Security and Privacy in Internet of Things (IoTs)

Objectives

- To study the Security and Privacy in Internet of things.
- To learn the issues related to IoT Data Security and Privacy preservation.
- To learn the latest trends in Security Protocols for IoT Access Networks.

UNIT I

Threats and Attacks: Internet of things as interconnection of threats, Attack, defense and network robustness of IoT, Malware propagation and control in IoT, A solution based Analysis of an attack on smart home systems.

UNIT II

Privacy and preservation: Privacy preservation Data dissemination, Exploiting mobility social features for location privacy enhancement in internet of vehicles, Lightweight and robust schemes for privacy protection.

UNIT III

Trust and Authentication: Trust models for IoT, Preventing Unauthorized access to sensor data,Authentication in IoT.

UNIT IV

IoT Data security: Computational security for IoT and beyond, privacy preserving time series data aggregation for IoT, security protocols for IoT access networks.

UNIT V

Social Awareness: A User-Centric decentralized Governance framework for privacy and trust in IoT, A privacy based approach for informed consent in IoT, security and impact of the IoT on Mobile networks.

Outcome

- Knowledge about all types of IoT attacks and threats
- Ability to develop privacy-preservation techniques related to the collection and distribution of data
- Ability to provide survey of IoT authentication issues.

TEXT BOOK:

- Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, CRC Press(7April 2016)

REFERENCE BOOK

1. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations Hardcover – Import, 7 Apr 2016 by Fei Hu (Author)

May be placed before Senate
S. Sabarkeeman
23 08 16
Chairman, DC.

Senate
nr