SNS COLLEGE OF TECHNOLOGY

(An Autonomous Institution)

Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai

Accredited by NAAC-UGC with 'A++' Grade (Cycle III) &

Accredited by NBA (B.E - CSE, EEE, ECE, Mech&B.Tech.IT)

COIMBATORE-641 035, TAMIL NADU

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19ECE306- SMART IoT APPLICATIONS

III ECE / V SEMESTER

UNIT V

5.2 Identity Management

1. Definition of Digital Identity (ISO/IEC 24760)

A digital identity is a collection of attributes tied to an entity, which can be a person, organization, or device. Attributes are unique properties of the entity, such as an address or phone number. In the IoT world, this concept extends to devices that need to interact with online services using their owner's credentials. This is known as the *inheritance principle*, where a device inherits parts of its owner's identity to perform tasks on their behalf.

2. Examples of Digital Identity Inheritance in IoT Devices

- **Smart TVs**: To access online content, a user must allow the TV to authenticate with the streaming service using their subscription credentials. This means the TV inherits a portion of the user's identity.
- **Smartphones**: If a user syncs their phone with a work calendar, the phone uses personal credentials to access the company's information.

This inheritance principle extends to Smart Cities, where digital identities may be used by systems for public services, such as transportation, healthcare devices, and inter-vehicle communication.

3. Digital Identity in Industrial Control Systems (ICS)

In industries, digital identities are vital as ICS and Supervisory Control and Data Acquisition (SCADA) systems often connect to the internet, allowing remote access and control. Digital identities here help manage access to critical infrastructure, assign roles, and control rights. Secure management of these identities is essential, especially for remote installations (e.g., oil pipelines) with minimal supervision. Strong authentication mechanisms ensure secure and trusted communication of control devices.

4. Digital Identities in Smart-Metering and Smart Grids

Smart meters are crucial in energy management, measuring consumption and sometimes production by users. As smart grids evolve, these meters will increasingly integrate with the energy distribution network and the user's home systems. Digital identities here are essential to:

- Securely manage the integration with energy infrastructure.
- Protect user privacy.
- Provide a framework that manages service access and information disclosure.

5. Challenges

Managing digital identities in IoT systems requires a balanced approach. It's essential to secure device access, manage permissions carefully, and maintain privacy while enabling smooth service operations. Developing a secure framework that controls information sharing and access permissions is critical in IoT for both citizens and industrial applications.