SMART METERS: – SECURITY CONSIDERATIONS:

Why Security is Important in Smart Meters:

Smart meters are connected to networks and handle sensitive data like:

- Energy usage patterns
- Billing details
- Consumer identity
- Load control signals

Without proper security:

- Hackers can manipulate billing
- Electricity theft may occur
- User privacy can be violated
- Power supply may be disrupted
- Therefore, strong security measures are necessary.

MAIN SECURITY REQUIREMENTS:

- Smart meter security is based on five important principles:

1. Confidentiality

- Data must be protected from unauthorized access.
- Example:
  Energy consumption data should not be visible to hackers.

2. Integrity

- Data should not be modified during transmission.
- Example:
  Billing information must not be changed.

3. Authentication

- The system must verify the identity of users and devices.

- Example:
  Only authorized utility servers can access the meter.

4. Authorization

- Access rights should be controlled.
- Example:
  Consumers can view data, but only utility providers can change settings.

5. Availability

- Smart meter system should function continuously without interruption.
- Example:
  System should resist Denial of Service (DoS) attacks.

Types of Security Threats in Smart Meters:

1. Unauthorized Access

- Hackers gain control of the meter remotely.

2. Data Theft

- Stealing consumer data and usage patterns.

3. Man-in-the-Middle Attack

- Attacker intercepts communication between meter and utility server.

4. Denial of Service (DoS)

- Overloading the network to stop meter communication.

5. Malware Injection

- Installing malicious software in smart meter firmware.

6. Physical Tampering

- Opening meter casing to manipulate readings.

Cyber Security Measures:

1. Encryption

- Encryption converts data into secure form.

Types:

- Symmetric Encryption (AES)
- Asymmetric Encryption (RSA)

Used to:

- Protect data during transmission
- Secure cloud communication

2. Secure Communication Protocols

Smart meters use secure protocols such as:

- SSL/TLS
- HTTPS
- Secure MQTT
- WPA3 (Wi-Fi security)
- These prevent data interception.

3. Authentication Mechanisms:

- Password-based login
- Two-factor authentication
- Digital certificates
- Device authentication
- Ensures only authorized devices join the network.

Physical Security Measures:

Smart meters must also be physically protected.

Measures include:

- Tamper-proof meter casing
- Anti-tamper sensors
- Sealed covers
- Alarm system on opening
- This prevents electricity theft and meter manipulation.

7. Firmware and Software Security:

- Smart meters contain embedded software.
- Prevents system hacking.

Data Privacy Protection

- Smart meters collect detailed energy usage data.

This can reveal:

- User lifestyle
- Presence/absence at home
- Daily routine

To protect privacy:

- Data should be encrypted
- Access should be restricted
- Data anonymization should be used