An offline alternative for Aadhaar-based biometric authentication

Subhashis Banerjee Subodh Sharma

Computer Science and Engineering, IIT Delhi
New Delhi 110016

August 11, 2018

The decision on the constitutionality of Aadhaar[1] by the supreme court remains a matter of speculation, but it has become abundantly clear that most of the use cases for Aadhaar based biometric authentication (ABBA) have turned out to be deeply problematic. That the use of biometrics as an authentication factor is conceptually flawed has been pointed out by many [Agrawal et al., 2017]. Biometrics are not secret information and are hence open to fraud. Further, the uncertainties in biometric matching, because of decision-making using a threshold score[2] which may lead to false negatives (referred to as 'probabilistic' by the petitioners in the supreme court), make them unsuitable because of the risks of causing exclusion and denial of rights in welfare [Drèze et al., 2017, Abraham et al., 2018, Kotwal and Ramaswami, 2018]. The requirement of reliable online connectivity compounds the problem.

In fact, the state's assurance that "nobody will be denied their entitlements because of biometric matching failure" does not pass muster. It is vacuous because there is no clear specification as to when the promise will apply and how such a false-negative set can be distinguished from the spurious attempts. Biometrics may only be good for de-duplication[3], and can perhaps also be used for identity

[1] Aadhaar or Unique Identification number (UID) is a 12-digit individual identification number issued by the Unique Identification Authority of India (UIDAI) on behalf of the Government of India. It captures the biometric identity – 10 fingerprints, iris and photograph – of every resident, and is meant to serve as a proof of identity and address anywhere in India.

[2] During biometric matching a similarity score between the presented and the stored fingerprints is computed. Incorrect rejection of a genuine person based on a threshold of the similarity score is called a false-negative.

[3] De-duplication is the offline process of pairwise matching of peoples fingerprints during Aadhaar enrolment to establish uniqueness.

verification under strict adversarial oversight. The latter use will require carefully designed protocols to deal with the false negative cases, and this can perhaps only be done at special centres where the required decision making expertise may be available.

Poor understanding of the identity instruments, broken processes, imprecise articulation of the objectives, and, most importantly, lack of clear understanding of the trust model of authentication, authorisation and accounting (AAA) have led to confusion and large scale social mistrust. In this note we outline the tentative design sketch of an alternate offline protocol, with digitisation and identity verification objectives similar to ABBA, which may satisfy more correctness properties and yet be free of the problems discussed above.

Trust model for the old fashioned identity card

Consider the traditional identity card that contains a name, a photograph and a few other details, and is typically used for identity verification. Common examples for general use, for instance, to prove one's identity for train travel in India, are the ration card and driving license, passport, voter id card, PAN card, cards issued by schools, colleges or government institutions and even the 'Aadhaar card'.

In the use of identity cards there is an implicit assumption that the human verifier is trusted, and is not expected to either collude with the presenter and identify falsely, or reject a genuine cardholder arbitrarily. Trust is also assumed for the presenter not to submit a card with a false name to the verifier, who often has no special means to tell a fake from a genuine. In the absence of a proof to the contrary it must be assumed that these identity cards can be faked. Most of these cards support indexing using a unique number. However, none of them support de-duplication and can claim one-to-one mapping between cards and people, even approximately.

It would appear that the trust model of the identity card is straightforward to analyse, and it ought to be easy to define appropriate, sensible and non-vacuous use cases based on them when the stakes are low. However, one is forced to wonder why exactly are such identity cards checked for admittance into government offices or hotels? Do they really expect that any person, either genuine or an imposter, will deliberately present an identity card where the name does not match the one declared, or the photograph does not match the face? Also, why would a corporate tech giant accept a false order against 'cash on delivery' [Pahwa, 2018] based on an uploaded Aadhaar card which can be easily faked?

KYC based on submission of (self) attested photocopies of such documents also have an identical trust model. It does serve an additional purpose of record

keeping and accounting. Though, the feasibility of a handful of telecom companies indexing and reliably maintaining paper copies of KYC documents of over half a billion customers is far from clear. Moreover, given the poor verifiability, it is impossible to be sure that a KYC obtained for one purpose will not be used for another, making both authorisation and accounting suspect.

Trust model for ABBA

The perceived trust deficit in the presenter and the verifier under certain situations was precisely the reason for which more complicated protocols like ABBA were introduced. However, even if we assume that biometric matching is perfect and there is no possibility of false presentation of biometric data, what are the implications for the trust model?

Though there is no trust assumption required for the presenter, trust on the verifier - the person manning the machine - is still implicit. Even if the verifier cannot control the remote authentication, which is based on centralised matching of biometric data, most usage protocols trust the verifier for authorisation and accounting. The protocols typically assume that the verifier will use genuine equipment, and not store the data and replay the process fraudulently. They also assume that a successful authentication will not be used to trigger false authorisation and accounting; for example, to open a bank account after obtaining an authorisation to only issue a SIM card [PTI, 2017], or to record a higher quantity of sale than what is actually supplied in PDS ration [Drèze et al., 2017]. Is this trust model correct for preventing leakage in PDS or for banking with micro-ATMs according to the food and finance ministries?

Moreover, if the authentication outcome is not communicated directly by the UIDAI to the user, but is instead routed through the verifier, then it opens up another set of trust based vulnerabilities. The issues with Aadhaar based eKYC are similar.

Clearly the AAA protocols need to be tightened. If the authentication is online from UIDAI, then UIDAI will also have to change their accounting model and record the precise purpose of authorisation. This, in turn, will require them to proactively adopt privacy preserving techniques and refrain from using inane phrases like “we do not record the purpose” and “privacy-by-design”.

Trust model for QR codes and smart cards with chips

The information in an identity card can also be embedded in a QR code or a smart card chip to facilitate machine readability. Examples of such QR based cards are

the PDS ration cards in Tamil Nadu [Khera, 2018] and West Bengal where verification is offline, and also the 'Aadhaar cards'. Most driving licenses all over the country use smart cards with chips, as do some 'offline' ration cards. If the contents are not digitally signed, as they do not appear to be in most of the above examples, then they can be altered fairly easily, and the trust model for these instruments is identical to that of the traditional identity cards. The only comparative advantage is machine readability which facilitates automation and accounting.

The largest QR code can hold about 3KB, and can be carried in passive cards or printouts, or even as images in smartphones. They are read optically. Smart cards with chips, which can be both contact based and contact less (radio), have more real-estate, but whatever can be stored in them can also be stored in smartphones, and they offer no special functional advantages over smartphones. They however are inexpensive, and can be used by people who do not carry smartphones. Their main advantage over QR based cards is that they can hold more data and can be used for both reading and writing whereas the QR cards are read-only. However, storing transaction logs and accounting data in a smart card is superfluous, because the data is required centrally for accounting in any case and it is easy to ensure storage reliability at the POS. Besides, any accounting data stored only in a smart card can easily be lost or damaged.

Offline biometric matching with biometric data stored in smart cards suffer from the same 'probabilistic' uncertainties of matching as in Aadhaar. Moreover, with such distributed offline low-end local storage, the biometric data is not fault tolerant. Also, de-duplication using biometrics requires centralised access for matching. So, there is no special advantage in using the local write facility in smart cards.

And, if we do not write data in smart cards, QR code based cards provide a simpler alternative. They are also more effective because they are portable to multiple forms and can be regenerated easily.

Trust model for offline identity verification with signed QR codes

Digitally signing the contents of a QR code with the secret key of an appropriate authority makes it tamper-proof, and altering even one bit of the content invalidates the signature. The authenticity of the content can then be verified at the POS terminal using the public key of the signing authority. This becomes an useful instrument for offline identity verification, considering the connectivity problems that plague the online methods. Indeed, the UIDAI has announced a redesign of the Aadhaar card for offline identification purposes [PTI, 2018], which is based on a digitally

signed tamper-proof QR code (one of us – SB – helped in the initial design discussions). Apart from the standard textual information the QR code also contains a facial photograph. It does not appear from their webpages that the QR coded ration cards used in Tamil Nadu and West Bengal have photographs embedded in them or are digitally signed.

A machine readable identity card with digitally signed tamper-proof textual information and a photograph has superior trust properties than fingerprints or iris images, because the latter can be faked. There is no trust assumption on the presenter carrying a signed QR code with a photograph. However, the verifier still needs to be trusted for AAA. This is slightly weaker than ABBA, but the possibilities of automatic matching failure and false presentation are absent altogether.

A protocol for offline AAA using a digitally signed QR code

Any offline protocol that has to remove the requirement of trust on the verifier, and neither use automatic matching to avoid false negatives, nor use unfamiliar instruments like passwords or crypto keys, must rely on ex-post audit, at least of some randomly picked instances.

Consider the following protocol. The verifier can use a tamper-proof POS device to read the QR code, which can automatically verify the genuineness of the content using the public key of the signing authority. The verifier can then manually compare the photograph read from the QR code with the face of the person carrying the card. To make it irrefutable, the decision of identity verification, either positive or negative, can then be stored in the POS machine, along with both the time-stamped photograph read from the QR code and a live time-stamped photograph recorded using the POS machine (with a liveness test to prevent replay attacks [Kähm and Damer, 2012]). If the verification is positive, the verifier should complete the transaction. The POS machine should record the transaction, and print and issue an appropriate receipt to the user. If required, the receipt can also be spoken out by the POS machine in a local language. For the authorisation and accounting to be complete, the verifier must also obtain an authorisation-cum-receipt from the user by an audiovisual recording using the POS machine. Optionally, tamper-proof peripheral devices like an electronic weighing machine, or a cash dispenser and deposit machine, can also be connected to the POS and at least the electronic parts can be made tamper proof. The complete transaction, along with the final video receipt, can then be stored encrypted and signed in the POS machine for lazy uploading whenever internet connectivity is available. The encrypted data can also be periodically transferred to a central server by physical means. Even assuming a hundred transactions a day, the data requirement will not be more than

a few hundred MBs per day, which is eminently manageable. Time stamped logs of all transactions must be recorded in the POS. Redundancy in POS and batteries may be necessary to ensure uninterrupted business.

The protocol ensures that the integrity of the transaction, including all of AAA, are irrefutable and can be audited. All it assumes is that the verifier cannot tamper with the POS terminal and the overall trust properties are superior to ABBA. Exclusion is possible only if there is a genuine mistake in face matching by the verifier. The offline audit of authentication can either be manual, either on random samples or on demand; or can be even be done automatically using face matching software of the type that has been announced by the UIDAI.

Strict enforcement of identity verification and physical presence, such as in ABBA or in the protocol described above, prevents transferability of identity instruments. A facility to be able to transact on behalf of another person is a crucial feature in transaction protocols, especially if they have to be deployed in welfare or for financial inclusion. It is not inconceivable to build such a feature on top of the protocol described here by finding appropriate exceptions to the physical presence requirement.

There are several groups in the country which can undertake design of such tamper proof POS and other embedded devices, perhaps with *trusted execution environments* [Sabt et al., 2015], which can be queried to prove their integrity on demand. And, for such critical use cases, it will be imperative to refine any design such as the one we have presented by formally modelling the trust and non-exclusion property requirements, and run the design through a theorem prover for automatic verification. However, before that, most importantly, any such design proposal must be thoroughly examined by field workers, administrators, independent researchers and other experts who have crucial ground-level understanding of the issues.

Online AAA for other transaction use cases provide many more interesting possibilities, but that can be the topic of another discussion.

References

Ronald Abraham, Elizabeth S. Bennett, Rajesh Bhusal, Shreya Dubey, Qian (Sindy) Li, Akash Pattanayak, and Neil Buddy Shah. State of Aadhaar Report 2017-18. Technical report, IDinsight, 05 2018.

Shweta Agrawal, Subhashis Banerjee, and Subodh Sharma. Privacy and Security of Aadhaar: A Computer Science Perspective. *Economic and Political Weekly*, Vol. 52(Issue No. 37), 16 2017.

Jean Drèze, Nazar Khalid, Reetika Khera, and Anmol Somanchi. Aadhaar and Food Security in Jharkhand. Pain without Gain? *Economic and Political Weekly*, Vol. 52(Issue No. 50), 16 2017.

O. Kähm and N. Damer. 2D face liveness detection: An overview. In *2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)*, pages 1–12, Sept 2012.

Reetika Khera. Smarter than Aadhaar: Govt's insistence on disruptive option is bewildering, 2018. URL http://www.business-standard.com/article/opinion/how-successfully-last-mile-authentication-has-recorded-pds-118031301260_1.html. [Online; posted 14-March-2018].

Ashok Kotwal and Bharat Ramaswami. Aadhaar that doesnt exclude, 2018. URL http://www.ideasforindia.in/topics/poverty-inequality/aadhaar-that-doesn-t-exclude.html. [Online; posted 11-April-2018].

Nikhil Pahwa. By Revealing His Aadhaar Number, the TRAI Chairman Has Opened a Can of Worms, July 2018. URL https://thewire.in/tech/trai-rs-sharma-aadhaar. [Online; posted 30-July-2018].

PTI. UIDAI suspends Airtel, Airtel Payments Bank's e-KYC licence over Aadhaar misuse, December 2017. URL https://economictimes.indiatimes.com/news/politics-and-nation/uidai-suspends-airtel-airtel-payments-banks-e-kyc-licence-over-aadhaar-misuse/articleshow/62096832.cms. [Online; posted 16-December-2017].

PTI. UIDAI brings updated QR code for offline Aadhaar verification, April 2018. URL https://timesofindia.indiatimes.com/india/uidai-brings-updated-qr-code-for-offline-aadhaar-verification/articleshow/63818793.cms. [Online; posted 18-April-2018].

M. Sabt, M. Achemlal, and A. Bouabdallah. Trusted execution environment: What it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 57–64, Aug 2015. doi: 10.1109/Trustcom.2015.357.