July-December 2019 Volume 28 Issue 2 PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW

Official Publication of Medicolegal Association of Maharashtra

MULTISPECIALITY, MULTIDISCIPLINARY, NATIONAL
PEER REVIEWED, OPEN ACCESS, MLAM (SOCIETY) JOURNAL

Editorial Office Address
Department of Forensic Medicine, Third Floor, Library Building, Seth G S Medical College & KEM Hospital, Parel, Mumbai-400 012
Email id: mlameditor@gmail.com Phone: 022-24107620 Mobile No. +91-9423016325

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW
(Official Publication of Medicolegal Association of Maharashtra)
Email.id: mlameditor@gmail.com

PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

Letter to Editor

Amalgamation of Biometric systems like 'AADHAR' with the traditional methods of identification: Can it be a solution for identification in forensic cases in future?

Tumram Nilesh K[a]*

[a] Associate Professor, Department of Forensic Medicine & Toxicology, Indira Gandhi Government Medical College, Nagpur, Maharashtra, India-440018.

To,

The Editor in Chief, JFMSL.

Identification of an individual can be an important part of investigation in cases of homicide, accident, suicide etc.[1] Currently the identification process done by the investigating officers or the forensic medicine expert, or forensic science person is limited to facial photos, fingerprints, anthropometric measurements, dentistry or DNA profiling etc.

A recent progression in biometric technology which is equipped with computational intelligence techniques is substituting manual identification approaches in forensic science.[2] Biometrics is a important verification mechanism that identifies individuals on the basis of their physiological and behavioral features.[2]

In recent years biometric system of data had been generated by our government through Unique Identification Authority of India (UIDAI) and made biometric identification cards like AADHAR cards an essential entity. Similarly, some private or semi government organizations have also developed their own sets of biometric identity system like smart card etc.

What is Aadhaar biometric ID system?

Aadhaar is a 12-digit unique identity number that can be received voluntarily by residents of India, based on their biometric and demographic data.[3] The data is gathered by the Unique Identification Authority of India (UIDAI), a statutory authority constituted in January 2009 by the government of India, under the jurisdiction of the Ministry of Electronics and Information Technology, following the provisions of the Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016, check resident's eyes and fingers for fitness (missing/amputated). If the resident has any deformities due to which it is not possible to take fingerprints/iris, these also have to be captured as a biometric exception.[3]

How to cite this article: Tumram NK, Amalgamation of Biometric systems like 'AADHAR' with the traditional methods of identification. J For Med Sci Law 2018;27(2):58-61.

***Corresponding author:** Tumram Nilesh K, Associate Professor, Department of Forensic Medicine & Toxicology, Indira Gandhi Government Medical College, Nagpur, Maharashtra, India-440018. email:- ntumram@rediffmail.com, ntumram@gmail.com (M) +91-9422819766.

The number is linked to the resident's basic demographic and biometric information such as a photograph, ten fingerprints and two iris scans, which are stored in a centralized database. Facial Image, IRIS and Fingerprints for all the residents above 5 years in age is taken. In case of any children who are below 5 years in age, only Facial Image and any one parent’s Biometric Confirmation is captured.

Aadhaar is the world's largest biometric ID system. World Bank Chief Economist Paul Romer described Aadhaar as "the most sophisticated ID programme in the world".[4] Now can such a large data pool of information be utilized for the purpose of identification in forensic cases is a matter of research? If properly channelized and used the biometric system of identification can be easily utilized for the same. This together with the traditional methods of identification can go much nearer to the identity of the person in question of the investigation. In India, currently many government beneficiary schemes are linked with AADHAR cards. Hence, many of the peoples have registered themselves with the AADHAR biometric system. mAadhaar is an official mobile application developed by the UIDAI to provide an interface to Aadhaar number holders to carry their demographic information including name, date of birth, gender, and address along with photograph as linked with their Aadhaar number in smartphones.

Possible uses of AADHAR biometric system in Forensic cases

Tertiary care hospital, district hospitals, rural hospitals, primary health centers caters medical services ranging from treatment to dealing with medicolegal cases related to sexual offenses, accidents, homicide, suicides etc. in the process when the identity of the individual admitted to the hospital in unconscious state, or in comatose condition becomes of paramount importance than various traditional methods of identification like clothes, ornaments, mole, tattoo, height, weight, colour complexion, etc are noted for identification purpose. However, utilization of such methods for identification takes its own course leading to unnecessary delay in identification of individual causing grave harm medicolegally to the case. Services like AADHAR linked biometric system if utilized with due permission and process of the government can be a great boon in quick identification of the individual leading to solving of problems as small as tracing of relative to nabbing of accused in relevant cases.

Similarly, during postmortem examination many a times unknown, unclaimed bodies are brought by the police for postmortem that remain unidentified even after several days of admission and postmortem examination. This can be to a certain extent resolved with the help of AADHAR linked biometric system. Also, the investigating agencies can easily utilize its services in cases of kidnapping, child theft and in places where there are large crowd gathering like kumbh mela, devotional yatra like Amarnath yatra, pandharpur vari etc. to identify the person in question. If at all a system be developed where in a fingerprints found at the crime scene be properly developed and subjected to identification through AADHAR biometric system, this can lead to quick solving of many serious nature of offenses.

Requirement for AADHAR Linked biometric system[3]

1 Authentication Devices & Documents

Authentication devices are host devices/electronic actors that form a critical link in the Aadhaar authentication ecosystem. These devices collect personal identity data (PID) from Aadhaar number holders, prepare the information for transmission, transmit the authentication packets for authentication and receive the authentication results. Examples of authentication devices include form factors ranging from desktop PCs, laptops, kiosks to Point-of-Sale (PoS)/handheld mobile devices (microATMs) and tablets. Such devices are expected to be used for a variety of purposes specific to every requesting entity’s requirements.

Authentication devices are deployed by requesting Entities. Based on the mode of operation, such devices are classified as Self-Assisted and Operator Assisted devices.

Self-Assisted devices are the devices where Aadhaar authentication transaction is carried out by the Aadhaar number holder himself/herself without any assistance. Operator-Assisted devices are the devices where the Aadhaar authentication transaction of the Aadhaar number holder is performed with the assistance of requesting entity's operator.

2 Biometric Devices

Biometric devices means the devices that are used for capturing the biometric data inputs i.e Fingerprint / Iris /both the information from Aadhaar number holders. These biometric devices fall under two categories viz. Discrete Devices, Integrated Devices.

Discrete Devices: These type of devices refer to the class of biometric devices (Fingerprint/IRIS) that require connectivity to a host device such as PC/laptop/Micro ATM etc.

Integrated Devices: The integrated devices have the sensor integrated into the device package i.e. phone/tablet etc.

The form factors in which biometric devices may be deployed include: Hand-Held / PoS Device such as MicroATMs, attendance devices, USB device connected to PC, Mobile phone with biometric sensor, Kiosks such as ATMs, MNREGA job request kiosks.

Requesting Entities may choose appropriate authentication type (Fingerprint/Iris in case of biometric modality) based on their service delivery needs, nature of service, volume of transactions, desired accuracy levels and risk factors associated with their service delivery. Once the modality is chosen as Fingerprint/Iris/a combination of both/ multi-factor authentication involving OTP along with biometrics (Fingerprint/Iris/Both), the requesting entity can leverage the published list of certified device suppliers for the purpose of procurement of certified biometric devices (Fingerprint/Iris).

UIDAI Requires that only registered devices should be used by all Authentication Eco partners.[3]

"Registered Devices" refer to devices that are registered with Aadhaar system for encryption key management. Aadhaar authentication server can individually identify and validate these devices and manage encryption keys on each registered device.

Device identification – every physical sensor device having a unique identifier allowing device authentication, traceability, analytics, and fraud management.

Eliminating use of stored biometrics – every biometric record is processed and encrypted within the secure zone eliminating transmission of unencrypted biometrics from sensor to host machine.

Legality of sharing data with law enforcement[5]

In 2013 in Goa CBI approached a local court in the case of a rape of a schoolgirl, for acquiring UIDAI database for matching the fingerprint obtained from crime scene with the UIDAI database of all the persons in Goa. The court asked the UIDAI to hand over all data of all persons in Goa to the CBI.

The UIDAI appealed in the Bombay High Court saying that accepting such a request would set precedent for more such requests. The High Court rejected the argument and on 26 February 2014 in an interim order directed Central Forensic Science Laboratory (CFSL) to study the technological capability of the database to see if it could solve such a crime. The UIDAI then appealed in the Supreme Court. It argued that the chance of a false positive was 0.057% and with 600 million people in its database it would result in hundreds of thousands of false results.

On 24 March 2014, the Supreme Court restrained the central government and the UIDAI from sharing data with any third party or agency, whether government or private, without the consent of the Aadhaar-holder in writing. Vide another interim order dated 16 March 2015, the Supreme Court of India has directed that the Union of India and States and all their functionaries should adhere to the order passed by this court on 23 September 2013.

Conclusion

AADHAR linked biometric system has now well established itself in our country. Majority of the current population are aware regarding registering themselves in this system. This has created an enormous data pool for identification purpose. Though currently there are some legal and technical hurdles for utilization of this system for the purpose of identification in forensic cases. This will not remain the same in near future. With advancement in technology and more and more people getting registered in this system, it will definitely help in identifying not only the missing or unknown person but also people accused for any crime related offenses. The merits of utilization of such system together with the traditional system of identification can greatly over-weigh the demerits. Hence, the time has ripen now for the investigating agencies, doctors, forensic experts handling medicolegal cases to seriously look in for the utilization of such unique identification system.

References:

1. Reddy KSN, Murty OP. Chapter 3. Identification. In The Essentials of Forensic Medicine and Toxicology. 34th edition, Jaypee Brothers Medical Publishers. 2017; page 28-50.
2. Saini M, Kapoor AK. Biometrics in Forensic Identification: Applications and Challenges. J Forens Med. 2016;1:108.
3. https://uidai.gov.in. Authentication Devices & Documents. Biometric Devices. Assessed on 26/09/2019
4. http://www.daijiworld.com/news/newsDisplay.aspx?newsID=442948. Adhaar' most sophisticated ID programme in the world : World Bank. Assessed on 26/09/2019
5. https://www.deccanherald.com/content/392748/uidai-approaches-sc-over-sharing.html"UIDAI approaches SC over sharing data with CBI". Deccan Herald. 17 March 2014. Assessed on 27/09/2019.