Is your Privacy Safe with Aadhaar?: An Open Discussion

Amit Kumar Tyagi,
School of Computer Science & Engineering,
Lingayas Vidyapeeth,
Faridabad- 121002, Haryana, India
amitkrtyagi025@gmail.com

G.Rekha
Department of Computer Science and Engineering,
K L University,
Hyderabad- 500075, India
gillala.rekha@klh.edu.in

N. Sreenath
Department of Computer Science and Engineering,
Pondicherry Engineering College,
Puducherry, 605014, India.
nsreenath@pec.edu

Abstract- The Aadhaar project is the world's largest national identity project, launched by Government of India in 2009, which seeks to collect biometric and demographic data of residents and store this information in a centralised database. To date, more than approximate 1.1 billion users have enrolled for Aadhaar/ in this system, and the government has spent at least 1000 million USD on this project. Basically, this project is completely free for its citizens/ people. No agency/ centre require money for issuing Aadhaar (as first time). But recently/ in the last five years, several issues like privacy and security have emerged with this project. This work examines these issues from a Computer Science perspective and provides several valuable suggestions (needed to be done/ overcome in near future). Also, this work investigates the privacy and security issues of Aadhaar from a technology point of view. Our analysis suggests that privacy protection in Aadhaar will require a) an independent third party that can play the role of an online auditor, b) study of several modern tools and techniques from computer science, and c) strong legal and policy frameworks that can address the specifics of authentication and identification in a modern digital setting. Aadhaar is premised on the infallibility and security of an individual's biometric data, i.e., her fingerprints and iris scans. However, this is only a myth because section 28(5) of the Aadhaar Act refuses an individual access to the biometric data that act as core of his/ her unique ID. In summary**,** this paper describes a detail discussion and reaches on a result that how Aadhaar can be good or bad for people of India.

Keywords- Privacy, Computer Science, India, Security, Cryptography, Authentication, Identification.

I. INTRODUCTION

Aadhaar was the one of the main proposals of the Kargil Review Committee (KRC) [1], which was built up to audit the condition of national security in the wake of the Kargil intrusions. It was the solution of/ issue of "Multi-purpose National Identity" cards to villagers living in struggle zones. It was along these lines chose to stretch out this plan to all natives, and that turned into the beginning purpose of Aadhaar [2]. The primary rationale in this development was to guarantee the welfare of citizens by generally facilitating their availability to different government plans/schemes via providing *a* single identification document. This prompted the foundation of a devoted establishment for revealing the Aadhaar work called the Unique Identification Authority of India (UIDAI) on 28 January 2009.

Following quite a while of discussions and considerations, the Aadhaar Act at last became effective on 11 March 2016. As the Aadhaar venture gained ground, at the same time the encompassing discussions saw a structural move, i.e., from continuous grumblings about the showcase of wrong information or absence of clearness over its centrality to graver issues of digital security, fraud or information breaks. Regardless of whether the administration is all around prepared to deal with something like the Aadhaar database still remains a piece of the current talk. Subsequently, figure 1 discusses about the working of Aadhaar in brief. In that, the UIDAI distributes an exceptional identifier (Aadhaar Number) to every citizen and stores their biometric and demographic information in a Central Identities Data Repository (CIDR). Aadhaar or Unique Identification Number (UID) (Nationally) is a 12-digit number that serves as a unique identifier for Indian citizens [11]. Aadhaar's database has the records of over 1.12 billion registered users and is rapidly becoming the government's base for public welfare and citizen services scheme [9, 10].

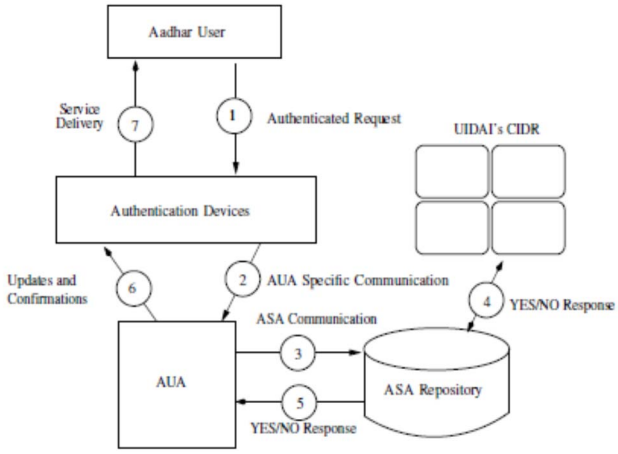

Figure 1: The Aadhaar Authentication Framework [3, 4]

Aadhaar verification process approves an individual identity with a 'yes' or 'no', by utilizing one of the six demographic fields (name, date of birth, sex, address, mobile or email) alongside with either biometrics or One Time Password (OTP). This process is designed in such a way that "neither the purpose of the transaction nor any other context is known to the Aadhaar system in order to ensure the safety of any transaction". Likewise, the UIDAI document claims that "Each enrolment information is 'always' stored on disk in PKI (Public Key Infrastructure) encrypted form and is never decrypted/ modified by any illegal/ insider/ outsider attacker during making a transition. Hence, this feature makes Aadhaar database completely inaccessible to any system/ unknown persons (Note that this assurance is given by UIDAI always to people and government but what is truth?

no one knows, and how it is possible for a stranger to transfer an amount in account of an Aadhaar holder?).

As indicated above, Aadhaar is generated completely free for its people (only for first/creation time). No agency/centre requires money for issuing Aadhaar. But no one wants to share his/ her secret personal information with organisation in free of cost. These systems (Aadhaar enrolment centre, which collect Aadhaar data) can be breached by unauthorized users/ can sell user's data to other organisations. Which is an essential issue to solve/ overcome? Further, some other perspectives on Aadhaar can be discussed as:

A. Benefits with Aadhaar

There are several benefits using of (with) Aadhaar for people/ its citizens given by government [12]. Some of the benefits (of using Aadhaar) are: Aadhaar based Direct Benefit Transfer (for receiving Subsidy like LPG, Ration, etc.) for its citizens, Jan Dhan Yojana (opening of bank account at zero balance for poor people), Issuing of Passport in few days (via reducing verification process), Digital Locker (a platform to keep records online securely), Voter Card Linking (reducing fraud voters), Monthly Pension (identification of genuine and correct people eligible for pension like disable, old-age, etc.,) Provident Fund, Opening new bank account (for all people belonging to urban and rural areas), Digital Life Certificate, Transfer of scholarship/ fellowship amount to right candidate, Securities and Exchange Board of India (SEBI), etc. (see figure 2).

Figure 2: Use of Aadhaar card [11]

Additionally, these advantages of Aadhaar number can't be overlooked, now onwards Aadhaar has been made an essential card (among all valuable cards (like Permanent Account Number (PAN), Voter id, etc.)) for doing everyday work/ exercises. Also it is linking with several other schemes/ services for reducing fraud. For example, issuing a new mobile number/ linking of Mobile number (now verdict given by Honourable Supreme court not to use, but mandatory for PAN linking, i.e., for tax purpose), issuing/ linking of Driving license, for investments, for existing bank account holders, for making a financial transactions above Rs. 50, 000, and so on.

Hence, all above benefits show that why Aadhaar (12-digit unique number) is a must thing or card for every Indians/ for their everyday life/ to get services from organisations.

B. Perspectives on Aadhaar: Pros and Cons

Basically, Aadhaar act used to "create a method for identification of citizens, to provide services, subsidies and other benefits to people of the country" [11, 13]. In that, leaking of information/ privacy of citizens (during taking benefits using Aadhaar from several welfare schemes) has been raised. Linking/ using Aadhaar with several schemes create a digital platform. Note that any digitisation (at centre) require unique id (e.g., like Driving Licence, Passport, etc.), whereas social welfare schemes (at state level), require local unique ids (like ration or job card). Standardising the digital records with certain level of security, and linking the other local ids like Driving licence, PAN card, etc. with this unique national number (provided by Aadhaar) is a hectic process, i.e., it alike to virtually collating the different/ other digital records/ tables into one place. Though these (all) digital records may still be geographically distributed, i.e., Later, these records can be used in real-time access of any data/ record. In general terms, *Aadhaar ids* can be used for authorising (preventing attack), auditing (reducing fraud), and monitoring (tracking an illegal/ corrupt users), etc. purposes by central and state governments/ organisations. Thus, interlinking Aadhaar numbers provide a single index table for all services. On the other hand, the *Aadhaar* can be used to create local ids (for state governments) with interlinking of records with Aadhaar (called digitisation of records). For example, now a days "Aadhaar is used to linking of local ids in several areas like census, education, healthcare and immunisation records, birth and death records, land records, property registration, income tax, banking, loans and defaults, police verification and law enforcement, disaster management, security and intelligence and such others". Thus, Aadhaar does not provide only enable efficient design, delivery services or monitoring, auditing, etc. services, but also provides huge data (after interlinking with several ids, can be called as 'Big Data') which is essential for performing modern data analytics techniques (for finding large scale correlations/ predicting necessity or used subsidies via area wise/ gender wise, correlate education levels, family incomes and nutrition across the entire population; or disease spread with income and education, etc.) [15]. Also, this data (huge/ big data) can be used in designing several social policies/ strategies or early detection and warning systems [14]. This data will be too useful for governments for tracking subsidies/ money provided to its citizens. Apart above benefits, Aadhaar is used to "provide econometric analysis, epidemiological studies, automatic discovery of new topics and causal relationships across different domain of the economy" [3].

With extending the use of Aadhaar (from identification/ authentication a system for social welfare schemes to generating huge data for predicting or providing warning), it also attracts several criticisms like loss of privacy/ information or disruptions and exclusions in social welfare schemes, civil liberties due to careless deployment and uncertainties in biometric matching/ storing information in Aadhaar database [15]. We believe that all the above issues require careful analysis and rigorous evaluation with respect to technological, legal glitches for making this national identity scheme successful.

Hence, the organization of this paper is organized as: Section 2 reviews related work with respect to Aadhaar. Further, several issues with Aadhaar have been discussed in Section 3. Then, in Section 4, we investigate several challenges with respect to Aadhaar and its database. Section 5 presents an open discussion for all researchers/ communities and provides a future perspective or positive perspective with respect to Aadhaar. In last, this work is concluded in brief in section 6.

II. RELATED WORK

According to Calcutta High Court, Aadhaar is "proof of identity", not a "proof of address/ citizenship" (see figure 2). Any person who is living since six month (at least) in India can apply for issuing this national unique number. As discussed in introduction (or section 1), leaking of privacy/ information related to the Aadhaar project have become a hot topic now days. Several civil societies, social activists and opposition have expressed their concerns several times. Even opposition and these activists have suggested several recommendations to improve weak privacy provisions in the current Aadhaar project and bill [7]. This issue (leaking of user's information) also increasing everyday (i.e., become ambiguous) because of double stands of the government and UIDAI. Moreover this, to protect government's stand, the Attorney General of India (AGI) told to a bench in the Supreme Court (SC), that Indian citizens have no constitutional right to privacy [6]. The finance minister, while getting the Aadhaar bill passed as a money bill, announced that "the government pre-supposes privacy as a fundamental right" and claimed that the bill has tightened privacy provisions when compared to what was there in the previous version [5]. Recently, Supreme Court (SC) gave a verdict that "Right to Privacy is fundamental right and it is intrinsic to right to life (i.e., needs to be protected)" [18].

However, neither the government nor the UIDAI makes it clear arguments about privacy concerns that are being leaked or need to be addressed. The UIDAI describe and share information like "not to share" your private (personal) information with strangers/ unknown users. Also, UIDAI always maintain security of Aadhaar database with different mechanisms (with upgraded technologies). Aadhaar issuing authority describe the security measures time to time, but does not provide an analysis of the measures with respect to perceived threat levels and potential privacy breaches. It creates doubts against working structure of UIDAI and governments. By the way, government has taken several reforms to build trust in people against/ solving leaking of information issue, for example, using of Virtual Identification (VID, a16-digit number) in place of Aadhaar in various welfare schemes, i.e., Organizations/ Local governments need to use VID from June 1, 2018 for preserving the privacy of respective users/ customers. But now, it creates confusion among customers (people who are properly aware), local organizations and governments to share Aadhaar number or Virtual ID. Also recently, Honourable Supreme Court ordered that there is no need of using Aadhaar for KYC purpose like with Bank or Mobile Organisation (issuing a new connection) but make Aadhaar as compulsory for interlinking with PAN Card (whereas PAN number is compulsory always in Bank for fraud detection/ preventing fraud). In result, this put an overall confusion (among users/ people) about the impact on privacy engendered by the Aadhaar project. In summary, today's Aadhaar has open doors to mass surveillance (of citizens) for governments, unbounded criticisms to oppositions/ activists. However, whether breach of privacy is inevitable, and whether there may exist technological and legal provisions which can make Aadhaar more safely. This is one important question that needs to be adequately addressed today. We note that some crucial gap in the identification and authentication processes of Aadhaar have been pointed out in [4], which also makes several important suggestions including implementation of recommendations of Shah [8] and Sinha [13] committees. Apart these, thorough analyses of the possible ways in which privacy can be breached and possible countermeasures both from technological and legal perspectives are remain missing. In this work, with respect to leaking of user's privacy, we endeavour to fill in some of this gap from a computer technology point of view.

Hence, this section discusses pros and cons with Aadhaar (in general). Some of the Privacy and Security concerns with Aadhaar are discussed in next section.

III. ISSUES WITH AADHAAR (IN CURRENT)

As discussed in section 1 and 2, privacy or leaking of information (due to not having proper security in current Aadhaar database) is a major issue. Further, we examine following main concerns pertaining to privacy and security in Aadhaar:

a. Identification and authorization of individuals without revealing their unique (nationally) Aadhaar number/ demographic and biometric data.
b. Mass surveillance, tracking or profiling of people with legal provisions (i.e., with the permission of government/ UIDAI/ centralised database), and protection from external hacks or insider attacker (leaks), etc.
c. Others: In this, we need solution for some crucial questions (for ensuring safety of Aadhaar) like:
    1. Is there any way to protect user data or his/ her demographic location/ information via manually or with updated software/ any mechanism by UIDAI/ by government (i.e., it prevents from unauthorised surveillance)?
    2. Can it possible to ensure that all transactions, investigations and analytics be carried out in a safe way only through audited, pre-approved and tamper proof computer programs? Additionally, can it be ensured that the programs are true to legal and policy frameworks?
    3. Is there any way or strategy for recovering or protected already reveal data?

In summary, this work reaches to conclusions that above questions are essential and need to be solved (for privacy preservation in computerised databases). Hence, complete privacy protection can be achieved with complete isolation from the world. Also privacy of information can be preserved if that information is used only for that purpose for which it was collected or stored (i.e., cannot be used for any other purpose).

A. How would an Attacker attack on Aadhaar databases?

Recently in July 2018, one hacker deposits Rs. 1 in TRAI chief's account and share this incident/ accounts details online (for proof). Also, this French ethical hacker challenges Respected Prime Minister "Narendra Modi" to share his Aadhaar details online. So now big question arise that "How ethical hackers are getting further information related to Aadhaar number/ by an Aadhaar number"? Is it easily accessible for an attacker to get further information (with respect to the Aadhaar) about a user? We learn this problem via Aadhaar ecosystem which consist an infrastructure layer, a data layer and an application layer. For Aadhaar ecosystem, Aadhaar enrolment centre plays an important role (in collecting user's biometric/ personal information). And data collected in Aadhaar enrolment centre kept (with implementing strongly encryption schemes) between the base infrastructure and end user application. For future work/ purpose, this information can be used by an Authenticating User Agency (AUA, like NPCI), or a sub-Authenticating User Agency (ICICI Bank) or a "Terminal Device" (a Xiaomi or Asus or Micromax mobile phone etc.). Similarly, an application layer is managed by non-UIDAI entities (PayTM, Jio, etc.). While Aadhaar regulations require all contracting parties to "put appropriate network security in place to ensure their systems are protected from attack", it is impossible to ensure systems-wide compliance.

India's digital supply chains are based abroad, effectively resulting in a situation where the security standards of Smartphone X differ widely from Smartphone Y. Note that it is worth noting that four of the top five smartphone models by market share in India are Chinese. If an adversary assumes control of a mobile phone, the additional layer of authentication provided by a one-time password to effect Aadhaar-based transactions would be rendered useless. There is also no national encryption policy to regulate data security at the application layer. These applications rely on end-to-end protocols that encrypt financial data but not the user's information (such as the name, telephone number, number of successful/ failed login attempts, details of purchases, etc.). The more these welfare or service applications link with together with Aadhaar, it become easier for an attacker to map the behaviour of users (i.e., background or homogeneity attack). Later, this information can be used by an attacker for their financial purpose/ counter-intelligence/ extortion/ blackmail against a user (owner of information).

On the other hand, when the Aadhaar database is linked with a user's personal information, it becomes goldmine for outside attackers (critical for users) to exploit and disrupt digital networks of India. For example, if an operator (of nuclear power plant) need attendance of his/ her employees with biometric. Here, a breach of the UID database will render them vulnerable by exposing their daily activities to a malicious user/ attacker. Because, these biometric stored in nuclear plant database and biometric stored in Aadhaar database are same. In the future, Internet of Things (IoT) ecosystems will likely to be connected to Aadhaar databases, i.e., for example, to allow traffic monitoring systems to directly deduct a fine from the motorist's bank, her driving license/ plate could be linked to an Aadhaar number, which in turn connects to a bank account. The security of IoT systems leave much to be desired, and could potentially compromise Aadhaar databases as well. Hence to counter these strategic threats, India's policymakers/ government must urgently consider:

- Designing of a Unique Identification Databases as "critical infrastructure" including testing of all Aadhaar-enabled applications with respect to security (at server side).
- Proposing a novel encryption policy for Aadhaar-enabled applications. Also encouraging device-level encryption for mobile phones and laptop computers.
- Creating a Computer Emergency Response Team (CERT) to monitor or prevent attacks on Aadhaar (central) database.
- Need to work with the private sectors like the International Electronic and Electrical Engineers (IEEE) and the Internet Engineering Task Force (IETF) or Internet Society to create unique security standards/ platforms for this national identity scheme.
- Throwing an open challenge for all (after implementing above points, for checking strengths/ weaknesses of Aadhaar updated technology/ database) for building trust among people.

Hence, this section discusses several Privacy and Security concerns with Aadhaar and how an adversary attack on Aadhaar. Now next section will discuss several challenges in Aadhaar in detail.

IV. CHALLENGES IN AADHAAR

There are several problems with the Aadhaar UID card/ project, included as:

- Privacy concerns from Aadhaar leaks.
- The cost of the Aadhaar project.
- Coercion to register for Aadhaar-voluntary and mandatory.
- No legal basis for the UID project.
- False claims of preventing corruption.
- The new bailout plan for banks.
- Potential for misuse.
- Illegal immigration and terrorism.
- Unauthorized use of Aadhaar cards.
- Irrelevant storage of Aadhaar data: If some time, we need to delete dead people data/ verify some people data in UID, then it is really tough to know it will work or not/ which is data of alive and dead ones, i.e., it is a big problem with the Aadhaar data.

In summary, Aadhaar has gained popularity as "proof of identity" (e.g., many checkpoints like railways, airports or protected areas have started using Aadhaar card as a source of identity), not "proof of Address". But in general, Aadhaar is just a plain card and does not any specific security feature (contain only a QR (Quick Response) code, not a hologram), i.e., can be easily tampered (after downloaded from web or a coloured printout/ via Xerox). Another flaw in Aadhaar's security came to the limelight when a random blogger talked about how easy it is to access Aadhaar information with just a basic Google search. With the exponential growth in

cybercrime, this centralised database may provide valuable information to criminals. This might lead to either illegal tracking of individuals or identification without consent. Such records may also aid in providing data on the precise location, time and context of the services availed by that individual. Moreover, sensitive financial information of individuals and companies may also be exposed through breaches of the UID database or internal collusion. An example of data breaches was seen when UIDAI temporarily halted Aadhaar payments by Axis Bank, Suvidhaa Infoserve and eMudhra because of unauthorised authentication and impersonation through the illegal storing of Aadhaar biometrics. This infringement caught the UIDAI's attention after one individual conducted almost 397 biometric transactions between 14 July 2016 and 19 February 2017.

In a report by an investigative website, those associated with the Aadhaar project "agreed to make Aadhaar Cards for applicants without any proof of identification or address" for charges ranging from Rs. 500 to 2500. The website asserted that almost anyone, "be it Indian or an illegal immigrant can get an Aadhaar Card made without any proof of identity. More importantly, they get an Indian identity". Though there were several reported cases of such activities, one that acquired a lot of attention was reported last month when a UIDAI operator in Bhilwara's Mandal area tried to outwit the authorities by trying to get an Aadhaar card for slain terrorist Osama Bin Laden. However, the UIDAI got alerted due to the discrepancies in the personal data form and filed a complaint against the operator.

Hence, this section discusses several challenges of using Aadhaar or using several mobile services using Aadhaar enabled applications like Bank, LPG connection etc. Now next section will provide an open discussion to discuss about bad things and good things of using or not using Aadhaar with any organisation. Next section also provides a future perspective of Aadhaar to all people and future researchers who are working in this area.

V. OPEN DISCUSSION AND FUTURE PERSPECTIVE FOR (OF) AADHAAR

As discussed above in Budget 2017, Aadhaar was made mandatory for availing Permanent Account Number (PAN) cards and filing Income Tax Returns. Furthermore, the central government is standing firm on its statement that it would provide social welfare benefits only to those with UID numbers by June 30, 2017. Later, this date was extended many times for using different services. But, this interlinking of Aadhaar with various utility platforms (Banks, PANs, Birth Certificates, etc.) will facilitate interconnectedness by making a network of networks (which will produce huge data). It would pay more accountability and transparency, although at the same time such a massive scale of digitisation and data centralisation may attract several threats and hence are crucial to outline, for example, numerous instances of cyber-attacks like the one of the Bangladeshi bank account at the Federal Reserve Bank of New York allowed hackers to steal more than USD 81 million. Also the Wannacry Ransomware attack in 2017 that affected almost 150 countries, have given rise to concerns over cyber security. In this context, the question remains as to whether Aadhaar is a readymade factory for criminal minds? Note that biometric authentication can even be extracted/ faked externally (without/ with the help of a software/ hardware hack), for example, fingerprints can be copied (extracted) from a variety of surfaces (even from the surface of the scanner device itself)/ images and used to create a dummy finger [17]. Similarly, "Iris images can be skimmed from photographs and supplanted on an artificial eye-like object". Further, todays some of the issues are also presented with discussing that why we should curious about our privacy? Hence, we had issues with Aadhaar like;

- Need to update biometric information throughout lifetime.
- No access to biometric records in the database.
- Uncertainty of biometric authentication.
- Risk of identity theft.

Also, an important question from government, i.e., what about to that data which is already leaked? Is there any remedy/ solution or technology now to recover this leaked data? Apart this, time to time, the critics of Aadhaar have been arguing that India is at the risk of becoming a surveillance state (e.g., incident happened with TRAI's chief in July 2018, i.e., 1 Rupee was deposited in his account with the help of Aadhaar by an unknown French person), but government is try to listen anyone. In fact in an interview, Union Minister for Electronics and IT, Ravi Shankar Prasad told that most of the criticisms given by many people/ opposition are completely false and misplaced. Also he told "Aadhaar is completely safe, secure and robust" [2, 16]. Moreover this, even Nandan Nilekani (first chairman of UIDAI) discussed several benefits that Aadhaar offers, also addressed several security concerns in his book "Rebooting India". He also added that critics are needed to forget whereas ideas are to empower the citizens (of a county/ state). Note that from starting (launching of Aadhaar), Aadhaar has adopted "the principle of security by design" (i.e., no agency is able to track/ profile any individual [2]). Also in addition, the *Aadhaar Act* contains several guidelines for protection of information (from illegal leaking) with subsequent punishment and penalties [2, 7, and 11]. Adding to this view, one official spokesperson of the Axis Bank said "In case a person misuses biometrics, it is much easier to trace him using Aadhaar-Enabled Payments System (AEPS) as compared to other modes of digital transactions such as internet banking and card payments and that itself is the biggest security that Aadhaar can provide". To make safe this Aadhaar's critical data, UIDAI will upgrade all pre-existing biometric devices (including all software) to protect security of the transmitted data. Regarding this on 22 February 2017, UIDAI had proposed a draft to the "IT ministry" on "registration of biometric public devices to guarantee the safety of transactions and end-to-end traceability of the authentication process" [2]. UIDAI also ensure that all the updated devices (registered under it) will work from 1 June 2017. Also, to enhance privacy of users and protecting data from leaking, government introduced use of Virtual Identification (VID) in place of using Aadhaar number. The Government ordered all organizations to ask for VID not for Aadhaar under it) from people (from 1 June 2018). In summary, Aadhaar database on which platform it stands may infallible, robust and safe, *i.e.,* such issues are very essential and needed to be solved/ overcome.

Hence, this section discusses an open discussion for Aadhaar and put several future perspectives regarding Aadhaar. In summary, we reached to a conclusion that giving our fingerprint or sharing Aadhaar number for getting benefits from several welfare schemes does not reveal any kind of your personal information to other party/ organisation. As discussed above, we (all) are sharing our iris scan as face-lock and fingerprints to our smart devices whereas this information is collected by respective mobile company at their server. Remember always, a user is always responsible person for leaking his/ her identity or personal information to malicious users. Privacy preservation to users can be provided by proving higher un-linkability or higher anonymity to user's information or building trust among people. Now next section will conclude this work in brief.

VI. CONCLUSIONS

We have analysed the Aadhaar project from the point of views of privacy and security and have pointed out some technical weaknesses and possible remedies. Specifically, we have found that the Aadhaar number, which is a single national identifier that is supposed to work across application domains, makes individuals vulnerable to privacy breaches. A design alteration can however make it safe. The slightly different concepts of authentication and identity verification need to be well demarcated, and careful use case analysis is required to determine precisely what is required for each application. The legal framework must also make note of these. In current Aadhaar database the biggest threat to user's privacy comes from insider attackers/ insider leaks. The Current Aadhaar technology architecture has tried to overcome such attacks but still does not have designed a strong system which can protect such insider leaks. Moreover this, there might be several prevalent concerns over Aadhaar's data security, these do not outweigh the benefits it has to offer. Besides, one cannot entirely overlook the government's efforts to make Aadhaar more secure. Hence, some technical glitches or hardware improvements immediately need to be taken by UIDAI, to ensure enough security of Aadhaar. Today's Privacy is still remains a threat to people. For that, we need some concrete privacy laws by government for its citizens, i.e., to ensuring their security (including in surveillance of terrorists, or unknown people/ strangers to protect nations from insiders and outsider attack). Trust in people by government can be built by making Aadhaar as "fool-proof database" rather "work in progress". Thus, with appropriate measures on the security front, Aadhaar can be associated with numerous benefits like a cashless society, reduction of voter fraud and legitimate allocation of subsidies.

Hence, in present there are serious privacy concerns with Aadhaar but when it comes to share this 12-dgit number, then it does not create any problem at all. Sharing Aadhaar number is like as sharing your 10- digit mobile number with others. And if there is any loop-hole in Aadhaar database, then we believe that government will not take a risk to lose their citizen's privacy to unknown users and surely will provide a safe, secure Aadhaar database. For that as discussed above, the legal framework needs to be more specific and requires significant strengthening. For future research, we need comprehensive policy debates with covering all angles (with respect to essential uses of Aadhaar) with future scientists/ researchers (who are working in this area). All who are working in this area, invited to do their research work with effectiveness of biometric identification/ enhancing security of Aadhaar database.

ACKNOWLEDGEMENTS

We thank Government of India for providing this service, and research members who are working with Aadhaar for discussions, and suggestions on improving our manuscript. The first author specially thanks Prof. N. Sreenath for many helpful comments.

REFERENCES

[1] http://www.claws.in/images/journals_doc/1400824637Report%20of%20the%20Kargil%20Review%20Committee%20%20CJ%20SSummer%202009.pdf

[2] https://idsa.in/idsacomments/analysing-aadhaar-through-the-prism-of-national-security_kroy_220617

[3] Shweta Agrawal, Subhashis Banerjee and Subodh Sharma, Privacy and Security of Aadhaar: A Computer Science Perspective, Computer Science and Engineering, IIT Delhi, New Delhi 110016.

[4] UIDAI. 2016a. Authentication Overview. https://uidai:gov:in/auth:html. [Online; accessed 31-July-2016]. UIDAI. 2016b. Operating Model Overview. https://uidai:gov:in/authentication-2/operation-model:html. [Online; accessed 31-July-2016].

[5] Arun, Chinmayi. 2016. Privacy is a fundamental right. http://www:thehindu:com/opinion/lead/lead-article-onaadhaar-bill-by-chinmayi-arun-privacy-is-a-fundamentalright/article8366413:ece. [Online; posted 18-March-2016].

[6] Bhatia, Gautam. 2015. Sorry, Mr. Attorney-General, We Do Actually Have a Constitutional Right to Privacy. http://thewire:in/2015/07/28/sorry-mr-attorney-general-wedo-actually-have-a-constitutional-right-to-privacy-7398/. [Online; posted 28-July-2015].

[7] 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].

[8] The Planning Commission: Government of India. 2011 (December). Report of the Group of Experts on Privacy chaired by Justice A P Shah. http://planningcommission:nic:in/reports/genrep/rep privacy:pdf.

[9] http://aadhaar-articles.blogspot.com/2017/06/11545-analysing-aadhaar-through-prism.html

[10] https://yourstory.com/2016/07/aadhaar-global/

[11] https://uidai.gov.in/

[12] http://vikaspedia.in/e-governance/online-citizen-services/government-to-citizen-services-g2c/all-about-aadhaar/17-benefits-of-aadhaar-card

[13] http://www.prsindia.org/uploads/media/UID/uid%20report.pdf

[14] https://thewire.in/government/aadhar-privacy-analysis

[15] https://www.cgdev.org/files/1426371_file_Zelazny_India_Case_Study_FINAL.pdf

[16] https://economictimes.indiatimes.com/opinion/interviews/aadhaar-is-secure-concerns-misplaced-ravi-shankar-prasad-minister-for-electronics-and-it/articleshow/57999344.cms

[17] https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

[18] https://timesofindia.indiatimes.com/india/right-to-privacy-is-a-fundamental-right-supreme-court/articleshow/60203394.cms