

Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 12
Lecture: 35

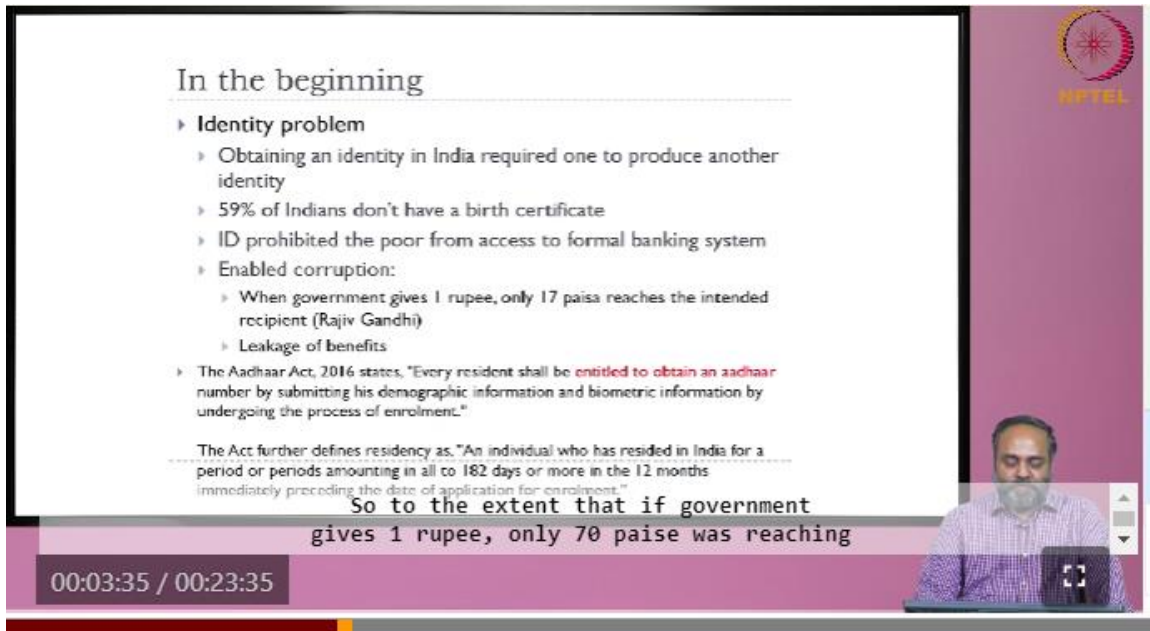
So, one thing that we should discuss is, no person in the country may be deprived of his life for personal liberty except according to procedure established by law. So, Aadhaar as a government initiative, as a government established entity, you need Unique Identification Authority of India, right. That is the particular entity, government agency which is in charge of the Aadhaar database or Aadhaar data collection and Aadhaar database. So is it according to the procedure established by the law? The answer is yes, we do not have to debate because there was an Aadhaar Act before Aadhaar actually came into existence, government actually had to pass an act in the parliament called Aadhaar Act. So, it is actually legal, government can collect this data. So now as you said what is the context in which government actually, so government's role is to govern and government's role is welfare of people.

Government is the guardian of the assets of the country and therefore government needs to do its job and at the same time it has to protect privacy also. So in India, as India was becoming increasingly digital or e-government initiatives began, so it actually, whether it was the current government or government ruled by another political party, it does not matter. All governments actually started exploring the potential of information technology. You can see the IRCTC today, right, the making the railways, railway reservation online was a major initiative by the Indian Government.

So from government to government, the government tapped into the potential of digital technologies and that benefited people and a huge reduction in information asymmetry and corruption. Often corruption stems from asymmetry of information between two agents. The information that you have, if you go to a clerk, you know whether there is a seat available or not, we are just dependent on what the clerk says because we cannot access that information. There is an asymmetry of information, that is what actually digital technologies actually address, you know it removes the asymmetry between actors. So because of that, so in almost in line with that, there is an identity problem and corruption was prevalent in India because an Indian citizen could have multiple identities and there is no unique identity.

And therefore since you can actually get these identities, multiple identities in different places, for example you can have a ration card potentially in Tamil Nadu, one in Kerala

and one in Uttar Pradesh or Bihar. So it is, today it may not be possible as unique identification actually is referred to but if you go back to, say 15 years ago, it is quite possible. Similarly voter IDs. So that actually was identified or assessed as a major issue. So to the extent that if government gives 1 rupee, only 70 paise was reaching the actual targeted recipient, intended recipient and that is called leakage by economists.



The screenshot shows a slide from an NPTEL video lecture. The slide title is "In the beginning". It contains a list of bullet points under the heading "Identity problem". The bullet points are: "Obtaining an identity in India required one to produce another identity", "59% of Indians don't have a birth certificate", "ID prohibited the poor from access to formal banking system", and "Enabled corruption:". Under "Enabled corruption:", there are two sub-bullets: "When government gives 1 rupee, only 17 paise reaches the intended recipient (Rajiv Gandhi)" and "Leakage of benefits". Below the list, there is a quote from the Aadhaar Act, 2016: "Every resident shall be entitled to obtain an aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment." Below the quote, there is a definition of residency: "The Act further defines residency as: 'An individual who has resided in India for a period or periods amounting in all to 182 days or more in the 12 months immediately preceding the date of application for enrolment.'" At the bottom of the slide, there is a line of text: "So to the extent that if government gives 1 rupee, only 70 paise was reaching". The NPTEL logo is in the top right corner. A video player interface is visible at the bottom, showing a timestamp of 00:03:35 / 00:23:35 and a small video window showing a man speaking.

In the beginning

- › Identity problem
 - › Obtaining an identity in India required one to produce another identity
 - › 59% of Indians don't have a birth certificate
 - › ID prohibited the poor from access to formal banking system
 - › Enabled corruption:
 - › When government gives 1 rupee, only 17 paise reaches the intended recipient (Rajiv Gandhi)
 - › Leakage of benefits
 - › The Aadhaar Act, 2016 states, "Every resident shall be entitled to obtain an aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment."

The Act further defines residency as: "An individual who has resided in India for a period or periods amounting in all to 182 days or more in the 12 months immediately preceding the date of application for enrolment."

So to the extent that if government gives 1 rupee, only 70 paise was reaching

00:03:35 / 00:23:35

So government wanted to address this problem by creating a unique ID which is a very valid, very rational approach to addressing this problem. So the country is facing a major issue in terms of corruption, in terms of not able to deliver its services effectively and efficiently. Both effectiveness as well as efficiency comes into picture here and therefore, the Aadhaar initiative from government to government. So we do not have to say it is the idea of one government, one political party or the other but country as a whole understood that there is a need for this. So you know who actually headed this initiative.

This is actually headed by the, one of the well-known IT gurus of our country, Nandan Nilekani who came from Infosys and was given the charge of leading the Aadhaar initiative and he has written two books on this. I read one of the books and I am just giving some excerpts from this book and it is a really good collection of experiences leading a mega project, a big project like Aadhaar in our country. And one has to function cutting across political parties, across the ruling party and the opposition to get something of this scale done and at the same time, technology has to be very robust and very reliable to collect and store data pertaining to more than a billion people. Amidst the oppositions and concerns and privacy as a fundamental right and all this but the Aadhaar project had

to move on. So you all know that the 12 digit Aadhaar is a unique identification for every individual and it is world's largest ID system and it makes every Aadhaar record unique because it, if you go second time to get one more Aadhaar, you know it is simply not possible because of the, because of the way the application is built and the comparisons it makes before it accepts a ID and it is built as a platform you know.

So if you read the book, you will understand the concept of platform here. So it is basically a database and it is so, this is a database on which applications could be built or other participants could actually connect and build more. So the concept of platform, you know you call Facebook a platform because it is not just one player, it is not just one category of participants, there are multiple categories of participants. So platform is a base on which different types of people can connect and give inputs and also take benefits. So like the Google, right, the advertisers and the users and the Google as a platform provider.

So their interests are very different but the platform unites them. So Aadhaar is a database, is a platform which unite the interest or which synchronizes or orchestrates in other word, in the language of music. So he would assert that minimum data should be collected, not the demographic data of individuals, only the basic identification data that is required. So at the collection itself, it is following a very minimalist approach. Yeah, just I referred Machiavellian, I am sure some of you have read, The Prince.

I suggest this book for all managers because to appreciate the complexity of politics, the real world. So there are good kings and bad kings but all are kings. So you rule based on whatever principles you follow. And then ultimately if you have to survive and be a king, you have to follow certain rational guidelines in political science. So Machiavellian is one, of course we are more familiar with Chanakya of our country.

But it is a small book. You can actually read when you are traveling, The Prince. So I was giving the context of Aadhaar because it is very much tied to our privacy. So why privacy became an issue? Because government needed to collect data, personal data of citizens and store it in a single database. And that is required by the government.

Now the questions are, can it be made mandatory for government services? Well, that is where actually the Aadhaar was challenged in the court and the debate was public and finally Supreme Court actually restricted where Aadhaar can be used and where Aadhaar should not be made mandatory. I do not have that list with me but you can see that certain fundamental services you do not need to have Aadhaar, you can provide other identities as well. Taking into consideration, well nothing should be made so absolute to get basic services of the government. But if you have to get a cell phone or the wireless service today, you need an Aadhaar. So that is, sort of you know, a service if you need, you can

provide your data if you do not need, you can sit at home.

And similarly for many services, private services like banking, insurance, in so many areas, Aadhaar actually becomes a unique identifier and as soon as you share your Aadhaar ID as privacy aware people, we also know that we are sharing a unique ID with them. So potential for misuse does exist. And so the other debate which engaged our country over the past few years, I would say from 2015 and it is still going on because it has the PDP has not, DPDP has not become a law yet. So if the debate is still on how safe or how secure is the Aadhaar database? What is the guarantee that the data will not pass or data will not be leaked in the system or in the architecture that is built for Aadhaar database? So when this question was asked to Gulshan Rai, India's Cybersecurity Chief, he sometime back answered that Aadhaar biometric data is 100 percent secure and there is a 10 foot wall. I think the data center is in Haryana, that is what I read.

So in terms of the infrastructure, it is very well secured, that was the claim made by the government or the government agency. But is that okay? The 10 foot wall will protect the data. That looks like a little trivial but there should be some reason why he made that statement. He is a techie, he is a technical person. Yeah, it is about building a 11 foot ladder, good answer, yeah.

The diagram, titled "Aadhaar data architecture", illustrates the following components and their interactions:

- Aadhaar User**: Initiates an **Authenticated Request** (1) to **Authentication Devices**.
- Authentication Devices**: Send **AUA Specific Communication** (2) to the **AUA**.
- AUA** (Authentication User Agency): Communicates with the **ASA** (Authentication Service Agency) via **ASA Communication** (3).
- ASA**: Interacts with the **ASA Repository** (Data Repository) to receive a **YES/NO Response** (5).
- ASA**: Sends a **YES/NO Response** (4) back to the **AUA**.
- AUA**: Provides **Updates and Confirmations** (6) to the **Authentication Devices**.
- Authentication Devices**: Deliver **Service Delivery** (7) to the **Aadhaar User**.
- UIDAI+CIDR** (Central Identities Data Repository) is also shown as a component in the architecture.

Legend:
AUA: Authentication User Agency
ASA: Authentication Service Agency
CIDR: Central Identities Data Repository

So my research had policy implications.

00:12:31 / 00:23:35

But that is not the, that is not the real point but it was so, he made a statement about the physical security. And this is a cartoon that subsequently appeared in the Hindu, Keshav's cartoon. So it is very secure from the front but seems to be, the back door seems to be open. So you have heard that saying - No chain is stronger than its weakest link. No chain is stronger than its weakest link.

So a chain, if there are 100 chains, 99 maybe very strong but one weak link is enough to break the chain. So that is why I shared that paper, research paper written by, I guess three scholars from IIT Delhi, Computer Science department. So they published this paper and I was very heartened to see that Justice Sri Krishna commission referred this research paper in the draft bill. If I am a researcher I will, that will be one of the finest moments for me because a policy, a policy refers my research. So my research had policy implications.

So you can see that paper in the footnotes. When I was reading the document, I found this paper. So that is why it is giving, given us a reading reference. So it, they actually discusses the the weaknesses in the Aadhar system. But I am not sure if Aadhar data ever got leaked from the database.

But the architecture is like this. You can see how it is depicted in the paper, Aadhar data architecture. So you can actually see there are, it basically has three constituents. So this is the central identities data repository or the Aadhar database.

Aadhar data resides here. This is the data center around which there is a 10 foot wall. So that is the database in a data center. But how can access be made? Even if you jump into the data center, you cannot actually collect anything and go because it is digital. So that makes, the whole thing does not make any sense. But the point is, there are, the access to this database is through a layered architecture.

So there are multiple layers. You can see that there is an ASA layer which is called authentication service agency. The second layer below the database is the AUA layer which is the authentication user agency. And then comes the authentication devices. It could be the fingerprint readers or any device that is used to sort of collect data about the user. Finally it is a user here who actually wants a service.

Suppose you go for your passport renewal or you go for a new SIM card. So you are the user here. Whom you go to? You go to and you go to a service provider. It could be a Jio or a Airtel or Idea service center that you go.

And then you want a service. So the service center possesses, of course the authentication device. So what they want is that, they want to authenticate. We discussed what is authentication. You claim that you are someone. And what is that claim? How you make that claim? Of course, you have to disclose your ID.

In the case of Aadhaar identification, the ID is your 12 digit number. The 3 into 4, 12

digit number. You have to disclose, then you claim this is my ID. You have made a claim and they have to authenticate you are the one whom you claim to be.

So place your fingertip, fingerprints. So that is the authentication device. And in this case the telecom service provider is the AUA, authentication user agency. So using the device, using the fingerprint reader this device can access the Aadhaar database through another layer called ASA repository. ASA repository is having the direct link, digital link. It could be through a wired link with the database.

So this particular agent actually is between the AUA, the service provider, the user service provider, be it a bank, be it a telecom service provider or passport service. That is where the service actually gets provided to the user. But if the access is made through an ASA repository which is actually at the technical part of it. So there are ASA vendors also with, which are enlisted with, enlisted and approved. If you claim to be someone with an ASA expertise, being able to connect data access services then you have to actually provide your credentials and get enlisted with UIDAI.

And the UIDAI or the Aadhaar has disclosed in public domain who are the ASA providers. All telecom service providers are also ASA providers. They have the network to connect with the, with the Aadhaar database. BSNL is of course one and NIC is one. So they are all approved service providers for providing connectivity to the Aadhaar database.

And then the core database. That is how the architecture of Aadhaar is. Now looking at this architecture, this is of course 10 feet, huge infrastructure and maybe they have the secured database, very secured database. We discussed security, security by encryption. So it is maybe very difficult to actually tap into this database by interception. But what would you think are the weak links in the chain, seeing it as a chain? Who? Some rogue or malicious service entity.

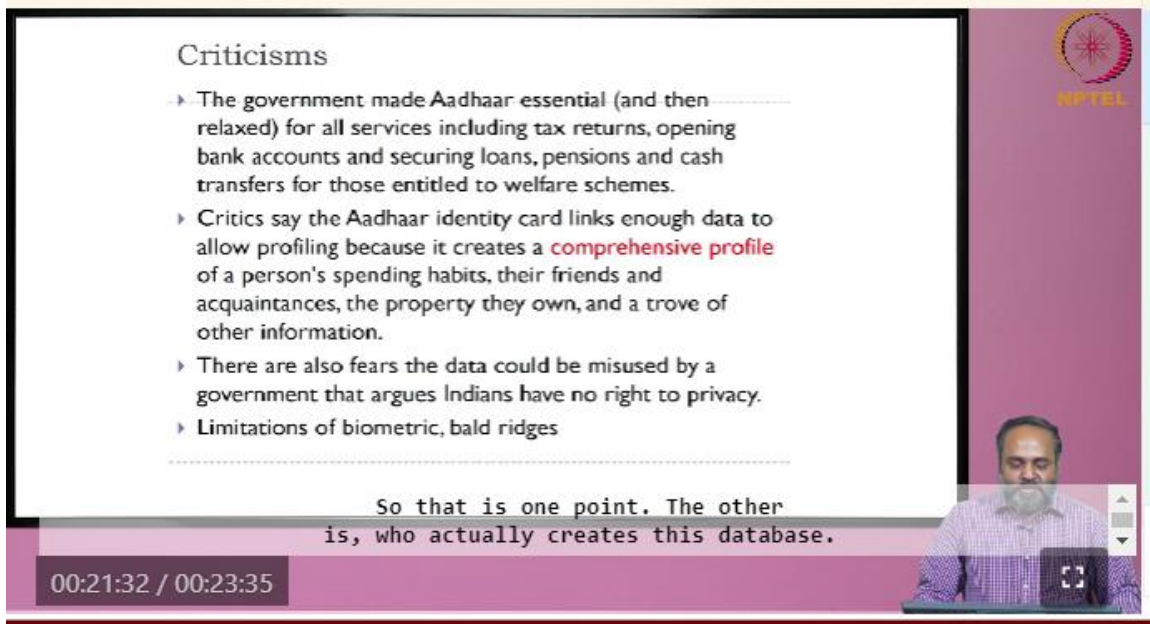
But where would they get access to the data? All that you do, the biometric data is in the custody of the Aadhaar, the UIDAI. They are the custodians of that data. You provide your fingerprints, they do the authentication service. But you cannot get that data of the individual.

The device, service delivery point. They get to know your Aadhaar number because you disclose your ID. To that extent fine. So now there is a debate on where you should disclose your, you should not give your Aadhaar card, you should give your pseudo number. That is one aspect of the challenge or the issue, security issue.

Your Aadhaar number gets known. In the weak links, we can say that the authentication device, like he said, they can only collect the data of those people who are authenticating. But accessing the internal data like UIDs, it will be very difficult because they are just giving yes no response, they are not releasing the data. So the weak point will be very difficult to find here. It will be only regarding the authentication device, they will collect the data of those who are authenticating. But you may have read newspaper reports about Aadhaar data open in public.

So where did it get leaked? So how did it reach there? There have been particularly enquiries into this. Like many organizations collect Aadhaar numbers. So maybe that is how they reach the open internet. They did not fetch it from the UIDs data but from the websites and organization.

Let me summarize the criticisms of Aadhaar. There are several limitations and weaknesses of the Aadhaar system that was highlighted in the news in recent times. I actually collected all that but I am giving a summary of it. One is actually the agencies which collect Aadhaar as an ID and they can aggregate it and then actually link. There is something called linking, we discussed this, you know, link other data with the ID or a unique ID and then use that to profile the customer. So that is one potential leakage which now they, the Aadhaar actually provides you a pseudo ID if you want.



The screenshot shows a presentation slide with the following content:

Criticisms

- ▶ The government made Aadhaar essential (and then relaxed) for all services including tax returns, opening bank accounts and securing loans, pensions and cash transfers for those entitled to welfare schemes.
- ▶ Critics say the Aadhaar identity card links enough data to allow profiling because it creates a **comprehensive profile** of a person's spending habits, their friends and acquaintances, the property they own, and a trove of other information.
- ▶ There are also fears the data could be misused by a government that argues Indians have no right to privacy.
- ▶ Limitations of biometric, bald ridges

So that is one point. The other is, who actually creates this database.

00:21:32 / 00:23:35

The slide also features the NPTEL logo in the top right corner and a video inset in the bottom right corner showing a man with a beard speaking.

So this can be prevented. So this is one way of preventing. So you decide whether you want to give your Aadhaar card or not and you should be very careful because there is a potential that somebody is getting your ID. So that is one point. The other is, who actually creates this database.

One is that once database is created it is safe. We believe that it is safe. Nobody can tap in there. But who actually collects the data? Is it Nandan Nilekani who comes and who is very credible and reliable, who comes directly and collect the data? When you went to a particular center for giving your ID details, it was an agency which did this exercise. So actually Aadhaar enlisted thousands of vendors, thousands of vendors across India for Aadhaar data collection. And there was an inquiry, a journalistic inquiry into the Aadhaar data leakages and which was published and in a short time Aadhaar, actually the UIDAI fired about thousand vendors.

There is a, this actually happened. So if there was no case of Aadhaar data leakage, why this vendor should be fired? So there was, it appears that actually lot of leakages of Aadhaar data happened through the vendors. And vendors, the government is finally dependent on a vendor to collect this data. And vendors are people. So it was quite possible for data to leak through those agencies at the time of collection. And then there are many pitfalls but over a period of time government became aware and it has been correcting its course.