power quality audit
power quality audit

SNS COLLEGE OF TECHNOLOGY

(An Autonomous Institution)

UNIT-V- Basics of CLOUD Computing & Cyber Security for Smart Grid

Cloud Computing

- **Cloud Computing:**
- **Definition:** Cloud computing refers to the delivery of computing services, including storage, processing power, and software, over the internet. Instead of owning and maintaining physical servers or infrastructure, users can access these resources on-demand from cloud service providers.
- **Key Characteristics:**
- **On-Demand Self-Service:** Users can provision and manage computing resources as needed without human intervention from the service provider.
- **Broad Network Access:** Services are available over the network and can be accessed through standard mechanisms (e.g., smartphones, laptops, tablets).
- **Resource Pooling:** Resources are pooled to serve multiple customers, with different physical and virtual resources dynamically assigned and reassigned according to demand.
- **Rapid Elasticity:** Resources can be rapidly and elastically provisioned to quickly scale up or down based on demand.
- **Measured Service:** Cloud systems automatically control and optimize resource use, and users are billed based on their actual usage.

Cloud Computing

- **Cybersecurity for Smart Grids:**
- **Definition:** Cybersecurity in the context of smart grids involves protecting the digital infrastructure and communication networks that support the smart grid system from cyber threats and attacks.
- **Key Components:**
- **Authentication and Authorization:** Ensuring that only authorized personnel and devices have access to critical systems and data.
- **Encryption:** Protecting data in transit and at rest through encryption to prevent unauthorized access.
- **Integrity:** Ensuring the accuracy and reliability of data by preventing unauthorized tampering.
- **Firewalls and Intrusion Detection Systems (IDS):** Implementing barriers and monitoring systems to detect and prevent unauthorized access and malicious activities.
- **Incident Response and Recovery:** Establishing protocols and plans to respond to and recover from cybersecurity incidents.
- **Application to Smart Grids:**
- **Secure Communication:** Implementing secure communication protocols to protect data transmitted between smart grid devices and control centers.
- **Access Control:** Implementing strong access controls to prevent unauthorized access to critical infrastructure.
- **Monitoring and Anomaly Detection:** Continuous monitoring of network traffic and behavior to identify and respond to abnormal activities.
- **Firmware and Software Security:** Ensuring the security of firmware and software running on smart grid devices to prevent vulnerabilities.
- **Regulatory Compliance:** Adhering to industry standards and regulations to ensure the security of smart grid systems.

THANK YOU