Real Virtual IDentification (RVID): Providing a Virtual, Secure and Anonymous ID Service to Indian Users

Amit Kumar Tyagi, G. Rekha and N. Sreenath

Abstract Today using (sharing) Aadhaar with several welfare schemes/organisations, provide several essential benefits (to get government schemes benefits) to Indian citizens. But on the other hand, revealing/sharing their Aadhaar number with government and organisation raised several issues like security and revealing of personal information of the user. For that the government makes several enhancements from time to time like recently, government forces and give an option to use virtual IDs irrespective of using Aadhaar number. But virtual ID is not fixed and a user can generate multiple VIDs, it means it is a confusing process to user/people belonging to rural area. So to solve this issue of VID, this work describes a novel approach to provide a secure and anonymous (yet transparent and immutable) identification management system, which provide a Real Virtual ID (RVID) with respect to every user's Aadhaar number. This ID (16-digit ID, i.e. containing combination characters and letters) can be used to take several benefits or can be used irrespective of sharing Aadhaar number with organisations. A prototype shows that such ID management system is feasible, and solves the problem of duplication of data. It is also immune to many ID attacks like guessing attack, etc.

Keywords Aadhaar · Social/welfare schemes · Governments · Attack · Identification provider · Anonymous · Transparent · De-duplication

A. K. Tyagi (✉)
School of Computer Science & Engineering, Lingayas Vidyapeeth, Faridabad 121002, Haryana, India
e-mail: amitkrtyagi025@gmail.com

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

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

S. Choudhury et al. (eds.), *Intelligent Communication, Control and Devices*,
Advances in Intelligent Systems and Computing 989,
https://doi.org/10.1007/978-981-13-8618-3_56

1 Introduction

Till today, more than 100+ crore Aadhaar card has been issued by Government of India (GoI) to its citizens free of cost (for first time/creation time). Aadhaar has saved millions of rupees via reducing fraud in government offices or providing benefits/needs to respective users (based on this unique Aadhaar number). Every citizen (of India) contains this unique number as nationally, not globally. Basically, the actual UIDAI-Aadhaar number is 11 digits and not 12 digits. This doubt is clear here by 'the first 11 digits of the 12 digit Aadhaar number (just a random generated number) displayed on an Aadhaar card is the actual UID Number and the 12th digit is the checksum associated with Verhoeff Algorithm scheme' [1]. Note that in generation of an Aadhaar number, it does not contain any formula like other identities (like PAN, Passport, etc.), i.e. collection of pin code, demographic location or name, etc. Today in Aadhaar, Identification management, authentication, authorisations and service (IDs in short) are important research problems to work.

As discussed, Aadhaar does not contain any hologram, it just contains QR code which can be easily tempered. This tempered Aadhaar can be used in any illegal activities by any terrorists. Basically, Aadhaar was initially proposed and recommended by the Kargil Review Committee (KRC) to provide a unique identification number to its citizen or to every people. Today, Aadhaar is just used as 'proof of identity', not as a 'proof of address'. Moreover, several issues and challenges have been raised with Aadhaar time to time by several politicians and social activists. For that government has taken several steps to improve people privacy. The government has provided several new features like locking your biometrics online, sharing of Virtual Identification (VID) to its citizens with respect to Aadhaar, i.e. to protect their personal information from strangers. In general, the VID is a temporary, revocable 16-digit random number which can be generated multiple times by users and have no expiry time. The VID will allow the user to authenticate transactions and e-Know-Your-Customer (KYC) services instead of providing their 12-digit Aadhaar number to organisations [2]. Note that, a generated VID works with indexing/mapping process with the respective Aadhaar number. But generating these ID or using Internet technologies is challenging to most of citizens, i.e. to rural people.

In authorising or verifying exact/genuine user, user's registered mobile number and one-time password pair is still a very effective approach to do authentication and authorisation [2]. Unique Identification Authority of India (UIDAI) does not store any combination of password or usernames (of their citizens) in their database because most of the users use simple surname and password pair, which can be easily guessed by attackers. So, it (UIDAI) always works with One-Time Password (OTP) concept to verify the authenticity of user. In recent, providing of VID and sharing only this ID has been emerged as a revolution to citizens of India. But sharing of this VID does not provide enough security and privacy to its citizens. Hence in this work, we build a novel type of ID management and ID service, i.e. Real Virtual Identification (Real Virtual ID) with secure decentralised anonymity, unlinkability, transparency and immutability. Such IDs are necessary to provide a unique identification to peo-

ple with protecting their privacy. The proposed Real Virtual IDentification (RVID) is used for building a secure and anonymous yet transparent and immutable identification IDs via providing ID management to users/Aadhaar system, i.e. authentication, authorisation, storage, and ID service. In addition, the Real Virtual ID use one extra layer of security to reduce accessing time or updating time (to a database) of generated Virtual ID to users. Using this service, a user can be anonymous or can access all services without revealing his identity inside a crowd. The Real Virtual ID can also use characteristics to identify devices and products. Using Real Virtual ID, users can access several benefits, i.e. without revealing their Aadhaar number. Some of the benefits (of using Aadhaar) are: Aadhaar-based Direct Benefit Transfer (for receiving LPG Subsidy) for its citizens, Jan Dhan Yojana (opening of bank account at zero balance for poor people), Issuing of Passport in a few days (via reducing verification process), Digital Locker (a platform to keep your records online securely), Voter Card Linking (reducing fraud voters), Monthly Pension (identification of respective and correct people eligible for pension like disable, old-age, etc.) Provident Fund, Opening new bank account (for all people), Digital Life Certificate, Transfer of scholarship/fellowship amount to right candidate, SEBI, etc. [9]. Also, these benefits of Aadhaar number cannot be ignored now onwards as it has now been made mandatory for the most important day to day activities we do. For example, for tax/fund-related activities. Note that issuing a new mobile number/linking of mobile number now verdict given by Honourable Supreme Court (SC) is that organisations/government cannot ask for Aadhaar for linking (with their mobile number) from users, but it makes mandatory for PAN linking, i.e. for tax purpose, linking of driving license, for investments, for investments, for existing bank account holders, for making a financial transactions above Rs. 50,000 and so on.

Hence, all the above benefits show that why it is must for every Indian moving forward to use Aadhaar (12-digit unique number). The organisation of this paper is as follows: Sect. 2 discusses Virtual ID fundamentals, mandatory requirement for issuing Aadhaar and feature of virtual ID. Further, Sect. 3 discusses our purposed concept/approach with respect to Aadhaar, various issues with Aadhaar, etc., in detail. Then in Sect. 4, we provide an open discussion with respect to our proposed approach, i.e. Real Virtual IDentification. Finally, this work is concluded in brief in Sect. 5 with future possible enhancements.

2 Virtual ID Fundamentals

We provide the UIDAI virtual ID instead of our Aadhaar number to organisations/agencies and protect our basic Aadhaar details from outside world/malicious users/being accessed by someone else. Aadhaar Virtual ID is a 16-digit temporary code that can be used for Aadhaar authentications.

But a big question is raised here, i.e. why we need it (VID) here? In the past, there have been a number of cases (several times) where information from UIDAI/Aadhaar has been leaked. So, people became very much concerned about their information

stored with UIDAI. UIDAI has addressed the concerns of people and has come up with the virtual ID. Virtual ID (VID) is an alternative to Aadhaar number, provided by the Government of India to its citizens to protect their privacy/personal information against several attacks. When users/citizens use their respective virtual IDs instead of Aadhaar number, organisations/local agencies cannot collect the Aadhaar number of the respective user/applicant. All organisations/local agencies do authentication with virtual ID only. This virtual ID works based on mapping process, i.e. provides a relationship between VID and Aadhaar number [3]. VID provides anonymity to local agencies/organisations, i.e. preserve private information of user from the outside world. Using this VID, the Aadhaar details are not accessed by the outside world, i.e. VID is keeping the Aadhaar number and other details safe from being hacked. Aadhaar holders can generate VID either once or multiple times (expiration period is not fixed for VID) and use it (VID) to authenticate user for providing a service to respective user/Aadhaar holder. Once the authentication is complete, the user can regenerate his virtual ID (in future) so that the saved details with the organisations became useless. Hence, Fig. 1 shows connection among Central Identities Data Repository (CIDR), and Authentication User Agency (AUA) or KUA. Creating several VIDs put a burden to Aadhaar database and confusion with organisations, which is a serious issue. These Authentication User Agencies (AUAs) collect and generate Aadhaar number to its people/citizens after collecting their personal information and biometrics in their system [2]. Note that according to the Aadhaar Act 2016, a requesting entity means 'an agency or a person that submits Aadhaar number and demographic information or biometric information, of an individual to the Central Identities Data Repository (CIDR) for authentication' [4, 5]. Here, Authentication User Agency (AUA) is 'an entity who is engaged in providing Aadhaar Enabled Services to Aadhaar holder (using authentication facilitated by the Authentication Service Agency (ASA))' [5]. Hence, Fig. 1 shows that a requesting entity (such as AUA, KUA) connects to the CIDR through an Authentication Service Agency (ASA) (either by becoming ASA on its own/by contracting services of an existing ASA).

2.1 Mandatory Security Requirements

Several mandatory security requirements have been issued (or used) for a requesting entity/issuing entity to generate Aadhaar (in last years). Some of them are listed as:

- An Aadhaar number should be never used openly (as we have discussed in [9] that sharing an Aadhaar number is just like sharing a mobile number, but when we share openly our Aadhaar number with our physical card, then we lose our identity and demographic location also). And in the case of Aadhaar-enabled centre (or operators assisted devices), operators need to be authenticated via password, Aadhaar authentication, etc., mechanisms [6].
- Personal Identity Data (PID) blocks (collected for Aadhaar authentication) need to be encrypted during collection/capture without sending over a network. Also,

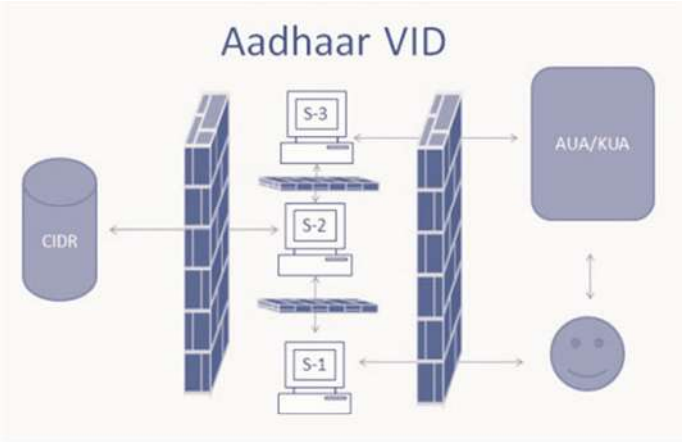

Fig. 1 Process of existed virtual identification mechanism

do not store the encrypted PID blocks (with updated/good key of combinations), unless it is for buffered authentication for a short span of time (currently this time is 24 h).
- Biometric and One-Time Password (OTP) data collected for Aadhaar authentication should not be stored on any permanent storage/database [5, 6].
- The metadata and the responses should be logged for audit purposes for detecting bogus users/reduce fraud users.

Note that network between AUA and ASA should be secured all the time. Here as discussed above, an AUA is 'any entity that uses Aadhaar authentication to enable its services and connects to the CIDR through an ASA, whereas ASAs are entities that have secure leased line connectivity with the CIDR' [5]. ASAs (ASAs work with a formal contract with UIDAI) transmit authentication requests to CIDR on behalf of one or more AUAs.

2.2 Features of the Aadhaar Virtual ID

Unique Identification Authority of India (UIDAI) has made various upgrades in its system through the VID. Some of the salient features of the virtual ID are:

(a) The virtual ID is a temporary 16-digit code that will replace Aadhaar for authentication,
(b) There is only one virtual ID issued at a time. When a new VID is issued, the old one is replaced out (or removed from database/record),
(c) Agencies have to update their system to include VIDs by 1 June 2018,
(d) Aadhaar number cannot be retrieved from the virtual ID,

(e) There is no cap on the generation of virtual IDs,
(f) It is not compulsory to generate VIDs. A person can furnish his Aadhaar instead of the VID,
(g) Agencies cannot force applicants to provide Aadhaar number for e-KYC or verification,
(h) Agencies have to take consent from the user for authentication using VID,
(i) No agency is authorised to store the virtual ID or any other Aadhaar details taken for authentication,
(j) The virtual ID is valid till the user generates a new one,
(k) When you retrieve your Aadhaar, the last generated VID is sent to the registered mobile number.

Note that we can generate virtual IDs for other Aadhaar numbers as well for your family. A user can use VID from 1 June 2018 with organisations irrespective of sharing his Aadhaar 12-digit number [2]. The generated VID is completely temporary, revocable and 16-digit random number. It can be created by users multiple times. So storing different VIDs every time will create more confusion among local authorities. Also, it will put a burden/require additional database to store multiple VIDs, which may create a reason to lose user's privacy. Toda, losing of privacy in computer technology/during making a communication process is a critical issue [8]. Hence, this section discusses Virtual ID system, which is provided by UIDAI and also explains several features of VID. Now, next section discusses our proposed approach or enhancement of VID in detail.

3 Real Virtual ID: Our Proposed System

Multiple Virtual Identifications put a burden on Aadhaar database or agencies/local organisations. To reduce this load and confusion and increasing efficiency and improving accessing cost, we proposed a novel approach, i.e. proposing real virtual identification using a token. Figure 2 demonstrates the work flow of our proposed approach. The following Fig. 2 describes the detail steps of our proposed approach of real virtual identification. Using pseudonyms or Providing extra layer as unique token reduce searching process in our Aadhaar database. When a user creates multiple VIDs for himself/his Aadhaar number, then it is difficult to match or indexing his generated VIDs to his respective Aadhaar number. It requires a lot of time and a complex process. In this case, a lot of irrelevant information is created for that respective user. So to reduce the complexity and improving the accessing or searching level in Aadhaar, we use an extra level of term, like providing a unique token to each user, i.e. based on user's Aadhaar number (see Fig. 2).

With providing this, we provide anonymity to users and we do not have to think about storage because this token has all possible match or generated virtual ID for every user.

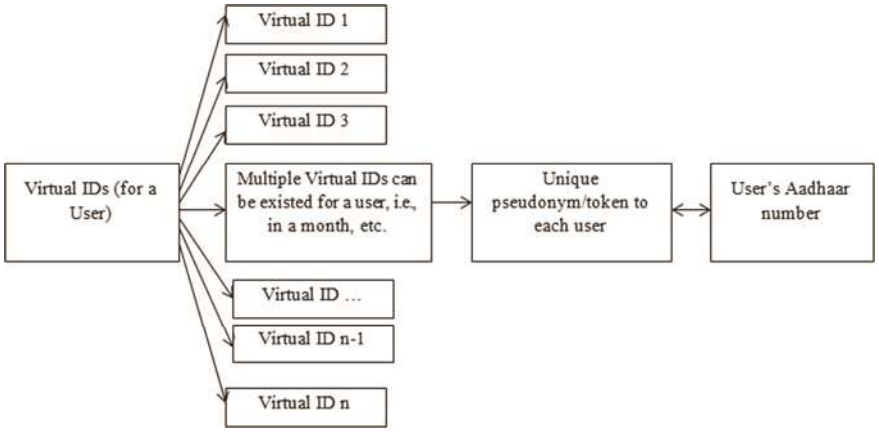

Fig. 2 Real virtual identification system

3.1 Virtual ID Generations

Generating Real Virtual ID (RVID) system is not a complex task. Real Virtual ID can be generated by any user/citizen of India any time from Intranet, Internet or from UIDAI website. Note that for generating a real virtual ID, a user should hold an Aadhaar card and he should also register a number with Aadhaar database. Then only, he/she can generate a virtual ID for himself/herself. Hence, there are some steps to generate Real Virtual ID are:

(a) Step 1: A user visit UIDAI's website at http://uidai.gov.in/.
(b) Step 2: User click on the 'RealVirtual ID (RVID) Generator' from Aadhaar services section.
(c) Step 3: User will be moved to a new VID Generation page https://goo.gl/vFQgic.
(d) Step 4: User need to enter his 12-digit Aadhaar Number and the security code.
(e) Step 5: Now user need to click on the 'Send OTP' button.
(f) Step 6: A One-Time Password (OTP) will be sent to user's mobile number (which is registered with UIDAI/Aadhaar database).
(g) Step 7: user enter the OTP and select the option to either 'Generate RVID' or 'Retrieve RVID'.
(h) Step 8: Now user click on the Submit button.
(i) Step 9: User will receive a message like 'Congratulations! Your VID Number Successfully Generated and sent to your registered mobile'.
(j) Step 10: Hence as the last step, user will get the message on his registered mobile number mentioning the 16-digit real virtual ID for Aadhaar number and the last 4 digits of Aadhaar is xxxxxxxx9870, generated at 25-09-2018:01:01:01.

Hence as output, we get a RVID like that (after Step 10), congratulations! Your RVID has been created which is 1024wesvb67er17s for your Aadhaar number xxxxxxxxx9870.

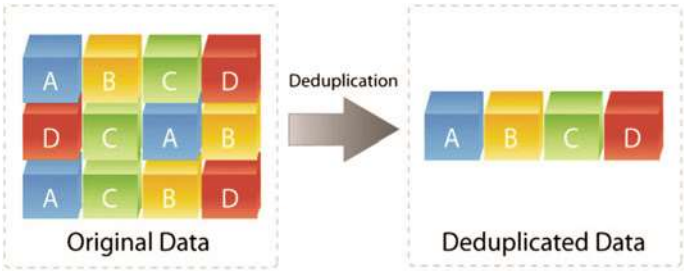

Fig. 3 De-duplication of data in generating RVID

3.2 Benefits of Real Virtual ID

We provide enough security and fast accessing and updating process/Aadhaar database. Also in our proposed system, several VIDs can be generated by a user but here. a unique token contains 16-digits, i.e. a combination of characters and numbers. The process to generate RVID is similar like generating simple VID, but here our system will allocate a unique token to each user, then it will generate VID to user based on this generated token.

De-duplication of data cannot be done by any agencies in our proposed system. Our approach eliminate of duplicate or redundant information to make accessing fast in Aadhaar database (see Fig. 3).

3.3 Issues with Real Virtual ID

As discussed above, RVID is an extra layer of security to protect Aadhaar card information or user's information. But, what about that entire information/Aadhaar card's information which has already been revealed or already has been shared with several local organisations in past? By the government, there is no expiry period is defined for a VID, i.e. multiple VIDs have been created by users with respect to their Aadhaar numbers. A VID (a 16-digit digital ID) is valid till next one VID is not generated. Generating and accessing of RVID depend on user's mobile number, i.e. to generate this ID, user receives an OTP to authenticate himself.

Hence, this section discusses our proposed approach with several benefits and issues raised in brief. Now, the next section will provide an open discussion with research communities with respect to previous existing ID, i.e. virtual and with our proposed approach, i.e. Real Virtual ID.

4 Open Discussion

Biometrics is the most useful discipline among all (except mathematics), used related to human characteristics for identification, authentication and access control. Using biometrics like fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, etc., considered for providing security to a system (Aadhaar database). Also, some other metrics are used to authenticate purpose (or for accessing a system) like voice, typing rhythm [7]. But among all of them, biometrics provides good and better accuracy (with technology advances). For authentication, we need to complete the authentication process in less time (in milliseconds), i.e. the time to get information is needed to be faster with affordable (low) price. Also, one essential feature of biometric authentication is needed to be detecting fake thumb impression/biometrics as quickly (for real time authentication). In several applications, biometrics is using to differentiate people and robots. But here, the main challenge is to detect non-human biometrics efficiently in less time with low cost. Differentiating human from robots is essential to use in applications like which requires anonymity but identifiable human natures. We will use methods like Principal Component Analysis (PCA), Wavelets and Correlations to test such Classification/Proposed System. Also as discussed above, in the proposed Real Virtual ID (RVID) system, captured biometrics is being used but not stored (more than 1 week). So, it becomes hard to get original biometrics after a particular time span. In addition, it also needs to reduce the probability of false positive in biometric collection. Note that, it is clearly impossible to have similar biometrics for two different persons/twins (within certain thresholds).

We have illustrated a novel approach of ID management and authorisation service using an extra token. We noticed that providing extra token/a unique token number is a good step (fit) for ID management and service. By using extra token, the updated system became immune to many attacks like background attack, homogeneity attack, an ID attacks, etc. Hence, a prototype implementation will demonstrated (in extension of this work) that RealVirtualID serves and overcome all Aadhaar privacy issues (feasible) with handling strangers or malicious attackers. Our approach will show that it does not reveal any information of any user to anyone, i.e. it provides (complete) high uncertainty and high anonymity in a system. Also in extension of this work, more robustness tests like including of cryptographic applications will be done in future. By the way, collection, and protection of captured biometric information (stored with UIDAI) is another area to address. In summary, we need fast accessing (with low cost, and less time) with technology improvements/advances in biometrics usage. But in real scenario, things are different, i.e. installation of biometric systems put a financial burden to organisation (via new equipment). So, we hope Real Virtual ID can provide such services without revealing information of users and avoiding irrelevant cost to implement, it will attract many users to use this scheme (also to prevent ID misuse by ID theft). On the other side, several devices are being developed and sold in the market (openly) for public use. Finally, the Real Virtual ID is a demonstration of

ID management and service. This idea can be extended and exploited to any other system, which requires anonymity and accountability.

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/organisations. 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 the respective mobile company at their server. Remember always, the user is always a responsible person for leaking his/her identity or personal information to malicious users. Privacy preservation to users can be provided by proving higher unlinkability or anonymity to user's information or building trust among people. Now, the next section will conclude this work in brief.

5 Conclusion

We need Real Virtual ID to provide anonymity (also unlinkability to user's information) to different organisations to users. This RVID cannot be generated by the user without the presence of Internet. This generated RVID cannot be used or tampered by agencies like AUA/KUA/ASA for de-duplication. Data de-duplication reduces storage costs and processing overhead, i.e. accessing cost and maintaining cost. In this approach, redundant data blocks are removed and replaced with pointers to the unique data copy for providing fast accessing to particular information. In the past research/literature work, we 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. For that government initialised a concept of using VID in the place of using their Aadhaar number. But using VID was an easy task but every time, it was a burden to Aadhaar database/system. So this work enhances and removes this issue by providing an extra layer of security, i.e. 16-digit unique token to every Aadhaar card holder. In future as the extension of our proposed work, we will come back with experimental results, i.e. with respect to this approach. Hence, in simple terms, a good design alteration can make Aadhaar system safe.

Privacy still remains a point of paradox and in the absence of concrete privacy laws, citizens might be subjected to mass surveillance in the name of national security. 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. Hence, we/future researchers and the government still require so much research to be done with respect to protect Aadhaar database. Also, the government needs much more dedicated, informed and comprehensive security

policies and accelerated efforts to realise Aadhaar's full effectiveness. 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.

Author Contributions Amit Kumar Tyagi conceived of the work, and drafted the manuscript, whereas G. Rekha designed the schemes. Amit Kumar Tyagi and Sreenath Niladhuri contributed to the original ideas and scheme design.

References

1. https://simplybanking.wordpress.com/2013/07/14/the-actual-uidai-aadhaar-number-is-11-digits-long-and-not-12-digits/
2. https://economictimes.indiatimes.com/wealth/personal-finance-news/aadhaar-everything-you-need-to-know-about-it/articleshow/60173210.cms
3. https://scroll.in/article/864698/explainer-what-is-virtual-id-and-how-is-it-different-from-aadhaar
4. https://www.paisabazaar.com/aadhar-card/aadhaar-authentication/
5. https://uidai.gov.in/authentication/authentication-partners/user-agency.html
6. https://authportal.uidai.gov.in/home-articles?urlTitle=requesting-entities&pageType=partners
7. Ríha, Z., Matyáš, V.: Biometric Authentication Systems, FI MU Report Series (2000)
8. Tyagi, A.K., Sreenath, N., Priya, R.: Never trust anyone: trust-privacy trade-offs in vehicular ad hoc network. Br. J. Math. Comput. Sci. **19**(6), 1–23 (2016, November). ISSN: 2231-0851
9. Tyagi, A.K., Rekha, G., Sreenath, N.: Is your privacy safe with Aadhaar?: an open discussion. In: Proceedings of Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC) 2018, India (2018)