ISSN 2250-3153

AADHAAR – Possibilities with 1 to n authentication

Shyam Singh Amrawat

Syscom Corporation Limited

Abstract: When it comes to human trafficking, more than 90% of countries have laws to tackle this but having law only does not prevent, suppress the crime rate. The report published by UNODC[1] mentioned that even when 90% of countries have legislation to criminalize but between 2010 and 2012, some 40 per cent of countries reported less than 10 convictions per year. Some 15 per cent of the 128 countries covered in this report did not record a single conviction.

So let government agencies do their work to reduce trafficking. But today India has a strong system which can be used to track back an individual and possibly rejoin the trafficked child with his/her family. The system is AADHAAR.

Also same system can be used to identify unidentified dead bodies for which biometric data can be collected.

Index Terms: AADHAAR, Identity tracking

I. Introduction

AADHAAR is an initiative of Government of India, where every resident of India will get a 12 digit unique number after obtaining his/her biometric data and verification of demographic data.

Today AADHAAR authentication is preordained for establishing identity, improving efficiency / transparency in service delivery & address / demographic Verification. Following are the different entities involved in AADHAAR authentication:

Following are the key actors in AADHAAR[2] authentication

- **Unique Identification Authority of India (UIDAI):** UIDAI is the overall regulator and overseer of the Aadhaar authentication system. It owns and manages the Central Identities Data Repository (CIDR) that contains the personal identity data (PID) of all Aadhaar-holders.
- **Authentication Service Agency (ASA):** ASAs are entities that have 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.
- **Authentication User Agency (AUA):** An AUA is any entity that uses Aadhaar authentication to enable its services and connects to the CIDR through an ASA. An AUA enters into a formal contract with UIDAI.
- **Sub AUA:** An entity desiring to use Aadhaar authentication to enable its services through an existing AUA. Examples: (i) IT Department of a State/UT could become an AUA and other departments could become its Sub AUAs to access Aadhaar authentication services. UIDAI has no direct contractual relationship with Sub AUAs.
- **Authentication Devices:** These are the devices that collect PID (Personal Identity Data) from Aadhaar holders, transmit the authentication packets and receive the authentication results. Examples include PCs, kiosks, handheld devices etc. They are deployed, operated and managed by the AUA/Sub AUA.
- **Aadhaar holders:** These are holders of valid Aadhaar numbers who seek to authenticate their identity towards gaining access to the services offered by the AUA.

[1] https://www.unodc.org/documents/data-and-analysis/glotip/GLOTIP_2014_full_report.pdf
[2] https://uidai.gov.in/authentication-2/

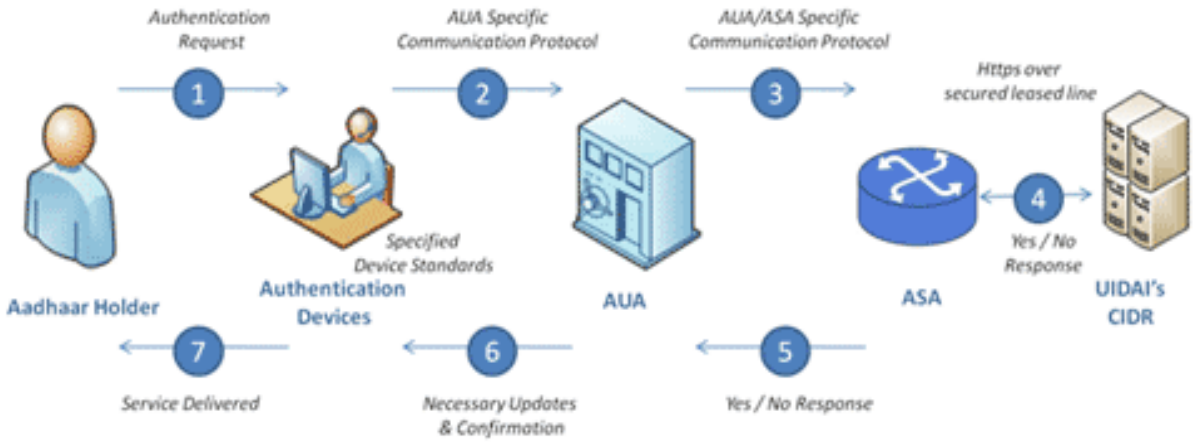

Figure 1: Authentication framework

There are five different modes are defined for authentication.

1. **Type 1:** 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:** 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:** Through this offering, service delivery agencies can authenticate residents using one of the biometric modalities, either iris or fingerprint.
4. **Type 4:** 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:** This offering allows service delivery agencies to use OTP, fingerprint & iris together for authenticating residents.

Figure 2: Authentication mechanism

In all form of authentication, AADHAAR number has to be provided so that authentication is reduced to a 1:1 match. But it does not mean that the system does not have capability to do 1:n matching. During allotment of AADHAAR number, system performs de-duplication within existing data. But this 1:n facility is not extended beyond this phase.

II. Proposal

AADHAAR authentication with 1:n facility equips security agencies for identification of suspected individuals and at the same time brings huge hope for families whose loved ones are missing. To make this happen we need to extend the scope of "**Introducer's Aadhaar No**" or "**Head of Family Aadhaar No**" and authentication facility.

Role of "Introducer's Aadhaar No" or "Head of Family Aadhaar No": Today this field is used when an individual cannot produce any document as a proof of identify/address. In such case all verification will be based on the Introducer or HOF.

To ensure effective usage of 1:n authentication following would need to be mandated:

- Every kid's AADHAAR must be linked with introducer / HOF ➔Parent / Guardian: Ensure that every kid's biometric identify is associated with their parents/guardian, so that in hour of need it can be used.
- Introducer is also must in case HOF is not alive: There may be situation where an individual may not be able to present AADHAAR related data of his/her parents/guardian. In that case mandate the need of introducer who can be called upon in case of need.
- In all cases Introducer/HOD authentication is must during enrollment process.

Authorized entities need to be listed who can do 1:n verification without presenting AADHAAR number. Security agencies would be the first option but the service should be extended to each individual with some rational charges.

Apart from this a legal framework should be designed so that parents can get information/alert about their children's 1:n authentication.

III. Benefits

Security agencies will be able to track back individuals.

Parents of trafficked children can get alert.

In accidental cases Hospitals will be able to process medical claim when the person who is injured and not able to present his/her medical insurance policies.

IV. Limitation

Children & kids above 1 year of age can apply for AADHAAR card. Kids' biometrics data, such as finger prints, keep changing frequently upto 5 years of age. Therefore no biometric data will be collected for kids below 5 years age. For children below 5 year age, the AADHAAR card will be linked to their guardian / parents.

When the child turns 5 years age, his/her biometric data will be collected and linked to his/her AADHAAR card. When the child turn 15 years age, his/her final biometric data will be taken once again (for the last time) and linked to the AADHAAR card.

V. Challenges

Trafficking is crime and criminals may go extreme to hide biometric identity of trafficked person. They may try to damage biometric identify of trafficked person.

Tracking individual to its ancestral path may raise concern over privacy.

Author

Shyam Singh Amrawat has 10+ years of experience in smart card industry. Currently working with Syscom Corporation Limited (A Morpho Company) as Sr. Manager.

Contact Info:Personal: shyam.amrawat@gmail.com; **Office**: shyam.amrawat@morpho.com https://in.linkedin.com/in/amrawat