Resolution Techniquesfor Current Breaching Methods of Capturing The Biometrics: Privacy Preserving Management of UIDAI

MACHIRAJU SIVAKUMARRAJU

Department of Computer Science

SRI SAI DEGREE AND P.G COLLEGE OF COMPUTER SCIENCES

Abstract:

We investigate the privacy preserving issues of Aadhaar from UIDAI serverin a current technology point of view. Specifically, we investigatethe possibilities of identification andauthentication without using the consent of Aadhaar number or capturing thebiometrics, and unlawful accessing of Aadhaar data in the central database repository. Our analysis suggests that privacy preserving methods in Aadhaarsystem willrequire.

a) an independent third party that can play theimportant role of an online auditor.

b) study of several modern tools and techniques from computer science, and c) strong legal and policy frameworks that can address the specifics of authentication and identification in a modern digital setting.

Key terms: UIDAI, Aadharauthentication, Bio-metric captures, Misleading of Aadhar, Resolution methods privacy, security, cryptography, authentication, identification.

I. Introduction

The Aadhaar project is one of the India's largest national identity project, whichis launched by government of India, which seeks to collect biometrics (figure prints) and demographic (Irish) data of peoples and to store this information in a centralized database. Till today, 1036 million users have enrolled in the system, and the government has spent at least 890 million dollars on the project (As per UIDAI survey report 2019). However, recently there has been considerable deliberations over the privacy and security issues related to the Aadhaar authentications.

In this research, we examine various illegal breaching issues for data corruption and losing the data confidentiality ofAadhar, and how to reduce this kind of drawbacks by using Cryptographic methodologies and its useful application in computer science.

II.Background

Data of all Aadhaar holders is safe and secure in the Central Identities Data Repository (CIDR) of UIDAI. Aadhaar database in CIDR has never been breached in all these years of its existence. Some organizations, to follow transparency protocols, had published their beneficiary data on their websites, which included Aadhaar details. UIDAI took appropriate steps to get this removed and has also sensitized all related organizations and agencies in the matter. UIDAI is working closely with all user agencies to enhance data security measures when it comes to sensitive user details like Aadhaar.
UIDAI uses advanced security technologies to keep your data safe and keeps upgrading them to meet emerging security threats and challenges.

III. Privacy and security concern mechanisms

We examine the following main concerns pertaining to privacy and security in Aadhaar:

1. Identification of individuals without consent using the global Aadhaar number.

2. Identification and authentication without consent using demographic and biometric data.

3. Surveillance, tracking or profiling of people beyond legal sanctions using the centralized database, either through external hacks or through insider leaks and collusion.

Specifically, we ask the following questions which we believe are crucial for ensuring safety of Aadhaar.

1. Is it possible to ensure that user data and identification and authentication trails are completely protected from manual inspection by the UIDAI or the Government or any other entity or individual, thereby effectively preventing unauthorized surveillance.

2. Is it possible to ensure that all transactions, investigations, and analytics can be carried out in a safe way only through audited, pre-approved and tamper proof computer programs? Additionally, can it be ensured that the programs are true to legal and policy frameworks, do precisely and only what they are supposed to do, and maintain tamper proof logs of all authorizations chains and results? We believe that the above questions capture the essence of privacy protection in computerized databases. Privacy protection does not demand that data should not be collected, stored or used, but that there should be provable guarantees that the data cannot be used for any purpose other than those that have been approved.

IV. Our Aim

Recent advances in Computer Science offer several powerful solutions, ideas to address many of the privacy and security challenges posed by the project. Our goal is to carefully examine the security concerns, survey the technological tools that may aid us and provide a first order analysis of what might be feasible. Our approach is as follows. We first capture the functionality desired by the Aadhaar project. Next, we analyze the security risks and vulnerabilities engendered by each entity and each communication link in the Aadhaar model. We examine the security measures proposed by UIDAI and discuss where these may be lacking. We elucidate recent tools from computer science, particularly from the fields of cryptography and 3 security, which may assist in providing safeguards: this puts some stated concerns to rest while simultaneously raising multiple unforeseen issues.

Overall, we hope that our work provides a rigorous and scientific treatment of privacy concerns regarding Aadhaar and enables well informed and well-reasoned decisions regarding deployment. The rest of the paper is organized as follows.

1.we describe the Aadhaar functional architecture, and the various entities involved and their roles.

2.we analyze the privacy and security requirements of the Aadhaar project.

3. we discuss the differences between identity verification and authentication and point out that failure to demarcate the two may lead to authentication without consent.

4.we analyze the possibilities of privacy breaches through the Aadhaar number and suggest possible remedies.

5.In this Section, weanalyze the threats for potential privacy breaches from the Aadhaar database and the field devices and explore possible approaches that may be adopted to mitigate the risks. Finally, we conclude the proposal.

V. ThePresent Model Of UIDAI-Aadhaar

1. The Unique Identification Authority of India (UIDAI) is responsible for providing the basic identification and authentication services. It provides a unique identifier (Aadhaar number) to each resident and maintains their biometric and demographic data in a Central Identities Data Repository (CIDR). The UIDAI manages the CIDR and provides identification and authentication services with yes/no answers.

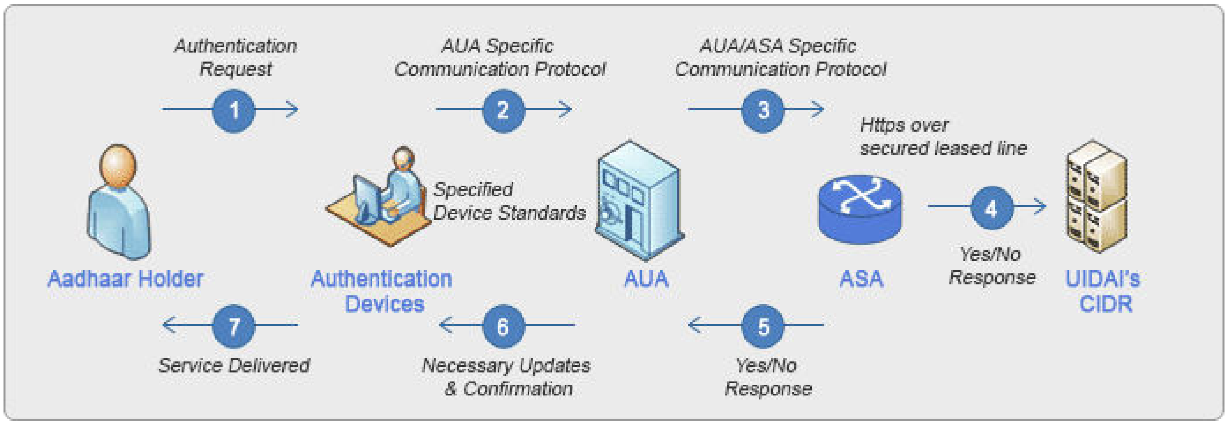
2. An Authentication Service Agency (ASA) is an entity that has a secure leased line connectivity with the CIDR. ASAs transmit authentication requests to CIDR on behalf of one or more AUAs. An ASA enters into a formal contract with UIDAI.

3. The users, namely, the residents of the country who enroll themselves with UIDAI and are issued unique identification numbers (Aadhaar numbers). A user must present this number as the basic identification to an AUA for availing Aadhaar authentication services. The Aadhaar number for a user is common across all AUAs and service domains.

4. The Point of Sale (POS) device, also known as authentication device which collects personal identity data from Aadhaar holders, prepares the information for transmission, transmits the authentication 4 packets for authentication and receives the authentication results.

5. An Enrolment Station, which is a collection of field devices used by enrolment agencies appointed by UIDAI to enroll people in to the Aadhaar database and capture their demographic and biometric particulars. The Aadhaar number is common across all AUAs and service domains.

This operating model outlines the actors involved in the Aadhaar Authentication ecosystem. The following figure identifies the key actors in the Aadhaar authentication model and depicts the data flow in which the key actors could engage with each other. The brief description of key actors and the scenarios in which they engage with each other are indicated in the figure below.


Authentication Request
1
AUA Specific Communication Protocol
2
AUA/ASA Specific Communication Protocol
3
Https over secured leased line
Specified Device Standards
4
Yes/No Response
Aadhaar Holder
Authentication Devices
AUA
ASA
UIDAI's CIDR
7
Service Delivered
6
Necessary Updates & Confirmation
5
Yes/No Response

VI. Identity verification vs authentication

Aadhaar is a national identity project, but we believe that the subtle difference between identity verification and authentication is itself not well understood, and this leads to confusions in policy making and deployment. Below, we attempt to first demarcate the two concepts. According to standard notions of digital authentication, a security principal (a user or a computer), while requesting access to a service, must provide two independent pieces of information - identity and authentication. Whereas identity provides an answer to the question "who are you?", authentication is a challenge-response process that provides a "proof of the claim of identity", typically using an authentication credential. Common examples of identity are User ID (Login ID), cryptographic public keys, email ids, ATM or smart cards; some common authentication credentials are passwords (including OTPs), PINs and cryptographic private keys. Identity may be considered public information, but an authentication credential must necessarily be private - a secret that is known only to the user. Moreover, authentication must be a conscious process that requires active participation by a user, but not necessarily so for identity verification. As example use cases, a bank may want an identity verification while opening an account at which stage no secret like a password is usually necessary, but a user needs to authenticate with a PIN for transactions like ATM withdrawals. No publicly known information should be used as an authentication credential.

VII. Privacy protectionfundamental assumptions

To determine the extent to which security and privacy are achieved, we must first define the desired expectations in this context. Our analysis is based on the following assumptions, which we believe are fundamental: 1. Authentication without consent should never be possible under any circumstances. Identification without consent should also not be possible except in some special situations like disaster management, identification of accident victims, law enforcement and such others. It should be noted that providing one's identity for obtaining services in any local context is always with consent. 2. Unapproved profiling, tracking and surveillance of individuals should not be possible. There should be sufficiently strong measures to prevent such breaches in privacy, with user-verifiable proof of the same. 3. The technical implementation of privacy and security must be provably correct with respect to the legal framework. The legal framework, in turn, needs to be suitably enhanced with special provisions to protect the privacy of individuals and society in an advanced information technology setting.

VIII. Possible Ways of Breaching the Privacy in Aadhar

we briefly examine the various ways in which the privacy of an individual can be compromised in a setting such as in Aadhaar.

1. Correlation of identities across domains: It may become possible to track an individual's activities across multiple domains of service (AUAs) using their global Aadhaar ids which are valid across these domains. This would lead to identification without consent.

2. Identification without consent using Aadhaar data: There may be unauthorized use of biometrics to illegally identify people. Such violations may include identifying people by inappropriate matching of fingerprint or iris scans or facial photographs stored in the Aadhaar database or using the demographic data to identify people without their consent and beyond legal provisions.

3. Illegal tracking of individuals: Individuals may be tracked or put under surveillance without proper authorization or legal sanction using the authentication and identification records and trails in the Aadhaar database, or in one or more AUA's databases. Such records will typically also contain information on the precise location, time and context of the authentication or identification, and the services availed. We wish to emphasize that insider attacks are the most dangerous threats in this context. For instance, the second and third attacks above are much more likely if the attacker can collude with an insider with access to various components of the Aadhaar system.

IX.Authentication without consent

Authentication without consent should not be possible under any circumstances. Additionally, it should be possible to revoke an authentication credential in case it is compromised, with the identity of the individual remaining intact. UIDAI defines Aadhaar authentication as follows (UIDAI, 2016a): "Aadhaar authentication is the process wherein Aadhaar number, along with other attributes (demographic/biometrics/OTP) is submitted to UIDAI's Central Identities Data Repository (CIDR) for verification; the CIDR verifies whether the data submitted matches the data available in

CIDR and responds with a Yes/No. No personal identity information is returned as part of the response". (UIDAI, 2016a) goes on to define five types of Aadhaar based authentication:

1. Type 1 Authentication: Through this offering, service delivery agencies can use Aadhaar Authentication system for matching Aadhaar number and the demographic attributes (name, address, date of birth, etc) of a resident.

2. Type 2 Authentication: This offering allows service delivery agencies to authenticate residents through One-Time-Password (OTP) delivered to resident's mobile number and/or email address present in CIDR.

3. Type 3 Authentication: Through this offering, service delivery agencies can authenticate residents using one of the biometric modalities, either iris or fingerprint.

4. Type 4 Authentication: This is a 2-factor authentication offering with OTP as one factor and biometrics (either iris or fingerprint) as the second factor for authenticating residents.

5. Type 5 Authentication: This offering allows service delivery agencies to use OTP, fingerprint, and iris together for authenticating residents.

5.1. The Aadhaar number and the possibility of identification without consent

The Aadhaar number is at the heart of the Aadhaar scheme and is one of the biggest causes of concern. Recall that the Aadhaar number is a single unique identifier that must function across multiple domains. Given that the Aadhaar number must necessarily be disclosed for obtaining services, it becomes publiclyavailable, not only electronically, but also often in human readable forms as well, thereby increasing the risk that service providers and other interested parties may be able to profile users across multiple service domains. Once the Aadhaar number of an individual is (inevitably) known, that individual may be identified without consent across domains, leading to multiple breaches in privacy.

Another major issue is that of identity theft, whose potential for damage now increases manifold. As an illustrative example, let us consider the US Social Security Number (SSN). The primary difference between Aadhaar and SSN is that the SSN does not have any biometric identifier attached and it does not support authentication. The SSN associated with a person provides a single interface to the person's dealings with a vast number of public and private bodies, very similar to how the usage of the Aadhaar number is being envisaged. While this facilitates use of administrative data for useful data analytics, the ease of obtaining the SSN from across public and private databases also results in extremely high number of identity theft cases.

X. Conclusions

We have analyzed the Aadhaar project from the points of view of privacy and security and have pointed out some technical weaknesses and possible remedies. Specifically, we have found that.

1. The Aadhaar number, which is a single global identifier that is supposed to work across application domains, makes individuals vulnerable to privacy breaches. A design alteration can however make it safe.

2. The slightly different concepts of authentication and identity verification need to be well demarcated, and careful use case analysis is required to determine precisely what is required for each application. The legal framework must also make note of these.

3. In an Aadhaar like setup, the biggest threat to privacy comes from potential insider leaks. The Aadhaar technology architecture does not seem to have been explicitly designed to have strong protections against such insider leaks.

4.We believe that effective protection against insider leaks necessarily requires a third-party auditor under independent administrative control. With such a provision in place there are several tools from computer science that can provide reasonable guarantees for security and privacy protection.

XI.References

1.N. Alliance, "5g white paper", Next Generation Mobile Networks White paper, 2015.

2.M. Peng, S. Yan and H. V. Poor, "Ergodic capacity analysis of remote radio head associations in cloud radio access networks", IEEE Wireless Networks.

3.N. Nikaein, E. Schiller, R. Favraud, K. Katsalis, D. S-tavropoulos, I. Alyafawi, et al., "Network store: Exploring slicing in future 5g networks" in Proceedings of the 10th International Workshop on Mobility in the Evolving Internet Architecture, ACM, pp. 8-13, 2015.

4.C. Castelluccia, E. Mykletun and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks", The second annual international conference on mobile and ubiquitous systems: networking and services, pp. 109-117, 2005.

5.X. Lin, R. Lu and X. S. Shen, "Mdpa: multidimensional privacy-preserving aggregation scheme for wireless sensor networks", Wireless Communications and Mobile Computing, vol. 10, no. 6, pp. 843-856, 2010.

6.R. Lu, X. Liang, X. Li, X. Lin and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications", IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1621-1631, 2012.

7.C. Wu, H. Mohsenian-Rad and J. Huang, "Vehicle-to-aggregator interaction game", IEEE Transactions on Smart Grid, vol. 3, no. 1, pp. 434-442, 2012.

8.L. Gan, U. Topcu and S. H. Low, "Optimal decentralized protocol for electric vehicle charging", IEEE Transactions on Power Systems, vol. 28, no. 2, pp. 940-951, 2013.