Old Dominion University

School of Cybersecurity

Aadhaar Breach of 2018

Kerina Drummond

Introduction to Cybersecurity, CYSE 300

Malik Gladden

September 8, 2024

What is Cybersecurity? According to the Cybersecurity and Infrastructure security agency (CISA), Cybersecurity is the practice of protecting networks, devices, and data from unauthorized access and criminal misuse (CISA, 2021). With constant connections to the internet, cybersecurity has become increasingly crucial to protect citizens from bad actors and attackers. Unfortunately, this trust in our systems has betrayed billions, with copious amounts of breaches, and trillions of bits of data stolen, especially the 1.3 billion Indians connected to Aadhaar in 2018.

Aadhaar is a biometric system presented as a resource by the Unique Identification Authority of India (UIDAI) for Indians in 2009, it provided users with 12-digit code that could link various aspects of their lives, from driver's licenses to medical records. Over the years new government regulations encouraged citizens to join the database. By 2016, Aadhaar could access banking information using only a fingerprint (Jain, 2019). However, Aadhaar held billions of users' most sensitive information under a system without strong enough security to protect it and led to one of the largest data breaches in history known as the Aadhaar Breach of 2018. The breach was caused by various vulnerabilities including faulty website and system security, and third-party involvement.

Faulty website and system security allowed attackers to infiltrate Aadhaar's database. Aadhaar was not equipped with sufficient security measures to securely protect personal data. There were multiple security lapses previously with Aadhaar that made "the system prone to data leaks (Jain, 2019)." The mAadhaar application failed security checks, and bugs in the app allowed an IIT graduate to create the program, Aadhaar eKYC, and effectively bypass security protocols, accessing Aadhaar's database (Business Bliss FZE, 2024). In 2018, government websites exposed Aadhaar's citizens personal data making billions of personal data public to

anyone (Jain, 2019). The information made available ranged from a user's address information to pension benefits. Attackers preyed on these vulnerabilities by creating third-party false websites to trick citizens into giving out their personal information, selling personal information on apps and websites including WhatsApp and Breach Forums, where almost 815 million Aadhaar records were leaked (Sharma, 2023).

This data breach led to severe repercussions for citizens. Sensitive data such as Driver's licenses, passports, address information, and bank account details, Identity theft and financial fraud were abundant. This breach also led to mistrust in the government. These repercussions could have been avoided if the government had taken more security measures such as proper education and training, screen third party websites and pop-ups, background checks for authorized users, etc. (Gopal, 2022). Proper education and training would teach the individuals in charge the ways to look for vulnerabilities in the program, solve them, and educate the public. Screen third parties can block attacks trying to fool citizens and break in. Lastly, doing background checks on government officials can stop internal attacks.

In conclusion, The Aadhaar breach in 2018, was a terrible and preventable situation, but any person or organization can be the target for a cyber-attack, to better protect ourselves from a data breach we must take responsibility for our own security and take precautions. Monitor credit reports and bank statements to ensure there aren't any unauthorized transactions, create strong passwords, do not use the same password for too many accounts, and watch what you share online.

References

Business Bliss FZE. (2024, August 18). *Aadhar Breach – A Case of Data Privacy in India*. Ukessays.com; UK Essays. https://us.ukessays.com/essays/information-technology/aadhar-breach-a-case-of-data-privacy-in-india.php

CISA. (2021, February 1). *What is Cybersecurity?* Cybersecurity and Infrastructure Security Agency CISA; CISA. https://www.cisa.gov/news-events/news/what-cybersecurity

Gopal, R. V. (2022, December 19). *Aadhaar Data Breach — How Sensitive Data Of 1.3 Billion Indians Was Compromised*. Medium; The Deep Hub. https://medium.com/thedeephub/aadhaar-data-breach-how-sensitive-data-of-1-3-billion-indians-was-compromised-cb01d0c2d7d3

Schram, P. J., & Tibbetts, S. G. (2021). *Introduction to criminology: why do they do it?* (3rd ed.). Sage Publications, Inc.

Sharma, A. (2023, November). *What we know and don't know about the alleged Aadhaar data leak*. India Today; India Today. https://www.indiatoday.in/india/story/aadhaar-data-leak-what-we-know-and-dont-know-about-breach-2456474-2023-11-01

Spektor, H. (2024, February 21). *Understanding IoT Security: Threats, Standards & Best Practices | Sternum IoT*. Sternum IoT. https://sternumiot.com/iot-blog/understanding-iot-security-challenges-standards-and-best-practices/#:~:text=IoT%20devices%2C%20due%20to%20their%20connectivity%2C%20have%20the