iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8317

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Privacy and Security Issues in Aadhaar

A.K.R.S.Anusha[1], Dr. G. Rajkumar [2]
[1, 2] *Assistant Professor, Department of Computer Applications, N.M.S. S. Vellaichamy Nadar College, Madurai, Tamilandu. India.*

Abstract: Aadhaar number a twelve digit unique identification (UID) number issued for all people who are living in India, both adults and children. It is issued by the Unique Identification Authority of India (UIDAI). Aadhaar number is used for unique identification of people who live in India. Aadhaar can be used as a single source of identity proof of an individual who reside in India. It enables the downtrodden people to avail the services provided by the Government. Aadhaar uses biometric information for identification and authentication of people of India. The Aadhaar life cycle involves collection, transmission, and storage of biometric information in a central repository. The UIDAI stores Aadhaar details of individuals in a centralized database called Central Identities Data Repository (CIDR). This database and other hardware and software involved in the Aadhaar process can be subject to a variety of passive and active attacks. Several Acts and Legislations have been passed to preserve the privacy of individuals and security of Aadhaar details. This paper analyzes the purpose, benefits, and the privacy and security issues associated with the collection, transmission and storage of Aadhaar details. Aadhaar details will be a boon if used with proper security measures. Any compromise of biometrics of a person will have serious consequences on the individual throughout his/her life.

Keywords: Aadhaar, UID, UIDAI, CIDR, Biometrics, Privacy, Security, Identity, Authentication, Resident, Registrar,Authenticator, Access Control.

I. WHAT IS AADHAAR?

Aadhaar is a unique identification card issued to the people of India for their unique identification in India. Aadhaar card is issued by Unique Identification Authority of India (UIDAI). The basic objective of UIDAI is to uniquely identify an individual based on the person's biometric and demographic information. User Identification (UID) number is a 12-digit unique number with no intelligence built into it. Aadhaar uses face, iris, and fingerprint biometric for unique identification of people and to check for duplicate identity. Aadhaar can be used to uniquely identify a person out of the entire Indian population and to eliminate duplicate identity. Aadhaar number will be available to every resident of India, both citizen and non-citizen.

A. Benefits of Aadhaar

1) The UID can serve as a single source of verification of the identity of an individual.
2) Using Aadhaar, a person's identity can be verified and authenticated in an easy and cost effective way.
3) Aadhaar can be used to eliminate duplicate and fake identities.
4) The UID will also facilitate Indian people, both citizens and non-citizens from utilizing the services provided by the government.

B. What is Biometrics: Identity or Authentication?

An identity is defined as "who you are", authentication is defined as "How you can prove your identity". In a UIDAI system, biometric serves both as an identifier and as an authenticator of a person.

C. Accuracy of Biometric Identification

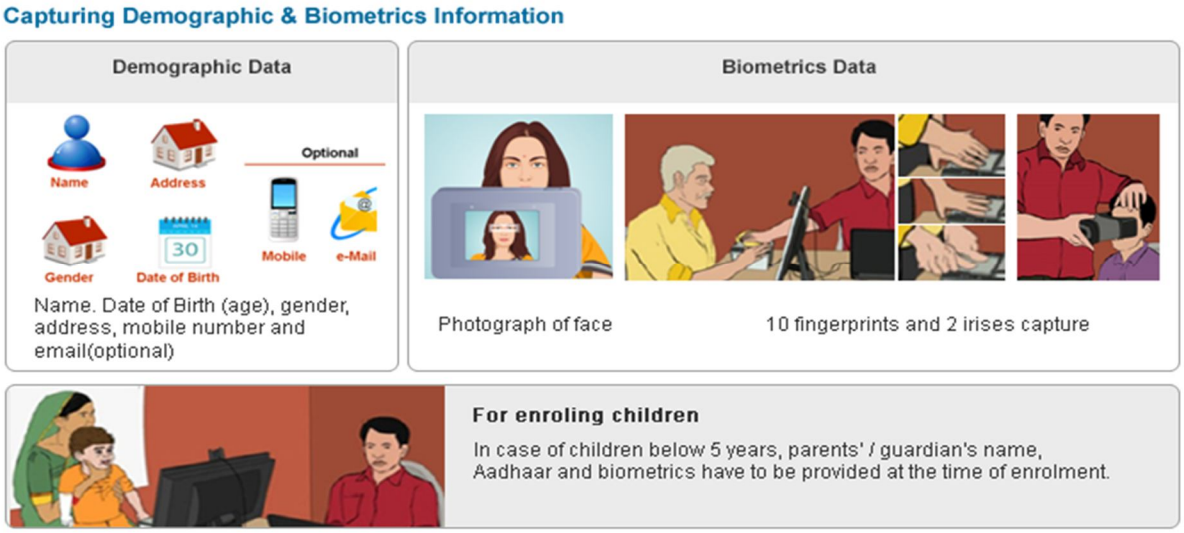
At present, there is no technology based on Biometrics which is 100% accurate. The accuracy of the best system available is estimated to be 98.6 percent of the time on single-finger tests, 99.6 percent of the time on two-finger tests, and 99.9 percent of the time for tests involving four or more fingers. So, chances of false positives still exist even while using a biometric system which is proved to be very robust.

Number of Fingers	FRR%	FAR%
2	10.3	29.2
10	10.9	0.0

FRR – False Rejection Rate
FAR – False Acceptance Rate

D. Data Flow of UIDAI Model

1) An Indian resident applies for UID and submits the required documentation.
2) The registrar sends the information to UIDAI.
3) UIDIAI verifies the uniqueness of the resident, and issues UID if unique.
4) The resident provides his UID and biometrics for authentication.
5) Authenticator sends the data to UIDAI for verification.
6) CIDR authenticates the resident data and sends back to the authenticator.
7) Upon successful identification, the authenticator provides the requested service to the resident.



II. LIFECYCLE OF AADHAAR

A. Security and Privacy Issues in Aadhaar Life Cycle

Although Aadhaar provides many benefits to individuals, it is not free from privacy and security problems. Many security and privacy issues can occur during various stages of the Aadhaar lifecycle. Security and privacy issues may happen during the collection, transmission and storage of Aadhaar details in the centralized database. These issues have to be taken care of meticulously. Otherwise, the individuals may be affected by a variety of serious problems.

Aadhaar uses biometric details for unique identification of individuals and for authentication. Biometric systems may become vulnerable to potential attacks. Some of these security vulnerabilities include the following:

1) *Vulnerabilities in Biometric Capture Devices*: UIDAI has issued contract to several companies for technical support. It receives technical support for biometric capture devices, from L-1 Identity Solutions, Inc. (now MorphoTrust USA), a US-based intelligence and surveillance corporation. Accenture Services Pvt. Ltd is another company which is awarded contract for taking care of the major aspects of the Aadhaar project. Accenture works with US Homeland Security, and Ernst & Young and Selection of Managed Service Provider (MSP).
2) *Private Players and Data Leakage*: Initially, the registrars of Aadhaar collect details of individuals and store the data that is collected from the residents; this creates a major chance for data leakage. There are many private personnel involved in the entire sequence of processes of registration and generation of Aadhaar numbers before the database finally goes to the government-controlled Central Identities Data Repository (CIDR). The integrity and accountability of the people involved in the tasks needs to be ascertained.

3) *Cryptographic Algorithms:* Aadhaar's Central ID Repository (CIDR) is protected by commercial network security and cryptographic products purchased from different vendors. The possibility for data destruction, damage or eavesdropping, surveillance or hacking of sensitive and private data increases exponentially due to the use of these products. The effect on individual privacy is undoubtedly adverse due to these vulnerabilities.
4) *Infrastructure Failures:* Infrastructure malfunctioning due to power failure or a server failure may lead to loss of sensitive personal information. Also, natural calamities can cause break down of any part of the UIDAI infrastructure, leading to damage and loss of information.
5) *Access Control:* Access Control is another basic security measure that should be taken care of. Access rights that control who can access Aadhaar data and the applications that manage these data need to be properly defined and monitored. Any penetration and modification of access control information will lead to disastrous consequences.
6) *Human Error:* Human beings involved in the whole process of issue of Aadhaar numbers may cause problems either accidently or maliciously. Agents might leave system unlocked and storage tapes may be lost in transport.
7) *Security and Privacy Challenges in a Centralized UID Database:* The CIDR database is a centralized database that contains information about everything concerning an individual. Snooping and hacking into this database is always possible. The creation of a large centralized database, the transmission of sensitive data over networks in real-time, present significant operational and security concerns. If the database collapses, the entire identification system will fail. To circumvent this problem, designers should provide high redundancy by using parallel systems and mirrors to ensure reliability and availability. However, this may increase the security issues and privacy of the biometric data. There are also significant risks associated with transmitting biometric data over computer networks where they may be tapped, copied, and altered, even without any detection.

B. Active and Passive Attacks

Several active and passive attacks may be targeted on the CIDR database. Strong security measures should be adopted in order to thwart security attacks. Some of the most important attacks are discussed in the following section.

Spoofing Attacks	It has been proved that a biometric system can be fooled on some instances by applying fake fingerprints, face or IRIS image, etc.
Eavesdropping	An attacker captures the communication between the Registrar system and CIDR and reads the data without being detected.
Cryptanalytic attacks	These attacks directly target the cryptographic algorithms in order to break the confidentiality of the transmitted information.
Substitution attack	If an attacker gets access to the CIDR database, he can overwrite the legitimate user's data with his own.
Tampering	Data stored in the CIDR database may be modified through illegal penetration into the CIDR database.
Masquerade attack	A hacker can create a digital "artifact" image from a fingerprint template and can submit it to the system in order to produce an illegal match.
Trojan horse attacks	Some parts of the system, e.g. a matcher, can be replaced by a Trojan horse program that always outputs high verification scores even for fake details.
Man-in-the-middle attack	The attacker is located between the Registrar system and the server/middleware and communicates with both sides and eavesdrops information without the knowledge of the communicating parties.
Falsification of Content	The falsification of content by unauthorized writing into the file system due to access control problems is a severe threat.

C. Authorized Sharing of Aadhaar Details

A provision in the NIAI Bill facilitates Aadhaar information to be disclosed to security agencies. A provision in the Aadhaar form prompts people to tick if they are willing to link their Aadhaar numbers to their bank accounts and whether their biometric

information can be shared with other agencies. People unknowingly permit UIDAI from sharing information about them to security agencies. This is a breach of individual privacy. Proper measures are to be taken to prevent misuse of private details about individuals on the pretext of security concerns.

D. Legislations for Ensuring Privacy and Security of Aadhaar Data

Several acts and legislations have been passed to ensure the privacy and security of individuals of India. Data Protection including protection of personally identifiable information are based on the amended IT Act, 2008, and the following Supporting Acts and Legislations.

Act(s)

1) The Indian Penal Code, 1860
2) The Indian Telegraph Act, 1885
3) The Indian Contract Act, 1872
4) The Specific Relief Act, 1963
5) The Public Financial Institutions Act, 1983
6) The Consumer Protection Act, 1986
7) Credit Information Companies (Regulation) Act, 2005

E. Special Legislation(s)

1) The Information Technology Act, 2000
2) The Information Technology (Amendment) Act, 2008

UIDAI has announced severe punishment for fraud or unauthorized access or use of Aadhaar data by violating the privacy of individuals. However, there is no comprehensive Privacy Law in India which causes serious concerns about one's privacy and security.

III. CONCLUSION

UIDAI claims that access to its database will not be permitted to any agency, and will be secure from intelligence agencies that spy on citizens. But, this claim is questionable since Aadhaar enables surveillance and tracking of individuals in the pretext of controlling terrorism. Also, CIDR database containing personal information of individuals is vulnerable to a variety of active and passive attacks. Stringent security measures should be adopted to thwart such cryptographic attacks. Biometric information collected from people can be mishandled if not backed by adequate legal safeguards. Compromise of biometric information of a person can cause untold harm to the person and society. Proper care and legal security should be provided to ensure the privacy and security of Aadhaar details.

REFERENCES

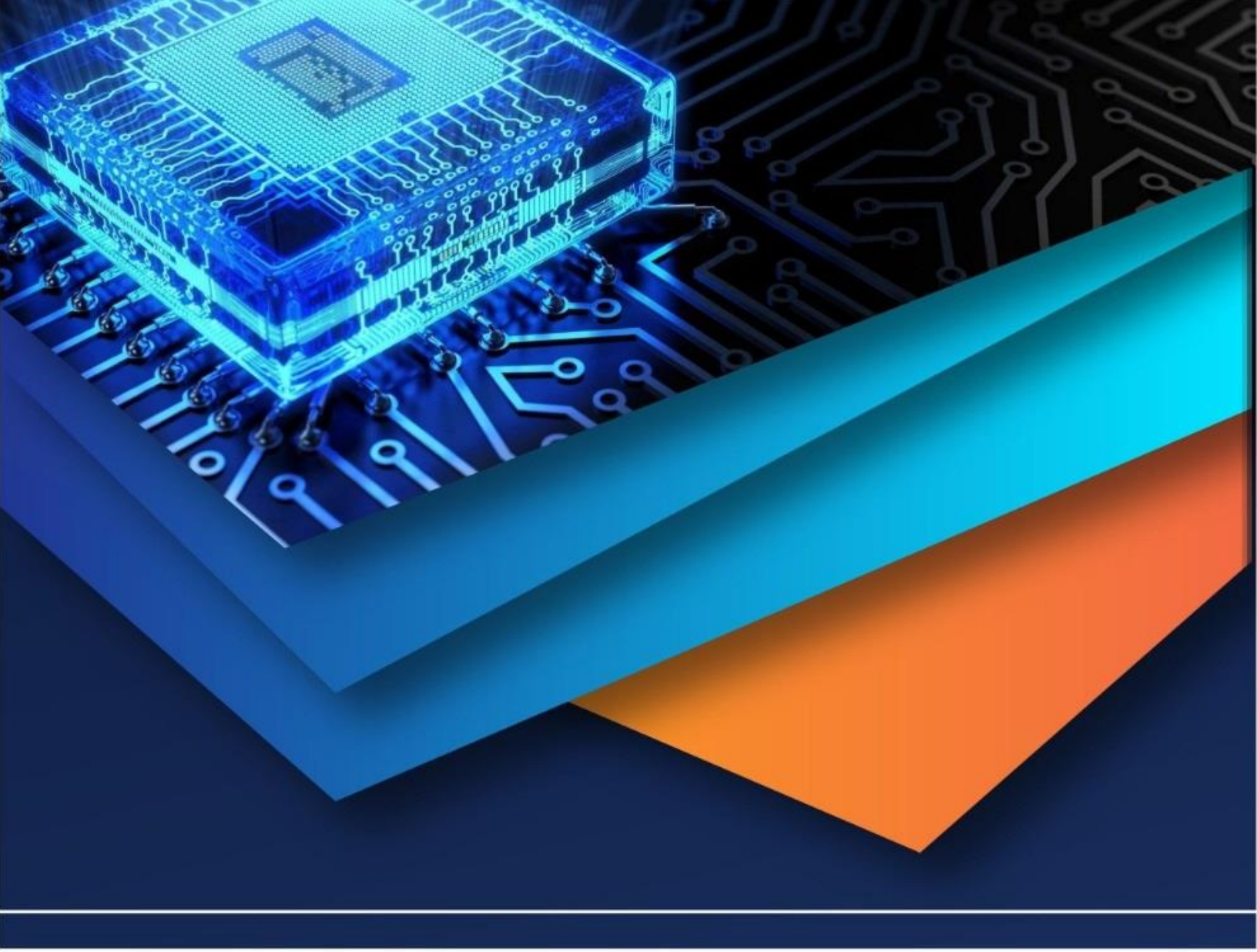
[1] Barak, Boaz, Goldreich, Oded, Impagliazzo, Rusell, Rudich, Steven, Sahai, Amit, Vadhan, Salil, & Yang, Ke. 2001. On the (im) possibility of obfuscating programs. Pages 1–18 of: Annual International Cryptology Conference. Springer.
[2] Bellare, Mihir, Boldyreva, Alexandra, & ONeill, Adam. 2007. Deterministic and efficiently searchable encryption.Pages 535–552 of: Annual International Cryptology Conference. Springer.
[3] Billet, Olivier, Gilbert, Henri, & Ech-Chatbi, Charaf. 2004. Cryptanalysis of a white box AES implementation. Pages 227–240 of: International Workshop on Selected Areas in Cryptography. Springer.
[4] Centre for Internet & Society, The. 2016. List of Recommendations on the Aadhaar Bill, 2016-Letter Submitted to the Members of Parliament. http://cis-india:org/internet governance/blog/list-ofrecommendations-on-the-aadhaar-bill-2016. [Online; posted 16-March-2016].
[5] Curtmola, Reza, Garay, Juan, Kamara, Seny, & Ostrovsky, Rafail. 2011. Searchable symmetric encryption: improved definitions and efficient constructions. Journal of Computer Security, 19(5), 895–934.
[6] Dodis, Yevgeniy, Reyzin, Leonid, & Smith, Adam. 2004. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. Pages 523–540 of: International Conference on the Theory and Applications of Cryptographic Techniques. Springer.
[7] Duggal, Pavan. 2011. Does the UID project infringe on privacy? http://www:business-standard:com/article/opinion/does-the-uid-project-infringe-on-privacy-111080300006 1:html. [Online; posted 3-August-2011].
[8] Jayaram, Malavika. 2015. Aadhaar debate: Privacy is not an elitist concern it's the only way to secure equality. http://scroll:in/article/748043/aadhaar-debate-privacy-is-not-anelitist- concern-its-the-only-way-to-secure-equality. [Online; posted 15-August-2015].
[9] Khera, Reetika. 2015. Five Myths about Aadhar. http://www:outlookindia:com/website/story/ five-myths-about-aadhar/295364. [Online; posted 18-September-2015].
[10] Kumar, Ashwani. 2015. Privacy, a non-negotiable right. http://www:thehindu:com/opinion/lead/privacy-a-nonnegotiable-right/article7519148:ece. [Online; posted 10-August-2015].

[11] Mehta, Pratap Bhanu. 2016. Privacy after Aadhaar. http://indianexpress:com/article/opinion/ columns/privacy-after-aadhaar-money-bill-rajya-sabha-upa/. [Online; posted 26-March-2016].

[12] Sakashita, Taiki, Shibata, Yoichi, Yamamoto, Takumi, Takahashi, Kenta, Ogata, Wakaha, Kikuchi, Hiroaki, & Nishigaki,Masakatsu. 2009. A Proposal of Efficient Remote Biometric Authentication Protocol. Berlin, Heidelberg: Springer Berlin Heidelberg. http://dx:doi:org/10:1007/978-3-642-04846-3 14. Pages 212–227.

[13] UIDAI. 2014. Aadhaar Technology & Architecture: Principles, Design, Best Practices, & Key Lessons. https://uidai:gov:in/images/AadhaarTechnologyArchitecture March2014:pdf. [Online; accessed 31-July-2016].

[14] UIDAI. 2016a. Authentication Overview. https://uidai:gov:in/auth:html. [Online; accessed 31-July-2016].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY