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

5.5 . A Policy based Framework for Security and Privacy in Internet of Things

Governance and Security in IoT Using SecKit

1. Introduction to SecKit

SecKit is a toolkit designed for managing security and governance in IoT systems. It is used to enforce policy management across all infrastructure layers, including Virtual Objects (VOs), Composite Virtual Objects (CVOs), and Services. SecKit relies on a collection of meta-models to address privacy, data protection, and interoperability requirements.

2. IoT System Modeling with SecKit

SecKit uses a model-based approach to design IoT systems with a focus on security. Its architecture divides the system into two domains:

- **Entity Domain**: Defines entities and their interaction points, representing how entities communicate.
- **Behavior Domain**: Details each entity's actions, interactions, and security-related attributes.

SecKit allows for specifying system behavior along with models for data, identity, trust, and security, ensuring seamless integration and interoperability across different domains.

3. Context Model and Situations

SecKit includes a context model to define types of context information and context situations, which are specific conditions (e.g., a patient's high temperature or an object within a one-kilometer range). Events are generated as these conditions begin and end,

helping enforce policy rules, such as granting temporary access to patient data during an emergency and ensuring its deletion afterward.

4. Policy Management and Security Rules
Policies in SecKit are essential for managing data access and protection. These policies follow an Event-Condition-Action (ECA) format, where:

- **Event**: Represents a specific condition or trigger.
- **Condition**: Specifies requirements that must be met.
- **Action**: Determines the response (e.g., allow, deny, modify, delay) to the event.

For instance, a policy may allow access to traffic data but restrict specific location details to protect user privacy.

5. Data Transmission and Security Policies
When transmitting data, SecKit ensures policies are followed:

- Devices map application-specific policies to data-gathering rules.
- Devices apply appropriate encryption based on data sensitivity and energy efficiency needs.

Example: In traffic monitoring, a device may send only the average speed per segment to maintain user privacy, while other applications with access privileges might receive exact location data.

6. Policy Dissemination and Integrity
SecKit securely disseminates policies to devices, ensuring that only authorized applications access sensitive data. Policies are validated to prevent unauthorized access and maintain data integrity, such as restricting unauthorized apps from retrieving privacy-sensitive data.

7. Security Rule Templates and Enforcement
SecKit uses security rule templates to enforce non-functional requirements, like confidentiality, integrity, and authorization. These templates follow ECA rules, with actions that may involve allowing, denying, or modifying an operation. For example, a security policy might allow temporary access to sensitive data, followed by its deletion once the situation ends.

8. Policy Delegation and Trust Management
Policies can be delegated between administrative domains in IoT, such as between a smart home and a smart vehicle, allowing them to enforce shared data policies. Trust management mechanisms are crucial here to ensure the receiving domain respects these policies.

Summary: SecKit provides a comprehensive framework for managing IoT security and privacy through context-aware policies and secure data transmission. It ensures

that devices follow established rules, protecting user privacy and data integrity across interconnected systems.