Aadhar system can be breached and data leak could happen. Agencies should be ordered to develop secured IT infrastructure to protect and stop data leaks.

Access to data from third parties must be restricted. API access management and intrusion prevention systems must be strengthened. Security protocols are evaluated regularly to ensure that no attacks on the e-hospital infrastructure occur (Tech2 2018). As a result, a relatively small number of articles is taking measures to safeguard the Aadhar information through well-strengthened infrastructure facilities.

Creating a new password:

As the organization collaborates with its internal management staff, external consultants, and law enforcement authorities to investigate and mitigate the Quora incident, it has taken further steps to enhance platform security. To begin, the information-sharing site emailed all impacted users and signed them out of their Quora accounts. Furthermore, it has made all impacted Quora users' passwords null. So, disabled users must create a new password for their accounts. So, it concludes that the article portrays that the Quora company asked they disable users to create a new password to secure their account.

Legal punishment:

Indian police officials arrested the IIT graduate for accessing the "Aadhaar KYC" data without authorization between Jan 1-26 (*ibid*). Legal action against operators who malpractice of accessing Aadhaar information (*ibid*). Pathak (2018) mentioned that police registered a second FIR with the Byculla police station against Chaudhary, and he was taken into custody for further investigation. UIDAI blocked the operator involved in the leakage of M.S Dhoni Aadhar card for ten years. Some unauthorized websites illegally collect Aadhar information and their details from Delhi people. So UIDAI filed FIR against those unauthorized websites (ExpressNews 2017). An FIR has allegedly been filed against Sameer Kochar. A notice has been given to the agency performing authentication using stored biometrics. Any agencies' licenses were revoked (Singh 2017). Employees of Reliance Jio in Madhya Pradesh use consumer biometrics to unlock additional SIM cards and sell them to others. So alleged persons were arrested for financial fraud (PTI 2019). As a result, legal actions in arresting or fixing charge sheets against the attackers control the misuse of Aadhar information.

Data removal:

Some government websites publish the Aadhar details of the public on the internet. All the published information was removed from government sites (Tech2 2018). Kerala University research scholar information was leaked, and their Aadhar numbers were removed (SFLC 2017). Similarly, the Aadhaar card number of the Andhra Pradesh state housing corporation has been deleted from the primary list display. The Aadhaar card number is masked to show only the last four digits in each person's comprehensive view. onmanorama (2017) reported that 3.5 million pensioners published on websites, ration cardholders' data, and student's details on the E-grant website in Kerala was removed. Most government websites publish Aadhar information, financial and personal details on their respective websites. After the publishing information came to notice, such government websites removed the information in their websites. So, it is clear that most websites remove the data from the sites.

Shutdown the websites and apps:

UIDAI has taken steps to remove the fraudulent websites and apps that provide attackers with information. It also blocked 5000 officials who accessed the portals without authorization (Tech2 2018).

Debar third-party to access Aadhaar information:

Airtel and Airtel payment banks misusing the information. As per the Aadhaar Act, the third-party was barred from accessing customer information without their prior consent.

Thus, it concludes that measures are taken to control data breaches of government websites resolved through data removal of Aadhar information in the respective websites. Secondly, attackers took legal actions to raise the first information report. In most cases, attackers are arrested by Indian police officers.

4.4. Summary of primary outcome

Aadhaar card enrolled billions of people demographic and biometric information. But the security and privacy issues widespread in the workings of Aadhaar lead to leaks and vulnerabilities. Such issues arise owing to the third-party. So, this study measured the security issues and its challenges concerning use through third parties. This study had the data set as newspaper articles. These

articles were evaluated through thematic analysis. The theme for the study was data leakages, privacy issues, security breaches and data protection &privacy measures. Before evaluating the detailed description of themes, this study applied word frequency using NVIVO. The outcome of NVIVO presents below.

Word frequency: It revealed the most frequently used words in media articles. The frequently used words were data, Aadhaar, access, breach, hackers, leakage, cards, UIDAI, information, security, users, personal details, government, security, breach, leaked, and claims. In contrast to the frequency words, online, petition, protection, system, beneficiaries disclosing, vulnerable and authentication were the least used words. After determining the less and most frequent words, a detailed description of themes has been discussed.

The first theme was data leakages of the Aadhar card. Data leakages may be intentional or unintentional threats. The intentional threats were raised because third-party companies breached the information from the central database storage. In contrast to the intentional, improper encryption, publishing in websites and environmental hazards were the inadvertent threats. In environmental hazards, data breaches were made because of vulnerable data storage and third-party data breaches in the dark internet. For improper encryption, data breaches are raised only through third parties. It may be either in websites & apps or an online gateway platform. Data breaches of Aadhar information was the major concern for Indian residents because it was widely available and easily accessible on government websites. There was no prior authorization for accessing the information from the respective government websites.

The second theme was privacy issues. Privacy issues occur owing to misuse of personal information and unauthorized access. Most data breaches happened either to give the attackers political or financial gain. The third theme was security issues. It occurs because of data theft, sabotage and social engineering. A relatively small number of articles, indicating that the third-party breaches the Aadhaar information.
In contrast to data theft, most breaches were made under sabotage. Hackers were doing it for their competitive gain. Finally, a small number of attackers were using social engineering to breach the data.

The fourth and final theme was data protection and privacy measures. Such measures were physical access control, personal data protection, creating a new password, legal actions, data

removal, shutting down websites and apps, and debar the third-party to use the information. Articles represented that a few actions had been taken on physical access control, personal data protection, the shutdown of apps and debar the third-party to use information. On the contrary, most breaches were resolved through data removal in the respective websites or apps. Some of the legal actions (arrest, filling FIR) were taken to avoid raising issues in the Aadhar card.

4.5. Discussion

Aadhar cards data breaches are still largely unsolvable as this concern broader awareness amongst various stakeholders and other participants. So, this study focuses on this particular aspect of the security concerns and tries to explore the context through analysis of media discourses. Similar media discourses have been used previously by (Cross et al. 2019; Guasti, Mansfeldová 2015; Wojtkowski et al. 2020). In this study, media discourses were analysed with the help of qualitative research methods. Several authors have used qualitative research methods to measure security and privacy issues (Guasti and Mansfeldová (2015); Arifin and Lennerfors (2021); Cross et al. (2019); Fornaciari (2014); Aripova, Bashmakova (2019). Some other studies evaluated the Aadhar card security and privacy issues in qualitative research methods. It has been widely used in the literature Agrawal et al. 2017; Anand 2021; Banerjee, Sharma 2019; Bergström 2015; Datta et al. 2020; Ghangare, Ranade 2018; Gordon et al. 2005; Jain 2019; Popović, Hocenski 2010; Shekhar 2018; Tyagi et al. 2018).

Similar methods have been used previously for third-party breaches by Saleem, Naveed 2020; Saleem, Naveed 2020; Cheng et al. 2017; Furnell et al. 2020. On the contrary to the available method, I noticed mixed methods used to measure the media discourse on privacy issues Wojtkowski et al. (2020). To sum up the methods, this study utilized qualitative research methods to measure security concerns through media discourses analysis. Next, data collection for qualitative research was through national newspaper articles. A similar way of data collection is widely used to know the concerns of third-party breaches of Aadhar card Fornaciari (2014); Aripova, Bashmakova (2019); Cross et al. (2019); Wojtkowski et al. (2020). With the support from the Integrated review method, the study gathers the information from the secondary news articles. A similar method of gathering information was found in the previous literature (Guasti and Mansfeldová (2015); Arifin and Lennerfors (2021); Cross et al. (2019); Fornaciari (2014); Aripova, Bashmakova (2019). In this study, qualitative analysis of thematic analysis had

considered. It must be noted that this has been a proven tool for measuring security and privacy issues Agrawal et al. 2017; Anand 2021; Banerjee, Sharma 2019; Bergström 2015; Datta et al. 2020; Ghangare, Ranade 2018; Gordon et al. 2005; Jain 2019; Popović, Hocenski 2010; Shekhar 2018; Tyagi et al. 2018).

In this study, themes observed from the analysis were data leakages, privacy issues, security breaches and data protection &privacy measures. These themes are consistent with previous studies Cheng et al. 2017; Banerjee and Sharma (2019); Raju et al. (2017); Bergström 2015; Agrawal et al. 2017; Anand 2021; Banerjee, Sharma 2019; Bergström 2015; Datta et al. 2020; Ghangare, Ranade 2018; Gordon et al. 2005; Jain 2019; Popović, Hocenski 2010; Shekhar 2018; Tyagi et al. 2018; Saleem, Naveed 2020; Saleem, Naveed 2020; Cheng et al. 2017; Furnell et al. 2020.

CONCLUSION

Over the years, media discourses reported the improper security of thrid parties and breaches of the Aadhar information and educating people on the incidents over Aadhar card. Indians face more breaches, leading to the risk of financial frauds and threats. Apart from the above threats, security issues (Easy access to databases, duplicate cards, publishing of Aadhaar information on government websites) and privacy issues are known concerns in past studies. The problem of third-party data breaches of Aadhar cards is still unsolved. The study analysed the role of media in reporting third-party breaches of Aadhar cards by focusing on addressing the issues in critical discourse analysis. This analysis evaluated the issues based on text and discourse practices and the Aadhar card breaches were classified into four themes: data leakages, privacy issues, security breaches and data protection & privacy measures.

Privacy issues of Aadhar cards are in the form of misuse of personal information, and unauthorized access of information is common for Aadhaar data breaches. Such breaches make in giving political gain or financial gain to the attackers. Next is security issues which include data theft, sabotage and social engineering. Out of three security issues, data theft was higher in Aadhar than sabotage and social engineering issues. Later observing the issues, some actions were taken to protect the information. The actions are physical access control, personal data protection, creating a new password, legal actions, data removal, shutting down websites and apps, and debar the third-party to use the information.

When privacy and security issues come to light, most government websites remove the information from the respective sites. A relatively small number of attackers face legal actions for Aadhar data breaches. So, the study concludes that data breaches of Aadhar information of the third-party prevail more in India. UIDAI should take action to protect the Aadhar ecosystem. Such action can diminish data breaches to happen shortly.

The implication is that UIDAI should be concerned about the media discourses on the Aadhar data breaches and take preventive measures to avoid data breaches in the Aadhar card. However, the

impact of media discourses on the government or UIDAI on changing the data and security policies over third parties cannot be measured. But, this might affect the population sentiments on how UIDAI handles the privacy of the Aadhar data and might invite headwinds in policy trajectory. Fear is a dominant emotion for the population because media discourse affects the population sentiment. Creating awareness through conducting programs, social media campaigns, webinars and development programs can diminish the fear of the population.

Limitations: The findings cannot be generalised due to limited articles portraying Third-party data breaches. Newspaper articles considered for the study are small, and hence it is difficult to exhibit the outcome specific to third-party breaches. In this study, the qualitative analysis examines only the issues, and therefore the results are limited to specific issues. The findings are limited as the study primarily focused on security issues, privacy issues of the third-party and did not explore the data breaches of the third-party.

LIST OF REFERENCES

Agrawal, S., Banerjee, S., Sharma, S. (2017). Privacy and Security of Aadhaar A Computer Science Perspective.

Anand, N. (2021). New Principles for Governing Aadhaar: Improving Access and Inclusion, Privacy, Security, and Identity Management. *Journal of Science Policy & Governance*, 18(01).

Anusha , A. K. R. S., Rajkumar, G. (2017). Privacy and Security Issues in Aadhaar. *IJRASET*, 5(8).

Asnani , V., Godse, V., Bajaj , K. (2010). Security and Privacy Challenges in the Unique Identification Number Project.

Babu, A. (2018). An *Aadhaar data breach proves a design flaw*. Retrieved from https://www.theweek.in/theweek/specials/aadhaar-data-breach-proves-design-flaw.html, 21 January 2018

Banerjee, S., Sharma, S. (2019). Privacy concerns with Aadhaar. *Communications of the ACM*, 62(11), 80-80.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53, 419-426.

Cheng, L., Liu, F., Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5), e1211.

Christopher, N. (2018). *Security experts say need to secure Aadhaar ecosystem, warn about third-party leaks*. Retrieved from https://economictimes.indiatimes.com/news/politics-and-nation/there-is-a-need-to-secure-full-aadhaar-ecosystem-experts/articleshow/63459367.cms, 26 March 2018.

Pali, I., Krishania, L., Chadha, D., Kandar, A., Varshney, G., Shukla, S. (2020). A Comprehensive Survey of Aadhar and Security Issues. *arXiv preprint arXiv:2007.09409*.

Datta, P., Bhardwaj, S., Panda, S.N., Tanwar, S., Badotra, S. (2020). Survey of security and privacy issues on biometric system. In *Handbook of Computer Networks and Cyber Security* (763-776). Springer, Cham.

Drèze, J. (2016). *The Aadhaar coup*. Retrieved from https://www.thehindu.com/opinion/lead/jean-dreze-on-aadhaar-mass-surveillance-data-collection/article8352912.ece, 15 March 2016.

ET. (2017). *Aadhaar mandatory for opening bank account, financial transactions of Rs 50,000 and above.* Retrieved from: https://economictimes.indiatimes.com/news/economy/policy/aadhaar-mandatory-for-opening-bank-account-financial-transactions-of-rs-50000-and-above/articleshow/59177273.cms?from=mdr.

Express News Service. (2016). *Aadhar Bill passed in Lok Sabha, Opposition fears 'surveillance'.* Retrieved from https://indianexpress.com/article/india/india-news-india/aadhar-card-uid-bill-lok-sabha-arun-jaitley/, 12 March 2016.

ExpressNews. (2017). *Now, the Swachh Bharat portal leaks Aadhaar details online.* [Retrieved from https://www.newindianexpress.com/nation/2017/apr/25/now-swachh-bharat-portal-leaks-aadhaar-details-online-1597359--1.html, 25 April 2017.

Fasulo, P. (2021). *What is a third-party breach?.* Retrieved from https://support.securityscorecard.com/hc/en-us/articles/360059301612-What-is-a-third-party-breach-.

Feng, X., Behar-Horenstein, L. (2019). Maximizing NVivo utilities to analyze open-ended responses. *The Qualitative Report*, 24(3), 563-571.

firstpost.com. (2018). *AADHAAR SECURITY BREACHES: HERE ARE THE MAJOR UNTOWARD INCIDENTS THAT HAVE HAPPENED WITH AADHAAR AND WHAT WAS AFFECTED.* Retrieved from https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html, 25 September 2018.

Furnell, S., Heyburn, H., Whitehead, A., Shah, J.N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, 2020(12), 6-12.

Ganjoo, S. (2018). *Quora reports massive data breach, data of 100 million users stolen.* Retrieved from https://www.indiatoday.in/technology/news/story/quora-reports-massive-data-breach-data-of-100-million-users-stolen-1401950-2018-12-04, 04 December 2018.

Ghangare, A., Ranade, A. (2018). Aadhar card–Perspectives on privacy. *Journal of International Pharmaceutical Research*, 46(5), 135-142.

Goddijn , I., Kouns , J. (2021). *Risk based security. 2020 q1 report data breach quick view*.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R. (2005). 2005 CSI/FBI computer crime and security survey. *Computer Security Journal*, 21(3), 1.

Government press. (2003). *Gazette Vide GSR No. 937(E)*.

Gupta, R., Gupta, A., Gupta, S. (2018). Aadhaar:-A Digital Financial Revolution.

Gurung, M. (2021). *MobiKwik Hacked! Sensitive Details Of 10 Crore Users Being Sold For Rs 69 Lakh; Company Denies.* Retrived from

https://trak.in/tags/business/2021/03/30/mobikwik-hacked-sensitive-details-of-10-crore-users-being-sold-for-rs-69-lakh-company-denies/, 30 March 2021.

Halpern, E. S. (1984). Auditing naturalistic inquiries: The development and application of a model (Doctoral thesis). Indiana University.

Hassanzadeh, Z., Biddle, R., Marsen, S. (2021). User Perception of Data Breaches. *IEEE Transactions on Professional Communication*.

Hearst, M.A. and Rosner, D. (2008). Tag clouds: Data analysis tool or social signaller?. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)* (160-160). IEEE.

India, G. (2010). *Policy on Open Standards for e-Governance.* Retreived from http://egovstandards.gov.in/sites/default/files/Policy%20on%20Open%20Standards%20for%20e-Governance.pdf.

Jain, M. (2019). The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment. *The Henry M. Jackson School of International Studies at the University of Washington*.

Jain, R., Gill, P. (2020). *CSC BHIM site left Aadhaar cards, PAN numbers, and biometric information exposed — could be used to carry out financial fraud and identity theft, says report.* Retreived from https://www.businessinsider.in/tech/news/bhim-app-left-aadhaar-cards-pan-numbers-and-biometric-information-exposed/articleshow/76135419.cmsU, 01June2020.

Johari, A. (2016). *In drought-hit Saurashtra, a poor internet network can often mean no food rations.* Retreived from https://scroll.in/article/810683/in-drought-hit-saurashtra-no-internet-can-often-mean-no-food-rations, 29 June 2016.

Justice, M. (2008). *A national framework for greater citizen engagement.* Retreived from: http://data.parliament.uk/DepositedPapers/Files/DEP2008-1881/DEP2008-1881.pdf, 06 July 2008.

Kabir, S. M. (2016). Sample and sampling designs.

Khaira, R. (2018). *Rs 500, 10 minutes, and you have access to billion Aadhaar details.* Retreived from https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361, 05 January 2018.

Khera, R. (2019). *Dissent on Aadhaar: Big Data Meets Big Brother.* Retreived from https://orientblackswan.com/details?id=9789352875429

Kodali, S. (2017). *The major website which was leaking 10,96,41,502 Aadhaar numbers was the mnrega MIS portal. The state-wise split and Bank A/C connections in the pic.* Retreived from https://twitter.com/digitaldutta/status/859047296096514048, 01 May 2017.

Kumar, A. (2019). *A presentation by a Technical expert of UIDAI.* Retreived from http://trai.gov.in/sites/default/files /presentations & cv/Day-3_25Aug2017/Session2_Digital %20world/Digital%20Identifier Ashok%20Kumar.pdf.

Kumar, A. (2019). *A study of security, privacy and acceptability aspect of Aadhaar* (Doctoral dissertation, IIPA, New Delhi).

Lincoln, Y. S., Guba, E. G. (1985). Naturalistic inquiry. Thousand Oaks, CA: Sage.

Logix. (2018). *With the increasing third-party leaks, Aadhar Card systems need security reviews.* Retreived from https://blog.logix.in/aadhar-card-third-party-leaks/.

Madan, H.K.S.D.S. A Study on Aadhar Privacy and Personal Security Issues in India.

Meta. (2016). *List of Recommendations on the Aadhaar Bill, 2016 - Letter Submitted to the Members of Parliament.* Retreived from https://cis-india.org/internet-governance/blog/list-of-recommendations-on-the-aadhaar-bill-2016, 16 March 2016.

Mukherjee , A. (2019). *Aadhaar leaks again: Indane Gas website, app leak data of 6.7 million subscribers.* Retreived from https://www.indiatoday.in/technology/news/story/aadhaar-leaks-again-indane-gas-website-app-leak-data-of-6-7-million-subscribers-1459499-2019-02-19, 19 feburary 2019.

NDTV. (2016). *Truth vs Hype: Aadhaar One Billion Challenge.* Retreived from https://www.ndtv.com/video/list/shows/truth-vs-hype/page/5

NDTV. (2018). *In A Week, Aadhaar Data Of 70 Lakh Children On Andhra Pradesh Government Sites.* Retreived from https://www.ndtv.com/india-news/despite-laws-no-action-against-government-agencies-displaying-aadhaar-data-1844747, 30 April 2018.

onmanorama, 2017. *Aadhaar leak: 35 lakh people in Kerala have their data breached.* Retreived from https://www.onmanorama.com/news/kerala/2017/04/25/aadhaar-leak-people-kerala-personal-data-breached.html, 25 April 2017.

Onwuegbuzie, A. J., Leech, N. L. (2007). Validity and qualitative research: An oxymoron? Quality & Quantity, 41(2), 233-249.

Opderbeck, D.W. (2015). Cybersecurity, data breaches, and the economic loss doctrine in the payment card industry. *Md. L. Rev.*, 75, 935.

Pali, I., Krishania, L., Chadha, D., Kandar, A., Varshney, G., Shukla, S. (2020). A Comprehensive Survey of Aadhar and Security Issues. *arXiv preprint arXiv:2007.09409*.

Pathak, M. K. (2018). *Forty bank accounts opened using forged documents in Mumbai, used for export-import business.* Retreived from https://www.hindustantimes.com/mumbai-news/40-bank-accounts-opened-using-forged-documents-in-mumbai-used-for-export-import-business/story-7JpH2wGBI4SwlIBnmhBdcL.html, 31 March 2018.

Ponemon Institute. (2019). *Cost of a Data Breach Report*, IBM Security.

Popović, K., Hocenski, Ž. (2010). Cloud computing security issues and challenges. In *The 33rd international convention mipro* (344-349). IEEE.

Pratap, K. (2021). *Exclusive: Millions of Airtel numbers with Aadhaar details and user data likely leaked, were accessible on web.* Retreived from: https://www.indiatoday.in/technology/news/story/exclusive-millions-of-airtel-numbers-with-aadhaar-details-and-user-data-likely-leaked-were-accessible-on-web-1765247-2021-02-02, 2 feburary 2021.

PTI. (2017). *Over 200 govt websites made Aadhaar details public: UIDAI.* Retreived from https://timesofindia.indiatimes.com/india/210-govt-websites-made-public-aadhaar-details-uidai/articleshow/61711303.cms, 19 November 2017.

PTI. (2019). *MP: Major SIM card fraud involving biometrics busted, five held.* Retreived from https://www.business-standard.com/article/pti-stories/mp-major-sim-card-fraud-involving-biometrics-busted-5-held-119120901099_1.html, 09 December 2019.

Raju, R.S., Singh, S., Khatter, K. (2017). Aadhaar Card: Challenges and Impact on Digital Transformation. *arXiv preprint arXiv:1708.05117*.

Report, G. (2021, September 10). Republic TV least, NDTV most trusted news channel: oxford survey. Ground Report. https://groundreport.in/republic-tv-least-ndtv-most-trusted-news-channel-oxford-survey/

Rivadeneira, A.W., Gruen, D.M., Muller, M.J., Millen, D.R. (2007). Getting our head in the clouds: toward evaluation studies of tagclouds. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (1995-998).

Sabarwal, H. (2020). *Over 1 lakh national IDs of Indians put on Dark Web for sale: Report.* Retreived from https://www.hindustantimes.com/india-news/over-1-lakh-national-ids-of-indians-put-on-dark-web-for-sale-report/story-tRQeExGVzO0lVYTpSwL0BP.html, 3 June 2020.

Saleem, H., Naveed, M. (2020). SoK: Anatomy of Data Breaches. *Proc. Priv. Enhancing Technol.*, 2020(4), 153-174.

Sandelowski, M. (2001). Real qualitative researchers don't count: The use of numbers in qualitative research. *Research in Nursing & Health*, 24, 230-240.

ScrollStaff. (2021). *BJP accused of stealing Aadhaar data in Puducherry for poll campaign, Madras HC expresses concern.* Retreived from https://scroll.in/latest/990652/bjp-accused-of-stealing-aadhaar-data-in-puducherry-for-poll-campaign-madras-hc-expresses-concern, 26 March 2021.

Sethi, A., Bansal , S., Roy, S. (2017). *Details of over a million Aadhaar numbers were published on the Jharkhand govt website.* Retreived from https://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFlScg5Dn5neLyBzrkw1I.html, 19 July 2017.

SFLC. (2017). *News reports of Aadhaar numbers and related information leaking have frequently been appearing since early February 2017.* Retreived from https://sflc.in/uidai-aadhaar-breaches-and-leaks, 24 April 2017.

Sharma, S.A.S.B.S., Privacy and Security of Aadhaar.

Sharma, V. (2011). Aadhaar-a unique identification number: Opportunities and challenges ahead. *Research Cell: An International Journal of Engineering Science*, 4(2), 169-176.

Shekhar, S. (2018). Privacy and Security in Aadhaar.

Sifty, (2020). *409 GB of 72.30 lakh Indians leaked, NPCI says BHIM app is safe.* Retreived from https://www.sify.com/finance/409-gb-of-7230-lakh-indians-leaked-npci-says-bhim-app-is-safe-news-topnews-ugbt9gchjdcae.html, 2 June 2020.

Sikri, A. (2018). *Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September 2018.* Retreived from https://indiankanoon.org/doc/127517806/.

Sinclair, J., Cardew-Hall, M. (2008). The folksonomy tag cloud: when is it useful?. *Journal of Information Science*, 34(1), 15-29.

Singh, P. (2021). Aadhaar and data privacy: biometric identification and anxieties of recognition in India. *Information, Communication & Society*, 24(7), 978-993.

Singh, V. (2017). *UIDAI plugging data leak: Author.* Retreived from https://www.thehindu.com/news/national/uidai-plugging-data-leak-author/article17413747.ece, 06 March 2017.

Sinha, A., Kodali, S. (2017). Information Security Practices of Aadhaar (or Lack Thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information. *The Centre for Internet and Society, India*, 16.

Soni, Y. (2019). *Thousands Of Farmers' Aadhaar Data Exposed In Andhra Pradesh.* Retreived from https://inc42.com/buzz/farmers-aadhaar-data-exposed-in-andhra-pradesh/, 29 May 2019.

Soni, Y. (2019). *Yet Another Data Leak In Indian Government Database, Exposes Multiple Citizen IDs.* Retreived from https://inc42.com/buzz/yet-another-data-leak-in-indian-government-database-exposes-multiple-citizen-ids/, 20 September 2019.

Sundareswaran, V. (2018). STUDY OF CYBERSECURITY IN DATA BREACHING.

Tech2. (2018). *AADHAAR SECURITY BREACHES: HERE ARE THE MAJOR UNTOWARD INCIDENTS THAT HAVE HAPPENED WITH AADHAAR AND WHAT WAS AFFECTED.* Retreived from https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html, 25 September 2018.

Tessem, B., Bjørnestad, S., Chen, W., Nyre, L. (2015). Word cloud visualisation of locative information. *Journal of location Based services*, 9(4), 254-272.

TimesNow. (2021). *'How did BJP get numbers of voters linked to Aadhaar in Puducherry?': Madras HC directs UIDAI to probe matter.* Retreived from https://www.timesnownews.com/india/puducherry/article/how-did-bjp-get-numbers-of-

voters-linked-to-aadhaar-in-puducherry-madras-hc-directs-uidai-to-probe-matter/739795, 01 April 2021.

TimesNowDigital. (2020). *Student's details leaked from Sainik School database, parents file a complaint - Read details here.* Retreived from https://www.timesnownews.com/education/article/students-details-leaked-from-sainik-school-database-parents-file-complaint-read-details-here/543834, 23 January 2020.

Totapally, S. et al., (2019). *State of Aadhaar: A People's Perspective.* Retreived from https://stateofaadhaar.in/assets/download/SoA_2019_Report_web.pdf.

Tyagi, A.K., Rekha, G., Sreenath, N. (2018). Is your privacy safe with Aadhaar?: an open discussion. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (318-323). IEEE.

UIDAI. (2010). *UIDAI Strategy Overview*, New Delhi.

UIDAI. (2015). *Unique Identification Authority of India.* Retreived from https://uidai.gov.in/about-uidai.html.

UIDAI. (2019). *Aadhaar Myth Busters.* Retreived from https://uidai.gov.in/my-aadhaar/about-your-aadhaar/security-in-uidai-system.html.

UIDAI. (2019). *What is Aadhaar*. Retreived from https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html.

UIDAI, n.d. *The UIDAI Ecosystem.* Retreived from https://uidai.gov.in/ecosystem/uidai-ecosystem.html.

Vidyut, (2018). *#AadhaarLeaks – A Continuously Updated List Of All Aadhaar Data Leaks.* Retreived from https://www.medianama.com/2018/05/223-aadhaar-leaks-list/, 04 May 2018.

Vikaspedia, n.d. *Benefits of Aadhaar card.* Retreived from http://vikaspedia.in/e-governance/online-citizen-services/governmentto-citizen-services-g2c/all-about-aadhaar/17-benefits-of-aadhaar-card.

Viswanath, L. (2017). *Four Reasons You Should Worry About Aadhaar's Use of Biometrics.* Retreived from https://thewire.in/rights/real-problem-aadhaar-lies-biometrics, 28 March 2017.

Vudali, S. (2019). *Aadhaar details of 7.82 crore from Telangana and Andhra found in possession of IT Grids (India) Pvt Ltd.* Retreived from https://timesofindia.indiatimes.com/city/hyderabad/aadhaar-details-of-7-82-crore-from-telangana-and-andhra-found-in-possession-of-it-grids-india-pvt-ltd/articleshow/68865938.cms, 13 April 2019.

Wilson, M., Hurlock, J., Wilson, M. (2012). Keyword clouds: having very little effect on sensemaking in web search engines. In *CHI'12 Extended Abstracts on Human Factors in Computing Systems* (2069-2074).

Wirestaff. (2018). *Unsecure Utility Service Provider is Leaking Aadhaar Details, Says Report.* Retreived from https://thewire.in/government/unsecure-utility-service-provider-is-leaking-aadhaar-details-says-report, 24 March 2018.

Yadav, A. (2016). *Rajasthan presses on with Aadhaar after fingerprint readers fail: Well, buy iris scanners.* Retreived from https://scroll.in/article/806243/rajasthan-presses-on-with-aadhaar-after-fingerprint-readers-fail-well-buy-iris-scanners, 10 April 2016.

APPENDICES

Appendix 1. Word frequency for Aadhar security issues where actions were taken

Word	Length	Count	Weighted Percentage (%)	Similar Words
data	4	87	2.59	data
aadhaar	7	61	1.82	aadhaar
number	6	58	1.73	number, numbers
details	7	35	1.04	detailed, details
cards	5	31	0.92	card, cards
uidai	5	30	0.89	uidai
access	6	29	0.86	access, accessed, accessible, accessing
breach	6	29	0.86	breach, breached
information	11	27	0.81	information, informed
security	8	27	0.81	secure, security
users	5	24	0.72	user, users, users’
india	5	23	0.69	india
hackers	7	21	0.63	hacker, hackers
personal	8	21	0.63	person, personal
phone	5	21	0.63	phone, phones
leaked	6	21	0.63	leak, leaked, leaks
used	4	20	0.60	use, used, uses, using
airtel	6	19	0.57	airtel
bank	4	19	0.57	bank, banking, banks
group	5	19	0.57	group, groups
also	4	16	0.48	also
report	6	16	0.48	report, reportedly, reports
bjp	3	15	0.45	bjp
million	7	15	0.45	million, millions
allegedly	9	14	0.42	allegation, allegations, alleged, allegedly
like	4	14	0.42	like, likely, likes
researchers	11	14	0.42	research, researcher, researchers
team	4	14	0.42	team, teams
website	7	14	0.42	website, websites
whatsapp	8	14	0.42	whatsapp
added	5	13	0.39	added, adding

mobile	6	13	0.39	mobile
name	4	13	0.39	name, named, names
public	6	13	0.39	public, publicly
puducherry	10	13	0.39	puducherry
government	10	12	0.36	government, governments
accounts	8	12	0.36	account, accounts
address	7	12	0.36	address, addresses
including	9	12	0.36	include, includes, including
may	3	12	0.36	may
one	3	11	0.33	one
party	5	11	0.33	parties, party
voters	6	11	0.33	voters
web	3	11	0.33	web
database	8	11	0.33	database, databases
aadhar	6	10	0.30	aadhar
asked	5	10	0.30	ask, asked, asks
authority	9	10	0.30	authorities, authority
exposed	7	10	0.30	exposed, exposing
indian	6	10	0.30	indian, indians, indians'
linked	6	10	0.30	link, linked
privacy	7	10	0.30	privacy
sharing	7	10	0.30	share, shared, shares, sharing
make	4	9	0.27	make, makes, making
500	3	9	0.27	500
bhim	4	9	0.27	bhim
booth	5	9	0.27	booth, booths
cloning	7	9	0.27	clone, cloned, cloning
company	7	9	0.27	company
cyble	5	9	0.27	cyble
hacked	6	9	0.27	hack, hacked, hacking, hacks’
however	7	9	0.27	however
lakh	4	9	0.27	lakh
level	5	9	0.27	level, levelled
people	6	9	0.27	people
provide	7	9	0.27	provide, provided, provider
sale	4	9	0.27	sale
state	5	9	0.27	state, stated
email	5	9	0.27	email, emails
get	3	9	0.27	get, getting
biometric	9	8	0.24	biometric, biometrics
claimed	7	8	0.24	claim, claimed, claiming, claims
court	5	8	0.24	court
fingerprints	12	8	0.24	fingerprint, fingerprints, fingerprints’

mobikwik	8	8	0.24	mobikwik
pan	3	8	0.24	pan
police	6	8	0.24	police
received	8	8	0.24	received, receiver, receiving
records	7	8	0.24	record, records
service	7	8	0.24	service, services
theft	5	8	0.24	theft, thefts
created	7	7	0.21	create, created, creating
individual	10	7	0.21	individual, individuals
reveal	6	7	0.21	reveal, revealed, reveals
act	3	7	0.21	act, acts
citizen	7	7	0.21	citizen, citizens, citizens'
correspondent	13	7	0.21	correspondent
dark	4	7	0.21	dark
identity	8	7	0.21	identity
ids	3	7	0.21	ids
mail	4	7	0.21	mail, mails
matter	6	7	0.21	matter
money	5	7	0.21	money
online	6	7	0.21	online
petition	8	7	0.21	petition, petitions
protection	10	7	0.21	protect, protected, protection
system	6	7	0.21	system, systems
beneficiaries	13	6	0.18	beneficiaries, beneficiaries'
complete	8	6	0.18	complete, completely
confirm	7	6	0.18	confirm, confirmed, confirming

Source: NVIVO, author's calculations

Appendix 2. Word frequency for Aadhar security issues where actions were taken

Word	Length	Count	Weighted Percentage (%)	Similar Words
aadhaar	7	209	3.73	#aadhaar, aadhaar
numbers	7	78	1.39	number, numbers
details	7	71	1.27	detailing, details
government	10	71	1.27	governance, government, governments, governs
uidai	5	58	1.04	@uidai, uidai
report	6	57	1.02	report, reported, reportedly, reporter, reporters, reports
website	7	50	0.89	website, websites, websites’
security	8	45	0.80	secure, secured, securing, security
accounts	8	42	0.75	account, accountability, accountable, accounts
breach	6	41	0.73	breach, breached, breaches, breaching
database	8	41	0.73	database, databases
information	11	32	0.57	information, informed
access	6	32	0.57	access, access’, accessed, accessible, accessing
leaked	6	31	0.55	leaked, leaking, leaks
states	6	29	0.52	state, stated, states, stating
police	6	27	0.48	police
cards	5	26	0.46	cards
million	7	23	0.41	million, millions
public	6	23	0.41	public, public’, publication, publicly
citizens	8	23	0.41	citizen, citizens
india	5	22	0.39	india
jharkhand	9	22	0.39	jharkhand
people	6	22	0.39	people
authority	9	21	0.38	author, authored, authorities, authority
according	9	19	0.34	according, accordingly
biometric	9	18	0.32	biometric, biometrics
company	7	18	0.32	companies, company
official	8	18	0.32	official, officials
system	6	18	0.32	system, system’, systems
investigative	13	17	0.30	investigate, investigated, investigating,

				investigation, investigations, investigative, investigator
found	5	17	0.30	found
identification	14	16	0.29	identification
using	5	16	0.29	using
including	9	16	0.29	include, included, includes, including
personal	8	16	0.29	person, personal, persons
services	8	15	0.27	service, services, services’
digital	7	15	0.27	digit, digital
provider	8	15	0.27	provide, provided, provider
users	5	15	0.27	users
exposed	7	14	0.25	expose, exposed, exposes, exposing
filed	5	14	0.25	filed, filing
address	7	14	0.25	address, addressed, addresses, addressing
based	5	14	0.25	based
indian	6	14	0.25	indian, indians
social	6	14	0.25	social
unique	6	14	0.25	unique
without	7	14	0.25	without
claims	6	13	0.23	claim, claimed, claiming, claims
court	5	13	0.23	court, courts
private	7	13	0.23	private
complaint	9	12	0.21	complaint, complaints
design	6	12	0.21	design, designation, designed, designing
documents	9	12	0.21	documents
individual	10	12	0.21	individual, individuals
issue	5	12	0.21	issue, issued, issues, issuing
naming	6	12	0.21	named, names, naming
publishing	10	12	0.21	publish, published, publishing
technology	10	12	0.21	technological, technologies, technology
pradesh	7	11	0.20	pradesh
related	7	11	0.20	related
scheme	6	11	0.20	scheme, schemes
school	6	11	0.20	school
several	7	11	0.20	several
supreme	7	11	0.20	supreme
allegedly	9	10	0.18	allegations, alleged, allegedly
department	10	10	0.18	department, departments

illegally	9	10	0.18	illegal, illegally
andhra	6	10	0.18	andhra
first	5	10	0.18	first
making	6	10	0.18	makes, making
multiple	8	10	0.18	multiple
pension	7	10	0.18	pension, pensioners, pensions
since	5	10	0.18	since
affected	8	9	0.16	affect, affected
anderson	8	9	0.16	anderson
customers’	10	9	0.16	custom, customer, customer’, customers, customers', customers’
cyber	5	9	0.16	cyber
demographic	11	9	0.16	demographic
direct	6	9	0.16	direct, direction, directly
director	8	9	0.16	director, directorate, directors
hacks	5	9	0.16	hacked, hacking, hacks
identity	8	9	0.16	identities, identity
legal	5	9	0.16	legal, legality, legally
misuse	6	9	0.16	misuse, misused, misusing
phone	5	9	0.16	phone, phones
portal	6	9	0.16	portal, portals
questions	9	9	0.16	question, questioned, questioning, questions
right	5	9	0.16	right, rightful, rights
taken	5	9	0.16	taken
vulnerable	10	9	0.16	vulnerabilities, vulnerability, vulnerable
authentication	14	9	0.16	authenticate, authentication, authenticator, authenticity
tweeted	7	9	0.16	tweet, tweeted, tweets
action	6	8	0.14	action, actions
allows	6	8	0.14	allow, allowing, allows
anyone	6	8	0.14	anyone
beneficiaries	13	8	0.14	beneficiaries
chaudhary	9	8	0.14	chaudhary
dhoni	5	8	0.14	dhoni
disclosing	10	8	0.14	disclose, disclosed, disclosing
major	5	8	0.14	major, majority

Source: NVIVO, author’s calculations

Appendix 3. Media articles gathered

S. No	Article	Source	Date
1	"Chinese Hackers Targeted Aadhaar Database, Times Group: Report"	"https://www.ndtv.com/india-news/chinese-hackers-targeted-aadhaar-database-times-group-report-2549166"	Sep, 2021
2	"How did BJP get numbers of voters linked to Aadhaar in Puducherry?': Madras HC directs UIDAI to probe matter"	"https://www.timesnownews.com/india/puducherry/article/how-did-bjp-get-numbers-of-voters-linked-to-aadhaar-in-puducherry-madras-hc-directs-uidai-to-probe-matter/739795"	Apr, 2021
3	"Puducherry BJP accused of stealing Aadhaar info to add voters to WhatsApp groups"	"https://www.thenewsminute.com/article/puducherry-bjp-accused-stealing-aadhaar-info-add-voters-whatsapp-groups-145928"	Mar, 2021
4	"MobiKwik Hacked! Sensitive Details Of 10 Crore Users Being Sold For Rs 69 Lakh"	"https://trak.in/tags/business/2021/03/30/mobikwik-hacked-sensitive-details-of-10-crore-users-being-sold-for-rs-69-lakh-company-denies/"	Mar, 2021
5	"Millions of Airtel numbers with Aadhaar details and user data likely leaked, were accessible on web"	"https://www.indiatoday.in/technology/news/story/exclusive-millions-of-airtel-numbers-with-aadhaar-details-and-user-data-likely-leaked-were-accessible-on-web-1765247-2021-02-02"	Feb, 2021
6	"UP: Man learns 'cloning fingerprints' online, 'hacks' 500 bank accounts"	"https://timesofindia.indiatimes.com/city/bareilly/man-26-learns-cloning-fingerprints-online-hacks-nearly-500-accounts-with-bank-mitrass-help/articleshow/81158623.cms"	Feb, 2021
7	"Copies of your Aadhaar card, PAN card, passport might be on dark net for sale"	"https://www.livemint.com/news/india/copies-of-your-aadhaar-card-pan-card-passport-might-be-on-dark-net-for-sale-11591178597910.html"	Jun, 2020
8	"CSC BHIM site left Aadhaar cards, PAN numbers, and biometric information exposed — could be used to carry out financial fraud and identity theft"	"https://www.businessinsider.in/tech/news/bhim-app-left-aadhaar-cards-pan-numbers-and-biometric-information-exposed/articleshow/76135419.cms"	Jun, 2020
9	"Gujarat real estate authority website leaked confidential data such as PAN passport, Aadhaar, and income tax information due to one of its unprotected download URL.	"https://inc42.com/buzz/yet-another-data-leak-in-indian-government-database-exposes-multiple-citizen-ids/"	Sep, 2019

	https://gujrera.gujarat.gov.in/download"		
10	"IT Grids, a firm hired by the Telugu Desam Party (TDP) to build its Seva Mitra app, has allegedly stored the data of 7.82 crore Indians from Andhra Pradesh and Telangana."	"https://www.firstpost.com/india/aadhaar-data-leak-details-of-7-82-cr-indians-from-ap-and-telangana-found-on-it-grids-database-6448961.html"	Apr, 2019
11	"Aadhaar leaks again: Indane Gas website, app leak data of 6.7 million subscribers"	"https://www.indiatoday.in/technology/news/story/aadhaar-leaks-again-indane-gas-website-app-leak-data-of-6-7-million-subscribers-1459499-2019-02-19"	Feb, 2019
12	"Jharkhand government has allegedly been spotted leaking the Aadhaar numbers and other personal details of thousands of governments workers on its website"	"https://gadgets.ndtv.com/internet/news/aadhaar-leak-jharkhand-government-reportedly-exposed-details-of-thousands-of-workers-1986719"	Feb, 2019
13	"Quora, the hack exposed the sensitive details of 100 million people. This contains information such as a user's name, email address, and an encrypted version of their password. Users' information imported from other related networking services has also been hacked."	"https://www.indiatoday.in/technology/news/story/quora-reports-massive-data-breach-data-of-100-million-users-stolen-1401950-2018-12-04"	Dec, 2018
14	"An IIT graduate was arrested in August 2017 for allegedly accessing the Aadhaar database between January 1 and July 26 without authorization. He developed an app named 'Aadhaar eKYC' by breaking into the servers of a 'e-Hospital infrastructure' built as part of the Digital India initiative. Both requests will then be routed via those servers by the eKYC client."	"https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html"	Sep, 2018
15	"TRAI chief's personal details leaked after he shares Aadhaar number in challenge to hackers"	"https://www.newindianexpress.com/nation/2018/jul/28/trai-chiefs-personal-details-leaked-after-he-shares-aadhaar-number-in-challenge-to-hackers-1850002.html"	Jul, 2018
16	"A Hyderabad-based cyber security researcher found 3	"https://www.ndtv.com/india-news/despite-laws-no-action-against-	Apr, 2018

	different portals of the Andhra Pradesh government disclosing Aadhaar numbers of 90 lakh adults and 70 lakh children in the last seven days."	government-agencies-displaying-aadhaar-data-1844747"	
17	"40 bank accounts opened using forged Aadhar cards documents in Mumbai, used for export-import business"	"https://www.hindustantimes.com/mumbai-news/40-bank-accounts-opened-using-forged-documents-in-mumbai-used-for-export-import-business/story-7JpH2wGBI4SwlIBnmhBdcL.html"	Mar, 2018
18	"A state-run utility service provider's unsecure application programming interface (API) is leaking Aadhaar information."	"https://thewire.in/government/unsecure-utility-service-provider-is-leaking-aadhaar-details-says-report"	Mar, 2018
19	"Aadhaar app hacked in one minute; 22,000 card details exposed"	"https://www.newsbytesapp.com/news/india/ethical-researcher-hacks-aadhaar-app-within-a-minute/story"	Mar, 2018
20	"The Aadhaar data leak demonstrates a programming error. Aadhaar was never created with the individual in mind. It was never intended to be concerned with the sensitivity of people's data, as well as their safety and rights. - Rajeev Chandrasekhar, Member of Parliament"	"https://www.theweek.in/theweek/specials/aadhaar-data-breach-proves-design-flaw.html"	Jan, 2018
21	"The Indian Express, money was fraudulently deducted from bank accounts using customers' Aadhaar numbers."	"https://www.thequint.com/news/india/aadhaar-data-breach-glitches-data-security-compromised-earlier#read-more"	Jan, 2018
22	"Rs 500, 10 minutes, and you have access to billion Aadhaar details"	"https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361"	Jan, 2018
23	"UIDAI, more than 200 Central and state government websites publicly showed information such as names and addresses of some Aadhaar beneficiaries on November 19, 2017."	"https://www.thequint.com/news/india/aadhaar-data-breach-glitches-data-security-compromised-earlier#read-more"	Nov, 2017
24	"UIDAI reveals 210 govt websites made Aadhaar details public, did not specify when breach took place"	"https://www.firstpost.com/india/uidai-reveals-210-govt-websites-made-aadhaar-details-public-did-not-specify-when-breach-took-place-4217597.html"	Nov, 2017
25	"The major website which was leaking 10,96,41,502 Aadhaar numbers was mnrega MIS	"https://twitter.com/digitaldutta/status/859046376084303873"	May, 2017

	portal. The state wise split and Bank A/C connections"		
26	"Kerala University has been discovered to be leaking research scholar info. On April 30, 2017, it was reported"	"https://sflc.in/uidai-aadhaar-breaches-and-leaks"	Apr, 2017
27	"Andhra Pradesh State Housing Corporation was discovered to be leaking beneficiary information such as identity, ration card number, Aadhar card number, and more."	"https://thelogicalindian.com/news/aadhaa r-data-leak/"	Apr, 2017
28	"The Kendriya Sainik Board Secretariat, Ministry of Defense, Central Government, was discovered to have released Aadhaar information of 5500 scholarship students."	"https://www.timesnownews.com/education/article/students-details-leaked-from-sainik-school-database-parents-file-complaint-read-details-here/543834"	Apr, 2017
29	"The Social Justice Department of Gujarat leaked the Aadhaar numbers, identities, emails, mobile numbers, parents' names, bank account information, and institutions of many, but not all, of the 35,500 scholarship recipients."	"https://sje.gujarat.gov.in/showPage.aspx?&lang=English"	Apr, 2017
30	"In Kerala, information on 35,00,000 pensioners was leaked, including their Aadhaar number, name, photo, address, phone number, and bank account number."	"https://www.onmanorama.com/news/kerala/2017/04/25/aadhaar-leak-people-kerala-personal-data-breached.html"	Apr, 2017
31	"As a result of a programming mistake, the Jharkhand Directorate of Social Security leaked the names, emails, Aadhaar numbers, and bank account details of 1.6 million pensioners' beneficiaries."	"https://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFlScg5Dn5neLyBzrkw1I.html"	Apr, 2017
32	"Without any kind of authentication, the Kerala SC/ST scholarship website leaked students' records, including their Aadhaar number, bank account number, and more."	"https://english.mathrubhumi.com/news/kerala/data-leak-on-kerala-scholarship-website-resolved-claims-c-dit-1.5034523"	Apr, 2017
33	"The Aadhaar numbers were leaked by the Swachh Bharat	"https://www.newindianexpress.com/nation/2017/apr/25/now-swachh-bharat-	Mar, 2017

	Mission, Ministry of Water and Sanitation (Central Government).”	portal-leaks-aadhaar-details-online-1597359--1.html.”	
34	“Sameer Kochhar disclosed video evidence of a breach that could be used by using retained biometric information for authentication.”	“https://www.thehindu.com/news/national/uidai-plugging-data-leak-author/article17413747.ece”	Mar, 2017
35	“Employees of Reliance Jio in Madhya Pradesh is accused of using consumer biometrics to unlock additional SIM cards and then selling them to others.”	“https://www.business-standard.com/article/pti-stories/mp-major-sim-card-fraud-involving-biometrics-busted-5-held-119120901099_1.html”	Feb, 2017

Source: Author’s data gathering

Appendix 4. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[11]

I _____ (*author's name*)

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis
_____
_____
_____,
(*title of the graduation thesis*)

supervised by_____,
(*supervisor's name*)

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

_____ (date)

[1] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.*