



# Miranda House

## UNIVERSITY OF DELHI

### Departmental Annual Report - 3

#### Departmental Activities: Curriculum and Beyond

Department: Political Science

Academic Year: 2023

#### Part A.1

Students undertaking project work/field work/internship as part of experiential learning component of coursework

Programme:

Semester: First Semestar

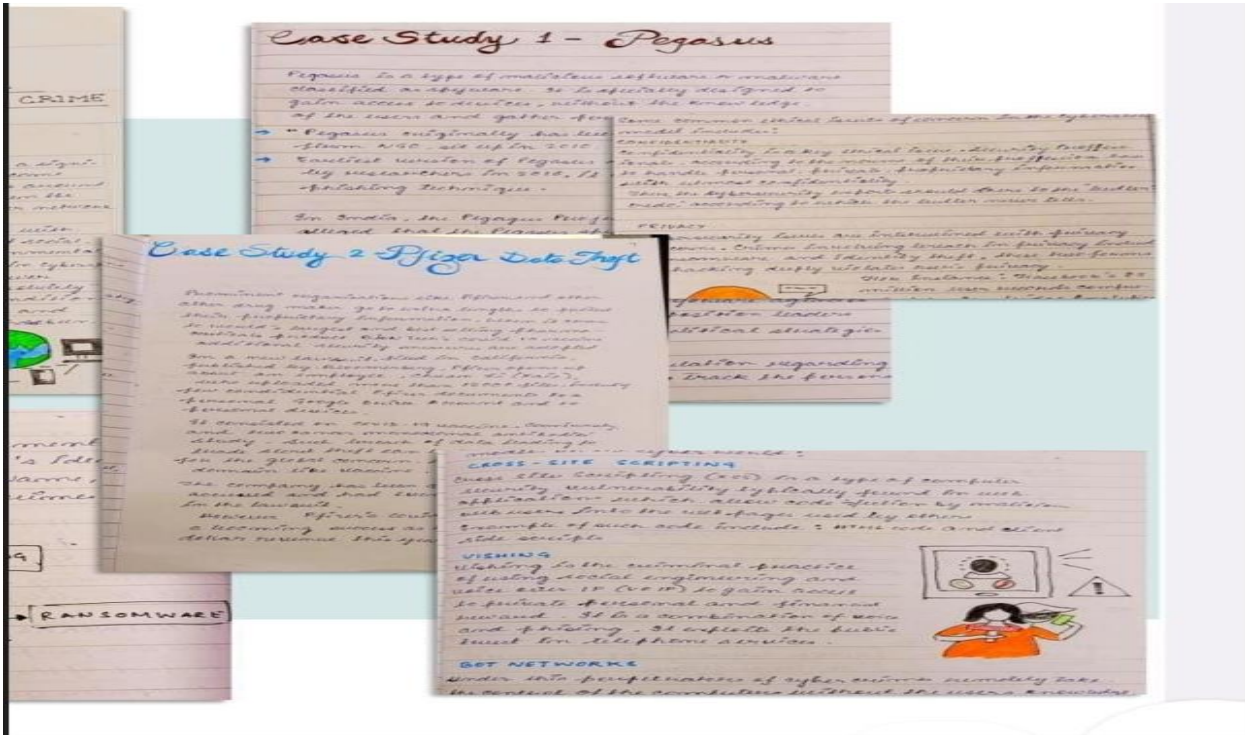
Course: SEC Cyber Sphere and Security: Global Concerns

Course Code: 3206000001

S.No	Name of the Student	Project Title	Supervised by
1.	Sagarika Ghosh	Case Studies of Cyber Security related to Government Institutions.	Pallavi Raj
2.	Garvita	Point of Sales Issues and Online Payment	Pallavi Raj



# Miranda House UNIVERSITY OF DELHI



### COMMON CASES OF CYBER ATTACK ON GOVT WEBSITES

- ADNHAR DATA BREACH**  
YEAR: 2018  
LEAK OF CITIZEN'S PERSONAL DETAILS INTO DARK WEB
- GOVT LAND REVENUE PORTAL ATTACK**  
YEAR: 2019, 2020  
ATTACKERS GOT UNAUTHORIZED ACCESS INTO LAND REVENUE PORTAL THROUGH ADNHAR AND APPS
- UIE CYBER ATTACK**  
YEAR: JULY 2017  
LEAK OF DATA INTO THE BANKING SYSTEM AND WIDE PEN OF THE INFORMATION
- KARNATAKA RAYERI WRESTLE ATTACK**  
YEAR: 2020, 2021  
CIVIL ATTACK LEADING TO TRASH OF PHONE, AND LEAK OF INFORMATION OF CITIZEN DETAILS

### WHAT HAPPENED?

ON 2018 ON 2018 MASSIVE DATA BREACH TOOK PLACE WITH THE PERSONAL DETAILS OF 15 MILLION INDIA'S INCLUDING THESE DETAILS: PASSPORT NUMBERS, PAN CARDS, VEHICLE REGISTRATION, AND OTHER DETAILS. THIS DATA WAS LEAKED TO THE DARK WEB AND ACCORDING TO A REPORT IN THE BUSINESS STANDARD

### PERSONAL DETAILS FOR ₹200

Personal details for ₹200. A report in the business standard mentioned that the personal details of 15 million Indians were leaked to the dark web. The details include passport numbers, PAN cards, vehicle registration, and other information. This data was sold for as little as ₹200 per record.

### ADNHAR DATA BREACH CASE

HERE OUR PRIME FOCUS WOULD BE THE STUDYING THE IMPORTANCE OF CYBER SECURITY INFRASTRUCTURE IN GOVERNMENT INSTITUTION. THROUGH A CASE STUDY HERE IT HAS BEEN KNOWN THAT HOW BREAKDOWN OF A CRITICAL INFRASTRUCTURE AT ONE POINT CAN RESULT IN VARIOUS CONSEQUENCES, WHERE CITIZEN BECOMES THE PRIME VICTIM

And our case in focus is **ADNHAR DATA BREACH CASE**

### CRIME LINKING OTHER CRIMES

#### KOLKATA FINANCIAL FRAUD CASE

In July, two residents of the joint area suffered losses when fraudulent payments of ₹15,000 each from their bank accounts via the AFS facility.

As per police records, a Gurfa resident recently lost more than ₹40,000 without receiving any alert on the generation of OTP or from the bank about the amount having been debited from the account.

On June 15, a complaint received an SMS about a "successful generation" of their AFS transactions from the savings account with a bank in Gurfa branch area. It was found that ₹4,000 had been debited from his account for an AFS transaction. The police cyber cell then advised him to block immediately Aadhar card.

### CRIME LINKING OTHER CRIMES

#### KARTARA GOVT PORTAL CASE

Two men from Bihar were caught using the Karnataka government's land registration portal to assist them in their Aadhar biometric fraud.

The respondents used the state government's Karnta Crime Services, a portal for emergency registration, to download the registration papers containing Aadhar numbers and thumb impressions.

8 biometric trees created a virtual image of the Respondents on various Enabled Payment System (AAPS) services like State Money and Expendy and also withdrew money through micro ATMs

### Aadhaar

DATA BREACH Impact Could be MASSIVE

- 9 Yrs Since Aadhaar Was Launched
- Spent ₹7,948 Bn On Enrollment
- 100+ States Register on Aadhaar No. (up to 100 million States)
- 50,000 Agents/Outlets for Aadhaar Enrollment
- 30 FIRs Filed For Mismatch of Aadhaar App
- 1198 Criminated Members
- 99% Indians Aged 18 & Above Have an Aadhaar No.
- 210 Datto Leaks In Nov 2017

### APPS FRAUDS

In these Aadhaar Enabled Payment System (AAPS), intimate account system Aadhaar biometric data is withdrawn from these bank accounts without their consent.

**AFTERMATH**

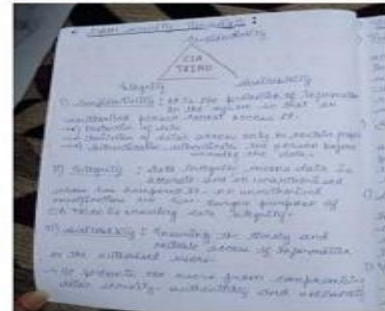
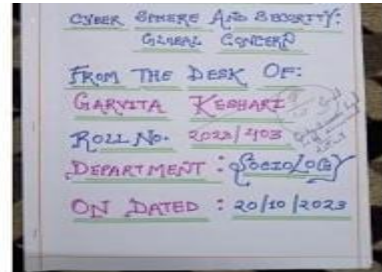
The data breach claim has come as a major jolt to the government, which has been taking steps to digitize the economy and has built digital public infrastructure (DPI) based on the biometric identification number Aadhar, insurance, medical numbers, and bank accounts as the backbone for the transfer of benefits and cooperation in the private sector.

### CAUSE

THIS THERE HAS BEEN GROWING LINKAGE OF ALMOST ALL MAJOR CITIZENSHIP DETAILS OF THE PEOPLE WITH THE ADNHAR INTERFACE. THIS MAKING USDT AUTHORIZED ADNHAR SITE A CRUCIAL TARGET FOR CYBER ATTACK



# Miranda House UNIVERSITY OF DELHI



## Part A.2

Students undertaking project work/field work/internship (beyond the requirements of coursework)

<https://www.mirandahouse.ac.in/centres/policycentreandgenderlab.php>