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 IV

IOT Standardization:ITU-T, OASIS

ITU-T

The International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) has been actively engaged in the standardization of the Internet of Things (IoT) since 2005. This initiative was catalyzed by the publication of a report titled "The Internet of Things," which laid the groundwork for the establishment of the Joint Coordination Activity on the Internet of Things (JCA-IoT). This body aims to foster collaboration and information sharing regarding the network aspects of identification systems, such as RFID technology.

With the recognition of IoT's significance in shaping future network infrastructures, the JCA-NID evolved into the JCA-IoT in 2011, leading to a formalized structure for the IoT Global Standards Initiative (IoT-GSI). This evolution has significantly expanded ITU-T's activities in the IoT domain, resulting in a wide array of Recommendations covering diverse applications, including networked vehicles, mobile payments, e-health, and energy-saving initiatives in home networks.

The ITU-T's efforts have also included various working groups dedicated to specific application domains, such as Smart Sustainable Cities and Intelligent Transport Systems. These focused groups, alongside ongoing studies related to future networks and cloud computing, highlight the ITU-T's commitment to addressing the complexities of IoT.

A notable milestone in the ITU-T's standardization efforts was the finalization of Recommendation Y.2060 in June 2012, which provided a widely accepted definition of the Internet of Things. This Recommendation outlines the essential features of IoT and recognizes Machine to Machine (M2M) communication as a fundamental enabler of IoT, although it acknowledges that M2M represents only a portion of the broader IoT capabilities.

The Focus Group on M2M Service Layer (FG M2M), established in 2012, has played a crucial role in defining the requirements and specifications for a common M2M service layer. FG M2M has particularly focused on e-health applications, working to integrate insights from various stakeholders, including the World Health Organization, to enhance remote patient monitoring and assisted living services. The group's deliverables encompass a comprehensive overview of e-health use cases, ecosystem analysis, service layer requirements, and a standards repository for M2M.

Moreover, the ITU-T has maintained strong collaborative relationships with external entities, such as the European Internet of Things (IERC) initiative. This cooperation has facilitated significant contributions to the development of IoT standards and has been instrumental in refining the definition of IoT and associated reference models. Ongoing joint activities are expected to further strengthen the integration of IoT into various sectors, addressing challenges related to semantics, big data, and specific applications like e-health and Smart Cities.

In summary, the ITU-T's comprehensive approach to IoT standardization demonstrates its commitment to creating a robust framework that supports diverse applications and promotes interoperability across different sectors. Through collaboration with various stakeholders and focused working groups, the ITU-T continues to shape the future of the Internet of Things, addressing the evolving needs of global communications and network infrastructures.

OASIS and IoT Standardization Landscape

The growth of the Internet of Things (IoT) necessitates the integration of various advanced information and communication technologies (ICT) to create scalable and efficient networks of diverse devices and sensors. Key requirements for these systems include:

Reliable Communication: Networks must utilize established messaging patterns and data protocols capable of high-speed, high-volume transactions. This ensures reliable interaction among heterogeneous systems.

Modularity and Reusability: Services and functions should be modular and reusable, allowing for flexible deployment across different systems, much like LEGO blocks. This facilitates the easy combination of services in diverse configurations. The rise of cloud computing emphasizes the need for services to create widely usable endpoints via Application Programming Interfaces (APIs).

Transaction Reliability: Reliable interaction patterns have evolved to support automated systems, addressing challenges like duplicate resolution and Quality-of-Service. OASIS has developed standards like MQTT and AMQP to enhance transactional protocols for IoT, ensuring efficient operation even under high-volume conditions.

Data Security and Privacy: The vast amount of data generated by IoT systems presents significant privacy and security challenges. Implementing robust access control and cybersecurity measures is critical to protect sensitive information. OASIS provides several standards for secure multiparty transactions, such as Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML), which help manage identity and access.

Access Control and Cybersecurity: OASIS has established protocols for access control, including advanced capabilities for role-based access and encryption. These standards ensure secure data transmission and management in increasingly complex network environments.

Privacy Management: To safeguard data and maintain trust, systems must incorporate privacy considerations from the outset. Projects like the OASIS Privacy Management Reference Model (PMRM) and Privacy by Design for Software Engineers (PbD-SE) aim to integrate privacy governance and compliance mechanisms into IoT architectures.

In summary, OASIS plays a crucial role in defining standards for the IoT landscape, focusing on reliable communication, modularity, cybersecurity, and privacy management. As IoT networks expand, the need for robust methodologies to manage transactions and protect data privacy will become increasingly vital.