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

5.9 .Conclusion and Future Developments in IoT Security and Privacy

As technology advances, societal perspectives on privacy and security evolve, influencing decisions on IoT data management. This conclusion outlines the achievements of the SecKit framework and explores directions for future development.

Key Takeaways

- **Balancing Security and Privacy:** Achieving an ideal balance between security and privacy requires more than just technological solutions. It demands societal engagement and ongoing adjustments as technology and understanding of its impact grow.
- **SecKit's Contribution:** This framework enables users to manage and control their data flow through policies. By allowing users to decide on data access, the SecKit approach empowers individuals to protect their privacy while ensuring security.

Limitations and Future Directions

The current framework has some limitations that need to be addressed to enhance its effectiveness and scalability:

Context Detection and Ambiguity: The framework's context recognition relies on sensor data, which may contain ambiguities or quality issues. Ensuring precise detection and context definition will be essential to improve decision accuracy and effectiveness in diverse IoT environments.

Scalability Challenges: In future IoT ecosystems, each device will interact with many others, posing scalability challenges. To address this, possible solutions include:

- **Cluster Approaches and Cloud Computing:** Using clustered systems and cloud-based resources to manage data flow can enhance the framework’s ability to handle high data volumes.
- **Partitioned Monitoring:** Dividing the monitoring function to process data in parallel reduces computation overhead and optimizes the data flow in large-scale IoT networks.

By addressing these areas, the SecKit framework aims to provide a scalable and flexible solution for managing security and privacy in rapidly growing IoT networks, creating a sustainable balance between technological capability and user privacy.