

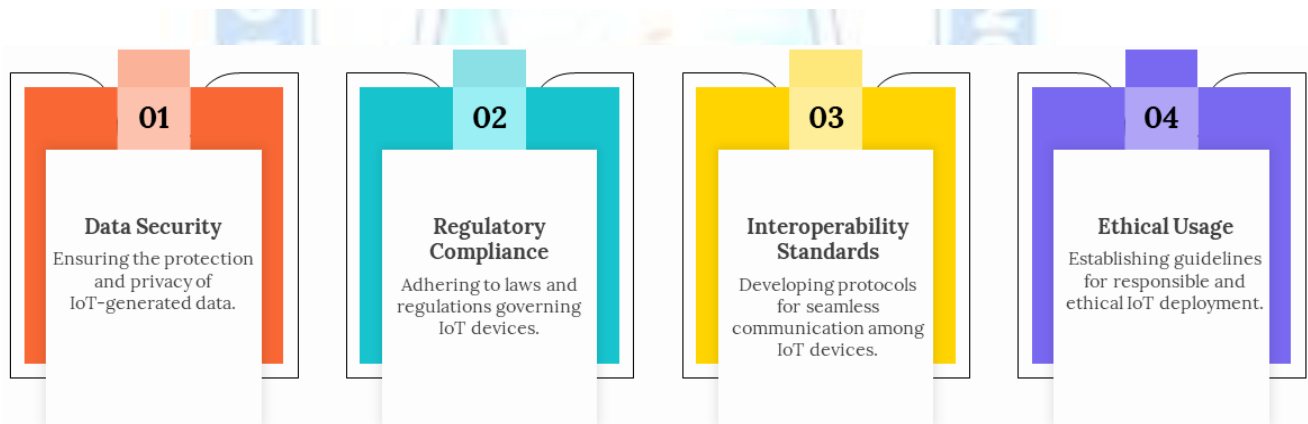
UNIT IV –IOT PRIVACY, SECURITY AND GOVERNANCE

Introduction, Overview of Governance, Privacy and Security Issues, Contribution from FP7 Projects, Security, Privacy and Trust in IoT-Data-Platforms for Smart Cities, First Steps Towards a Secure Platform, Smartie Approach. Data Aggregation for the IoT in Smart Cities, Security.

INTRODUCTION, OVERVIEW OF GOVERNANCE

- Governance, security and privacy are probably the most challenging issues in the Internet of Things (IoT)/While most of the organisation work on Internet governance, a logical step can extend these concepts to IoT governance. But the difficulty of IoT is that the high number and heterogeneity of technologies and devices, which require even more specific Governance solutions and approaches that are more complex in nature. Size and heterogeneity in fact, are the two main components that affect the governance of IoT.
- Heterogeneity requires security to overcome the impossibility of implementing efficient protocols and algorithms on all the devices involved across the many IoT application areas.
- Without guarantees in security, stakeholders of governance ecosystem are unlikely to adopt IoT solutions on a large scale. For this reason, the development of enforcement techniques to support scalability and heterogeneity, to anonymise users' data and to allow context aware data protection are key factors.
- In the IoT context, it is difficult to separate the concepts of Governance, Security and Privacy, because addressing privacy and security aspects to achieve trust in IoT would probably need governance mechanisms as well.
- Data governance is the practice of managing the availability, usability, integrity, and security of an organization's data assets. In the context of IoT, it ensures that data is collected, stored, processed, and analyzed in a consistent, reliable, and compliant manner. Here are some key reasons why data governance is crucial for IoT success:
- **Regulatory Compliance:** IoT devices often collect and process sensitive personal data, necessitating adherence to stringent regulations like GDPR, CCPA, and HIPAA. Data governance ensures that organizations can demonstrate compliance and avoid hefty fines.

- **Data Quality:** IoT devices can generate inaccurate or incomplete data due to various factors, such as sensor malfunctions or network connectivity issues. Data governance helps identify and rectify data quality issues, ensuring that decisions are based on reliable information.
- **Data Security:** IoT devices are potential targets for cyberattacks, making data security a paramount concern. Data governance establishes policies and procedures to protect sensitive data from unauthorized access, breaches, and data loss.
- **Data Privacy:** IoT devices often collect personal data, raising privacy concerns. Data governance helps organizations implement measures to protect individuals' privacy rights and comply with data privacy regulations.
- **Data Accessibility:** A well-governed data environment empowers users to access and analyze data, regardless of their technical expertise. Data governance fosters data literacy and enables data-driven decision-making across the organization.



Key Capabilities of a Data Governance Framework

A comprehensive data governance framework incorporates various capabilities to ensure data quality, security, and compliance. Let's delve into some of the critical capabilities:

1. **Data Catalog:** A data catalog provides a centralized repository of information about data assets, including their definitions, metadata, and relationships. It enables users to discover and understand data, accelerating data analysis and insights.
2. **Business Glossary:** A business glossary defines common business terms and their meanings, ensuring consistent understanding across the organization. It helps bridge the gap between technical and business users, facilitating effective communication and collaboration.

3. **Data Lineage:** Data lineage traces the journey of data from its source to its destination, revealing how data is transformed and used. It helps identify data dependencies, assess impact, and troubleshoot data quality issues.
4. **Data Discovery:** Data discovery tools enable users to search, explore, and visualize data. They help users find relevant data, understand its context, and gain insights without requiring deep technical skills.
5. **Data Quality:** Data quality management ensures that data is accurate, complete, consistent, timely, and relevant. It involves monitoring data quality metrics, implementing data cleansing and validation processes, and establishing data quality standards.

