Information Security Audit and Assurance

Dashboard / My courses / Information Security Audit and Assurance / General / Announcements

/ Supreme Court's judgement on Aadhaar card

Search forums

Announcements

Supreme Court's judgement on Aadhaar card

Settings

◄ Plug and Play - A Security Point of View

Preference of Mode of End Sem Exam ►

Display replies in nested form

Supreme Court's judgement on Aadhaar card

by Sudipta Halder - Tuesday, 11 April 2023, 4:58 PM

1) Introduction

- In a 4:1 verdict, the Supreme Court has declared the Aadhaar Act, 2016, constitutionally valid.
- The five-judge bench ruled that the Aadhaar programme served the “larger public interest” in ensuring that the poor have access to resources.
- The court said, Aadhaar does not infringe on an individual's right to privacy.
- It found that the programme eliminated any chance of duplication and that enrolment was foolproof.
- The court, however, struck down several sections of the Act.

2) What do we need Aadhaar for?

- Aadhaar is mandatory to avail benefits of welfare schemes, to file Income Tax returns and it is mandatory to link Aadhaar with PAN cards.
- It is not mandatory to provide Aadhaar to open bank accounts, get SIM cards, or for services from private companies.
- Aadhaar is also not necessary for school admissions or NEET, UGC and CBSE examinations.
- For the enrolment of children under the Aadhaar Act, it would be essential to have the consent of their parents/guardian.
- On attaining the age of majority, such children with the consent of their parents, shall be given the right to exit from Aadhaar, if they so choose.

3) Supreme Court Verdict

- The SC has held the biometric-based identification programme, Aadhaar, to be constitutionally valid.
- It said, obtaining Aadhaar continues to remain voluntary.
- Concerns about privacy of personal data have been addressed.
- SC asked the Central government to introduce a robust data protection law as soon as possible based on the recommendations of the BN Srikrishna committee report.
- It retains the primacy of its use in distribution of subsidies and social welfare benefits to the poor.
- It stated that Aadhaar empowers the marginalised sections of society and gave them an identity and dignity.
- The court also noted that the failure rate of the scheme was just 0.232%.
- The remedy is to plug the loopholes rather than axe the project, the Bench said.
- SC felt that the technology has become a vital tool for ensuring good governance in a welfare state.
- The Majority Judgement upheld the passage of the Aadhaar Act as a Money Bill.
- SC has made exception for children saying that no child can be denied benefits of any scheme if he or she doesn’t have Aadhaar card.

4) Key Takeaways from the Judgement

- The verdict marks the end of any confusion regarding the services for which Aadhaar is mandated, and by whom.
- The Court has restored the original intent of the programme: to plug leakages in subsidy schemes and to have better targeting of welfare benefits.
- The judgment narrows the scope of Aadhaar but provides a framework within which it can work.

5) Impact

- Many businesses are likely to be affected adversely with the decision.
- With respect to access to welfare schemes, the question of exclusion and discrimination may be raised again.
- The cost of acquiring subscribers could go up for telecom companies and new connections may be delayed.
- Fintech start-ups, which built entire business models around Aadhaar may be hit.
- Could lead to rise in costs for banks, widen account opening timeline.

Permalink Edit Reply

Re: Supreme Court's judgement on Aadhaar card
by Karan Negi - Tuesday, 11 April 2023, 5:10 PM

Supreme Court Judgement On Aadhaar:
1. Companies can't store your digital data: The previous rule that required companies to archive Aadhaar-based transaction logs has been struck down, and they can't save your metadata either. The idea is to preserve your Right to Privacy, even if you choose to use an Aadhar-based payment system authenticated by your thumbprint.
2.Not mandatory for school admissions: "No child can be denied any schemes if they are not able to bring their Aadhaar number. For the enrollment of children, it would be essential to have the consent of parents. They should be given an option to exit on attaining majority. CBSE , NEET, UGC making Aadhaar mandatory is bad and they cannot do so," the SC said. Besides, no child can be denied benefits for want of Aadhaar. Children can also opt out of benefits of Aadhaar upon turning adults.
3.Mandatory for ITR and PAN: The apex court upheld linking of Aadhaar with PAN or Permanent Account Number, which is mandatory for filing of income tax return (ITR).

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card
by Kushal Shah - Tuesday, 11 April 2023, 5:25 PM

The Aadhaar scheme was challenged before the Supreme Court by Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court. He claimed that Aadhaar infringes upon fundamental rights guaranteed by the Constitution.
- The main concern was should the Aadhar system be allowed since many welfare benefits require mandatory Aadhar which may violate fundamental rights. As Entitlements granted to individuals by the State’s social sector schemes are themselves a fundamental right that cannot be limited for any reason, including the failure to produce an Aadhaar Card.
- Also, there is the issue of privacy since the government does not have any safeguards and any private entity may request authentication by Aadhaar for any reason subject to regulations by the UIDAI.

The Supreme Court Judgement on the Aadhar system is that the system is constitutionally valid and does not violate fundamental rights. Although an Aadhar card should not be mandatory for opening a bank account, getting a mobile number, school admissions, etc. Certain policies were also implemented regarding the safeguarding of Aadhar information as stated in other comments.

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card
by Shatrunjay Rawat - Thursday, 13 April 2023, 10:33 AM

Good to see this conversation. In light of the discussion in the class today, please identify key concerns related to use of Aadhaar Card:
1. Privacy (e.g tracking our activities?)
2. Misuse of the biometrics (e.g. replay attack?)
3. Any other risk involved (e.g. misusing it for unintended purpose?)

Let us identify specific issues and then come out with the mitigation strategy for them.

Regards,
Shatrunjay

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card
by Sandeep Misra - Thursday, 13 April 2023, 11:26 AM

One of the privacy issue that comes up with Aadhar is the possible usage of AI to track people. Since biometric data are available with the government, it is possible to track activities of suspicious individuals. This might be helpful with controlling criminal activities, but it can also affect the individual privacy and might give more power to the government.

As an example, Punjab Police is using Punjab Artificial Intelligence system that uses face recognition to catch criminals. They believe that the accuracy of their system will increase as a result of linking with Aadhaar data. A government funded program called the Crime and Criminal Tracking Network & Systems is also creating a biometric database of criminals nationwide and the program wants to integrate with the Aadhaar database so as to better identify criminals.

While all these technology can help curb criminal activities or better identify suspicious individuals, they can also impact the privacy of individual and give more power to the government to control its citizens. Moreover, AI based technology introduces bias. With a large nation-wide biometric data and biased AI, such tracking tool can be dangerous if not regulated thoroughly.

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card
by Sudipta Halder - Thursday, 13 April 2023, 9:57 PM

1. Privacy (e.g tracking our activities?)

- **Data breaches:**
  - In January 2018, the Tribune newspaper published an article by its reporter, Rachna Khaira, who claimed to have been able to purchase access to the Aadhaar database for just Rs 500 ($7) from a group of anonymous sellers on WhatsApp.
  - The sellers reportedly provided Khaira with login credentials that allowed her to access the personal information of individuals, including their names, addresses, phone numbers, and other sensitive data.
  - Khaira's article also claimed that the sellers were able to bypass the security features of the Aadhaar system, including the requirement for biometric authentication, by using software that exploited vulnerabilities in the system.
  - The article caused a public outcry over privacy concerns, with many individuals and organizations calling for stricter safeguards to protect citizens' personal information.
  - In response to the controversy, the Unique Identification Authority of India (UIDAI), which administers the Aadhaar system, denied the allegations of security breaches and claimed that the system was secure and foolproof.
  - However, the UIDAI also announced a series of measures to enhance the security of the Aadhaar system, including the introduction of a virtual ID system and the requirement for facial recognition authentication in certain cases.
  - The Tribune and its reporter faced legal action from the government for allegedly violating data privacy laws and publishing false information, but the case was later dropped following widespread public backlash and criticism of the government's actions.
- **Misuse of Aadhaar data:** In one instance, a man from Jharkhand was able to obtain 14 SIM cards using different Aadhaar numbers, which he then used to run a call center scam. Similarly, there have been instances of fraudsters opening bank accounts in the name of unsuspecting individuals using their Aadhaar data. In such cases, the victims may not even be aware that their Aadhaar data has been misused until it is too late.
- **Linking of Aadhaar with various services:** The government has made it mandatory to link Aadhaar with various services, including bank accounts, mobile phones, and PAN cards. This has led to concerns about the government having access to individuals' personal information and activities. For example, if an individual's bank account is linked to Aadhaar, the government could potentially track their financial transactions.
- **Lack of proper regulation:** In the past, there have been reports of companies using Aadhaar data without proper authorization or consent. For example, in 2017, it was reported that a private company had created an app that allowed businesses to verify the authenticity of Aadhaar numbers, and in doing so, collected personal information of millions of Indian citizens without their consent.

2. Misuse of the biometrics (e.g. replay attack?)

- **Identity theft:** Aadhaar biometric data can be used by an attacker to steal an individual's identity. For example, an attacker could use a high-quality photograph of an individual's face to create a fake identity document, which they could use to open bank accounts or obtain loans in the individual's name.
- **Biometric data theft:** Biometric data collected for Aadhaar can be stolen through various means, such as hacking, phishing, or physical theft. Once an attacker has access to an individual's biometric data, they could use it to impersonate the individual or conduct fraudulent activities.
- **Social engineering attacks:** Attackers can use Aadhaar biometric data to conduct social engineering attacks, where they manipulate individuals into divulging sensitive information or performing actions that could compromise their

security. For example, an attacker could impersonate a government official and use an individual's Aadhaar biometric data to gain their trust and obtain access to their personal information.

- **Biometric data profiling:** Private companies could use Aadhaar biometric data to create profiles of individuals based on their physical characteristics, such as ethnicity, age, or gender. Such profiling could lead to discrimination and violation of individuals' privacy.
- **Biometric data surveillance:** Governments or private companies could use Aadhaar biometric data to conduct mass surveillance, monitoring individuals' movements and activities without their knowledge or consent.

3. Any other risk involved (e.g. misusing it for unintended purpose?)

- **Privacy violations:** While Aadhaar is intended to provide a secure and convenient form of identification, it can also lead to privacy violations if not properly managed. For example, the government or other entities may use Aadhaar information to track an individual's activities, monitor their communications, or access their personal information without their knowledge or consent.
- **Discrimination:** In some cases, Aadhaar may be used to discriminate against individuals based on their demographic or socioeconomic status. For example, an employer may require an Aadhaar card for employment, which could disproportionately impact low-income individuals or those living in rural areas who may not have access to the necessary documentation.
- **Exclusion:** The use of Aadhaar for access to government services and benefits can also lead to exclusion of certain segments of the population who may not have an Aadhaar card or may have difficulty obtaining one. This can include marginalized communities such as the homeless, migrant workers, and refugees.
- **Misuse of data by private entities:** Private companies may also misuse Aadhaar data for unintended purposes, such as targeted advertising or profiling. For example, a company may use Aadhaar data to link an individual's identity to their online browsing behavior or purchase history, leading to potential privacy violations and manipulation.
- **Cybersecurity risks:** As Aadhaar information is stored in digital form, there is always a risk of cyber attacks and data breaches. Any breach of Aadhaar information could lead to identity theft, financial fraud, and other types of cybercrime.

4. Mitigation

- **Limited sharing:** Individuals should limit sharing of their Aadhaar card details with third-party entities and only share it with trusted and authorized entities. For example, Aadhaar details should not be shared with telemarketers or unknown entities that request it over the phone or through email.
- **Two-factor authentication:** Aadhaar transactions should be authenticated using two-factor authentication (2FA) or multi-factor authentication (MFA). For example, a transaction could be authenticated using biometric verification along with a One-Time Password (OTP) sent to the user's registered mobile number.
- **Biometric lock:** The Unique Identification Authority of India (UIDAI) provides the option to lock an individual's biometric information, which prevents any unauthorized access or use of biometric data for authentication purposes. Here is the link to do so. https://uidai.gov.in/en/contact-support/have-any-question/925-english-uk/faqs/aadhaar-online-services/biometric-lock-unlock.html
- **Strong encryption and security measures:** Aadhaar data should be encrypted both at rest and in transit to prevent unauthorized access or interception. Additionally, Aadhaar databases should be secured with strong access controls and firewalls to prevent data breaches.
- **Regular security updates:** Aadhaar systems should be regularly updated with the latest security patches and upgrades to prevent vulnerabilities that could be exploited by attackers.
- **Awareness and education:** Individuals should be made aware of the privacy risks associated with Aadhaar usage and educated on how to protect their privacy and security. For example, users should be advised not to share their Aadhaar details with unauthorized entities and to be cautious of phishing scams that seek to obtain their Aadhaar details.
- **Legal protections:** There should be legal protections in place to prevent misuse of Aadhaar data and to hold accountable those who do misuse it. For example, there should be penalties for unauthorized access or misuse of Aadhaar data.

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card

by Hari U M - Thursday, 13 April 2023, 10:21 PM

https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/

Privacy: There are concerns that the vast amount of personal data collected through the Aadhaar program could be misused for government surveillance or other purposes beyond service delivery. There is also a risk that the biometric information collected could be used to track individuals' activities and movements, potentially violating their privacy.

Misuse of Biometrics: The biometric information collected through the Aadhaar program could be vulnerable to misuse, such as in a replay attack, where an attacker replays a previously captured biometric identifier to gain unauthorized access to a system or service.

Other Risks: The article highlights other risks related to the Aadhaar system, including the use of outdated software, the potential for insider threats, and the possibility of identity theft or fraud. These risks could undermine the credibility of the Aadhaar system and erode public trust in the government's ability to secure personal information.

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card
by Aaradhana Patnaik - Friday, 14 April 2023, 10:39 AM

There have been cases where biometric information of individuals have been misused. Aadhaar Enabled Payment System (AePS) was introduced to ease payment and other transactions using Aadhaar-based verification but the same technology has been misused by cyber criminals to perform fraudulent activities.

In many cases, it is not completely known how the cybercriminals were able to get access to biometric information of individuals in the first place. Here is one such example: https://www.hindustantimes.com/cities/gurugram-news/gurugram-man-s-aadhaar-data-fraudulently-used-to-withdraw-cash-101672684317206.html

In one case, the accused were registered as CSCs (Common Service Centres) for e-governance services through municipalities and villages. They used equipment to clone fingerprints of individuals and then withdraw money using AePS. More about this can be found here:
https://timesofindia.indiatimes.com/city/bhopal/4-arrested-for-cloning-fingerprints-in-aadhaar-payments-fraud/articleshow/91386924.cms

As a preventive measure, UIDAI provides the option to lock the biometric information of individuals. Locking biometric information prevents unauthorised access or use of biometric data for authentication purposes. It ensures that any entity by any means cannot perform biometric based Aadhaar authentication for that Aadhaar holder. Once resident enables Biometric remains locked till the Aadhaar Holder chooses to unlock it (temporarily) or disable the locking system.

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card
by Vishal Pawar - Friday, 14 April 2023, 11:25 AM

Various Reported Misuses of Aadhaar :-
Intermediary associated crimes:-
A large chunk of organized Aadhaar related crimes include misappropriation by private intermediaries with some authority or experience of collecting or processing Aadhaar related data. In 2018, an India Today TV undercover investigation revealed that enrolment agencies were willing to sell private data of thousands of Aadhaar applicants for merely Rs 2.

Such data could be used to conduct further financial and criminal crimes. The Crime Branch of the Mumbai Police busted a gang that operated out of a bank branch in Borivali West. Using their access at the Aadhaar card counter of the bank, the operatives created fake Aadhaar cards.

Criminal and Terrorism Related Cases :-
In recent times, several incidents of fake Aadhaar cards being used in terrorism and grave criminal cases have been reported.

Terrorist operatives of Pakistan-based terrorist outfit Jaish-E-Mohammad (JeM) and Lashkar-E-Taiyaba (LeT) operating in Jammu and Kashmir have been found in possession of fake aadhaar cards.
Such fake IDs are usually created by digital forgery of genuine Aadhaar cards collected from various sources.

In a widely reported case, arrested Mumbai Police cop Sachin Vaze had used a fake Aadhaar card to check in at a posh hotel in Mumbai.

Some other known cases of misuse of Aadhaar :-
In January 2018, eight persons were arrested in Chandigarh for purchasing expensive mobile phones with fraudulent loans secured using fake Aadhaar cards. The accused, among whom were former bankers and employees of a finance company, had placed their own photographs on others' Aadhaar cards to secure bank loans, and were booked for cheating, fraud, forgery and criminal conspiracy under the relevant sections of the Indian Penal Code.
This is just one among the 73 incidents of misuse of the Unique Identity Authority of India's (UIDAI) Aadhaar programme that have been reported in the English-language media so far this year (up to 7 May, 2018). This averages nearly four incidents each week, as per a new database created by independent researchers Anmol Somanchi and Vipul Paikra.

Aadhaar data combined with a person’s other details such as name, pin code, date of birth, phone number etc. has been used in extracting more personal data from Aadhaar related services such as hotel and travel reservations.

A genuine copy of a person's Aadhaar data could be exploited to avail some private services associated with Aadhaar that do not require a second degree of verification.

As of April 2018, more than 1.2 billion Indians–99.7% of the population–had enrolled under the programme. The Aadhaar database, which the government is keen to integrate with policy, regulation and benefits-transfer programmes, includes fingerprints, iris scans and demographic details of every enrolled individual. From 1 July, 2018, the system will also include facial recognition features for identity authentication.

Year-Wise Aadhaar Enrolment And Cases Of Fake Or Fraud Aadhaar Reported

Year	**Citizens Enrolled (Cumulative)**	**Reported Incidents Of Aadhaar Misuse**
2011	**100 million**	
2012	**210 million**	**3**
2013	**510 million**	**1**
2014	**720 million**	**4**
2015	**930 million**	**6**
2016	**1.11 billion**	**13**
2017	**1.18 billion**	**65**
2018*	**1.21 billion**	**73**

Source: Unique Identity Authority of India; Somanchi & Paikra’s database of media reports on Aadhaar-related forgery, counterfeit and fraud
Note: *Data as of May 2018

Appropriating of Aadhaar is punishable with penalties

- Under the Aadhaar Act, 2016, providing false demographic or biometric information is a punishable offence with jail term imprisonment up to three years or a fine of Rs 10,000 or both.
- Pretending to be an agency or intermediary authorized to collect data of individuals is punishable with a jail term for three years and a fine of Rs 10,000 for a person, and Rs 1 lakh for a company.
- Unauthorized transfer of Aadhaar related data is also a punishable crime with imprisonment for three years and fine of Rs 10,000 for individuals, and Rs 1 lakh for a company.
- Unauthorized access to the central identities data repository (CIDR) is punishable with a maximum jail term of 10 years and a fine of Rs 10 Lakhs.

Steps to taken in case of misuse of Aadhaar :-

If you suspect that your Aadhaar number is being misused, then you can check it online from your home by visiting the official website of the Unique Identification Authority of India (UIDAI). You are not charged any fee for this.

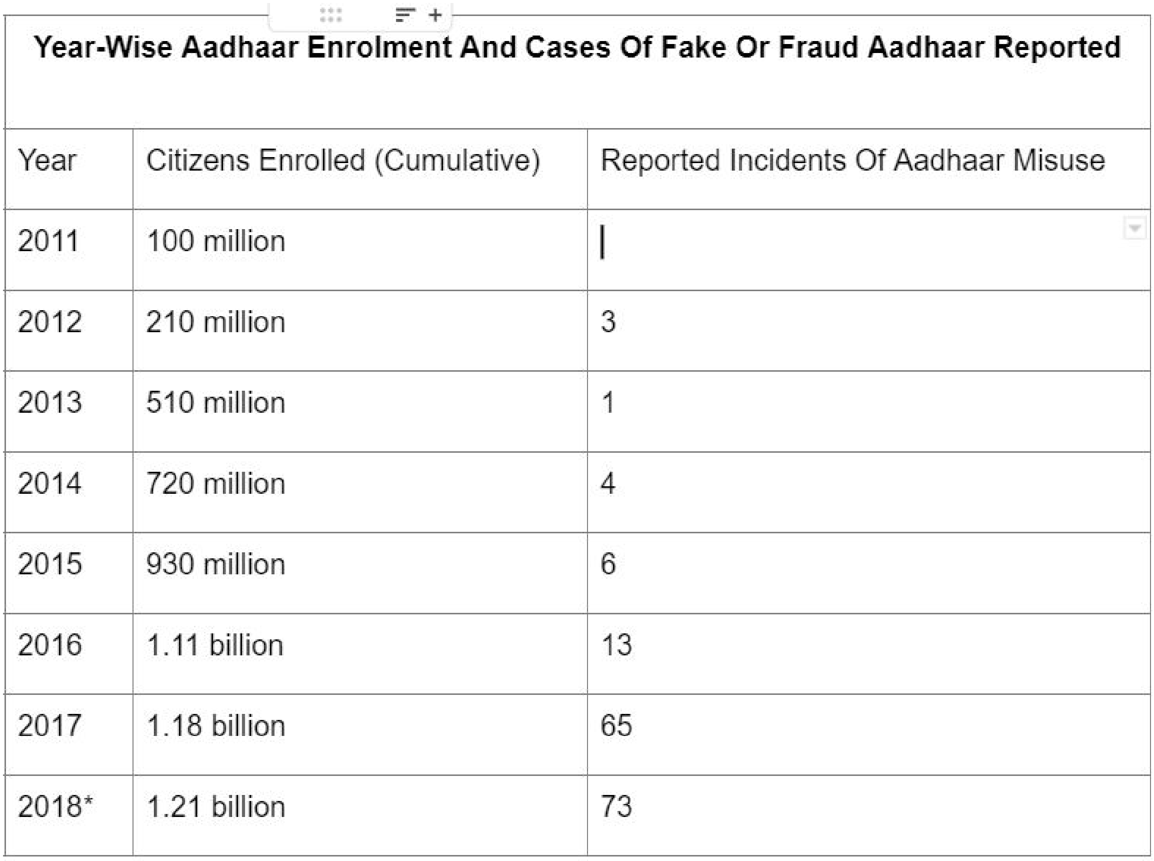
Here is its process

- First of all, you have to go to the Aadhar website or this link uidai.gov.in/.
- Here you will find the option of Aadhaar Authentication History at the bottom of Aadhaar Services, click on it.
- Here you have to enter the Aadhar number and the security code as seen and click on Send OTP.
- After this an OTP will be sent on the registered mobile number (RMN) linked with Aadhaar, enter this OTP and click on submit.
- After this, you have to fill all the information asked including authentication type, date range, and OTP. (Note- You can view data for up to 6 months)
- By clicking on Verify OTP, a list will appear in front of you, in which information will be given about when and where Aadhaar was used in the last 6 months.
- Complain about wrong use
- On seeing the records, if you suspect that the Aadhar card has been misused, you can immediately file a complaint. You can register a complaint by calling the toll-free number 1947 or sending an email to help@uidai.gov.in or lodge a complaint online at https://resident.uidai.gov.in/file-complaint link.

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card

by Vishal Pawar - Friday, 14 April 2023, 11:30 AM



Year-Wise Aadhaar Enrolment And Cases Of Fake Or Fraud Aadhaar Reported

Year	Citizens Enrolled (Cumulative)	Reported Incidents Of Aadhaar Misuse
2011	100 million	
2012	210 million	3
2013	510 million	1
2014	720 million	4
2015	930 million	6
2016	1.11 billion	13
2017	1.18 billion	65
2018*	1.21 billion	73

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card

by Mainak Dhara - Friday, 14 April 2023, 10:42 PM

An article about previous data breaches -
https://medium.com/@rithikvgopal/aadhaar-data-breach-how-sensitive-data-of-1-3-billion-indians-was-compromised-cb01d0c2d7d3
According to the article, the breach exposed sensitive information such as names, addresses, Aadhaar numbers, and biometric data of Indian citizens. This information can be misused for identity theft, financial fraud, and other illegal activities. The breach highlights the need for strong data protection measures and oversight of third-party service providers who handle Aadhaar data.

To mitigate the risks associated with privacy,replay attacks and other possible misuses we can take the following mitigation strategies -
To avoid unauthorized access, Aadhaar Card biometric data should be encrypted both during transmission and storage.
Multi-factor authentication, such as a combination of biometrics and a one-time password (OTP), should be required for Aadhaar Card authentication, making it more difficult for attackers to replay the data.
Aadhaar Card authentication and data retrieval can also be made time-bound, which means that a fresh authentication request is necessary after a set period of time. This can prevent attackers from repeatedly replaying the same data to obtain access to a sensitive system.
To prevent exploitation of the Aadhaar Card, the government should set clear norms and restrictions about its allowed applications.Citizens should also be made aware of the intended purpose of their Aadhaar Card, as well as their rights to regulate how their data is used, so that they do not supply sensitive information to fraudulent individuals.
Regular audits and vulnerability assessments should be conducted to identify and address any security weaknesses in the Aadhaar Card system.

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card

by Sourav Singh - Thursday, 13 April 2023, 10:56 AM

Privacy Concerns:
Privacy is a major concern when it comes to Aadhaar Card, as the unique identification number assigned to each cardholder can potentially be used to track their activities. To mitigate this risk, the government has implemented several measures to ensure the security and privacy of Aadhaar data.

Firstly, strict access controls are in place to limit access to Aadhaar data to authorized entities only. Only those who have a legitimate reason to access Aadhaar data, such as government agencies and financial institutions, are granted access. Additionally, access is restricted to only the necessary fields of data, and access logs are maintained to track who accessed the data and when.

Secondly, Aadhaar data is stored in an encrypted form to prevent unauthorized access. The encryption used is of a high standard, making it difficult for hackers to decode and access the data.

Finally, regular audits of the Aadhaar database are conducted to identify and fix any potential security vulnerabilities. This helps to ensure that the data is secure and not at risk of being breached.

Cardholders can also take steps to protect their privacy, such as limiting the sharing of their Aadhaar number and only providing it to authorized entities. They should also be cautious when giving out personal information and verify the identity of the entity requesting their Aadhaar data.

Misuse of Biometrics:
Another concern related to Aadhaar Card is the potential misuse of biometric information, such as fingerprints and iris scans. This information could potentially be stolen by hackers and used for identity theft or financial fraud. To mitigate this risk, the government has implemented several measures to safeguard biometric data.

Firstly, biometric data is stored in an encrypted form to prevent unauthorized access. Access to biometric data is also restricted to authorized entities only.

Secondly, the authentication process for Aadhaar Card involves the use of multiple factors, including biometric and OTP (one-time password) authentication. This helps to ensure that biometric information cannot be used alone to authenticate an individual.

Finally, the government has implemented strict security protocols to prevent replay attacks, where a hacker intercepts biometric data and uses it to authenticate themselves. To prevent this, the authentication process includes a time stamp and a unique transaction ID, making it difficult to use intercepted data for authentication purposes.

Cardholders can also take steps to protect their biometric data, such as keeping their Aadhaar Card safe and not sharing their biometric data with anyone except authorized agencies. They should also report any suspicious activity related to their biometric data to the relevant authorities.

Permalink Show parent Reply

Re: Supreme Court's judgement on Aadhaar card

by Mayur Kumar - Thursday, 13 April 2023, 11:28 AM

While there have not been any recent incidents of data breaches related to Aadhaar, but there have been such incidents in the past. One example is from January 2018, when a writer for The Tribune newspaper claimed that she had obtained access to the entire Aadhaar database through anonymous WhatsApp buyers for a fee of Rs. 500. Here is the link for the same. These buyers claimed that they could provide access to any Aadhaar number and associated personal and biometric information. Initially, the UIDAI denied the breach, stating that the journalist's allegations were unfounded. However, they eventually acknowledged the breach and filed a police report against the WhatsApp dealers. This breach exposed sensitive information, including names, addresses, phone numbers, Aadhaar numbers, and biometric data like fingerprints and iris scans.

In regards to the possibility of a replay attack using Aadhaar biometric data, for example, if a person uses their Aadhaar biometric data to verify their identity in order to access their bank account, the attacker may be able to replay the authentication process using the recorded biometric data in order to access the person's bank account and carry out fraudulent transactions.

Permalink Show parent Reply

◄ Plug and Play - A Security Point of View

Preference of Mode of End Sem Exam ►

Jump to... ⬍

Attendance ►