IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

Aadhaar Data Vault & Security

Anisha Shaktawat[1], Himani Mehta[2], Manan Mathur[3], Manasvi Tripathi[4] , Rishika Soni[5]

CSE, Geetanjali Institute of Technial Studies, Udaipur, India[1,2,3,4,5]

Abstract: The idea of Aadhaar was developed in response to the demand for an individual identifying system. The Unique Identification Authority of India (UIDAI), which is in charge of creating and managing user IDs based on demographic and biometric information, was founded by the Indian government to meet this need. Aadhaar's adoption has, however, been followed by a number of security issues and worries, notably with relation to its authentication procedure. In our paper, we explore Aadhaar's progress, charting its history and assessing its current situation. We give a thorough rundown of the authentication procedure and emphasise the improvements that have been achieved over time. . Additionally, we analyse the security threats that Aadhaar has already experienced, suggesting alternative defences and categorising them as necessary. Our main goal is to fully solve the security issues related to Aadhaar in order to reduce the danger of security breaches. To guarantee the relevance and timeliness of our analysis, we have also included the most recent Aadhaar-related changes and news.

Keywords*:* Biometrics, Security, Identity, Authentication, Access Control.

I. INTRODUCTION

In India, Aadhaar is the cornerstone of identity verification. The Indian government formed UIDAI (Unique Identification Authority of India) under the Ministry of Electronics and Information Technology in 2009 to provide a trustworthy method of identifying people. This action was taken in compliance with the Aadhaar Act of 2016, which gave UIDAI the authority to gather and handle data on all Indian people. Based on biometric and demographic information about an individual, the 12-digit Aadhaar number is produced. Before the advent of Aadhaar, passports and PAN cards were the primary forms of citizen identification in India. However, the usage of these credentials created problems for identity verification across the nation and resulted in a lack of inclusion. Recognizing the need for a trusted and unique identity proof for every individual in India, the government established UIDAI. UIDAI is responsible for generating a Unique ID (UID) for each individual, which is linked to their iris scan, fingerprint, and demographic data. The term "Aadhaar" derives from Hindi and signifies a foundational base that validates one's identity.

Aadhaar Features

A central system for managing the whole population has been established as a result of the adoption of Aadhaar. The necessity for separate proofs of address and identity has been removed, simplifying the authentication procedure for a number of services. The Aadhaar card has developed into a complete answer for authentication needs. Aadhaar is distinguished by these five factors:

- **Unique identifying numbers** provided by Aadhaar ensure that each person has a distinct identity that cannot be replicated or shared.

- **Availability:** People may readily get and use their Aadhaar cards for a variety of purposes because to the accessibility of Aadhaar services.

- **Random Nature:** To increase security and lessen the likelihood of recognisable patterns or correlations, Aadhaar's unique identity numbers are produced using random methods.

- **Centrally Managed Architecture:** UIDAI, which oversees the Aadhaar system, ensures the accuracy and consistency of the data linked to each person's Aadhaar card.

- **Technology:** To create a strong and dependable identity framework, Aadhaar makes use of cutting-edge technology like biometrics (including fingerprint and iris scans) and demographic data.

Aadhaar has transformed the identification process by merging these elements, providing a uniform and effective method for identity verification across many industries and services.

A. Aadhaar Benefits and Applications

Aadhaar is a highly practical and adaptable solution thanks to its many benefits. It is becoming an essential component of many services that demand authentication. Aadhaar's capacity to provide people distinct identities without considering factors like caste,

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

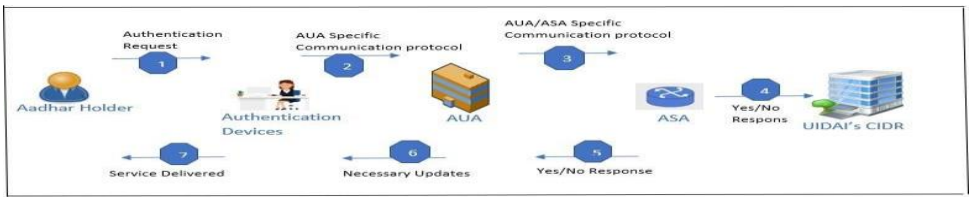
Vol. 10, Special Issue 2, May 2023

religion, money, or ethnicity is one of its main advantages. This openness makes sure that any citizen may take use of Aadhaar's advantages.

Aadhaar's function in enabling financial inclusion and the automated transmission of benefits is another noteworthy benefit. People may easily access applications that provide these advantages by using Aadhaar and associated authentication services. Some noteworthy Aadhaar apps are listed below:

- Aadhaar may be used **as identification** and address evidence while applying for a passport.
- **Creating Bank Accounts**: By acting as a legitimate identity document, Aadhaar streamlines the procedure for creating bank accounts.
- **Digital Life Certificate**: With the help of Aadhaar, it is now simpler for retirees to demonstrate their identity and qualify for benefits.
- Aadhaar facilitates **the Jan Dhan Yojana's** implementation, a government programme designed to offer financial services to the unbanked people.
- **Provident fund** payments are distributed more easily because to Aadhaar, which also streamlines the procedure for workers.
- **LPG Subsidy**: By assuring targeted LPG Subsidy distribution and preventing benefit leakages, Aadhaar guarantees that benefits are received by qualified recipients.
- Aadhaar may be used to make safe and simple reservations **for train tickets.**
- **ATM Security**: By connecting biometric data to account access, Aadhaar-based authentication improves ATM security.
- **E-voting systems** may be made more effective and secure by integrating Aadhaar, ensuring a transparent election process.
- **Know Your Customer (KYC) services** based on Aadhaar offer speedy and paperless verification for a variety of purposes, such as mobile connections and financial transactions.

These uses demonstrate Aadhaar's adaptability and usefulness by facilitating easy access to a variety of services and benefits for people working in a variety of sectors.



II. RELATED WORK

- Vikas Sharma (ICDEOL) released a research in 2011 that looked at the advantages and difficulties of the development of Aadhaar [1]. Sharma claims that impoverished people who previously had trouble proving their identities to access government programmes and the public distribution system now have a huge edge because to Aadhaar.

- We consulted a 2012 report by Chakrabarty et al. to learn more about the necessity of Aadhaar [3]. This paper describes how Aadhaar was first suggested in 2006 as a way to provide Below Poverty Line (BPL) families a distinctive identifier. Offering vital services and creating a primary identity for individuals who were financially excluded were the main goals of this unique identification.

- Agrawal et al. [5] looked into the potential for authentication utilising the Aadhaar number and related database in 2015. They also suggested ways to strengthen Aadhaar's security, realising that its function as a single global identity left it susceptible to privacy violations. They emphasised the requirement to change Aadhaar's architecture in order to guarantee its security. A detailed use case study is also required in order to comprehend the unique needs of each application.

- A.K.R.S. Anusha and Dr. G. Rajkumar did a research in 2017 [6] that looked at the goals, advantages, and privacy and security concerns associated with the collecting, storage, and transfer of Aadhaar information. The article begins with an explanation of Aadhaar's advantages and applications before delving into the privacy and security issues related to the Aadhaar life cycle.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

These studies give insight on the importance of Aadhaar, its benefits, and the issues with privacy and security that it encounters. They help us comprehend Aadhaar's significance and the steps needed to guarantee its successful deployment.

A summary of the literature has been compiled in the following table:

References	Proposed	Findings	Limitations
Vikas Sharma(ICDEOL), 2011 [1]	The study examined the benefits and challenges of Aadhaar's invention, including its impact on identity verification, access to government schemes, and the public distribution system.	Aadhaar, despite its numerous benefits, encounters significant challenges during its implementation, particularly in the context of the Aadhaar-UID system.	The implementation of the Aadhaar-UID system presents various complexities and challenges.
Singh et al. 2017 [2]	Aadhaar card, its wide range of applications, and the case studies surrounding data privacy and information loss form crucial aspects of analysis.	The scope of Aadhaar extends to linking the Aadhaar card with various systems, enabling individuals to access a wide range of services and reap the associated benefits.	Implementing robust encryption, secure data storage, stringent access controls, multi-factor authentication, regular audits, user awareness, and strong legal frameworks can address security and privacy-related issues in Aadhaar.
Chakrabarty et al. 2012 [3]	Aadhaar was proposed in 2006 to provide a unique identification system for Below Poverty Line (BPL) families, enabling their access to government welfare schemes and services.	The UID system facilitates financial inclusion through easier access to financial services, transparency in transactions, fraud reduction, and targeted subsidy delivery.	Authentication methods for Aadhaar users include biometric verification (fingerprint or iris), OTP verification, and demographic authentication to ensure identity verification.
Raja et al. 2017 [4]	The Aadhaar card is a unique identification document that offers numerous advantages, and its potential and benefits are further amplified when linked to various systems,	The project's launch emphasized the interoperability of different e-governance functionalities, aiming to maximize the utilization of Information, Communication, and Technology Infrastructure.	Implementing regular security audits, robust encryption, enhanced access controls, user education, strengthened legal frameworks, and collaborative efforts to address loopholes in the existing system.

III. AADHAAR AUTHENTICATION

Aadhaar authentication entails providing the Central Identities Data Repository (CIDR) with the Aadhaar number and additional features, such as demographic information and biometrics, for verification. It is advised to visit UIDAI's official website [17] for a thorough explanation of the components involved in Aadhaar authentication.

A. **The Working Of Aadhaar Model :** The use of an open data format in XML and a widely used stateless service like HTTPS facilitates the acceptance and deployment of Aadhaar authentication. The Aadhaar authentication service uses the following URL format:
The Aadhaar authentication service uses the following URL format: https://auth.uidai.gov.in/2.5/public/uid[0]/uid[1]/asalk
When the UID is used, "uid[0]" and "uid[1]" stand in for the first two digits of the Aadhaar Number. Additionally, "asalk" designates a legitimate ASA licence key that is obtained following the device's successful registration. The aforementioned URL will be correctly encoded to handle special characters as a result.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

B. **Privacy Concerns Regarding Aadhaar :** The Aadhaar number itself is one of the main issues surrounding the Aadhaar system. Being a single, universal identification that is utilised across several domains, it becomes both technologically and linguistically accessible. The unrestricted accessibility of Aadhaar numbers can result in numerous privacy breaches, which poses serious privacy issues. Here are several instances when the Aadhaar system could violate users' privacy:

1. Unauthorised identification using a UID: Because Aadhaar numbers are so widely used, it is possible to identify or monitor people without their knowledge or permission. Unauthorised access to personal information may be obtained by organisations using the unique identifying number.

2. Identification without consent using biometric information: Aadhaar also uses biometric information for authentication, such as fingerprint and iris scans. If this private biometric data is handled improperly or accessed without authorization, it may result in serious privacy violations and possible exploitation of personal information.

3. Illegal tracking of people: Due to the centralised structure of Aadhaar and its widespread application across several businesses and industries, there are worries that people may be illegally tracked.

To guarantee the safety of people's personal information and sustain the integrity of the Aadhaar system, it is imperative to address and mitigate these privacy problems.

C. **Recommendations Of UIDAI :** The UIDAI advises AUAs to keep their unique IDs and the Aadhaar number mapped. Assuming no privacy violations, UIDAI does not actively retain such mappings. Due to the concerns of identity correlation and unconsented identification posed by this lax provision, domain connections are hampered. In order to guarantee safe mapping and reduce privacy issues, more stringent procedures should be put in place.

D. **Comparision Of Various Aadhaar Version :** With each new iteration of the Aadhaar project in India, the number of users has increased and security has been continuously enhanced. We will concentrate on the 1.5, 1.6, 2.0, and 2.5 versions in this comparison. For a thorough comparison of various versions as described above, please see Table II.

COMPARISON OF VERSIONS

Version 1.5 [8]	Version 1.6 [9]	Version 2.0 [10]	Version 2.5 [11]
Meta element was inside PID block.	Meta element outside PID block.	• New Aadhaar holder consent for authentication. •	• Incorporated BFD (Biometric Failure Detection) feature into core authentication.
Meta element was optional	The Meta element and its attributes have been made mandatory. This means that the presence of the Meta element and its associated attributes is required in the Aadhaar system.	The inclusion of these extra attributes enables seamless communication and interaction between registered devices and the Aadhaar ecosystem.	the usage of VID (Virtual ID) and UID token has been incorporated into the Aadhaar system.
Session is sent always.	By synchronizing the session key with advanced use cases, the Aadhaar system can provide tailored security measures and access controls for different scenarios, ensuring that the session key aligns with the specific needs and authorizations of advanced users or applications.	SSK scheme removed with introduction to registered devices.	Session key must not be stored anywhere except in memory and should not be reused across transactions.
Txn attribute , optional	Txn attribute made mandatory for better working of system	In version 3.0, there has been an enhancement to the Info attribute of the response in comparison to version 2.0.	Information attribute version changed to 4.0 from 3.0
PID block is prsent in XML	The binary Protobuf format	the session key encryption	Data element contains Pid

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

format	is an alternative to the XML format and offers advantages such as smaller file sizes and faster data processing.	for the PID (Personal Identity Data) has undergone changes.	element which is a base-64 encoded encrypted block.

Aadhaar Security

Aadhaar's success depends on ensuring safe deployment and usage. To secure the usage of this identification, the Unique Identification Authority of India (UIDAI) uses a strong authentication process. There are possible weaknesses that attackers may take advantage of along the entire procedure, from data collecting through authentication.
To uniquely identify people and retain their corresponding data, UIDAI uses biometric methods. Biometric signatures are essential for confirming identification and streamlining the authentication procedure. The Aadhaar system's security depends critically on the biometric system's integrity.

The Aadhaar biometric system has various security flaws, which are listed in reference [10]. If the precise vulnerabilities indicated in reference [10] are discovered, more information can be supplied.

E. **CIDR Security Challenge :** A substantial security risk arises from keeping all resident information in the CIDR, a section of the UIDAI database, in one place. Strong security measures are essential since the repository's centralised structure makes it a prime target for attackers.

F. **Collection Phase Security Challenge :** The registrar gathers enrollments from sub-registrars and intermediary agencies during the data collecting process and sends them to the CIDR. As several parties are engaged in data aggregation and transfer, this phase presents security concerns that need for secure processes and safeguards to maintain the integrity and confidentiality of the information gathered.

G. **Transition Phase Security Challenge :** The next step after gathering citizen data is to validate the information with the main database to check for duplicates. Each intermediary organisation must communicate with the CIDR as part of this procedure. Since there are the most possible attackers during the transmission period, it is particularly prone to attacks. During this stage, establishing secure communication routes and putting in place reliable encryption techniques become essential.

Storage Phase Security Challenge : Given the enormous quantity of sensitive information involved, securely keeping the Aadhaar data of 1.3 billion people creates a significant difficulty. The security of this extensive, sensitive data that is dispersed over several touchpoints around the nation must be managed by the authorities. To protect the security and integrity of the stored data, strict access restrictions, encryption, and disaster recovery procedures must be implemented.

V. BREACHES IN SECURITY AND MEASURES FOR SECURITY

The physical, data connection, and application layers make up the three levels of the Aadhaar ecosystem. To ensure safe transmission, user data used for Aadhaar enrolment is highly encrypted using 2048-bit PKI. It's crucial to keep in mind, though, that the infrastructure and application layers could be controlled and owned by other parties, posing security risks. Although UIDAI mandates that contracting parties employ network security measures, it might be difficult to guarantee system-wide compliance. The necessity for preventative measures has been highlighted by several security breaches that have been revealed in different publications and reports. The likelihood of cyberattacks grows as the nation's digital transition progresses. We gathered security occurrences in India from 2017 to 2018 and divided them into several subcategories of cyberattacks.

We advise the following precautionary actions to fight these strategic threats:

1. Using Channels For Communication Which Are Secured : : Because the data is so sensitive, it is essential to deploy a VPN during the transmission phase, preferably an SSL-VPN or an MPLS cloud.

2. Use Of HTST : Enforcing HTTPS connections before sending connection requests to CIDR/UIDAI servers prevents attackers from downgrading the connection to unencrypted HTTP, avoiding SSL stripping.

3. Securely Testing Biometrics Applications Which Are Enabled by Aadhaar : Biometric templates shouldn't be kept for user verification to avoid replacement attacks. By securely tying a cryptographic key to the biometric data, biometric encryption renders it difficult to obtain the key or biometric from the template that has been saved. Only when the proper live biometric

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

sample is given for verification does the key get produced.These precautionary actions can strengthen Aadhaar's security and shield it from any assaults and security breaches.

4. Preventing Black Hole Attacks : The black-hole assault is one kind of network attack that takes place at the network layer. In order to trick any node attempting to interact with another node, the black-hole node pretends to have the fastest route to the target node. AODV may be used to recognise and isolate single and cooperative black-hole assaults by including a lightweight approach that makes use of timers and baits, protecting the network from attackers and guaranteeing that information is not collected.

5. Isolation Of Insider Attacks : The UIDAI keeps track of encrypted transaction logs and the decryption keys that go with them. However, an insider attack may occur if these keys were altered and unlawfully accessed by recalculating HMAC without the database administrator's knowledge. An impartial third-party organisation can be chosen to protect the cryptographic keys in order to stop such assaults.

6. Isolation Of Data Using Biometrics : It is feasible to keep a non-invertible hash of the data to protect sensitive information, such as biometric data. This safeguard makes sure that the data cannot be copied or altered.

VI. POTENTIAL APPLICATIONS THAT INCORPORATE AADHAAR AS A FEATURE

We need technology-driven structural reforms in our government, corporations, and society as a whole for a number of important fields.

1. **Voting In Elections :** As those with registered biometric data cannot vote twice, the government introduced a programme in March 2015 that combines voter IDs with Aadhaar in an effort to combat voter fraud. Only if electronic voting is deployed might the cumbersome voter registration procedure be sped up by combining Aadhaar and voter ID. The whole voting procedure, including voter registration, address updates, polling booth information, and casting ballots, may be done entirely using smartphone applications once the Aadhaar connection is established. With the use of this national ID programme, voters will be able to cast their ballots using their mobile devices and may do so at any polling location nationwide, as opposed to being limited to predetermined polling places. Since Aadhaar numbers are given out starting at birth, the Aadhaar system may also be used as a tagging tool for newly eligible voters who turn eighteen, allowing the system to automatically designate them as eligible to vote.

2. **Pharmaceuticals & Healthcare :** Hospital chains' telemedicine services have replaced traditional patient contact methods, allowing medical professionals to communicate and diagnose patients who are located hundreds of kilometres away. However, because medical service providers rely on their own independent data storage systems that function independently, patient development cannot be successfully tracked within the present medical system. When several technological service providers follow a set of interoperability rules, the adoption of Electronic Medical Record Systems (EMRS) can be a low-cost and effective patient management solution. The Aadhaar number would act as a natural patient identity within these systems, allowing customers to choose vendors of their choosing and switch between service providers with ease. It is possible to use an Aadhaar-backed EMRS as a rich source of big data that can be analysed to spot public health trends, gather statistics, track disease outbreaks, and spot epidemics. However, the development of new legislative and regulatory organisations, such as a National Information Utility (NIU), would be required for the foundation of an EMRS. As an alternative, a National Health Information Network (NHIN) platform might be created, serving as the nation's main repository for health information. All participants might be enrolled in advance of the NHIN launch using an asynchronous approach. Similar to how Aadhaar-linked bank accounts are used to disperse government payments, the government may use the Aadhaar-linked NHIN to simplify health-related payments for individuals.

3. **Studies & Education :** The RTE Act mandates that 25 percent of the total enrollment capacity be set aside for pupils from economically disadvantaged backgrounds and that they be provided with free education up to the primary level in order to guarantee that they have access to education. A part of the money can be utilised to assist this programme by making school vouchers that poor children can use to pay their tuition at the school of their choosing. For schools and students, a central registration and platform for issuing vouchers may be made using the Aadhaar system. Students' Aadhaar numbers may be used to register in the system and to give vouchers tied to the students' Aadhaar numbers. Parents can then use these vouchers to enroll their child in a school of their choice. In the educational sector, Aadhaar can be a helpful tool in reducing entrance exam fraud. An illustration of this fraud is the "engine-and-bogey" scheme, in which a good student is requested to sit in the centre while the other pupils mimic them. Before students enter the test room, Aadhaar may be used to verify their identity, and seats can be assigned at random to stop fraud. Aadhaar might also be used to confirm academic credentials in order to avoid false resumes. Assuring

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2023)

Geetanjali Institute of Technical Studies

Vol. 10, Special Issue 2, May 2023

someone's educational credentials through the government's Digital Locker project and Aadhaar-based authentication helps build confidence between companies and job seekers.

4. **Toll Plazas :** The existing manual toll collecting method does not support the objective of creating a contemporary and effective road network and can cause traffic congestion and fuel waste. A nationwide electronic toll collecting system can be implemented to ensure a smooth flow of traffic during peak hours. Similar to how Aadhaar is used for identification verification, the FASTag gadget may be used to allow cashless payments through a prepaid account linked to it at toll plazas. The FASTag RFID-enabled toll collecting system functions similarly to the prepaid telecom paradigm. Real-time transactions, user registration, and tag distribution make up the system's three basic building blocks. FASTag tags require no ongoing charge or battery maintenance because they only need to be mounted to the windscreen of the vehicle once. The tags have circuit chips and antennae that are connected to prepaid accounts. At toll plazas, transceivers scan the QR code and tag identification number to deduct money from the user's account and top up the tag. The Central Electronic Toll System (CES), which links all players including the radio tag vendor, the user adding cash to the prepaid tag, and the toll manager, also sends an SMS with the transaction information to the tag owner. Initial toll collection with FASTags was between 20 and 22% of the total. But once it became required, the proportion rose to 60%. The objective of attaining 100% implementation has not yet been met. This may be done by automating the real-time data collection process with the use of appropriate analytics, which will assist in generating the desired financial returns. Additionally, it will help in analysing the origin and destination of cars and determining how often each type of vehicle is using the roadways.

5. **Power & Energy :** Traditional power generating methods including coal, gas, and to some extent nuclear power plants are significantly reliant on in our energy industry. The existing grid infrastructure, however, only permits a one-way movement of information and electricity from power plants to consumers, rendering it unable to handle supply complexity and ineffective in reversing energy flow. Establishing two-way channels that include renewable energy sources into the system and provide consumers more information about their energy consumption while keeping an eye on the networks is necessary to alter our energy landscape.
We can engage India's sizable unmetered population and stop fraudulent operations by keeping track of the electrical demand carried by each transformer by tying Aadhaar to power plant developments. By equally dispersing the load to other transformers when one transformer is overloaded, the use of smart grid technologies can offer early warning systems to save downtime. The government may be able to track the trends of power providers' energy production and consumption using Aadhaar identity verification. Smart grids are able to effectively balance consumer demand and supply in real time as a consequence. However, the deployment of such a system necessitates the use of appropriate analytics to automate the collection of data and provide the desired financial returns while evaluating highway utilisation rates for various vehicle groups.

6. **Courts and Jurisdiction :** It is challenging for people in India to get information and manage the course of legal processes due to the opaqueness of the court system. There are several ordinary procedures that may be completed without a judge's involvement, including creating documents, gathering evidence, and scheduling trials. Several technologically based judicial changes have been put forth, although they are still in the planning stages.

The creation of a National Judicial Network (NJN), which might supervise the creation of a platform for paperless justice, is one potential remedy. Documents can be digitalized and electronically tagged to enable smooth transfer between courts by utilising Aadhaar and e-KYC. A searchable system may then be used to upload the papers and proof, improving case monitoring and performance management. This centralised platform will enable participants to sign up at their own speed and access the information that is accessible, doing away with the requirement for a paper-based system and enhancing the paperless court system.

VII. CONCLUSION

When it comes to Aadhaar, ensuring security and privacy is crucial, especially because it is being used for numerous government applications and transactions. Every subsequent iteration of the Indian Aadhaar project is intended to be more secure than the one before it.

We have listed the four most recent iterations of Aadhaar in a table (Table II) so that you may compare them. Experts have proposed the creation of Aadhaar Coins, which may become India's own cryptocurrency, to further increase the security of Aadhaar. This is an intriguing concept that may be investigated later.

REFERENCES

[1] Sharma, Vikas. ”Aadhaar-a unique identification number: Opportunities and challenges ahead.” Research Cell: An International Journal ofEngineering Science 4.2 (2011): 169-176,April 2011.

[2] Raju, Raja Siddharth, Sukhdev Singh, and Kiran Khatter. ”Aad- haar Card: Challenges and Impact on Digital Transformation.” arXiv preprint arXiv:1708.05117, 2017.

[3] Chakrabarty, Nirmal Kumar. ”UID (Aadhaar)Its effect on financial inclusion.” The Management Accountant 47.1 (2012): 35-37.

[4] Raju, Raja Siddharth, Sukhdev Singh, and Kiran Khatter. ”Aad- haar Card: Challenges and Impact on Digital Transformation.” arXiv preprint arXiv:1708.05117 (2017).

[5] Sharma, Shweta Agrawal Subhashis Banerjee Subodh. ”Privacy and security of Aadhaar: a computer science perspective.” Economic and Political Weekly (2017).

[6] A.K.R.S.Anusha, Dr.G.Rajkumar.”International Journal for Research in Applied Science & Engineering Technology (IJRASET)” ISSN: 2321- 9653; IC Value: 45.98; SJ Impact Factor:6.887Volume 5 Issue VIII, August 2017.

[7] Sen, S., Patel, M., Sharma, A.K. (2021). Software Development Life Cycle Performance Analysis. In: Mathur, R., Gupta, C.P., Katewa, V., Jat, D.S., Yadav, N. (eds) Emerging Trends in Data Driven Computing and Communications. Studies in Autonomic, Data-driven and Industrial Computing. Springer, Singapore. https://doi.org/10.1007/978-981-16-3915-9_27

[8] Arpana Chaturvedi, Dr. Meenu Dave, Dr. Vinay Kumar,”Security Al- gorithms for Privacy Protection and Security in Aadhaar.”,InternationalJournal of Scientific Research in Computer Science, Engineering and Information Technology 2017 IJSRCSEIT — Volume 2 — Issue 6 — ISSN : 2456-3307 2017.

[9] UIDAI, Aadhaar Authentication API 1.5 Report, https://www.scribd.com/document/72124822/AadhaarAuthentication-API-1-5

[10] UIDAI,Aadhaar Authentication API 1.6 Report, https://authportal.uidai.gov.in/static/aadhaarauthentication api 1 6.pdf

[11] UIDAI,Aadhaar Authentication API 2.0 Report https://uidai.gov.in/images/FrontPageUpdates/aadhaar authentication