Course - CYT145 –IT Security: Ethical and Legal Issues

Professor – Ionut Anghelache

Name - Yash Sanjaybhai Patel

Student ID – 134094184

Date - 21st September 2025

Introduction

The Aadhar data breach is one of the largest cybersecurity incidents in India, which occurred in early 2018. I have selected this because approximately 1.1 billion people were affected by this data breach [1]. This Aadhar card program is managed by Unique Identification Authority of India (UIDIA), which assigns 12-digit unique identification number to every Indian Citizen, and it is used for linking bank accounts, mobile numbers, government services and health related records [2].

This breach exposed sensitive information of Aadhaar card holders, including names, addresses, phone numbers, email addresses, bank account details, and Aadhaar numbers [2]. This incident shows significant risks associated with storing and managing large amount of personal data in digital databases.

Summary

In March 2018, around 200 official websites of government accidentally released personal Aadhar card details of Indian citizen. People were able to access it by simply doing a google search. People could easily access databases of government which have confidential information. Around 5000 officials were blocked because someone working for the government was accessing Aadhaar details [1]. People were very concerned after this data breach as biometrics which can’t be changed was a major risk factor for individuals.

In January 2018, reports stated by The Tribune, which is an Indian newspaper, that unauthorized access of Aadhar data is being sold on social media’s mainly on WhatsApp, for around 8$ [3]. By getting this data one could access name of the person, address, phone number and emails. Journalists found out a group on WhatsApp that was selling the details and when they pay for the details, they receive an ID and password to the portal, and when they log in they can see every detail which is linked to Aadhar card of the individual.

In mid-2018, Jharkhand, which is a state of India, it accidentally released data for 1.6 million people. The center also mentioned that 130 million Aadhar numbers were released in public, but the government denied that it was a leak [1]. In article, it is mentioned that this breach was through a Indane website which is a state-owned utility company. Application programming Interface which is known as API of the website was not granted with access controls, and it was directly connected to all the Aadhar database. As a result, hackers exposed this vulnerability, and access was being sold on medias as mentioned above [4].

This was basically a data leak rather than a cyberattack as it involved stealing of data and sensitive information due to not having enough security measures. The data stolen from this breach was fingerprints and iris scans, names of the individuals, emails, contact numbers, bank details, Aadhar unique identifying number, and their physical address. As mentioned in the article it says that there were some reports of the data being used unauthorizedly and also being sold on dark web [3]. Though UIDAI denied or data being accessed, this data breach could be a case study of the vulnerabilities linked with sensitive information stored in databases [3].

In October 2023, Resecurity's Hunter unit found millions of personal information including Aadhar cards of the dark web for sale. This team contacted the poster who was selling the data, and they asked for $80,000 for entire Aadhaar and Indian passport [5]. Following the breach many scams were going on, people who had all the information of the individuals. Scammers were running a call center in which they use to call individuals and threaten them to pay money, or they do scams from their identity as they had their sensitive information, and it was easy to do scams. People use to give money, and still they kept their information. Many cases were reported but some call centers were closed after catching few of them.

The actual cause of this data breach is still unknown. UIDAI and the Indian Government is still working on investigating the breach and implementing more security to the sensitive information for future incidents. They would also update the policies and enrollment of the Aadhar. There are high chances that the government will introduce AI programs which can scan suspicious activities, so that they can recognize suspicious [1].

Impact

The Aadhaar data breach 2018 has many implications for the government as well as Indian citizen, which highlighted mainly to protect data of national identity systems in future [7]. This data breach didn't just lead to identity theft but also had financial losses that were owing the identity theft. Santosh Das, the Principal product manager posted on LinkedIn in revealed some impacts of the Aadhaar data leak. He mentioned that the Aadhaar authentication were used by many service providers to identify the individuals. Also, the first thing the attackers do is social engineering and high priority data could bypass this step therefore it lowers the barrier, and the attackers enter to perpetrate cybercrime. It impacted lot of individuals whose data got stolen [6].

It also raised security concerns for Indian citizens about the safety of their personal information. This breach also lost trust of individuals from government who was not able to protect their sensitive data, and the individuals appealed for more transparency and accountability of data management. Because fraudulent activities drastically increased for millions of individuals whose identity was stolen. On the other hand, the impact on government was to reevaluate their data protection policies and implement more security if needed to secure the data. Also, because of the people selling personal documents on dark web, this incident attracted global attention raising question about handling of the digital identity. Moreover, government also face some legal challenges about working on more proactive approach to address the concerns and public outcry. This breach can be put as a case study for other government to protect their data and understand the importance of the national identity and large-scale biometric databases [7].

Conclusion

In conclusion, we can say that the Aadhaar data breach showed that how important it is to protect sensitive personal information details like names, addresses, bank account details, and biometrics. This all can be used and also can be a security risk if not properly managed or protected. This breach also broke people’s trust in government’s ability to keep their data safe and secure.

It also concludes that government need stronger security controls and better monitoring system to monitor unauthorized access. Government should respond quickly whenever this kind of data breach happens and should protect the data. Finally, this data breach was a lesson for public and organization worldwide to protect personal data. By learning from these organizations can implement more security and can get better and ensure data is handled ethically and responsibly.

Resources (IEEE)

[1] M. Jain, “The Aadhaar Card: Cybersecurity Issues with India’s Biometric Experiment - The Henry M. Jackson School of International Studies,” *The Henry M. Jackson School of International Studies*, May 09, 2019. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/

[2] A. T. Tunggal, “The 29 Biggest Data Breaches [Updated for 2020],” *Upguard.com*, Jan. 22, 2024. https://www.upguard.com/blog/biggest-data-breaches

[3] “Digital Disasters: The Biggest Data Breaches of All Time,” *VIPRE*, Aug. 29, 2024. https://vipre.com/blog/digital-disasters-the-biggest-data-breaches-of-all-time/?srsltid=AfmBOorAEoKAYjXr1H5ZvIutrLZnlho4l0ASxAmna87N6SnGVDW30qHC

[4] A. Skebaite, “The 20 biggest data breaches in history | NordVPN,” *nordvpn.com*, Jun. 28, 2024. https://nordvpn.com/blog/biggest-data-breaches/

[5] “Resecurity | PII Belonging to Indian Citizens, Including their Aadhaar IDs, Offered for Sale on the Dark Web,” *Resecurity.com*, Oct. 15, 2023. https://www.resecurity.com/blog/article/pii-belonging-to-indian-citizens-including-their-aadhaar-ids-offered-for-sale-on-the-dark-web?utm_source=chatgpt.com

[6] www.ETBFSI.com, “How did massive Aadhaar data leak happen, its impact - ET BFSI,” *ETBFSI.com*. https://bfsi.economictimes.indiatimes.com/news/industry/how-did-massive-aadhaar-data-leak-happen-its-impact/104901967

[7] “A Closer Look at the Aadhaar 2018 Cybersecurity Breach,” *Wolfe Systems - Eliminating Inefficiency*, Nov. 17, 2023. https://wolfesystems.com.au/a-closer-look-at-the-aadhaar-2018-cybersecurity-breach/