A REVIEW ON MITIGATING SECURITY THREATS IN AADHAAR

Reshmi Maulik

Assistant Professor, Meghnad Saha Institute of Technology,
Kolkata,India
reshmi.maulik@msit.edu.in

Abstract

The government has worked to amass a sizable data collection throughout the years to provide its own residents with various public service benefits. To safeguard confidential account information, the government has also attempted to impose various security measures at various stages. One such significant project that the government started in 2010 is Aadhaar. Every citizen is given a unique 12-digit number known as their "Aadhaar Number", which is enhanced by biometrics like fingerprint and retinal match technology. Only the size of the finger prints can change; no human being is able to alter these biometric features throughout their lifetime. These days, numerous departments, including the land registration, passport office, etc., where people occasionally need to provide the prints of all ten fingers of their hands, have their data stolen frequently. Unauthorized users may be able to compromise these security measures, which could endanger the person's identity and financial resources. In this study, we have tried to identify the inherent vulnerabilities of the Aadhaar system. We have suggested an algorithm for preventing the access of data from machines at public places by unauthorized users and a three-factor authorization which can prevent the fraudsters from incorporating spurious data into the Aadhaar database.

***Keywords*: Aadhaar, ABBA, Biometrics, AePS, PDS, Security, Privacy**

1. Introduction

Governments worldwide are relying on huge data repositories to provide public services to their citizens without putting their private information at stake. Government of India has started a new initiative in 2010 to identify its citizens based on a unique identification number, which also incorporates the biometric parameters such as finger prints and retinal scan. The government had also urged the banks to link the accounts of its customers to the respective Aadhaar number to increase the revenue of the tax department. But this linking of Aadhaar with the bank accounts has made the citizens of India vulnerable to the fraudsters. India is facing a huge problem due to Aadhaar-enabled Payment System (AePS) as the crime incidents are on the rise day by day. These incidents are caused when the victims unknowingly reveal their vital private information to unauthorized persons [Ghosh (2023a)]. AePS is a bank led model where the individual can use Aadhaar to do financial transactions from point of sale (POS) or micro-ATMs bypassing the requirement of OTP for authentication. This is only possible if bank account number is linked with Aadhaar. Linkage of Aadhaar with account number is also a preferred method for KYC. Also, the government had made it mandatory under section 7 of Aadhaar act to submit aadhaar number to banking service provider who wants to avail any benefit or subsidy [Ahmed (2023)]. Data released by Pune police had shown that there is a huge increase in cyber crime in recent days [Deshpande (2017)]. After the government had made it compulsory to link Aadhaar-based Biometric Authentication system (ABBA) in Public Distribution System (PDS) in 2016, there is a significant rise in crime incidents in six states such as Rajasthan, Jharkhand, Bihar, Uttar Pradesh, Haryana, and West Bengal, who had raised alarm [SNS (2023)], [Menon (2017)], [Ghosh (2023b)]. There have been reports of 37 Aadhaar-based fraud cases done in Kolkata in month of September 2023 which have kept the cops on toes [Ghosh (2023b)].

Rajesh Kumar, Chief Executive Officer, Indian Cyber Crime Coordination Centre (I4C), a cybercrime wing under the Ministry of Home Affairs, informed that frauds relating to biometric cloning and the Aadhaar-enabled Payment System (AePS) accounted for 11 percent of the cyber-enabled financial crimes in 2023 [Sarasvati NT (2024)].

The four main types of vulnerabilities that exist in the information security are operating system vulnerabilities, network vulnerabilities, human vulnerabilities, and process vulnerabilities. Insecure Direct Object References (IDOR) occur when users are given direct access to database objects through an application based on user-given input [Ahmad et al. (2023)]. This basically occurs when a website developer exposes a reference to an internal file, directory or database key as a URL or form parameter. This vulnerability of an existing system helps the unauthorised user to get direct access of the sensitive information of any database bypassing the required authorization [KumarShrestha et al. (2008)]. Using this vulnerability of the official government websites in 2018, more than 200 websites had made confidential data including Aadhaar data public leading to blocking of around 5000 official websites where data could have been obtained by unauthorized persons simply by Googling it [Jain (2019)]. Recently, a report regarding increase in AePS frauds in Kolkata have been published [Sarasvati (2023)]. It has been found that exploiting IDOR fraudsters are obtaining finger prints linked to a particular Aadhaar number from property registration deeds. Aadhaar based frauds have been reported from the southern city of Mangaluru in Karnataka in October 2023, where the biometric and the Aadhaar data have been compromised from the registry and the land record office. In this case police nabbed the culprits from North Bihar several thousand km away [Raghava (2023)]. With the growing use of ABBA for PDS, a flawless monitoring of the system is also a need of the hour [Menon (2017)]. If anyone desires to file a civil suit on anyone related to any land dispute, then it is required for lawyers and court to get the deed copy of the concerned person from the registration office. But these deeds can then make the concerned persons vulnerable, as the finger prints are mandatory and the Aadhaar card number is mandatory information required during land/flat registration for certain states. Even while it is not required in some places, including West Bengal, it is typically shared by common people, which makes it readily accessible to many illegal users. There is no clear official protocol for identifying the person who could be given the access to the sensitive information along with the deed. Furthermore, it has been discovered that there have been other instances of security breaches using Aadhaar data, mostly because of lax protection on official websites and individual computers at various hotels. [Dwivedi (2018), [Ganjoo (2018)]. The government should make a drastic change in its security and privacy policy to prevent their privacy and help its citizens to keep their sensitive and vital information secure. The certified copy of deeds given by the registration office or its downloadable copy must not have the finger prints, signatures and the Aadhaar number.

The State/UT-wise Percentage of Aadhaar Authenticated PDS Transactions during the month on June 2021 is shown in Figure 1.

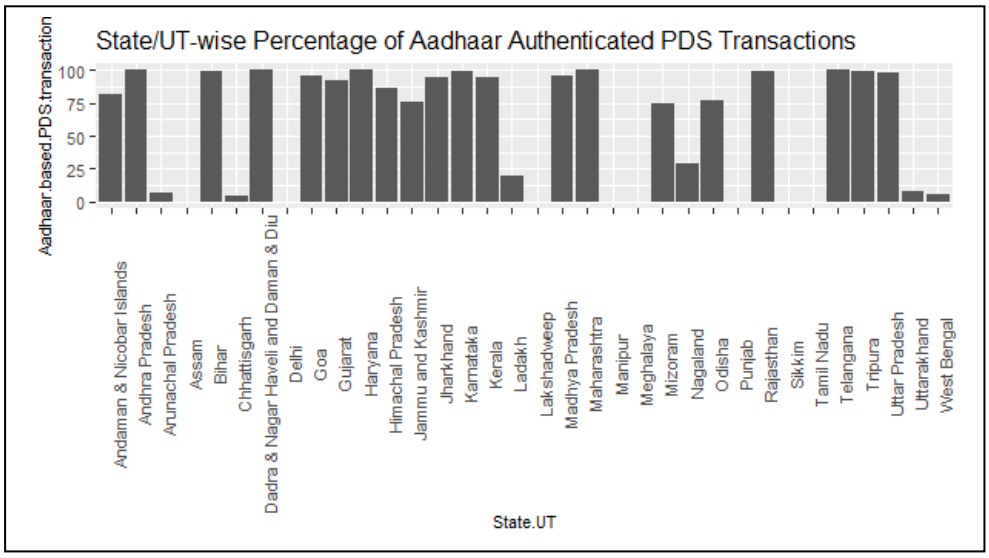

Fig. 1: The Bar Graph for Percentage of Aadhar based PDS transactions state-wise

The bar graph shows that many states are involved in Aadhaar based PDS transactions. (Source: https://data.gov.in (for the year 2021)).

In a recent press release, UIDAI formally acknowledged the Aadhaar data leak and its potential misuse [Dalal (2022)]. They warned the public not to use it somewhere, especially not in cybercafes, where unsecured computers are publicly accessible. They advised to use the 4-digit masked Aadhaar number if needed, and erase all downloaded e-Aadhaar versions from public computers. Cyber expert had advised people to disable the biometric details in myAadhaar website to avoid the problem of unauthorized access and withdrawal of money from bank account through AePS [Raghava (2023)].

In a recent security breach, Aadhaar information of more than 800 individuals has been made available on the dark web for $80,000 only [Fernandes (2023)]. Bengaluru Police had advised the citizens to lock their biometrics on the UIDAI website or app of Aadhaar [Outlook Money (2023)].

2. Security Issues

Below we have pointed out the different existing security issues related to Aadhaar card.

(1) ***User Awareness and Education:*** Most of the users are unaware of the potential risk associated with the leakage of Aadhaar data. This may be due to their limited knowledge or proper education. Most of the Aadhaar related security issues can be mitigated through proper education.

(2) ***Impersonation and Identity Theft:*** Aadhaar is required to establish one's identity. If data are stolen then anyone can impersonate any person who may be working in a high position, politically or financially important. Research is required to prevent this type of fraud.

(3) ***Privacy Concern:*** Preserving the privacy of the citizens and at the same time sharing what is required with the authorized persons are the major challenging areas for the researchers.

(4) ***Unauthorised Access and Data Breaches:*** Various government and private organizations require Aadhaar for authentication. Strengthening the Aadhaar Authentication Ecosystem (AAE) and providing security by properly identifying the vulnerabilities and reforming the organizational architecture is a major concern for the system administrators and researchers.

(5) ***Biometrics Data Security:*** Often the biometric data has to be sent over the network. So, it is required to be properly encrypted to prevent its access by unauthorized users and to avoid tampering of biometric data.

(6) ***Legal and Regulatory Framework:*** The laws regarding Aadhaar need to be strengthened. This may include privacy laws, data protection laws and the regulating the role of government authorities in ensuring the privacy and security of biometric data. This is very much required to enhance the trust of the citizens on the regulatory authority.

3. Methodology

We will try to offer a technique that will help to handle the issue of unauthorised access and data breaches mentioned in section 3.1. We all are aware that Aadhaar identity cards are used everywhere by Indian citizens – in PDS, hotels, banks, mobile phone kiosks and hospitals. People are unconcerned about the security of their personal Aadhar number since they are unaware of current security threats. Cybercriminals may view elderly people with vast homes but inadequate computer abilities as easy targets. Recently, senior adults are being deceived since they are compelled to provide their biometrics and Aadhaar numbers for Jeevan Praman Patra, according to a civil society organization called BBDBM or Manch. To lower the risk of biometric data compromise, the digital life certificate process, which requires fingerprint capture, should not be delegated to outside organizations [Moneylife (2023)]. To educate Central government pensioners and pension disbursing authorities in 100 cities, the Union Department of Pension and Pensioners' Welfare (DoPPW) has launched a national campaign. The campaign's goal is to reach 50 lakh pensioners, who are primarily extremely elderly, ill, and disabled pensioners who live in rural areas. The government must also try to increase public awareness related to phishing and vishing so that people check and confirm before providing their Aadhaar number to unauthorized people. Maulik et al. had defined different ways in which an individual can be attacked over

phone, SMS and websites to reveal their personal information to impersonated persons or fraudsters [Maulik and Chaki (2009)].

Another point of major leakage of Aadhaar data is from the database of the computer used at the land registry office. So, it is very much essential to boost up the security of these terminals, which are generally used by less computer savvy personnel. To enable these employees to protect their computer we have developed beginner-friendly Ubuntu-based software with GUI facilities named UBSAFE to automate the complex security procedure. Transparency and accountability in safety management are the features only to be found in UBSAFE's activity-based records and reporting. One of its unique features allows users to quickly adjust and limit access to USB, SSH, and TOR ports using log-based operations, eliminating a security vulnerability that attackers frequently exploit.

Since it might contain several harmful files, the Universal Serial Bus (USB) is a common security risk. USB blocking is the act of regulating or restricting how USB devices are used on a computer or network. This is done for security and data protection purposes. Smartphones, external hard drives, and other USB devices can be used to spread malware or transfer illegal data via networks and computers. To avoid these potential security risks, businesses and individuals install USB-blocking regulations or software solutions. There are numerous instances where USB is used to obtain access to a computer system. In 2014, a new kind of USB malware called BadUSB was found by researchers Karsten Nohl and Jakob Lell from Security Research Labs [Nohl et al. (2014)].

The Onion Routing (TOR) project is the brain child of mathematician Paul Syverson, computer scientists Micheal G. Reed and David Goldschlag, and employees of the United States Naval Research Laboratory that started in 1990s [Murdoch and Danezis (2005), Dingledine et al. (2004)]. It was later named as TOR by Syverson, computer scientists Roger Dingledine and Nick Mathewson and released as an open-source software in 2002. TOR provides a level of anonymity that is unparalleled and it also assists anyone to protect their privacy. The main objectives of TOR are to safeguard its users' right to privacy and freedom of confidential communication. TOR masks this identifiable evidence of your online behavior by rendering your IP address untraceable. Normally, whenever one participates in an online activity, a direct link is established between her computer and the website that she is surfing and that is visible to others. TOR, on the other hand, uses layers of encryption to pass information – hence, the onion metaphor – as opposed to showing it directly to a website. TOR sends one’s traffic over a global network of thousands of relays while protecting the application layer of that specific activity. As information passes from one node to another node, each one decrypts the layers that reveal the next node the data must pass through.

The cryptographic network protocol known as SSH, or Secure Shell, can be used to securely access and manage remote servers and devices over a potentially unsafe network, like the internet. For data transmission, authentication, and remote command execution, SSH provides a secure connection. Encryption has been applied to safeguard sensitive data exchanged between a client and a server, such as login credentials.

SSH is widely utilized for remote server administration, network tunneling, and private file transfers by system administrators, programmers, and network engineers. The cryptographic network protocol known as SSH, or Secure Shell, can be used to securely access and manage remote servers and devices over a clearly unsecure network, such as the Internet. It protects the privacy of your publicly transmitted messages.

3.1 Workflow of software UBSAFE

The workflow of operating system-based software namely UBSAFE is shown in Figure 2. To verify their identity, users must first log into the system. When a user's identity is verified, they are granted access to system resources, and the administrator receives an automatic message with the user's information and the access time. Three alternatives are shown to the user: blocking USB, blocking SSH, or blocking Tor.

In addition, the user can conduct partial operations like setting up firewalls, starting a virus scan, and recovering the machine. Each one of these jobs initiates a background script that the system kernel then runs to carry out the intended activity.

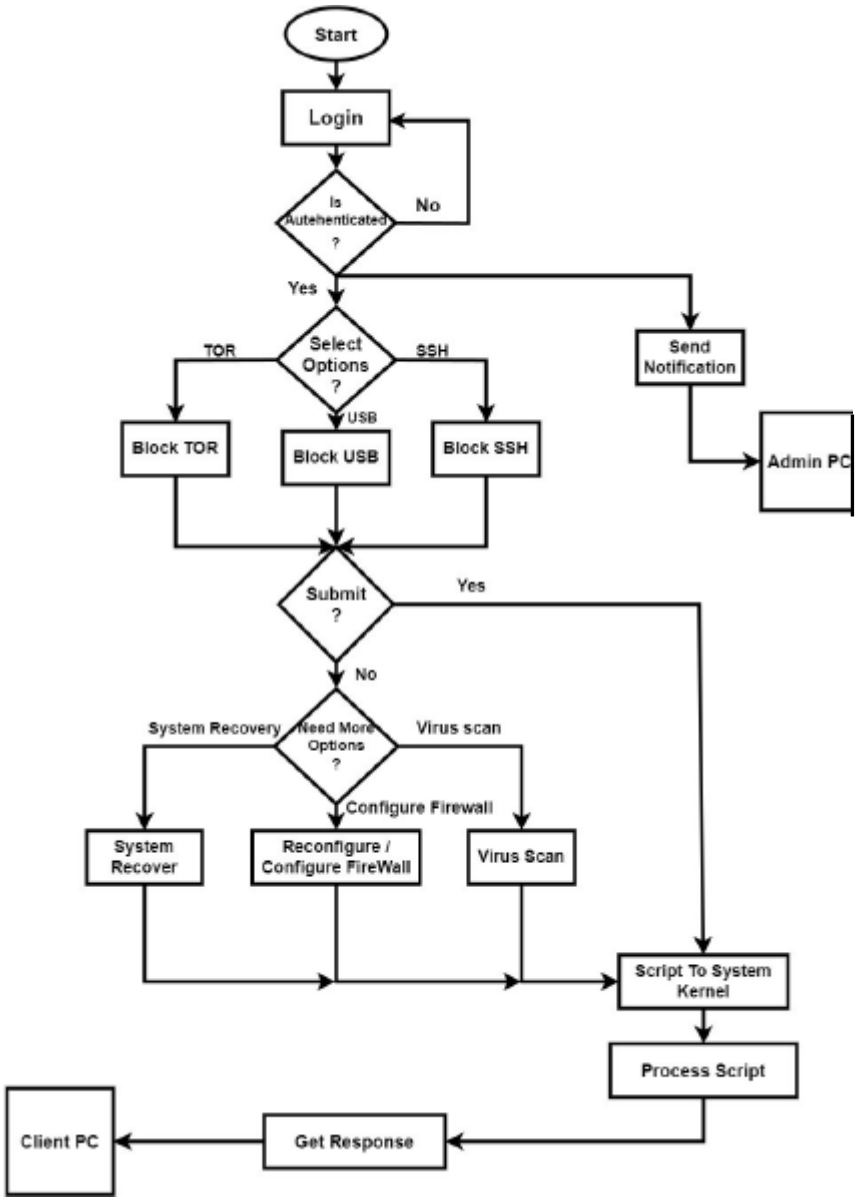

Fig 2: Workflow of UBSAFE software

3.2 Three-way factor authentication algorithm to prevent fraud of Aadhaar Database

According to a recent report, a police probe revealed that the majority of Aadhaar theft happens when updating addresses. Here, the fraudsters are altering the personal information in the Aadhaar database by forging official signatures and rubber stamps [PTI (2023)]. Obtaining the address change certificate from the UIDAI website and re-uploading it after it has been signed by public officials, such as doctors, gazette officers, municipal council members, etc., is one technique for updating address changes in the Aadhaar database. However, because of their extremely hectic schedules, they occasionally delegate this work to their employees, who sloppily deliver the rubber stamps and signatures in return for a little payment.

It is urgently necessary to alter the current procedure for updating addresses in the Aadhaar database. A lengthy address change procedure could make things more difficult for the general population. It is also crucial to identify and hold accountable the person responsible for making the alterations.

The absence of additional safety features like a microchip, hologram, or government seal that come with traditional picture identity proof makes the Aadhaar card more vulnerable to forgery [Jain (2019)].

Delhi police discovered in March 2023 that the Aadhaar system was not genuinely performing the facial biometric matching feature while creating an ID for any user [Jha (2023)]. The scammers were able to register bank accounts with the same photo at several banks owing to this flaw in the Aadhaar system. The fraudsters are also able to download and upload the photographs after modifications. The fraudsters were also configuring their system in every 2-3 days to match the GPS of their device with the GPS of the designated government office.

The Aadhaar system is unable to distinguish between an IRIS scan copy and a live copy, which is necessary to determine whether a person is present before the scanner.

Furthermore, the authorized agents' live finger print and silicon finger print cannot be distinguished by the Aadhaar system. Additionally, rather than treating a person's ten distinct fingerprints as separate identities; the Aadhaar system treats the combination of those fingerprints as a one entity. Fraudsters are also aware of these built-in weaknesses and how to take advantage of them to generate fake Aadhaar cards by combining multiple people's fingerprints [Jha (2023)].

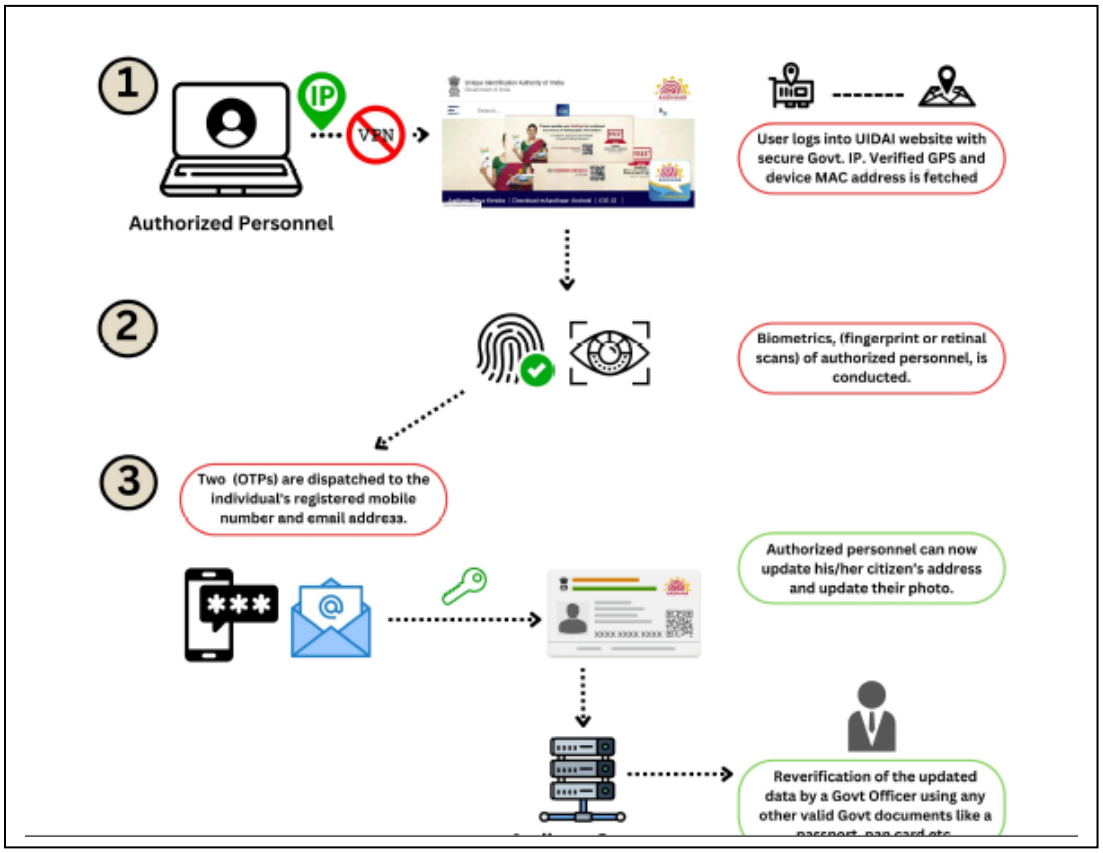

Fig. 3. Three factor authentication algorithm.

Figure 3. shows the three-factor authentication algorithm.
A unique three-factor authentication algorithm has been proposed which can be implemented through the UIDAI site before making any alterations to the Aadhaar data kept in the UIDAI system. The algorithm is explained below:

1. Initially, the user can only access the UIDAI website by using the government agencies' secure IP address. The user will not be able to manually modify the GPS position or the mac (hardware) address that the system will automatically retrieve during the logging procedure. This will solve the issue of fraudsters manipulating GPS data.

2. Biometrics, such as a finger print or retinal scan of the authorized personnel, can be used to perform the second level of authentication during logging in. Two codes that will be automatically produced and sent will be used for the third level of authorization following successful biometric authentication. Two codes are provided: one for the approved user's mobile number and another for their authorized email address. Once the correct code has been properly entered, authorized personnel will be able to modify the citizen's address. If the photo needs to be changed, it should be added along with the old version which cannot be permanently removed from the system.
3. An additional layer of verification must be completed by another randomly chosen authorized government employee selected by the system. When approving the changes to the citizen's photos, this randomly selected staff will only consider any legitimate government identification that the citizen may possess and had uploaded into the system for verification. Examples of such identification include the photo included in a scanned copy of the citizen's passport, voter ID, pan card, etc.

Furthermore, if authorized government staff are found to have provided any other unauthorized person access to their mobile number, email address, or biometrics at any point during the fraudulent Aadhaar data detection process, they would face severe disciplinary action.

4 Literature Review

For the UN sustainability mission, all the countries must make the Legal identification of its entire people by 2030 [Weber (2018)]. The author had suggested that to improve the privacy and security of Aadhaar, the UIDAI must be made an independent authority not controlled by the government [Anand (2021)]. This will also lead to the transparency and better governance of Aadhaar.

By limiting access and minimizing unnecessary paperwork, the authors had proposed rebuilding the operational architecture to improve the security and privacy of the individual data with reference to a case study done for a health unit [Agrawal et al. (2020)].

After speaking with members of a low-income group, Srinivasan et al. conducted a qualitative study and disputed the validity of the data collection methods and the need for such a huge number of papers collecting Personally Identifiable Information (PII) [Srinivasan et al. (2018)]. Big Data Applications have been used for Aadhaar Fraud detection [Ramya and Sumathi (2019)].

Menon conducted a case study of ration card-holding households in Ranchi. He asserted that the government's intensified push to integrate Aadhaar-based biometric authentication with the PDS had resulted in a decrease in transaction volume since citizens were unable to access their entitlements. This happens because of biometric errors, inaccurate cardholder information seeding, and administrative flaws brought on by insufficient failure reporting and system backup [Menon (2017)]. Sukhtankar et al. also did an extensive study for J-PAL lab on effect of Aadhaar on PDS in Jharkhand [Sukhtankar et al. (2022)].

Liu et al. had evaluated a block chain-based identity system and had noted the difficulties with storing blocks of data as well as the need for scaling due to the varying storage capacities of different users [Liu et al. (2020)]. R. Garg had also considered the block chain technology to overcome the shortcomings of the Aadhaar-based ecosystem. He noted that there are several forms of the distributed ledger such as blockchain, Directed Acyclic Graphs, Hashgraphs, Holochain or Tempo. The author emphasized that the time consumption and reliability of data increases throughout the world by using distributed ledger technologies [Garg (2022)].

None of the papers in the literature had focused on providing the security to the devices that collect the data. Our algorithm of the software provides an easy solution to the not so computer savvy personnel and enables them to handle and store data in their local databases in a more secured way.

In Table I, we have done a comparative study of the solutions provided for the Aadhaar security by different authors over time.

.

Reference	Key Contribution
Liu et al. (2020)	Blockchain is used to maintain data integrity in the distributed database. Confidentiality is maintained through smart contract. Different level of access for authenticated persons playing different roles. Data is publicly available. Non-repudiation can be guaranteed as data cannot be modified.
Agarwal et al. (2020)	The author had proposed a major change in Operational Architecture. But only the local data is considered. Confidentiality is ensured as data is maintained by authorized persons. Only Data controllers can access it and that also through authorized centers. However, non-repudiation principle of cyber security is not considered.
Garg et al. (2022)	The author had considered blockchain. Data integrity is maintained in the distributed database. Confidentiality is maintained through distributed ledger. The data can only be accessed through administrative departments. However, data will be publicly available though it cannot be modified by unauthorized person.
Ramya and Sumathi (2019)	The author had emphasized upon de-duplication of biometric data and de-duplication of demographic data during uploading and modification of Aadhaar data. The author had suggested a Naive Bayesian algorithm with less time complexity for fraud detection.

Table 1. Comparison among different existing methods.

5 Conclusion

This paper highlighted the significance of putting strong security measures in place by identifying Aadhaar system weaknesses, such as unsecured direct object references, which could allow unauthorized access to sensitive data. This paper emphasized the frequency of Aadhaar-based fraud instances, highlighting the critical need for improved security measures to stop financial crimes and biometric cloning. It advocated for tightening privacy and data protection regulations to increase public confidence in regulatory bodies, highlighting the need of user education and awareness to reduce security threats related to Aadhaar.

UBSAFE is a game-changer in the field of organizational security, setting new bench-marks for user-friendliness, adaptability, and thorough protection. If properly implemented using any operating system software then it can mitigate the data leakage issue from the personal computer at the public places. The suggested technique helps non-technical staff handle and store data safely by offering a mechanism for protecting data gathered by devices. The three-factor authorization approach that we have proposed, if properly implemented, can help the government to prevent Aadhaar database from the reach of fraudsters.

Acknowledgments

I would like to thank Aviraj Sardar and Biswarup Dutta, students of Department of Computer Application for help in drawing the flow chart and the work flow diagram. The authors have no conflicts of interest to declare.

References

[1] Agrawal, P.; Singh, A.; Raghavan, M.; Sharma, S.; Banerjee, S. (2020): An operational architecture for privacy-by-design in public service applications. arXiv preprint arXiv:2006.04654.

[2] Ahmad, H.; Dharmadasa, I.; Ullah, F.; Babar, M.A. (2023): A review on c3i systems'security: Vulnerabilities, attacks, and countermeasures. ACM Computing Surveys,55(9), pp.1-38.

[3] Ahmed, N. (2023). Explained gaps in aadhaar-enabled payment system (aeps) abused cybercriminals. https://www.thehindu.com/scitech/technology/explained-gaps-aadhaar-enabled-payment-system-aeps-abusedcybercriminals/article66842275.ece.

[4] Anand N (2021): New principles for governing Aadhaar: Improving access and inclusion, privacy, security, and identity management. Journal of Science Policy &Governance 18(01), pp.1-14.

[5] Dalal, S. (2022). Now That the Government Has Admitted to Security Issues with Aadhaar, People Need To Demand Better Security. https://www.moneylife.in/article/now-that-the-government-has-admitted-tosecurity-issues-with-aadhaar-people-need-to-demand-better-security/67362.html.

[6] Deshpande, S. (2017). Aadhaar linking is latest arsenal for cybercrime fraudsters. https://www.hindustantimes.com/pune-news/aadhaar-linking-islatest-arsenal-for-cybercrime-fraudsters/story- Vehm4cD8TLKxtBz7HGejLI.html.

[7] Dingledine R.; Mathewson N.; Syverson P.F. (2004). Tor: The second-generation onion router. In USENIX security symposium 4, pp 303-320.

[8] Dwivedi, S. (2018). In A Week, Aadhaar Data Of 70 Lakh Children On Andhra Pradesh Government Sites. https://www.ndtv.com/indianews/despite-laws-no-action-against-government-agencies-displaying-aadhaardata-1844747.
[9] Fernandes, J. (2023) Aadhaar data Leak; Personal information of 81.5 crore Indians on dark web. Available via https://www.livemint.com/news/india/aadhaardata-leak-personal-information-of-81-5-crore-indians-on-dark-web-top-7-things-toknow-11698737674480.html.
[10] Ganjoo, S. (2018). Quora reports massive data breach, data of 100 million users stolen. https://www.indiatoday.in/technology/news/story/quorareports-massive-data-breach-data-of-100-million-users-stolen-1401950-2018-12-04.
[11] Garg, R. (2022): A Technological Approach to Address Deficiencies in UID (Aadhaar). 3rd International Conference on Big Data, Blockchain and Security,Copenhagen Denmark. doi (Vol 10).
[12] Ghosh, D. (2023a). Rise in number of aadhaar fraud cases. https://timesofindia. indiatimes.com/city/kolkata/rise-in-number-of-aadhaarfraud-cases/articleshow/ 102817460.cms.
[13] Ghosh, D. (2023b). Aadhaar frauds in a month keep kolkata-cops on toes. https://timesofindia.indiatimes.com/city/kolkata/37-aadhaar-frauds-in-a-monthkeep-kolkata-cops-on-toes/articleshow/ 103544825.cms.
[14] Jain, M. (2019). The Aadhaar card: cybersecurity issues with India's biometric experiment. https://jsis.washington.edu/news/the-aadhaar-cardcybersecurity-issues-with-indias-biometric-experiment.
[15] Jha, R. (2023). How crooks are exploiting gaps in Aadhaar system in Delhi. https://timesofindia.indiatimes.com/city/delhi/how-crooks-are-exploiting-gaps-in-aadhaar-system-in-delhi/articleshow/98744284.cms.
[16] KumarShrestha, A.; Singh Maharajan, P.; Paudel, S. (2015): Identification and illustration of insecure direct object references and their countermeasures. International Journal of Computer Applications 114(18), pp. 39-44.
[17] Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Choo, K.R. (2020): Blockchain-based identity management systems: A review. Journal of network and computer applications 166: 102731.
[18] Maulik, R.;Chaki, N. (2009): PhishNet: Enhancing the Security Aspect of IMS Users.In: 2009 First International Conference on Networks & Communications, Chennai,India, Dec 2009. doi:10.1109/NetCoM.2009.34.
[19] Menon, S. (2017): Aadhaar-based biometric authentication for PDS and food security: Observations on implementation in Jharkhand's Ranchi District. Indian Journal of Human Development 11(3), pp. 387-401.
[20] Moneylife (2023). Jeevan Pramaan Life Certificate: BBDB Manch Warns about AePS and Phishing Frauds. https://www.moneylife.in/article/jeevan-pramaan-life-certificate-bbdbmanch-warns-about-aeps-and-phishing-frauds/72512.html.
[21] Murdoch S.J.; Danezis G. (2005): Low-cost traffic analysis of Tor. In 2005 IEEE Symposium on Security and Privacy (S&P'05), pp 183-195.
[22] Nohl, K.; Kribler, S.; Lehl, J. (2014): BadUSB-on accessories that turn evil.Black HatUSA 1(9):1-22.
[23] Outlook Money (2023) Massive Aadhaar Data Breach of 815 Million Indians: Here's How To Keep Your Details Safe. https://business.outlookindia.com///news/massive-aadhaar-data-breach-of-815-million-indians-heres-how-to-keep-your-details-safe.
[24] PTI (2023). Easy Address Change Process in Aadhaar Major Cause of Cyber Fraud: Police. https://www.outlookindia.com/national/easy-address-change-process-in-aadhaar-major-cause-of-cyber-fraud-police-news-273848.
[25] Raghava, M. (2023). Another victim loses money to aadhaar-enabled payment system fraud following registration of document at Mangaluru City sub-registrar's office. https://www.thehindu.com/news/cities/Mangalore/another-victim-losesmoney-to-aadhaar-enabled-payment-system-fraud-following-registration-of-landdocument-at-mangaluru-sub-registrars-office/article67408249.ece.
[26] Ramya, K.; Sumathi, A. (2019). Big Data Applications in Aadhar Card Fraud Detection. IJCSE 7(3) 5:865-867. doi:10.26438/ijcse/v7i3.86586.
[27] Sarasvati, N.T. (2023). What Made It Easier for Fraudsters to Access People's Biometrics, Aadhaar Details in Kolkata? https://www.medianama.com/2023/10/223-aadhaar-enabled-payment-systemfraud-kolkata.
[28] Sarasvati, N.T. (2024). Aadhaar-enabled Payment System Frauds Contributed to 11% of Financial Cybercrimes: I4C Data. https://www.medianama.com/2024/01/223-aadhaar-enabled-payment-systemaeps-financial-frauds-i4c-data.
[29] SNS (2023). Kolkata-police-commissioner warns of rising biometric-data-theft-bank-fraud-cases. https://www.thestatesman.com/bengal/kolkatapolice-commissioner-warns-of-rising-biometric-data-theft-bank-fraud-cases-1503223209.html.
[30] Srinivasan, J.; Bailur, S.; Schoemaker, E.; Seshagiri, S. (2018): Privacy at the margins— The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. International Journal of Communication 12, 2.
[31] Sukhtankar, S.; Niehaus, P.; Muralidharan, K. (2022): Integrating Biometric Authentication in India's Welfare Programs: Lessons from a Decade of Reforms.
[32] Weber, H. (2018). Politics of 'leaving no one behind': contesting the 2030 Sustainable Development Goals agenda. In the Politics of Destination in the 2030 Sustainable Development goals, pp. 399-414.

Authors Profile

Reshmi Maulik is an Assistant Professor in Meghnad Institute of Technology, Techno India Group, Kolkata, India. She received her Master's degree in Economics from University of Calcutta in 2000. She then completed C level (equivalent to M.Tech. in Computer Science) from DOEACC Society, Government of India, in 2005. She has also worked in the software industry for 3 years before returning to academia. She has authored several research papers in Journals and International conferences. She is currently pursuing PhD in Computer Science and Engineering from MAKAUT. Her current research focuses on cyber security and finding the ways to minimize the bug resolution time in software engineering.