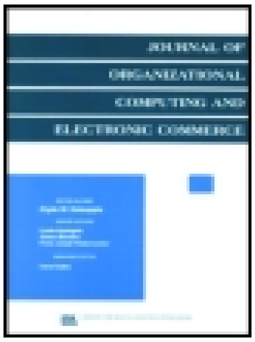

Taylor & Francis
Taylor & Francis Group

Journal of Organizational Computing and Electronic Commerce

ISSN: 1091-9392 (Print) 1532-7744 (Online) Journal homepage: https://www.tandfonline.com/loi/hoce20

Systems theoretic process analysis of information security: the case of aadhaar

Pratik Tarafdar & Indranil Bose

JOURNAL OF ORGANIZATIONAL COMPUTING AND ELECTRONIC COMMERCE
https://doi.org/10.1080/10919392.2019.1598608

Taylor & Francis
Taylor & Francis Group

Systems theoretic process analysis of information security: the case of aadhaar

Pratik Tarafdar[a] and Indranil Bose[a]

[a]Management Information Systems, Indian Institute of Management Calcutta, Kolkata, West Bengal, India

ABSTRACT

A new way of thinking about cybersecurity is much needed to deal with the complex and dynamic cyber-ecosystem. In this paper, we introduce a systems thinking based approach for solving problems related to cybersecurity. We adapt the powerful safety-hazard analysis method, Systems Theoretic Process Analysis (STPA) based on systems theory to analyze the cybersecurity related features of India's massive digital identity program, Aadhaar. Our findings produce important insights. On one hand, it helps identify the security gaps of the Aadhaar system, and on the other hand, it provides controls using systems thinking to overcome these gaps. We contribute to understanding the world of cybersecurity practices and develop risk mitigation strategies that can benefit the Aadhaar.

KEYWORDS

Aadhaar; cybersecurity; risk management; process analysis; systems theory; systems thinking

1. Introduction

With the rapid developments of IT and proliferation of the Internet of Things, the interconnectedness within the cyberspace is increasing. At the same time, it is creating a growing threat of cybercrimes in the form of social engineering attacks and hacking. Owing to this, there is an increasing demand for mitigating losses from cyber-incidents. The cyber-attack on critical infrastructures such as e-government systems has posed severe concerns across different government agencies, public-private sectors, and individual citizens (Gostojić et al. 2012). One such example is the series of security attacks on India's digital identification and authentication project Aadhaar. It is considered to be the world's largest biometric database of citizens built for financial inclusion and social protection. Such a huge store of valuable information is susceptible to both internal and external attacks.

In 2017, the Aadhaar data of over 3.5 million pensioners were leaked from the Kerala state pension department.[1] The pensioners had their bank account linked with the Aadhaar data to avail the 'direct benefit transfer' scheme.[2] Due to the security incident, their names, addresses, phone numbers, bank account numbers, Aadhaar numbers, and photographs were exposed on the service pension website (Raju, Singh, and Khatter 2017). A similar case had been observed in 2018 when the Andhra Pradesh State Housing Corporation[3] publicized sensitive data such as caste and religion of 0.1 million Aadhaar card holders (Suares 2018). Various other cases of data leaks from government domains have put the Aadhaar project on the radar of the cybersecurity regulatory body of India.

In the wake of the recent events when R. S. Sharma, the chairman of the Telecom Regulatory Authority of India voluntarily uploaded his Aadhaar number on Twitter to experiment whether

CONTACT Pratik Tarafdar ✉ pratikt15@email.iimcal.ac.in 🖃 Indian Institute of Management Calcutta, Kolkata, West Bengal 700104, India

[1] The pension department under the state government of Kerala in India.

[2] Direct Benefit Transfer is the mechanism launched by the Government of India on January 1, 2013 to transfer government subsidies directly to the beneficiaries through their bank accounts in order to avoid leakages, delays, etc.

[3] The Andhra Pradesh State Housing Corporation is a public sector corporation under the state government of Andhra Pradesh in India with the broad objective of facilitating affordable housing for the citizens of Andhra Pradesh.

mere knowledge of a number can harm any individual, there was a major controversy. Some of the Twitter users were able to dig out his personal and sensitive information linked with the Aadhaar number (Press Trust of India 2018). Thus, the security challenges related to the Aadhaar system is an open research problem that needs to be addressed. Therefore, the research problem we intend to address in this paper is as follows:

> *How can security breaches affect the existing Aadhaar system? What are the necessary controls to safeguard the system against such security breaches?*

2. Aadhaar the unique identification system of india

Several countries have implemented the personal identity system for its citizens (Pati, Kumar, and Jain 2015). For example, the United States has been using the Social Security Number, which is a nine-digit national identification number used for social security and taxation purposes. Hong Kong has implemented the Smart Identity Card System in the 1990s which has taken the form of an integrated chip on a smart card that stores minimal data including name, gender, digital image, date of birth, residential status, and both thumbprints. None of these countries have used biometric information such as fingerprint and retina patterns in their national identity program. However, India built up its unique digital identity program Aadhaar based on biometric data.

In 2006, the then government of India announced a project called Unique ID for Below the Poverty Line (BPL) families under the Department of Information Technology. This administrative initiative was an endeavor to emancipate the underprivileged from the corruption which was deterring their rights of free public services. For example, there were reports that the BPL families in India paid an estimated amount of US$ 203 million in 2008 to avail themselves of free public services (Khanna and Raina 2014). In the state of Uttar Pradesh in India, a widespread network of bureaucrats, village council leaders, transporters, and shop owners was operating to systematically exploit the flaws in the Public Distribution System[4] and steal 80% of the food and fuel aid (Khanna and Raina 2014). The lack of unique identification and authentication procedures created a major roadblock towards the success of various governmental schemes associated with different strata of the population. At the same time, the Registrar General of India was contemplating to create National Population Register[5] to issue multi-purpose identity cards to Indians. Consequently, an Empowered Group of Ministers was formed to merge the above two schemes, and the Unique Identification Authority of India (UIDAI) was set up in 2009 with the mandate to devise a smart solution to these problems.

The UIDAI was given the onus to implement the world's largest digital identity program Aadhaar geared towards financial inclusion and social protection. The Aadhaar system constituted by UIDAI included the following entities (Agrawal, Banerjee, and Sharma 2017):

2.1. *Central identities data repository (CIDR)*

The UIDAI maintained the biometric and demographic data of all individuals enrolled into the system in a repository called CIDR. It was mapped to a unique identifier, the Aadhaar number that identified and authenticated a particular individual.

2.2. *Enrollment agency*

It was the agency appointed by UIDAI to enroll people into the Aadhaar database thereby capturing their demographic and biometric information.

[4] Public Distribution System is the scheme by the Government of India that was launched in 1944 to give subsidized food and non-food items such as wheat, rice, sugar, and kerosene to the poor citizens of the country through a network of fair price shops (also known as ration shops).

[5] A register of the residents of the country.

2.3. *Users*

These were the residents of India who had to enroll themselves with UIDAI and possess a unique Aadhaar number. Users were required to provide either the Aadhaar number or a virtual ID (generated online from the Aadhaar number) to the service providers to avail the Aadhaar authentication services.

2.4. *Authentication user agency (AUA)*

It represented the agency that provided services to the users enrolled into the Aadhaar system. The AUA enabled the services to the customers by establishing a one-time validation protocol through CIDR. The entire customer profile was mapped to a corresponding Aadhaar number, and the customer data resided only in the AUA database.

2.5. *Authentication service agency (ASA)*

It represented the service provider to the AUAs. It transmitted the authentication requests from one or more AUAs to the CIDR through a secure connection. The response of the CIDR was also securely transmitted to the AUAs. In other words, the ASA served as an intermediary between the AUAs and the CIDR to effectively manage the request to and response from the server.

2.6. *Point of sale device*

It was the authentication device that validated the Aadhaar holders and stored their essential personal records in the proprietary databases.

Figure 1 highlights the control architecture for the Aadhaar system (excluding its links with the enrolment agency). With reference to Figure 1, we now discuss how the Public Distribution System (PDS) would fulfil its objectives effectively when institutionalized under the Aadhaar ecosystem. Suppose a beneficiary entitled to free ration for a particular month approached the ration shop. The attendant at the ration shop would receive his/her Aadhaar number along with the biometric information in the authentication device. She would provide the same information to the AUA (i.e., Public Distribution System database), and the authentication request would be transmitted to a suitable ASA. The request would be forwarded by the ASA through a secure connection to the CIDR database, and the response (in the form of Yes/No) would be transmitted back to the device at the ration shop. Once the person has been successfully authenticated, she would receive the ration. The transaction would be recorded in the AUA database, and the process would enable the PDS to serve the right beneficiaries with their right entitlements seamlessly while preventing fraud and leakage.

However, the United States and the UK had experienced serious problems in configuring Unique Identity proofs bearing biometric information (Pati, Kumar, and Jain 2015). The large-scale deployment of fingerprint identification systems was prone to errors due to sensor noise and poor quality of fingerprint images. Moreover, the presence of scars, warts, and deteriorating ridge/minutiae patterns in fingerprints from the rural population affected the performance of the fingerprint recognition systems (Vatsa et al. 2010). Security issues, legal concerns, and user privacy have been recurrent themes of concern related to biometric technologies (Laux et al. 2011).

Various security and privacy concerns were raised against the Aadhaar system such as illegal profiling and tracking of individuals, authentication without consent, collusion of multiple service providers to access confidential information, and use of fake biometrics (Agrawal, Banerjee, and Sharma 2017; Rajput and Gopinath 2017). Extant research has mostly provided technical solutions

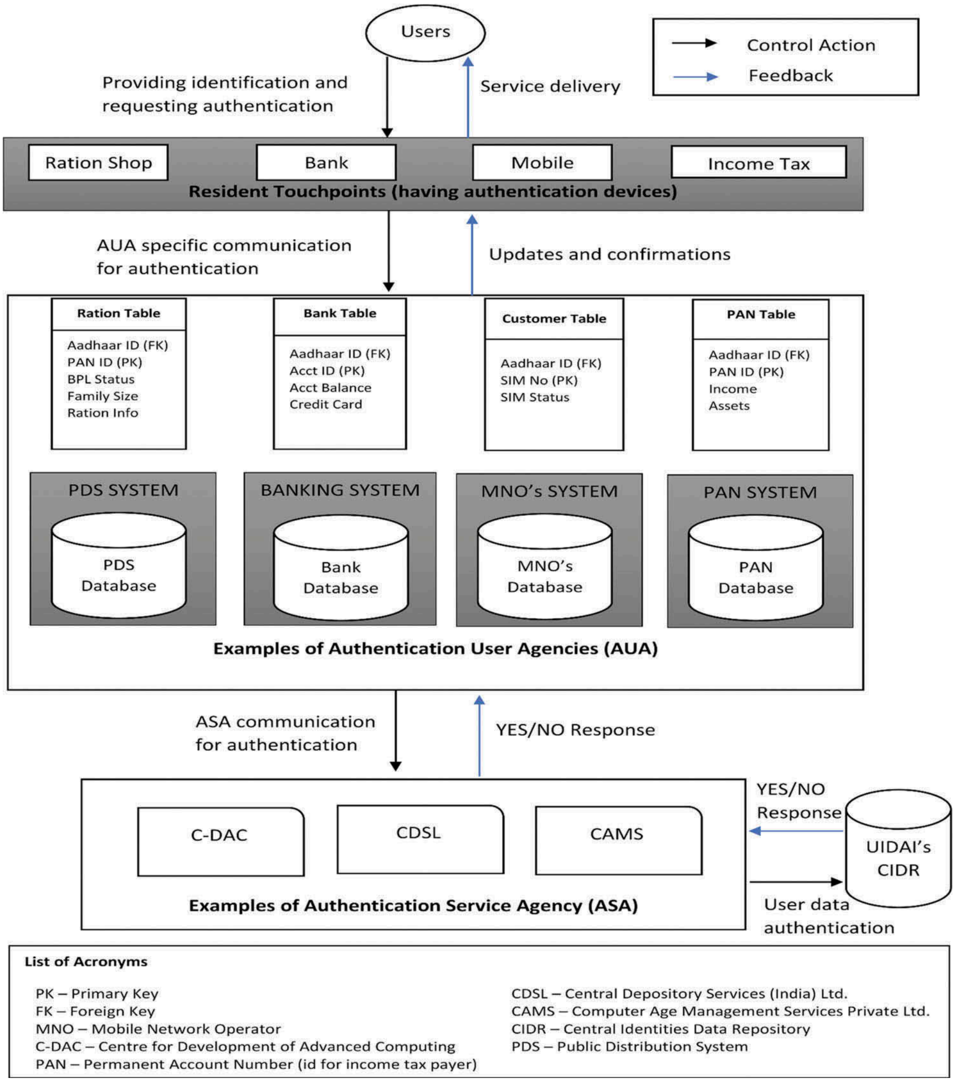
Users
Control Action
Feedback
Providing identification and requesting authentication
Service delivery
Ration Shop
Bank
Mobile
Income Tax
Resident Touchpoints (having authentication devices)
AUA specific communication for authentication
Updates and confirmations
Ration Table
Aadhaar ID (FK)
PAN ID (PK)
BPL Status
Family Size
Ration Info
Bank Table
Aadhaar ID (FK)
Acct ID (PK)
Acct Balance
Credit Card
Customer Table
Aadhaar ID (FK)
SIM No (PK)
SIM Status
PAN Table
Aadhaar ID (FK)
PAN ID (PK)
Income
Assets
PDS SYSTEM
PDS Database
BANKING SYSTEM
Bank Database
MNO's SYSTEM
MNO's Database
PAN SYSTEM
PAN Database
Examples of Authentication User Agencies (AUA)
ASA communication for authentication
YES/NO Response
C-DAC
CDSL
CAMS
Examples of Authentication Service Agency (ASA)
YES/NO Response
UIDAI's CIDR
User data authentication
List of Acronyms
PK – Primary Key
FK – Foreign Key
MNO – Mobile Network Operator
C-DAC – Centre for Development of Advanced Computing
PAN – Permanent Account Number (id for income tax payer)
CDSL – Central Depository Services (India) Ltd.
CAMS – Computer Age Management Services Private Ltd.
CIDR – Central Identities Data Repository
PDS – Public Distribution System

Figure 1. Architecture of the Aadhaar system.

for solving problems related to Aadhaar. This has included cryptography for strong encryption algorithms, enhanced system capacity for handling a huge number of transactions per second, and advanced biometric methods for avoiding errors in data recording and data compilation (Pati, Kumar, and Jain 2015; Rajput and Gopinath 2017). While there is a dire need to evaluate the cybersecurity risks of complex systems like Aadhaar, existing cybersecurity approaches have specifically focused on the technical aspects, leaving the systems perspective of cybersecurity under-researched (Salim and Madnick 2016). Narrowing the focus on the constituent parts of a holistic system and its technicalities and ignoring the interactions within and of the systems/sub-systems have led to the lack of an integrated approach for enhancing the overall cybersecurity of the system. For example, the CIDR was encrypted with a 2048-bit UIDAI issued key which made it difficult to

[6] The Andhra Pradesh State Housing Corporation is a public sector corporation under the state government of Andhra Pradesh in India with the broad objective of facilitating affordable housing for the citizens of Andhra Pradesh.

break. However, the Andhra Pradesh State Housing Corporation[6] was one of the AUAs that interacted with the CIDR through ASAs. It was also integrated with other AUAs. It lacked stringent security protocols to safeguard its relationship with the CIDR and exposed the Aadhaar numbers along with other sensitive demographic information in a security incident. Since the CIDR was the centralized database integrated with other prominent institutions, the knowledge of the Aadhaar number along with the demographic information gave rise to the chance of profiling individuals. Such instances did not arise because of the failure in the centralized database but due to the lack of understanding about the relationship between the centralized database and other system components. Likewise, cybersecurity problems for e-governance systems have often occurred due to lack of understanding of the people and processes that constituted the cyber-ecosystem (Kabanda, Tanner, and Kent 2018). Understanding the interdependencies and the interrelationships of the complex socio-technical system in the cyberspace was integral towards problem solving related to cybersecurity, and this was a major gap that we observed in the extant body of research related to Aadhaar. The lack of such holistic approaches can be explained by (a) the process of development of complex socio-technical systems that are mostly modular in nature, and (b) the difficulty in understanding of the interactions between the components of the technical system. The different components are developed in modules and implemented as an integrated whole. Hence, the security of the complete system is provided from the perspective of preventing failures in the various components of the system. The security loopholes are mostly identified post the occurrence of the breach. Security experts analyze the failure events and identify the point of failure and its causes through the evaluation of a chain of events. Subsequently, they fix the problem till another unanticipated interaction between components causes another failure event. However, the holistic understanding of the interactions between components remains unavailable.

Therefore, in this paper, we propose and discuss a safety analysis model incorporating systems thinking that can be effective in analyzing cybersecurity challenges for Aadhaar. We chose a popular safety-hazard analysis model based on systems theory known as Systems Theoretic Process Analysis (STPA) to critically analyze the cybersecurity features of the Aadhaar system.

3. Systems theoretic process analysis (STPA)

There are several prominent frameworks for the analysis of safety, failures, or accidents in traditional cybersecurity environments such as Linear Chain of Events Model, Fault Tree Analysis, and Cyber Kill Chain (Raina 2016). However, these approaches lack the intricate understanding of the socio-technical aspects of the system and deal with the problem in parts. Appendix provides a comparative review of STPA and all these popular frameworks to support our understanding. Since the Aadhaar is a complex and dynamic system, we need a model deep-rooted in systems thinking (i.e., a model that considers the complex interactions between people, technology, and organization). One such model is the Systems Theoretic Accident Model and Processes (STAMP). It was developed by Prof. Nancy Leveson at the Massachusetts Institute of Technology (Leveson 2012). Since then it has had a wide range of applications, such as the projects of NASA (Leveson 2009), safety modeling for aircraft rapid decompression event (Allison et al. 2017), analysis of patient safety for treatment with oral chemotherapy and anti-cancer drugs (Hall 2017), among others. Recently, it has been used extensively in security and privacy analysis (Shapiro 2016; Young and Leveson 2014). It has been used for investigating the Stuxnet cyber-attack (Nourian and Madnick 2018) and TJX cyberattack (Salim and Madnick 2016). In both cases, it provided promising results and recommendations regarding control measures that could be taken up to provide protection against major security breaches.

The STAMP consists of two methods – Casual Analysis based on the STAMP and Systems Theoretic Process Analysis (STPA). Casual Analysis based on the STAMP is meant for ex-post accident analysis to gain insights on why a loss occurred, whereas the STPA is an ex-ante hazard analysis to discover the system loopholes and implement security countermeasures. The STPA is performed using three fundamental processes – identification of the high-level system hazards and unacceptable losses, creation of the functional control structure of the system, and identification of the hazardous (or missing) control actions and finding the causal scenarios. The detailed steps have been shown in Figure 2. The goal of this paper is to demonstrate the application of the STPA for hazard analysis of the Aadhaar system and identification of security countermeasures. We systematically examine the Aadhaar system using the lens of the STPA and suggest improvements in systems security based on insights.

4. STPA of the aadhaar system

We perform the STPA for the Aadhaar system to examine the security hazards arising out of the system interactions. The process helps in developing the system-level constraints against unsafe control actions that can result in potential security incidents. Conceptually, the STPA is performed in the concept development stage before the development of the system to assist the design teams in incorporating all essential safety goals. However, our intent here is to identify the security gaps of the existing model of the Aadhaar system to take it to the next level of maturity and stability. Therefore, our hope is that the STPA would drive the development of a robust and advanced Aadhaar system through systematic inspection of the security threats to the system and identification of measures to protect against them.

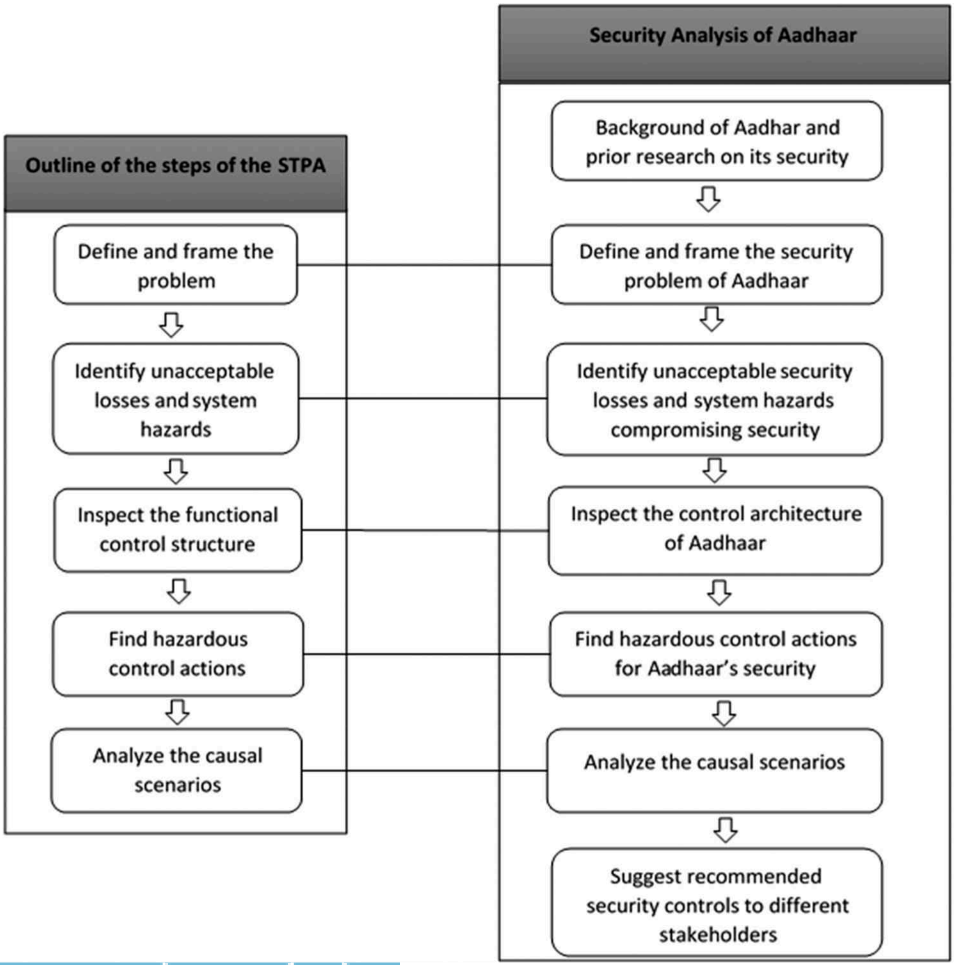
Outline of the steps of the STPA
Define and frame the problem
Identify unacceptable losses and system hazards
Inspect the functional control structure
Find hazardous control actions
Analyze the causal scenarios
Security Analysis of Aadhaar
Background of Aadhar and prior research on its security
Define and frame the security problem of Aadhaar
Identify unacceptable security losses and system hazards compromising security
Inspect the control architecture of Aadhaar
Find hazardous control actions for Aadhaar's security
Analyze the causal scenarios
Suggest recommended security controls to different stakeholders

Figure 2. Steps of the STPA.

The precursor of the STPA is the definition of the system purpose and goal, identification of the mission and key stakeholders, elaboration about the system components and their interaction. We discussed the mission and vision of the Aadhaar involving the key stakeholders as well as the conceptual architecture earlier in the paper. The subsequent steps of the STPA are performed as shown in the below sections:

4.1. *Framing the security problem*

Traditionally, practitioners have considered safety and security as distinctly different system properties. While safety experts have attempted to minimize losses due to unintentional actions by benevolent actors, security experts have looked for ways to prevent losses due to intentional actions of malevolent actors (Young and Leveson 2014). Though the intent of the actors differentiates security from safety, the primary concern in both cases is to prevent losses. Therefore, the security problem of Aadhaar can be thought of as a loss prevention problem through systematic analysis of the design. We aim to identify all possible security losses and shield the system against such losses.

4.2. *Identification of potential system hazards and corresponding security losses*

The security problems of Aadhaar can be translated into finding the system hazards that compromise cybersecurity and also understanding the associated losses. From the perspective of system hazards in STPA analysis, the most significant hazard of the Aadhaar system is the possibility of system hacks, insider leaks, or collusion. Other system hazards include authentication failure, identification without consent using the Aadhaar number, identification and authentication without consent using the demographic and biometric data (Agrawal, Banerjee, and Sharma 2017). Moreover, from the perspective of security losses in STPA analysis, these system hazards can cause significant losses such as denial of service to a rightful person, service provision to an impersonator, loss of information privacy of an individual, or tampering of authentication records and audit trails. For example, the authentication failure of the recipients at the ration shops can impede the rightful access to the facilities of Public Distribution System, while at the same time authentication without consent can open up the possibilities of duping the system and its beneficiaries. Such instances would erode the purpose of Aadhaar as the largest digital identity program for financial inclusion and social protection. All these system hazards and their security losses are obtained as an initial step of STPA from the high-level understanding of the Aadhaar system. Table 1 provides a hazard to loss cross-table to reflect on their interrelationships. By going through this exercise, we aim to understand the ineffectiveness of the control actions (set of instructions by the higher-level processes to impose control on the lower level processes) and the feedback mechanism (response mechanism of the lower level processes to those instructions) at each level of the control structure of the Aadhaar system that can possibly expose it to such hazards.

4.3. *Inspect control structure, find hazardous control actions and its causes, and suggest security controls*

The next step aims at analyzing control actions with respect to the Aadhaar system, finding the causal scenarios for hazardous control actions, and suggesting design recommendations to avoid the hazardous conditions. The results are shown in tabular form at three levels in Tables 2–4. At the first level, we identify the hazardous states of different control functions. Each control function can create a hazardous state due to four possible reasons – a control action is required but not provided, a control action is provided but not required, a control action is provided too early or too late, and a control action is provided at the incorrect time. We enumerate all these possibilities and the respective system hazards. Subsequently, we determine the respective causal scenarios at the second level of analysis. At the third level of analysis, we provide the security controls required between CIDR and ASA to mitigate the identified hazardous states.

Table 1. Hazard to loss cross-table depicting which system hazards result in what kind of losses.

Losses Hazards	L1: Denial of service to a rightful person	L2: Service provision to an impersonator	L3: Loss of information privacy exposing individuals to tampering of authentication records and audit trails
H1: System hacks, insider leaks, or collusion to control centralized databases		X	X
H2: Failure of authentication	X		
H3: Identification without consent using Aadhaar number		X	
H4: Identification and authentication without consent using demographic and biometric data		X	X

Table 2. The STPA for control action of ASA on CIDR.

	Hazardous Control Actions			
Control Actions (CA)	Not providing CA causes hazard H	Providing CA causes hazard H	Providing CA at a wrong time (too late/too soon) causes hazard H	Providing CA for an incorrect duration of time causes hazard H
CA1: User authentication request to CIDR from ASA.	H2: Genuine request for user authentication turned down.	H1, H4: Fraud authentication request approved.	H2: Genuine authentication request sent after a long time.	H2: Continuous authentication requests for the same user.
			Causal Factors	
	• The secured connection from the ASA to the CIDR is disrupted or compromised. • The CIDR has crashed or malfunctioned.	• The network connection between ASA and CIDR is hacked. • An intruder or an insider has breached ASA's security protocols.	• High network traffic.	• No response from CIDR due to greater data processing time or system failure.
			Required System Constraints	
	• Transfer the request to other ASAs in case of network failure. • Alert the ASA when the network is compromised. • Flag a warning signal when CIDR has crashed.	• Strengthen the network security between ASA and CIDR. • ASA needed to be a trusted and reliable authority.	• Scale up the network capacity as per the demand or transfer the requests to other ASAs.	• Scale up and optimize the CIDR performance. • Intimate the ASA when CIDR is non-responsive.

Similarly, Table 3 lists the security hazards that are probable during the communication between the ASA and the AUA for authentication. The causal factors reflect any security lapses from either of the organizations that can lead to security incidents. Following the identification of causal factors, we discuss the security measures that can be achieved by regulating the system interactions between AUA and the ASA.

Table 4 elucidates the circumstances under which the user interaction with the AUA for identification and authentication purposes can create a security hazard for the entire Aadhaar system. This occurs due to inadequate control of the user over the service processes of the AUA. We examine how the users' interaction with the AUA can be controlled to avoid security losses.

5. Recommended actions

Based on the STPA of the Aadhaar system, we gained a systems perspective on the implementation loopholes that can potentially cause security incidents. The analysis depicted in Tables 2–4 identifies

Table 3. The STPA for control actions of AUA on ASA.

	Hazardous Control Actions	
Control Actions (CA)	Not providing CA causes hazard H	Providing CA causes hazard H
CA2: Communication from AUA to ASA for authentication.	H2: Genuine request for user authentication turned down.	H1, H4: Fraud authentication request approved.
	Causal Factors	
	• The communication between AUA and ASA is affected. • Problems in the leased line connectivity provided by ASA to the AUA.	• Fraud AUA established the communication link with the ASA. • An intruder or an insider breached AUA's security protocols and exploited their proprietary database. • AUA has a weak barrier to contain security accidents.
	Required System Constraints	
	• Inform AUA about the service failure. • Channel the service request through an alternate route (maybe through another ASA).	• AUA cannot be unconditionally trusted with users' demographic and biometric data. • Enforce strict regulations of data privacy and data security on all AUAs.

Table 4. STPA for control actions of users on the AUA.

	Hazardous Control Actions	
Control Actions (CA)	Not providing CA causes hazard H	Providing CA causes hazard H
CA3: Authentication requests from users to the AUA through resident touchpoints.	H2: Genuine request for user authentication gets turned down.	H1, H3, H4: Fraud authentication request gets approved.
	Causal Factors	
	• Authentication failures due to change in biometric details (which occurs because of aging or wear and tear). • The authentication devices do not function properly. • Poor communication between resident touchpoints and the AUA.	• Sharing of Aadhaar number, demographic, or biometric data at the resident touchpoints increases the chances of identity theft. • The attendant at the touchpoint can misuse the system by hijacking a user's biometric details and availing the user's benefits.
	Required System Constraints	
	• Need to set up a fallback mechanism for authentication to make the system fault tolerant. • Maintain the performance of the authentication device at the highest level. • Establish rapid and strong communication channels between the resident touchpoints and the AUA.	• Restrict sharing Aadhaar number at resident touchpoints. • Regulate the storage of biometric data at resident touchpoints. • Perform security check of the authentication devices against security attacks such as data skimming. • Inform users about the progress of the authentication process including initiation, failure, rejection or acceptance through mobile devices.

the system constraints to safeguard the Aadhaar system against possible security breaches. The key stakeholders of the Aadhaar are the Indian government, the AUAs, the ASAs, and the Aadhaar users. In the next section we explain the key security risks and the suggested controls as defined in our analysis for each of the stakeholders of the Aadhaar system.

5.1. *Government as a stakeholder*

5.1.1. *Security risks*

- The AUAs or the ASAs can engage in fraudulent activities. They can collude amongst themselves to practice illegal profiling or tracking of user activities.
- The Central Identities Data Repository (CIDR) can crash due to workload. It may exhibit a long response time due to extensive data processing. Also, it may be the prime target for cyber-attacks through security hacks.

5.1.2. *Precautionary measures*

- The Indian government needs to impose strict regulations on these agencies' entry into the Aadhaar ecosystem. The security practices that are applicable to the central system of the UIDAI should also be applicable to its sub-systems (i.e., its agencies).
- As the scale of Aadhaar increases, the centralized database CIDR needs to be optimized and upgraded to seamlessly handle large-scale data processing. Secondly, the unlawful and unsecured access to the database should be prevented through effective security barriers. Lastly, the database needs to be fault-tolerant to protect against sudden and abrupt downtimes.

5.2. *AUA and ASA as stakeholders*

5.2.1. *Security risks*

- Due to limited knowledge and training about security practices, the AUAs are often susceptible to accidental data leakage and incapable of protecting sensitive and personally identifiable user data such as biometric information. For example, in one of the security incidents, the Food and Civil Supplies Department of Chandigarh lacked the cyber security knowledge and common practices which led to accidental publicization of Aadhaar numbers of its Public Distribution System beneficiaries.
- Due to the association of the AUA databases with the unique identity number, it is more vulnerable to internal and external threats. Being a part of the Aadhaar ecosystem, their databases can be continuously attacked.
- The network communication of ASA with the CIDR and that of AUA with the ASA are the weak zones susceptible to network hacking. Also, the network capacity of that ASAs can be ineffective in handling multiple authentication requests.

5.2.2. *Precautionary measures*

- The AUAs and the ASAs need to train their workforce to maintain the security standards in their organization at the highest level. The organization needs to spread awareness about possible security breaches due to complacency in following security protocols, their grave consequences, and certain best practices to avoid such incidents.
- The AUAs need to take strict action to protect user data from security incidents such as tampering of authentication devices, accidental data leakage, networks hacks in their communication with the ASA or resident touchpoints, insider leaks, and system hacks. Otherwise, their contract with the government in terms of access to the Aadhaar database will weaken.
- In the case of high network load due to multiple authentication requests or network failure of ASA, the AUA and ASA should communicate to transfer the request to any other ASA. Alternatively, the ASAs can scale up their network capacity and develop a fault-tolerant mechanism to cope up with such incidents.

5.3. *Aadhaar users as stakeholders*

5.3.1. *Security risks*

- With the roll-out of the Aadhaar system, the Aadhaar number and the biometric information of Indian residents will become essential in accessing different government and non-government facilities. These user attributes will be increasingly susceptible to social engineering attacks for granting access to critical resources of the individual.

5.3.2. *Precautionary measures*

- It is important for the users to protect their Aadhaar number and biometric records against any fraud. They need not divulge such details in any unsecured platform. The Indian government needs to educate its citizens on the security practices related to the Aadhaar.

6. Lessons learnt

The Aadhaar system bears the characteristics of a large-scale socio-technical system operating in cyberspace. The complexity of such a system makes it imperative for the organization to adopt an alternative approach to cybersecurity. This can be explained as follows:

6.1. *Non-linearity against linearity*

Socio-technical systems exhibit not only linear ‘cause and effect’ relationships among its system components but also non-linear or unpredictable relationships arising out of unforeseen interactions between the technology artifacts and the human agents. The intertwining of technology structures and the human agents necessitates a non-linear approach rather than seemingly intuitive approaches towards framing of cybersecurity problems.

6.2. *Bridging the disconnect between the systems view and the technical engineering view*

Very often, the socio-technical design methods treat the human, social and organizational factors differently from the engineering issues. Hence, the cybersecurity problems arising out of social interactions remain unaddressed in the engineering design during the process of development. Therefore, the underlying premise for the development of socio-technical systems should be the systems view while taking into account both social and technical factors impacting cybersecurity.

6.3. *Strategy over tactics*

Security tactics look at prudent means to guard networks and information assets, while security strategy shields the organization from unacceptable or heavy losses. While the tactics try to address “how best to guard the network against threats” the strategy looks into “what essential services and functions must be secured against disruptions” (Young and Leveson 2014). Hence, it is important to focus on cybersecurity strategy rather than cybersecurity tactics for managing system vulnerabilities.

6.4. *Collaborative efforts of stakeholders towards strategy formulation*

A large-scale socio-technical system involves several stakeholders. Security efforts at the individual level against threats from adversary actions do not secure the system completely. A collaborative effort towards the formulation of cybersecurity strategies or policies and commitment to prevent security losses at an integrated level can safeguard the system against all major forms of security breaches.

7. Conclusion

In this era when the Internet is ubiquitous and physical systems are increasingly getting connected in the cyberspace, cybersecurity is a growing concern. The techniques and approaches of cybersecurity need to be revisited, remodeled, and reimplemented from time to time to tackle the dynamic and advanced threats in the cyberworld. Savage and Schneider (2010) remarked that cybersecurity is "holistic – a property of a system and not just of its components". Any small change in the system can have catastrophic consequences for the overall cybersecurity of the system. Using the Aadhaar system as a case study, we demonstrate how the STPA can be utilized to develop the cybersecurity strategy for a large-scale, complex, dynamic, and socioeconomically predominant IT implementation. Firstly, we describe the Aadhaar system and its operations as well as the key stakeholders and their role. Secondly, we identify the security problems of the Aadhaar system by highlighting the system hazards that can cause losses. Thirdly, we discover the possible circumstances when such losses can occur and suggest controls that can mitigate it. Fourthly, we recommend actions for each of the stakeholders to implement the system controls and prevent security losses. Finally, we summarize the lessons learnt for cybersecurity management of socio-technical systems. To the best of our knowledge, this is the first endeavor to dissect the security problems of the Aadhaar using systems thinking. We use the emerging safety analysis technique called the STPA to devise a systematic plan for the safety of the Aadhaar system against security incidents. Our paper showcases a new direction of cybersecurity research by including systems thinking in it.

This study has its own limitations which may be overcome through future research. Firstly, the STPA framework for cybersecurity research in the context of Aadhaar is conceptual in nature, and the framework needs to be implemented for studying its implications. Secondly, the framework emphasizes cybersecurity issues like safety and control processes. It views the security problems from a safety perspective and does not address the ones that do not have a direct impact on safety. Future research can integrate well-established traditional security analysis techniques with this framework to overcome the above limitations. Thirdly, the framework needs to be re-modeled, re-evaluated, and re-implemented with incremental changes to adapt to the dynamism of the socio-technical environment. One of the strengths of the framework is that it supports temporal adaptability. However, the process of adaptation is an optimization process based on search strategies, and hence the framework needs to be enriched over time. Future researchers can consider collection of feedback from key opinion leaders and decision makers involved with providing information security for the Aadhaar system to improve the framework even more. The future research can also examine how the framework withstand the test of time and complexity.

Notes on contributors

Pratik Tarafdar is a doctoral candidate at the Indian Institute of Management Calcutta in the area of Management Information Systems. He holds an M.Sc. degree in Applied Mathematics from the University of Calcutta. His research interests include cybersecurity, immersive technology, business analytics, and large-scale machine learning. His research articles have appeared in conference proceedings of ACM SIGMIS. He has also written case studies for the IIM Calcutta Case Research Center.

Indranil Bose is Professor of Management Information Systems at the Indian Institute of Management, Calcutta. He acts as Coordinator of IIMC Case Research Center. He holds a B. Tech. from the Indian Institute of Technology, MS from the University of Iowa, MS and Ph.D. from Purdue University. His research interests are in business analytics, telecommunications, information security, and supply chain management. His publications have appeared in MIS Quarterly, Communications of the ACM, Communications of AIS, Computers and Operations Research, Decision Support Systems, Ergonomics, European Journal of Operational Research, Information & Management, International Journal of Production Economics, Journal of Organizational Computing and Electronic Commerce, Journal of the American Society for Information Science and Technology, Operations Research Letters, Technological Forecasting and Social Change etc. He serves as Senior Editor of Decision Support Systems and Pacific Asia Journal of the AIS, and as Associate Editor of Information & Management, Communications of AIS, Information Technology & Management, and member of Editorial Board for Journal of the AIS.

References

Agrawal, S., S. Banerjee, and S. Sharma. 2017. Privacy and security of Aadhaar: A computer science perspective. *Economic & Political Weekly* 52 (37):1–23.

Allison, C. K., K. M. Revell, R. Sears, and N. A. Stanton. 2017. Systems Theoretic Accident Model and Process (STAMP) safety modelling applied to an aircraft rapid decompression event. *Safety Science* 98:159–66. doi:10.1016/j.ssci.2017.06.011.

Gostojić, S., G. Sladić, B. Milosavljević, and Z. Konjović. 2012. Context-sensitive access control model for government services. *Journal of Organizational Computing and Electronic Commerce* 22 (2):184–213. doi:10.1080/10919392.2012.667717.

Hall, H. J. 2017. Applying system-theoretic accident model process view to patient safety for treatment with oral chemotherapy and anti-cancer drugs. PhD. Diss., Massachusetts Institute of Technology.

Kabanda, S., M. Tanner, and C. Kent. 2018. Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce* 28 (3):269–82. doi:10.1080/10919392.2018.1484598.

Khanna, T., and A. Raina. 2014. Aadhaar: India's unique identification system. Boston, MA: Harvard Business School Cases, Case No. 9-712-412.

Laux, D., A. Luse, B. Mennecke, and A. M. Townsend. 2011. Adoption of biometric authentication systems: Implications for research and practice in the deployment of end-user security systems. *Journal of Organizational Computing and Electronic Commerce* 21 (3):221–45. doi:10.1080/10919392.2011.590111.

Leveson, N. G. 2009. Technical and managerial factors in the NASA Challenger and Columbia losses: Looking forward to the future. In *Controversies in science & technology - from climate to chromosomes*, Vol. 2. Mary Ann Liebert, Inc. doi:10.1089/9780913113424.237.

Leveson, N. G. 2012. *Engineering a safer world: Systems thinking applied to safety*. The MIT Press. doi:10.1017/CBO9781107415324.004.

Nourian, A., and S. Madnick. 2018. A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet. *IEEE Transactions on Dependable and Secure Computing* 15 (1):2–13. doi:10.1109/TDSC.2015.2509994.

Pati, R. K., V. Kumar, and N. Jain. 2015. Analysis of Aadhaar: A project management perspective. *IIM Kozhikode Society & Management Review* 4 (2):124–35. doi:10.1177/2277975215610687.

Press Trust of India. 2018. Aadhaar becomes a plaything. *The Telegraph*. New Delhi, July 29. Accessed September 17, 2018. https://www.telegraphindia.com/india/aadhaar-becomes-a-plaything-248438?ref=india-hmstory-stry-dtl.

Raina, R. 2016. A systems perspective on cybersecurity in the cloud - Frameworks, metrics and migration strategy. PhD. Diss., Massachusetts Institute of Technology.

Rajput, A., and K. Gopinath. 2017. Towards a more secure Aadhaar. In *Information systems security. ICISS 2017. Lecture notes in computer science*, ed. R. Shyamasundar, V. Singh, and J. Vaidya, 283–300. Cham: Springer.

Raju, R. S., S. Singh, and K. Khatter. 2017. *Aadhaar Card: Challenges and impact on digital transformation*. Cornell University Library. http://arxiv.org/abs/1708.05117

Salim, H., and S. Madnick. 2016. Cyber safety: A systems theory approach to managing cyber security risks – Applied to TJX cyber attack. Working Paper. CISL, Sloan School of Management, Massachusetts Institute of Technology, Cambridge, MA.

Savage, S., and F. B. Schneider. 2010. Security is not a commodity: The road forward for cybersecurity research. A White Paper Prepared for the Computing Community Consortium Committee of the Computing Research Association. https://cra.org/ccc/resources/ccc-led-whitepapers/

Shapiro, S. S. 2016. Privacy risk analysis based on system control structures: Adapting system-theoretic process analysis for privacy engineering., Sanjose, CA. Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016, 17–24. IEEE. doi:10.1109/SPW.2016.15.

Suares, C. 2018. Bank details of 1.34l Aadhaar holders 'leaked' from AP govt website. *Deccan Chronicle*. Hyderabad, April 25. Accessed September 17, 2018. https://www.deccanchronicle.com/nation/current-affairs/250418/aadhaar-leak-from-andhra-pradesh-site.html.

Vatsa, M., R. Singh, S. Bharadwaj, H. Bhatt, and R. Mashruwala. 2010. Analyzing fingerprints of Indian population using image quality: A UIDAI case study. *International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics* 1 (August):1–5. doi:10.1109/ETCHB.2010.5559279.

Young, W., and N. G. Leveson. 2014. An integrated approach to safety and security based on systems theory. *Communications of the ACM* 57 (2):31–35. doi:10.1145/2556938.

Appendix

Table A1. A comparative review of STPA and other existing popular accident/failure models in cybersecurity.

Failure/ Accident Models in Cyber security	Analysis Procedure and Beneficial Outcomes	Use Case	Limitations
Linear Chain of Events	Analyze accident/failures in terms of multiple chronological events. Eliminate risks by implementing counter measures between events in the chain. Easy to construct and identify the causal factors.	Heinrich's domino theory of industrial accidents (Chung 2015).	Ignores non-linear relationship among events. Focuses only on the reliability of system components. Does not examine social, organizational, and economic factors responsible for the accident.
Fault Tree Analysis	Top down, deductive failure analysis. Maps the relationships between faults and sub-systems using Boolean logic by starting from the top event/ undesired state and applying a systematic backward reasoning process. Enables a high-level understanding of the system through quick detection of system faults or hazards.	Understanding data loss due to employee error and accidental leakage of sensitive information (Patil et al. 2012).	Requires intricate knowledge of design, construction, and system operations. For complex systems, fault trees may become large and complex. Inefficient in understanding underlying causes of error due to the interaction of components.
Cyber Kill Chain	Developed by the computer scientists at Lockheed-Martin corporation to defend network intrusions. Detects the phases of cyber-attacks. Develops a method of defense or preemptive action at each phase against the structure of attacks.	Understanding of cyber-attacks and related risks in cyber-physical systems through a multi-layered framework (Hahn et al. 2015).	Narrow focus on traditional perimeter-based and malware-prevention thinking. Fails to understand the nuances of socio-technical systems. Lacks understanding of security incidents due to the absence of safety constraints.
Systems Theoretic Process Analysis (STPA)	Identification of high-level system hazards and unacceptable losses. Identification of causal scenarios by analyzing control structure. Application of security measures. Safeguards single component failures and protects against system failures as a result of unanticipated interaction of components.	Analysis of safety and security for cyber-physical systems such as power grid or water distribution networks (Friedberg et al. 2017).	Strictly problematizes the cyber security incidents as a problem of control. The framework is evolving and in need of further development.

References

Chung, K. 2015. "Applying Systems Thinking to Healthcare Data Cybersecurity." *MSc. Diss., MIT Sloan School of Management*.

Friedberg, I., K. McLaughlin, P. Smith, D. Laverty, and S. Sezer. 2017. "STPA-SafeSec: Safety and Security Analysis for Cyber-Physical Systems." *Journal of Information Security and Applications* 34: 183–96. https://doi.org/10.1016/j.jisa.2016.05.008.

Hahn, A., R. K. Thomas, I. Lozano, and A. Cardenas. 2015. "A Multi-Layered and Kill-Chain Based Security Analysis Framework for Cyber-Physical Systems." *International Journal of Critical Infrastructure Protection* 11 (December): 39–50. https://doi.org/10.1016/j.ijcip.2015.08.003.

Patil, P., P. Zavarsky, D. Lindskog, and R. Ruhl. 2012. "Fault Tree Analysis of Accidental Insider Security Events." *Proceedings of the 2012 ASE International Conference on Cyber Security, CyberSecurity 2012*, no. SocialInformatics: 113–18. https://doi.org/10.1109/CyberSecurity.2012.21.