Aadhaar and Biometrics

*[Biometrics is at the heart of Unique ID Project of India christened as Aadhaar. As biometrics have never been used at such a massive scale to perform functions like de-duplication and authentication, there were serious apprehensions in the mind of various stake-holders relating to feasibility and accuracy of this exercise. This short paper describes as to how the choices made by UIDAI relating to biometric set, their specifications and the contractual arrangements with the service providers have helped the country in achieving something which looked very daunting in the beginning. Besides theory, PoC studies and their results provided the necessary comfort to UIDAI about the feasibility of implementation, cost and speed of this exercise. Today, when the count of Aadhaar numbers generated has crossed 900 million mark and the authentication system has become functional at scale, there are few doubts left about the project. Now, Aadhaar is at the centre of India’s public service delivery reforms and re-engineering.*

*The Author was the Director General and Missing Director (DG&MD) of this project and had worked there since the beginning in August 2009 till March 2014. He was at the centre of decision making relating to technologies and policies. Recapitulating the debates, concerns, methods to tackle the issues and finally putting this all into practice has acquired a new relevance from the perspective of designing large scale IT and governance projects and their implmentation.]*

# I. Introduction

1.1 Biometrics are at the heart of Aadhaar, the Unique Identity Project of India. Biometrics serve two basic purposes - (i) to ensure uniqueness and (ii) to enable online authentication.

1.2 When a person enrolls for Aadhaar, his basic demographic details along with finger (all ten fingerprints) and iris (both) images are captured. When this data is processed at the back-end, the biometric features of this person (say X) are compared with the biometrics of all those persons who have enrolled earlier and have been allocated Aadhaar numbers. The existing data-base is typically called the ‘gallery’. When the biometrics of X match with somebody in the gallery, we call it a 'hit'. Hit means that another person with the same biometric attributes already exists in the gallery and this 'other person' is the same as X. Hence the system rejects this new person declaring that he/she has already been enrolled and has been allotted an Aadhaar. This prevents issue of two IDs to the same person. There is, of course, a very small probability that the biometrics of two different persons match. This situation is called a 'false Hit' or false reject. In other words, we may reject allocation of Aadhaar to X due to this false match. Conversely, it may also happen that this person's data is already present in the gallery but the system fails to find the match. This is typically called ‘false acceptance’. False acceptance will mean that X will be issued an Aadhaar number while he/she already has one. This case militates against the uniqueness of IDs.

1.3 The objective function of this biometrics matching exercise is that we have no false rejects and no false accepts. Normally, both cannot be made zero and there is an inverse relationship between these two parameters. Tightening the system so as to reduce the false accepts may result in more false rejects and vice-versa. As the basic matching technique is a pattern matching and matching of certain features of the biometrics, this is not a one hundred percent accurate and there are chances of some errors. Both cases are possible - falsely rejecting someone's enrolment, resulting in denial of a number to someone and falsely accepting someone's enrolment and giving him two (or more) numbers. Having said that, the comforting fact is that the percentages of both these errors can be made to be exceedingly small using better technology and its management. The disconcerting side is that if the gallery is very large, then the number of such cases, even with small percentages of errors, can be quite large. For example, even with an accuracy level of 99.99%, there is a possibility that .01% population may end up in two or more IDs and that number, for a country like India with a population of 1.2 billion, is as large as 120 thousands!

# II. Setting the framework

2.1 Considering the importance of biometrics in UID system, UIDAI had constituted a Biometrics Committee (UIDAI, 2009) which was supposed to ‘review the existing biometrics standards and modify/extend/enhance them so as to achieve the goals and purpose of UIDAI for de-duplications and authentication’. This committee was constituted on 29th September 2009 and submitted its report in December 2009.

2.2 In the section titled “Biometrics Accuracy” the Committee observed:

*“12.4 Biometrics Accuracy*

*The UIDAI’s charter of assuring uniqueness across a population of 1.2 billion people mandates the biometrics goal of minimizing the False Accept Rate (FAR) within technological and economical constraints. All published empirical data is reported using Western populations and database sizes of tens of millions. An accuracy rate (i.e., True Acceptance Rate) of 99% is reported in the test of commercial system performance[23]. Two factors however raise uncertainty on the extent of accuracy achievable through fingerprints: First, the scaling of database size from fifty million to a billion has not been adequately analyzed. Second, the fingerprint quality, the most important variable for determining accuracy, has not been studied in depth in the Indian context.”(Para 12.4 pp 21 of the Biometric Committee Report)*

2.3 At another place in the same report, the committee had observed:

*“Based on rather extensive empirical results compiled by NIST and a first cut of Indian data analyzed in a short period, the following broad categorization can be made:*

*1. The UIDAI can obtain fingerprint quality as good as that seen in developed countries. There is good evidence to suggest that fingerprint data from rural India may be as good as elsewhere when proper operational procedures are followed and good quality devices are used. There is also data to suggest that quality drops precipitously if attention is not given to operational processes.*

*2. It is possible to closely predict the expected fingerprint recognition performance. In the experiments, at 95% confidence, the sample database of a rural region is expected to achieve similar accuracy as Western data. By extrapolating NIST analysis of Western data, it is possible to conclude that fingerprint alone is sufficient to achieve minimum accuracy level of 95%, with moderately good fingerprints images.*

*3. Face is an invaluable biometric for manual verification. Its potential to contribute materially to improved FAR rate is however, limited particularly because of extremely large database size and high value of target accuracy.*

*4. Iris can provide accuracy comparable to fingerprint. Therefore fused score of two uncorrelated modalities will provide better accuracy than any single modality and could achieve the target accuracy.*

*Empirical data has highlighted several non-technical factors that can impact accuracy more significantly than technical accuracy improvement efforts.*

* *Simple operational quality assurance. A few simple operational techniques such as keeping a wet towel or maintaining the device in good working order can be superior to squeezing an additional fraction of a percent in accuracy rates through technical improvements. An unchecked operational process can increase the false acceptance rate to over 10%.*
* *In the data analyzed, 2% to 5% of subjects did not have biometric records. Missing biometrics is a license to commit fraud. It is believed that the failure is due to poorly designed processes. The enrolment process when examined, had loopholes which prevented it from detecting such omissions.*
* *The biometric software needs to be tuned to local data. Un-tuned software can generate additional errors in the range of 2 to 3%.” (Para 22.4 page 22 of the Biometric Committee Report)*

# III. Iris: the critical biometric

3.1 It should be admitted that when the committee was deliberating on the issue of accuracy of biometrics (and we had consulted many biometrics experts during the deliberations), UIDAI was quite uncomfortable with the accuracy figures of 95% on western data. Fingerprints of our people will certainly be worse than those of Europeans - considering that we have large rural population and their fingerprint quality will be quite bad due do hard manual labor. An accuracy of 95% would mean a possibility that we may have as many as 5% false accepts - meaning thereby that we may have as many as 60 million people (5% of 1.2 billion) who can have two or more IDs. This will strike at the very root of Uniqueness - a property which is so integral that even the name of the organization implementing the project is Unique Identification Authority of India!

3.2 Iris was the only hope in this scenario. As the committee had observed, "*fused scores of two uncorrelated modalities will provide better accuracy than any single modality and could achieve target accuracy".*

3.3 As we know, the probability of two independent events is the product of probabilities of each of them. Hence if each of the modality (Fingerprint and Iris) had an error rate of 5%, then the probability of a false match happening when we have two uncorrelated (independent) biometrics will be 0.05 multiplied by 0.05, This is a mere 0.0025. In percentage terms this is 0.25%. This can give us an accuracy up to 99.75%.

3.4 While the recommendations of the Committee were being prepared, UIDAI argued very hard in favor of Committee recommending the inclusion of iris in the biometrics set to be collected by UIDAI. However, there were many members who did not agree with this. Registrar General of India (RGI) who had already collected finger-prints for some population argued that inclusion of iris will result in huge increase in the cost. He also argued that he will have to change his entire project report and the cost escalation will be substantial.

3.5 The Committee was not ready to recommend inclusion of iris. With all kinds of suggested formulations flying around in the mails, the Committee's recommendations on the issue could go only thus far:

*‘5. While 10 finger biometric and photographs can ensure de-duplication accuracy higher than 95% depending upon quality of data collection, there may be a need to improve the accuracy and also create higher confidence level in the de-duplication process. Iris biometric technology, as explained above, is an additional emerging technology for which the Committee has defined standards. It is possible to improve de-duplication accuracy by incorporating iris. Accuracy as high as 99% for iris has been achieved using Western data. However, in the absence of empirical Indian data, it is not possible for the Committee to precisely predict the improvement in the accuracy of de-duplication due to the fusion of fingerprint and iris scores.* ***The UIDAI can consider the use of a third biometric in iris, if they feel it is required for the Unique ID project.*** *[Emphasis supplied]'.*

3.5 Thus the Committee’s recommendations fell short of unambiguously recommending Iris. They left the decision on UIDAI. UIDAI management was convinced that if they did not include iris, the project was as good as dead – as then there will be no meaning of the word Unique - an objective so important for the country.

# IV. Inclusion of Iris

4.1 Inclusion of iris in the biometric set was not an easy proposition. Almost everybody in the system was opposed to it. there were a number of Committee of Secretaries (CoS) meetings where this issue was debated. UIDAI prepared a sort of white paper titled “Ensuring Uniqueness: Collecting iris biometrics for the Unique ID Mission” to argue the case as to why iris was necessary. This paper argued that inclusion of iris was important not only from the viewpoint of ensuring uniqueness; it was also important form a number of other reasons like inclusion of children and poor people. As iris are fully developed in the children at the age of five years (as opposed to fingerprints which stabilise at about 15 years of age), UIDAI will be able to include children in the identity system both for the purposes of uniqueness and authentication. It will also be good for the inclusion of poor people. The poor, due to occupations that usually involve physical labour, have fingerprints that are worn out and difficult to capture [as observed by the Biometrics Committee itself in their report]. Other factors were (i) Comfort (as iris capture is non-intrusive and contact-less, (ii) ease of use (iii) reducing risk of execution, (iv) reducing technology risks, (v) de-duplication process, (vi) applications, (vi) security and (vii) future development of identity systems.[[1]](#endnote-2)

4.2 On technology risk reduction we had argued as below:

“There are significant technology risks in the UID project – there are for instance, no examples to follow, with no previous such technology implementations of this scale. The project also pushes the boundaries of existing de-duplication and authentication technologies, due to the project’s unprecedented size.

While ten fingerprints, when collected with care with special emphasis on quality can give us high accuracy, this faces some uncertainties, considering the technology challenges stated above. The use of iris as an additional (and uncorrelated) biometric mitigates the project’s technology risks considerably.”[[2]](#endnote-3)

4.3 One of the strong points of opposition was that iris was a proprietary technology and there were serious risks of vendor lock-in. UIDAI categorically answered this question in the negative. Other concern relating to cost was also dealt with and detailed cost-sheets were provided to estimate the additional incremental cost which was estimated to be Rs. 4.40 per enrolment. Finally after a number of deliberations and presentations, iris was accepted as a biometric to be included in the UID project.

4.4 In retrospect, this was probably the most important decision which has saved this project. If iris was not included in the biometric set, the project would not have succeeded at all. Now that we are well into authentication of identities, we find that iris authentication is a better and more accurate authentication method. It is going to surpass fingerprint authentication in future for a number of applications – especially in self-service mode.

# V. Criticism relating to biometrics

5.1 One of the most common criticism of UID program revolves around the accuracy and usability of biometrics. The criticism broadly fall in two broad categories.

## Inaccuracy in de-duplication:

5.2 The first category of criticism ran as follows: The biometric de-duplication which is used to ensure uniqueness is not reliable. It is untested, in-accurate and may not work in Indian situations as the quality of finger-print biometrics is often-times bad, especially for those poor people who may need this ID most. It may also not work at such scale (1.2 billion) and if it does not work, the entire investment (of thousands of crores of public money) will be wasted. In support of this, the critics often quote the reasoning given in the biometrics committee report of the UIDAI quoted above. [Para 2.2].

5.3 The critics argued that when the UIDAI’s own Biometrics Committee had so many doubts about the technology, its accuracy and its applicability in Indian conditions, how can UIDAI justify going ahead with the project. They also argued that if nobody in the world had done any project of this size, why should India go ahead with it?

5.4 The range of critics is also quite large. They vary from social scientists who quote some absurd figures of 15% inaccuracy to some well-informed people with scientific approach who say that even 5% inaccuracy should be unacceptable. Then there are mathematicians who argue that the exercise of de-duplication is just not feasible.

Dr. R Ramakumar, a Professor in the School of Development Studies at Tata Institute of Social Sciences (TISS) in one of his papers entitled ‘The Unique ID project in India: A Skeptical Note’[[3]](#endnote-4) has questioned various aspects of UID Project. One of his major criticisms relate to use of and dependence on biometrics technology in UID project. Dr. Ramakumar also gave evidence before the Standing Committee on Finance (Standing Committee on Finance, December, 2011), the Parliamentary Committee which had examined the UID Bill. Quoting from the report:

“ In this regard, Dr. R. Ramakumar, Expert, in his post-evidence reply has, among other things, added as follows:-

―…..it has been proven again and again that in the Indian environment, the failure to enroll with fingerprints is as high as 15% due to the prevalence of a huge population dependent on manual labour. These are essentially the poor and marginalised sections of the society. So, while the poor do indeed need identity proofs, aadhaar is not the right way to do that….

12. The Planning Ministry in their written reply have stated, among other things, that :

― While there may be a number of factors contributing to the failure to enroll (like geography, age groups, occupation etc.) and the figures quoted…… may not hold good in all situations, failure to enroll is a reality…. For enrolment purpose, UIDAI has already built in processes to handle biometric exceptions.”

5.5 In another article titled " India's ID card scheme – drowning in a sea of false positives"[[4]](#endnote-5) , published in March 2011, the Author (David Moss) argued that the de-duplication was impossible for such a large population. There will be such a large number of false positives generated that it will be humanly impossible to make a determinations relating to the false positives! This article was based on the report of UIDAI which was published after the Proof of Concept of Enrolment process published in December 2010 (UIDAI, December, 2010). Interestingly Dr. Moss had used elementary mathematics to prove his point. However, it was pointed out that his mathematics had some elementary flaws and his concern that we will be drowned in a sea of false positives was, fortunately, unfounded.

5.6 There were many other articles which essentially argued that what UIDAI was attempting to do using biometrics was something impossible. The allegation was that UIDAI was pushing ahead with the project despite overwhelming evidence, both experimental and mathematical, to support the non-feasibility and impossibility of the task.

## VI. Inaccuracy and feasibility of Authentication:

6.1 The second criticism relates to online authentication of IDs – which is going to help delivery of large number of services – from pensions to LPG cylinders to mobile phone connections. There are a large number of applications which are planned to leverage authentication services of the UIDAI. In order to fully appreciate the apprehensions and criticism, we have to understand two simple terms of biometrics: FAR (False Acceptance Rate) and FRR (False Reject Rate). False Acceptance refers to a situation where a person (X) is falsely accepted as another person (Y) by the system. Its implication is that X will be able to impersonate Y and draw the benefits which legitimately belong to Y. X will be able to operate Y’s bank account, for example. The False Rejects, on the other hand, refers to a situation where X will not be able to be recognized as X by the system. In other words, X will not be able to operate his own bank account (signatures differ, giving today’s analogy). While FA will result in fraud, FR will result in denial of service to real beneficiary.

6.2 Let us examine each of these criticisms and apprehensions on the basis of hard data. Yes, it is a fact that when the project was started, UIDAI had no data to prove that biometrics will be able to bring about desired accuracy or to disprove other contentions relating to large percentage of failure to enroll, inaccuracies in authentication etc. While the biometrics Committee had evaluated the existing studies on sample biometric data relating largely to Europe, it did not have any comparable data relating to parameters like failure to enroll and de-duplication accuracy. Obviously there was no data relating to authentication as no country in the world is doing large scale biometric authentication. Even when there are such facilities, say at some airports in Europe, it is a closed system and not something which is large scale and open-standard based. Hence all the inferences drawn by the biometrics committee were based on extrapolation of existing data. One was not sure whether any system will be able to function and produce results when the data size became very large.

6.3 The question was: should UIDAI go ahead and do the project on the basis of ‘untested' technology at this scale? The answer at that point of time was : either you go ahead and do it or wait for somebody else to walk the path and then do it. Except China, no other country in the world has population similar to us. Hence it is most unlikely that some other country will do it at similar scale and we will have the benefit of their experience. Hence it is similar to a Moon shot. Nobody has done it before and yet you do it because nobody will ever do it before you.

# VII Reducing the risks

7.1 However, it is not as if the project was started on the basis of pure conjuncture. UIDAI first did the proof of concept of biometric capture, both of finger-prints and iris, and then analyzed the quality of capture etc. The results convinced that this could be done at a scale and the approach was right in principle. However, it should be realized that de-duplication algorithms have never been tested and scaled up to such numbers which will eventually happen in this case. Speed of algorithms normally depend on the input size (in this case gallery size of persons who have already enrolled), and the execution time can become very large as the gallery size increases. As there were no de-duplication algorithms in the open source domain, it was not known as to how the algorithms will behave at large input sizes. It should be understood that the computation complexity is a multiple of gallery size and number of enrolments on any given day. As an example, if we have issued UIDs for 750 million people and we have to process 1 million per day, the average number of comparisons required will be 750\*106\*106\*12. This number is 9\*1015 which is 9000 trillion (or 9 Quadrillion)! (We are multiplying by 12 as there are 12 biometrics per person – 10 finger prints and two iris).

7.2 To reduce the risk in the area of biometric de-duplication, UIDAI came up with a very novel solution. They decided to engage as many as three biometric service providers (BSPs). We are not aware of any such arrangement anywhere in the world. One the most prominent biometric capture programs, US-VISIT has engaged Accenture as their BSP. Other major programs also have only one BSP.

7.3 It turns out that this was one of the most innovative decisions relating to technology deployment. Broad features of this arrangement were as follows.

1. Each BSP will be given access to biometrics in the enrolment packet and they will extract features from the images and add to their gallery. In other words, each BSP has the same gallery. Of course the storage of the features will be in their proprietary format. This stage is described as ‘insert’.
2. Then the incoming packets will be distributed among the BSPs in some ratio (to be explained below) and each will be asked to de-duplicate. The results will be then be passed to the UIDAI by the BSPs, relating to the packets which have been given to them for de-duplication.
3. The ratio among the three will be determined through a formula having Accuracy and Speed as two input parameters with appropriate weightages.
4. There are threshold values of accuracy which, if breached, will result in suspension of the BSP. The concerned BSP will have to improve his algorithm to improve accuracy, demonstrate it to the UIDAI and then join the club again.
5. If a BSP is not able to perform with the required speed, he may also be suspended and asked to modify the algorithm to improve the speed.
6. Interestingly, having multiple BSPs solved the problem relating to measurement of accuracy also. What was done is that a certain percentage of biometrics are distributed to all the three BSPs None of the BSP knows as to which are the common biometrics. Each BSP carries out de-duplication on these common biometrics and comes up with results – unique or duplicate. Then the results from all the three are compared and we are able to determine as to who committed errors. This is the best way to measure the accuracy of the algorithms. It should also be remembered that it is a multi-modal biometric scenario.
7. Having multiple BSPs also reduced the implementation risk arising out of failure of a single BSP and the program coming to halt. The probability that all three will fail (here the failure arises out of not being able to deal with large galleries.) became pretty small. Then they are competing with each other to improve their speed and accuracy. Lastly, there is no cost disadvantage to UIDAI as each agency is being paid on the basis of successful de-dup rather than on the basis of ‘inserts’. Hence the money outgo from UIDAI is the same, except probably on those sample packets which are periodically being given to all three BSPs, their percentage being relatively small.
8. We should also add here that UIDAI got the cheapest rate of de-dup anywhere in the world. This was, of course, due to the fact that all the players wanted a piece of this pie as this will help them in testing their technology and algorithms at such scales and they will be able to get future orders on the strength of this experience.

# VIII. Accuracy of de-duplication

8.1 Now that UIDAI has issued more than 900 million Aadhaar numbers, it is a legitimate question to ask whether apprehensions relating to inaccuracy, failure to capture and scalability have turned out to be true or were just apprehensions. UIDAI had done a detailed analysis of accuracy and failure to capture at the time when their data size was 84 million. Following is a quote from the report entitled: “Role of Biometric Technology in Aadhaar Enrolment”, published on the basis of data as on 31st December 2011.

**“ *Biometric Accuracy***

*As of December 31st 2011, the UIDAI has true and tested statistics computed from real operational large-scale UIDAI system with the resident enrolment database size of 8.4 crores (84 million). It is unnecessary and inaccurate to attempt to infer UIDAI system performance from other systems which are ten to thousand times smaller. Specifically,*

*•* ***Failure to Enrol (FTE) Rate:*** *Zero. As a policy, every unique resident, regardless of their biometrics can be enrolled and issued Aadhaar number.*

*•* ***Biometric Failure to Enrol Rate:*** *0.14%. This implies that 99.86% of the population can be uniquely identified by the biometric system. The exceptions (0.14%) however are de-duplicated using demographic data and checked manually for fraud. The legitimate cases among these are issued Aadhaar number.*

*•* ***False Positive Identification Rate (FPIR):*** *0.057%. In practical terms, it means that at a run rate of 10 lakh enrolments a day, only about 570 cases need to be manually reviewed daily to ensure that no resident is erroneously denied an Aadhaar number. The UIDAI currently has a manual adjudication team that reviews and resolves these cases. After manual adjudication, there is a negligible number of legitimate residents who are wrongly denied an Aadhaar number*

*•* ***False Negative Identification Rate (FNIR):*** *0.035%. This implies that 99.965% of all duplicates submitted to the biometric de-duplication system are correctly caught by the system as duplicates. Given that currently approximately 0.5% of enrolments are duplicate submissions, only a few thousand duplicate Aadhaars would possibly be issued when the entire country of 1.2 billion is enrolled.*

*The analysis resulting from such a large data set (8.4 crore records) is empirically repeatable and statistically accurate. There is no longer a need to rely on small sample size tests or hearsay from other projects. The UIDAI is now capable of measuring the accuracy, performance and scalability of the actual production system, which is already among the largest in the world. The results lay to rest unfounded claims that the underlying technology is untested, unreliable and based on unproven assumptions.*

*Based on the analysis, it can be stated with confidence that UIDAI enrolment system has proven to be reliable, accurate and scalable to meet the nation’s need of providing unique Aadhaar numbers to the entire population. It is now safe to conclude that the system will be able to scale to handle the entire population.”*

8.2 Thus the apprehensions have been set to rest. Subsequent experience has also demonstrated that desired levels of accuracy in de-duplication have been able to be maintained.

# IX. Feasibility of Authentication

9.1 The other issue relating to biometrics is the accuracy and inclusiveness of authentication. A major apprehension expressed related to the fact that a large part of population, especially manual labourers whose finger-print impressions have worn out due to hard manual labour will not be able to authenticate. Consequently they will be denied the service to which they are legitimately entitled. Civil society representatives were very vocal on this issue.

9.2 To investigate the extent of failure to authenticate and authentication accuracy, a PoC was undertaken during the period January 2011 to January 2012 in five States/UTs of India (Karnataka, Delhi, HP, Maharashtra and Jharkhand) covering more than 50,000 Aadhaar holders (Unique Identification Authority of India (UIDAI), September, 2012). In this PoC, the impact of a number of factors which have bearing on authentication accuracy were studied. It was largely for finger-print authentication only.

9.3 Key findings of the study are as below:

*“The PoC conducted in the rural setting representing typical demography of the population establishes that it is technically possible to use fingerprint to authenticate a resident in 98.13% of the population. The accuracy of 96.5% can be achieved using one best finger and 99.3% can be achieved using two fingers. Further improvement is possible if the device specifications are tightened to include only the best devices and certain mechanical guide is used to aid proper placement of the finger. It was also be demonstrated through benchmarking that the CIDR infrastructure is able to sustain one million authentication per hour.*

*Accuracy could be further improved by using additional factors such as one-time-password (OTP), demographical data or second modality such as iris. It is recommended that a separate study in the line of the current study should be conducted for additional factors.”*

9.4 As was mentioned in this study, a separate study was conducted for iris authentication. This study was conducted in May and July 2012 covering about 18,000 online transactions and about 40,000 transactions in off-line mode.

9.5 This study also established that iris authentication is viable in Indian context. Indeed, the results of Iris authentication were better than the finger print authentication. As much as 95.89% of residents were able to authenticate in the first attempt with a single eye camera. This percentage was better with a dual eye camera and went up to as much as 99.29%. This percentage further improved in multiple attempts to 99.21% in single eye camera and 99.40% in dual eye camera. Failure to authenticate in case of iris authentication (FRR+FTC) was 0.79% and 0.60% in single and dual eye case.

9.6 Thus the feasibility of authentication was established beyond any reasonable doubt through these PoCs. Of course today we know that these authentications are being used in a number of applications like PDS, Banking, Mobile SIM allocations, proof of presence (attendance[[5]](#endnote-6), Jeevan Pramaan[[6]](#endnote-7) etc.). The scalability of authentication and their easy roll-out through inexpensive devices is becoming very popular. This is going to be a game changer for India especially in the context of Digital India program of the Government. As of now, UIDAI is doing about 2 million authentication transactions per day.

# X. Conclusion

10.1 As has been described in the preceding paragraphs, all the concerns relating to feasibility, accuracy, inclusion, speed, scalability, field deployment and cost relating to biometrics stand addressed. A combination of policies relating to technology, analysis and proof of concept (PoC) studies have helped UIDAI in achieving this goal. There are very few projects which have been so controversial on so many fronts and still successful. From a technology stand-point, India has done what no other country has done before. In fact, now other countries are trying to learn from India as the project has laid out an identity infrastructure which facilitates the authentication of identities in a digital world in a seamless manner with the applications. Many countries are still grappling with this issue and finding solutions in a round-about manner. Today it is possible to digitally sign documents online using Aadhaar authentication. A number of projects like eSign[[7]](#endnote-8) and Digital Locker[[8]](#endnote-9), which are indeed transformational as they will enable end-to-end paperless and electronic processes have been started. All these projects ride on Aadhaar identity platform. Linking mobile numbers with Aadhaar and using them to conduct transactions in a fully safe and secure manner is something only India can do[[9]](#endnote-10). We think that many countries will be creating similar platforms based on biometrics and India is going to become an example for them to emulate.

# Bibliography:

(Ensuring Uniqueness: Collecting iris biometrics for Unique ID Mission, 2010)

(Unique Identification Authority of India (UIDAI), March , 2012)

Dr David Moss, D. B. (March, 2011). India's ID Card Scheme - drowning in a sea of false positives. *http://dematerialisedid.com/BCSL/Drown.html* .

(2010). *Ensuring Uniqueness: Collecting iris biometrics for Unique ID Mission.* New Delhi: UIDAI.

Ramakumar, D. R. (2010). The Unique ID Project in India: a skeptical note. *ICEB'10 Proceedings of the Third international conference on Ethics and Policy of Biometrics and International Data Sharing* (pp. Pages 154-168 ). Berlin, Heidelberg ©2010 : Springer-Verlag .

Standing Committee on Finance. (December, 2011). *Report on Natiional Identification Authority of India Bill.* New Delhi: Lok Sabha Secretariat.

UIDAI. (2009). *Biometrics Design Standards for UID Applications.* New Delhi: UIDAI.

UIDAI. (December, 2010). *Proof of concept of Aadhaar Enrolments.* New Dehi: UIDAI.

Unique Identification Authority of India (UIDAI). (March , 2012). *Role of Biometric Technology in Aadhaar Authentication : Authentication Accuracy Report.* New Delhi: Unique Identification Authority of India (UIDAI).

Unique Identification Authority of India (UIDAI). (September, 2012). *Role of Biometric Technology in Aadhaar Authentication: IRIS Authentication Accuracy – PoC Report.* New Delhi: UIDAI.

Unique Identification Authority of India (UIDAI). (January, 2012). *Role of Biometric Technology in Aadhaar Enrollment.* New Delhi: Unique Identification Authority of India (UIDAI).

Supplementary Material

UIDAI's response to the article of Dr. David Moss titled India's ID card scheme – drowning in a sea of false positives

The author confuses FPIR (False Positive Identification Rate) that is used for 1: N identification with FMR (False Match Rate) used for 1:1 verification. FPIR and FNIR calculations already take into account the size of the gallery in a search. The requirement is 0.0025% false positives for every 1 to N search, NOT for every 1 to 1 comparison.

What is the total number of false positives at an FPIR of 0.0025% ? The number of searches (not comparisons) will be roughly 1.2B since every person will require a full gallery search to ensure uniqueness. The expected number of false positives will be 1.2 billion times 0.0025% or 30,000 false positives.

FNIR does not change much with change in gallery size while FPIR grows linearly with gallery size. The operating point of a biometric system is specified in terms of a tuning the system to keep the FPIR fixed by trading-off with FNIR. UID type systems which capture 10 fingerprints & 2 Irises have the flexibility to make such tradeoffs to keep the FPIR constant over 1.2billion gallery size.

At an FPIR rate of 0.0025% and a daily enrollment rate of 1M people, only 25 false positives need to be manually adjudicated each day. Hence we will not drown in a sea of false positives.

1. Ensuring Uniqueness: Collecting iris biometrics for the Unique ID Mission - UIDAI, 2010 [↑](#endnote-ref-2)
2. Ensuring Uniqueness: Collecting iris biometrics for the Unique ID Mission - UIDAI, 2010 [↑](#endnote-ref-3)
3. Ramakumar, D. R. (2010). The Unique ID Project in India: a skeptical note. *ICEB'10 Proceedings of the Third international conference on Ethics and Policy of Biometrics and International Data Sharing* (pp. Pages 154-168 ). Berlin, Heidelberg ©2010 : Springer-Verlag [↑](#endnote-ref-4)
4. Dr David Moss, D. B. (March, 2011). India's ID Card Scheme - drowning in a sea of false positives. *http://dematerialisedid.com/BCSL/Drown.html* . [↑](#endnote-ref-5)
5. http://attendance.gov.in/ [↑](#endnote-ref-6)
6. https://jeevanpramaan.gov.in/ [↑](#endnote-ref-7)
7. http://cca.gov.in/cca/index.php?q=eSign.html [↑](#endnote-ref-8)
8. https://digitallocker.gov.in/ [↑](#endnote-ref-9)
9. http://cdn.mygov.nic.in/bundles/frontendgeneral/pdf/white-paper-mobile-as-digital-identity-v0-2.pdf [↑](#endnote-ref-10)