Principles of Data and System Security

Syllabus:

- **Concepts of Security**: Confidentiality, Containment, isolation, Privacy, Anonymity, psuedo- anonymity etc., Policy specification, User authentication, Session management, multi-level security, multi-lateral security

- **Security Models for Information Systems**: Bell la Padua, Biba, Clark-Wilson, Lattice Model, Chinese Wall Model

- **Access Control**: Mandatory Access Control, Discrete Access Control, Principles of Least Privilege, Distributed Access Control , Role based Access, Attribute Based Access, Key Management, SPKI/SDSI

- **Information Flow Models**: Distributed Information Control, DIFC, Declassification, Non-Interference, RWFM Models, Information Flow Diagrams,
    - **Application to analysis of protocols, Protocol Specification and Verification**
    - **Database Access Control, Applications to IoT security**

- **Security and Privacy:** Issues and Challenges – applications, conference systems, privacy compliance in healthcare systems

- **Attacks and Vulnerabilities**: Static and Dynamic attacks, Malware analysis and Counter measures- difficulties, approaches, defense against untrusted code, exploiting Vulnerabilities, penetration tests

- **OS Security:** Principles, Secure OS types, run-time monitoring, secure OS like SELINUX, Secure OS based on IFC

- **Language based security:** Program analysis for Security, secure code practices and tools for secure code writing

- **Security Mechanisms**: Protection, Confinement, Isolation, Virtual machines, Non-interference Dealing with legacy code, Sandboxes, Separability, Data caging

- **Web security models**: application security, Browser Security, Information flow browsers

- **BlockChains: Applications, Currency realization – Bitcoins**

- **Special Topics:** Mobile phone security, Android Security, Cloud security etc.

Texts and References:

A. Text Books

1. Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, 2nd Edition, Wiley, 2008, SBN: 978-0-470-06852-6
2. Cryptography and Data Security – Dorothy Denning, Addison Wesley, 1988
3. Computer Security Art and Science – Matt Bishop, ISBN-13: 978-032124744
4. Building a Secure Computer System –Morrie Gasser, **ISBN-13:** 978-0442230227

B. Research Papers/ chapters

Teaching Assistants:

a. **BS Radhika (PhD Scholar)**
b. **Sundaram Gupta (PhD Scholar)**
c. **Anand Kumar (MTP)**
d. **Utkarsh Singh (MTP**