SOMAIYA
VIDYAVIHAR UNIVERSITY
K J Somaiya School of Engineering
(formerly K J Somaiya College of Engineering)

K. J. Somaiya School of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)
Department of Electronics Engineering
Electronics And Computer Engineering

Course Name:	**Information and Cyber Security Laboratory**	**Semester:**	**VII**
Date of Performance:		**Batch No:**	**B - 1**
Faculty Name:	**Prof. Makarand Kulkarni**	**Roll No:**	**16014022050**
Faculty Sign & Date:		**Grade/Marks:**	**___ / 25**

Experiment No: 9

Title: Study Cyber Crime Cases and Indian IT Act

Aim and Objective of the Experiment:

Study Cyber Crime Cases and Indian IT Act

COs to be achieved:

CO 5. Study and analyze Cyber Laws.

Books/Journals/Websites referred:

- Information Technology Act, 2000 (latest amendments)
- Indian Penal Code (cyber crime relevant sections)
- Cyber crime case studies from Indian law enforcement reports
- Scholarly articles and online resources on cyber laws in India

Tools required:

- Internet access for research
- Case law databases or legal repositories
- Document editor for report preparation

Theory:

Cyber crime involves illegal activities carried out through computers, networks, or the internet, including hacking, identity theft, cyber terrorism, financial frauds, and unauthorized data access. The Indian IT Act, 2000, enacted to provide legal recognition for electronic transactions and penalize cyber offenses, is a comprehensive legislation addressing cyber crimes and electronic commerce.

Important provisions include:

- Section 43: Penalty for unauthorized access, data damage, introducing viruses, and disruption of services.
- Section 66: Hacking and related offenses with punishments of up to 3 years imprisonment or fines.
- Section 66B-D: Related to receiving stolen devices, identity theft, and cheating by personation.
- Section 66E: Violation of privacy through capturing and transmitting images without consent.
- Section 66F: Cyber terrorism punishable with life imprisonment.
- Sections 67-67B: Publication and transmission of obscene or sexually explicit content.

The act empowers authorities to investigate, adjudicate cyber crimes, and regulate intermediaries like online platforms to curb harmful digital content. Several amendments have been introduced to keep the law relevant with evolving technology and threats.

Implementation details:

- Research authentic cyber crime cases from Indian law enforcement sources and news reports.
- Analyze the cases in the context of sections of the IT Act invoked for prosecution.
- Summarize key takeaways on the types of cyber crimes and the applicability of legal provisions.
- Prepare a detailed report showing understanding of cyber laws and their role in combating cyber crime.

Post Lab Subjective/Objective type Questions:

1. What preventive measures can users take to protect themselves from keylogger attacks?

- Install and maintain updated antivirus and anti-malware software regularly to detect and block keyloggers.
- Keep operating system, browsers, and software patched with latest security updates.
- Use password managers to reduce typing sensitive information manually.

- Enable firewalls to monitor and block suspicious network activity.
- Avoid clicking on unknown links, downloading attachments from untrusted sources, or visiting unsafe websites.
- Use two-factor authentication to secure accounts even if credentials are compromised.
- Regularly scan the system for malware and unusual processes.

2. Mention two signs that may indicate a keylogger infection on a computer.

- Noticeable system slowdowns or lag, especially when typing or launching applications, due to keylogger resource usage.
- Pop-ups, error messages, or unfamiliar processes running in the background without user initiation.

Conclusion:

This experiment reinforces the critical importance of understanding cyber crime and the legal framework established by the Indian IT Act, 2000 for protecting digital assets and users. The act covers a broad range of cyber offenses with substantial penalties, reflecting the seriousness of cyber crimes in modern society. Preventive measures against common threats like keyloggers along with vigilant monitoring are essential defenses for individuals and organizations. A legal and technical combined approach is key for effective cyber security in India.

Signature of faculty in-charge with Date: