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

5.3 Size and Heterogeneity of the System, Action's Control, Privacy by Design

1. Size and Heterogeneity of the System

The Internet of Things (IoT) is an integrated system where diverse devices (or "things") communicate and share commands. These devices vary significantly in their security levels, technology, communication protocols, and privacy policies. The challenge here is creating a unified framework to manage security and privacy across a wide range of devices with different designs and specifications. This framework must adapt to each device's unique features to maintain a consistent level of security and privacy across the system.

2. Control of IoT Actions

IoT devices can perform actions based on the context, such as activating physical devices (e.g., turning on a light) or handling data (e.g., deleting data after a specified time). To manage these actions, IoT systems require a language that clearly expresses actions, consequences, and data obligations. Additionally, a framework is needed to translate these instructions so all IoT devices can understand and implement them accurately, regardless of their technical differences.

3. Privacy by Design

IoT devices often collect data that can include sensitive information. For instance, traffic cameras capture images of pedestrians, potentially revealing their movements, while noise monitoring devices may inadvertently record conversations. Even anonymized data can expose personal details over time, as repeated data points can reveal patterns (e.g., daily commutes). Privacy by design aims to limit data collection to only the information necessary for specific tasks, reducing the risk of privacy breaches.

4. Data Linkability and Privacy Threats

One of the major threats to privacy is data linkability—the ability to connect data from different sources to identify individuals. For example, combining anonymized location data with other available data can reveal a person's identity, work location, or home address. To protect privacy, IoT systems should avoid data reuse across applications unless absolutely necessary, and consider context-aware mechanisms that prevent excessive data collection.

Conclusion

Managing security and privacy in IoT systems involves addressing the diversity of devices, ensuring actions are controlled and understood, and designing privacy-focused data management. Privacy by design and limiting data linkability are essential strategies to protect individuals in an interconnected IoT environment.