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

IOT SECURITY, PRIVACY FRAMEWORK

Introduction- Main Concepts and Motivation of the Framework

The rapid adoption of the Internet of Things (IoT) in daily life introduces substantial privacy and security challenges. IoT devices are now widely used in smart homes and cities, where they monitor and interact with the environment. In smart homes, devices like IP cameras, temperature sensors, and smart meters collect data and adjust home settings through connected actuators. For example, motion sensors may detect activity to control lighting or temperature.

In smart cities, IoT applications improve various aspects of urban living, such as environmental monitoring, traffic management, smart parking, and waste management. Traffic sensors can control traffic lights to reduce congestion, street lights adjust their brightness to conserve energy, and smart waste bins notify services when they need to be emptied. These innovations illustrate IoT's potential to enhance city life by enabling adaptive, data-driven decisions.

, the widespread integration of IoT also raises concerns about personal privacy and data security. IoT devices embedded in public areas can collect sensitive

information. For example, traffic cameras capture images of pedestrians, and if these images are not securely stored, unauthorized parties could access private data, revealing a citizen's location and behavior. Likewise, data from mobile phones used in traffic monitoring applications can unintentionally disclose a person’s movements, even if anonymized. Malicious users in crowdsourced applications could also provide false data, disrupting systems like "smart" traffic lights to prioritize their route.

The two major challenges in IoT environments are **security and privacy.** Addressing these concerns is crucial to ensure that IoT advancements do not compromise user trust or safety. Key considerations include data protection, secure communication, and regulations to prevent unauthorized access and misuse. Properly addressing these issues is essential for creating safe, reliable IoT systems in our increasingly connected world.