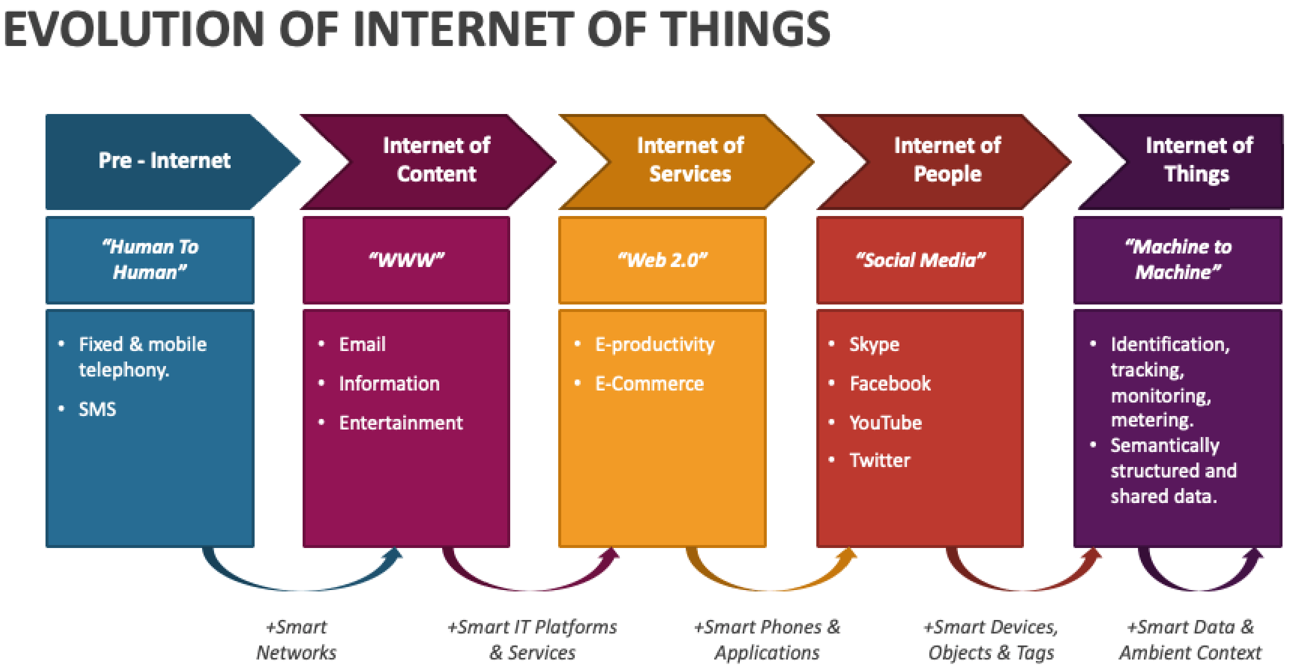
People
Process
The four pillars of IoE:
Data
Things

Internet of Everything DJS22CEC702

By Prof. Nilesh Ghavate

Module 1: Internet Evolution

- Introduction Overview of IoT:
  - IoT Evolution,
  - Characteristics of IoT,
  - IoT Stack,
  - Application areas of IoT,
  - IoT Challenges.
- M2M Technology
- Understanding IoE-IoE Pyramids,
- IoT 2.0
- IoE Benefits
- Disambiguation of IoT vs IoE vs M2M



EVOLUTION OF INTERNET OF THINGS

Pre - Internet	Internet of Content	Internet of Services	Internet of People	Internet of Things
"Human To Human"	*"WWW"*	*"Web 2.0"*	*"Social Media"*	*"Machine to Machine"*
• Fixed & mobile telephony. • SMS	• Email • Information • Entertainment	• E-productivity • E-Commerce	• Skype • Facebook • YouTube • Twitter	• Identification, tracking, monitoring, metering. • Semantically structured and shared data.

+Smart Networks

+Smart IT Platforms & Services

+Smart Phones & Applications

+Smart Devices, Objects & Tags

+Smart Data & Ambient Context

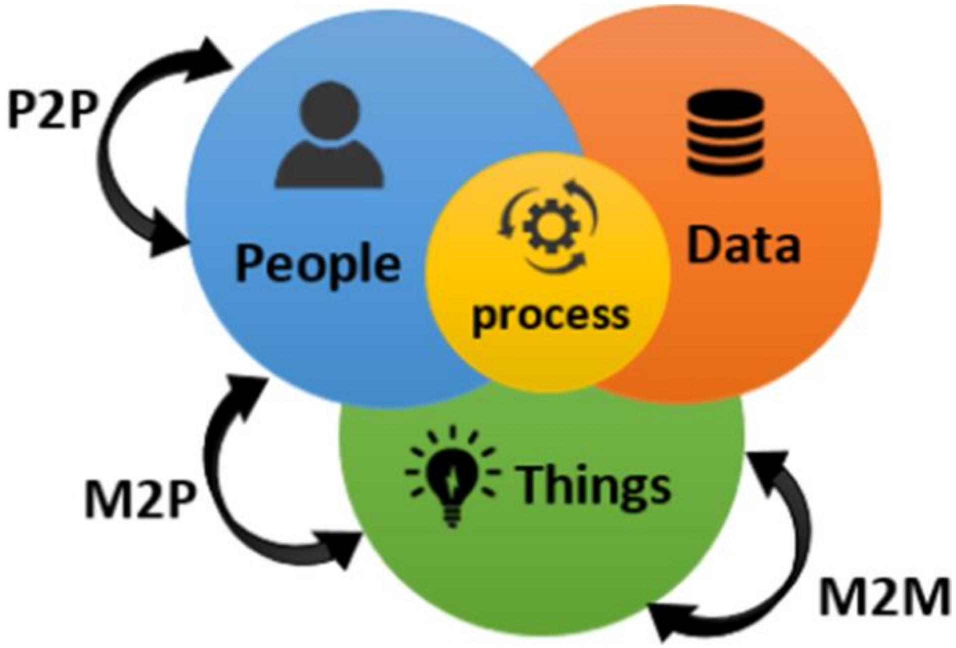
Introduction to IoE

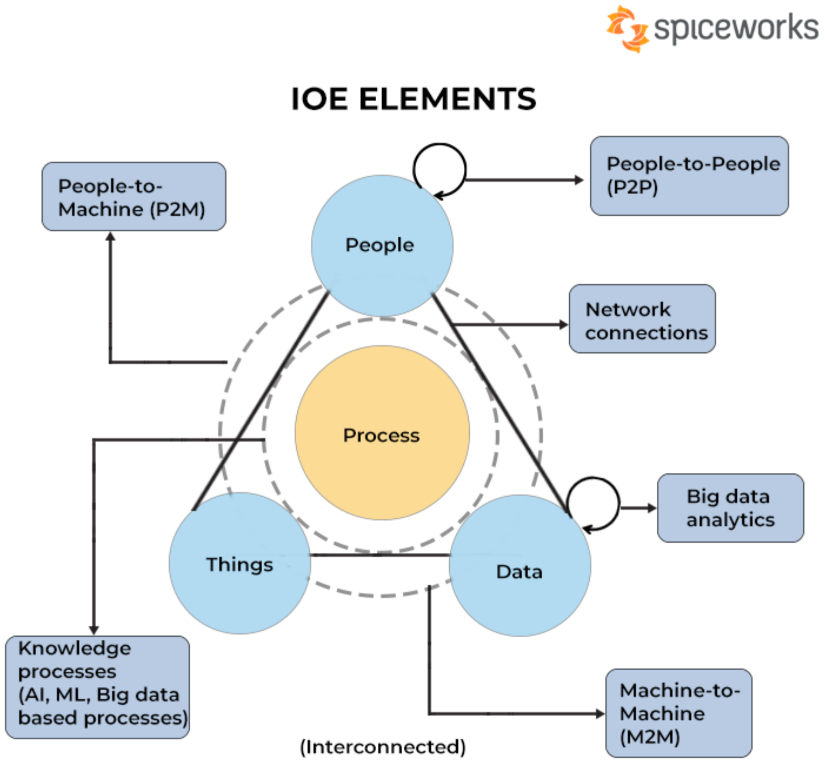
- IoE refers to the smart connection of **people, processes, data, and objects.**
- Envisions a world where billions of things are connected via either private or public networks.
- Devices are embedded with sensors to **measure, detect, and analyze status.**
- Covers a wide range of goods and services connected through the internet.
- IoE includes laptops, desktops, tablets, and smarter machines.
- Real-world applications use digital sensor tools, machine learning, etc.

Technological Context of IoE

- Several technological advancements led to the development of **packet switching, ARPANET**, and related technologies.
- Current research expands the Internet's infrastructure in terms of **scalability, performance, and high-level capabilities**. The operational structure includes both **technical and administrative** components.
- Due to its **social and collaborative nature**, many Internet users contribute to developing new technologies. **Commercial interest** helps in spreading research and integrating it with existing infrastructure.
- IoT brings together **people, devices, data, and processes**, connecting everyday devices (e.g., mobiles, PCs, wearables, coffee makers) as intelligent, communicating **network nodes**.

Elements of Internet of Everything (IoE)





People in IoE

- Key contributors in generating, sharing, and consuming data. People connect via PCs, phones, tablets, fitness trackers, smart clothing, Skin sensors, smart tattoos and social media platforms
- These tools generate data and insights for enterprises.
- Provide real-time feedback through devices and platforms
- Act as decision-makers and users in IoE systems
- Enable personalization and context-aware services
- Participate in collaborative innovation and problem-solving
- Bridge human intelligence with machinne data

Things in IoE

- Refers to physical devices like consumer gadgets, machines, sensors, and actuators.
- Enables communication across the network.
- Data is generated by devices and retrieved from surroundings.
- These things are context-aware, intelligent, and cognitive.
- IoT uses **sensors and actuators** for device communication and form the **core components** of IoT infrastructure

Data in IoE

PEOPLE
PROCESS
DATA
THINGS

- Devices linked to IoE generate raw data.
- Raw data is processed, analyzed, classified, and summarized.
- Processed data provides meaningful insights and empowers devices.
- Data helps in controlling and monitoring IoE systems.

Process in IoE

- Involves analyzing data using AI, ML, and IoT-based processes.
- Ensures correct information flows across networks.
- Supports business decision-making and competitive advantage.
- Helps in improving strategies and operations

Overview of IoT

- IoT stands for Internet of Things.
- It is system of interconnected computing devices , machines and digital machines, objects or people that have unique identifier and person-person network.
- It refers to the network of physical devices connected to the Internet.
- Devices collect and exchange data using embedded sensors.
- Examples: Smart thermostats, wearables, connected vehicles.

Working of Internet of Things (IoT)

Understanding how IoT devices collect, transmit, and act on data

1. Sensing (Data Collection)

- Sensors and devices collect data from the environment.
- Examples: Temperature sensors, motion detectors, GPS.
- This is the foundation for IoT – turning real-world conditions into digital data.

2. Connectivity (Data Transmission)

- Data is sent to cloud or processing units.
- Technologies: Wi-Fi, Bluetooth, ZigBee, Cellular (4G/5G), LPWAN (LoRa, NB-IoT).
- Enables real-time access and remote monitoring.

3. Data Processing

- Data is processed either in the cloud or locally (Edge Computing).
- Can involve filtering, analyzing, or running ML models.
- Example: Smart cameras detect intrusions in real-time.

4. Action or Decision

- Based on processed data, the system takes action or notifies the user.
- Examples: Turning on devices, sending alerts.
- Enables automation and smarter environments.

5. User Interaction / Monitoring

- Users interact via mobile apps, dashboards, or voice assistants.
- Allows remote control and real-time monitoring.
- Critical for user awareness and manual intervention if needed.

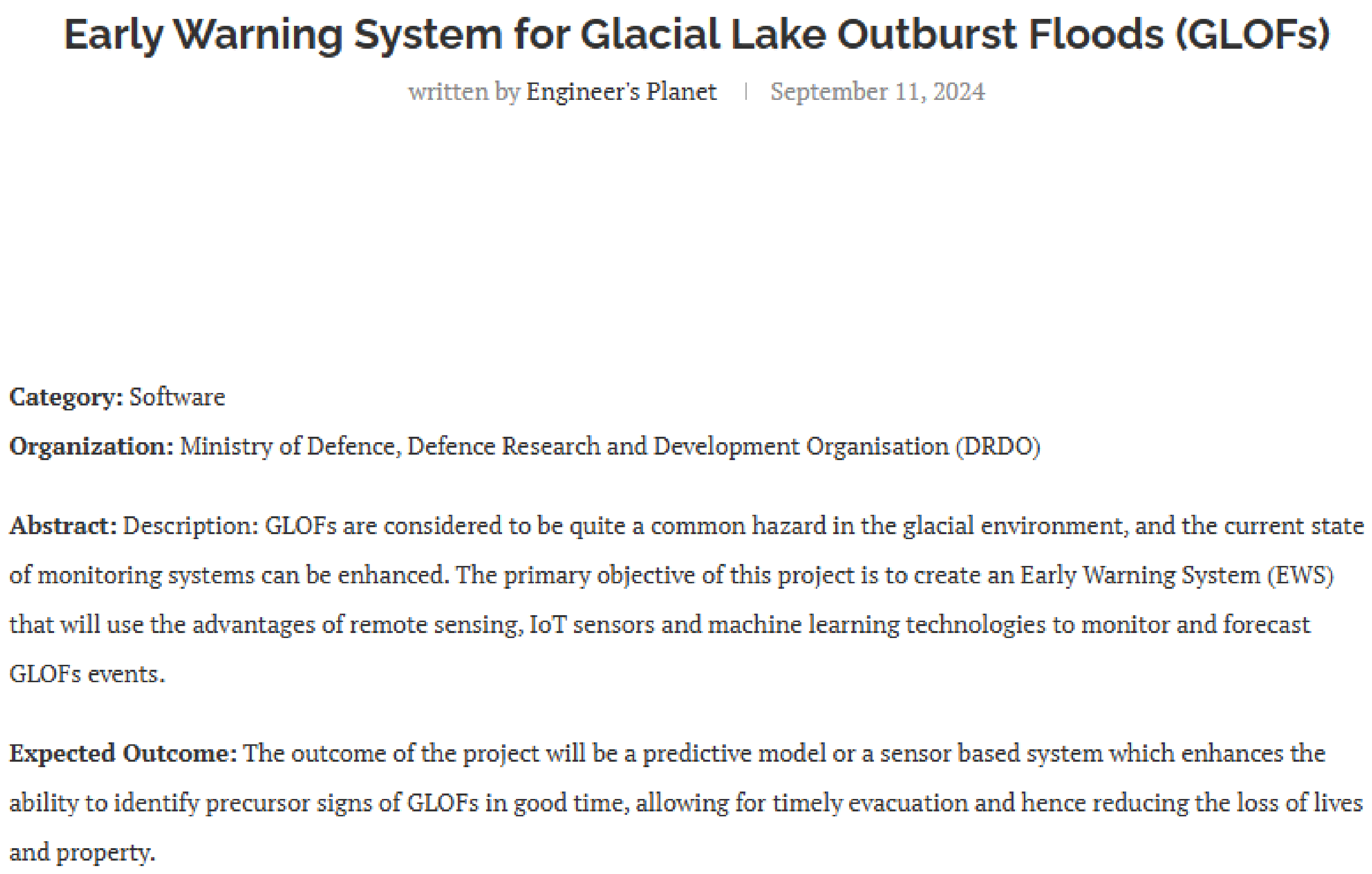
Advantages of IoT

- Automation and Control: Enables smart automation in homes, industries, and transportation.
- Efficiency and Time Saving: Reduces human intervention, saving time and effort.
- Improved Monitoring: Real-time tracking of resources, energy usage, and system performance.
- Better Decision Making: Data-driven insights improve forecasting and business strategies.
- Enhanced Quality of Life: Health monitoring, smart cities, and smart appliances improve living standards.

Disadvantages of IoT

- Security Issues: Devices can be vulnerable to hacking and data breaches.
- Privacy Concerns: Continuous data collection may infringe on users' privacy.
- Complex Infrastructure: Requires integration of hardware, software, and connectivity.
- High Initial Costs: Installation and deployment can be expensive for large systems.
- Dependence on Internet: Functionality relies heavily on internet connectivity.

SIH 2024 Problem statement



Early Warning System for Glacial Lake Outburst Floods (GLOFs)

written by Engineer's Planet | September 11, 2024

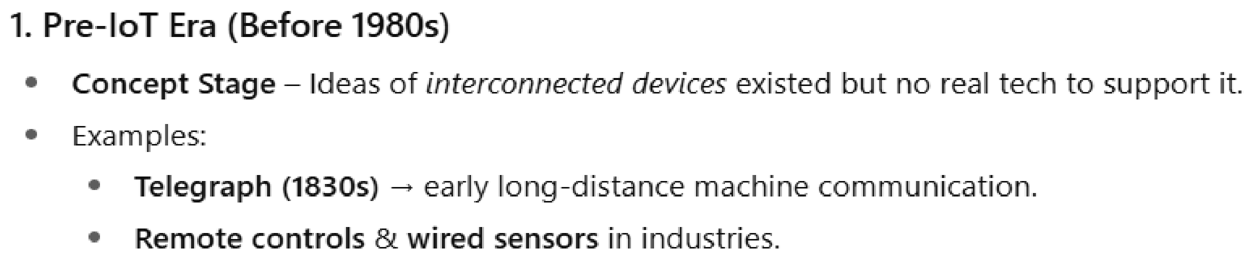
Category: Software

Organization: Ministry of Defence, Defence Research and Development Organisation (DRDO)

Abstract: Description: GLOFs are considered to be quite a common hazard in the glacial environment, and the current state of monitoring systems can be enhanced. The primary objective of this project is to create an Early Warning System (EWS) that will use the advantages of remote sensing, IoT sensors and machine learning technologies to monitor and forecast GLOFs events.

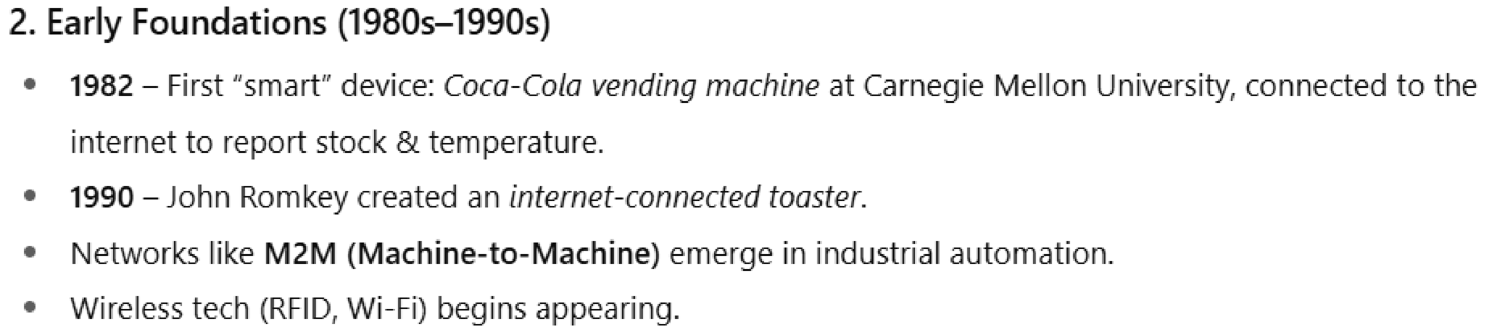
Expected Outcome: The outcome of the project will be a predictive model or a sensor based system which enhances the ability to identify precursor signs of GLOFs in good time, allowing for timely evacuation and hence reducing the loss of lives and property.

Evolution of IoT



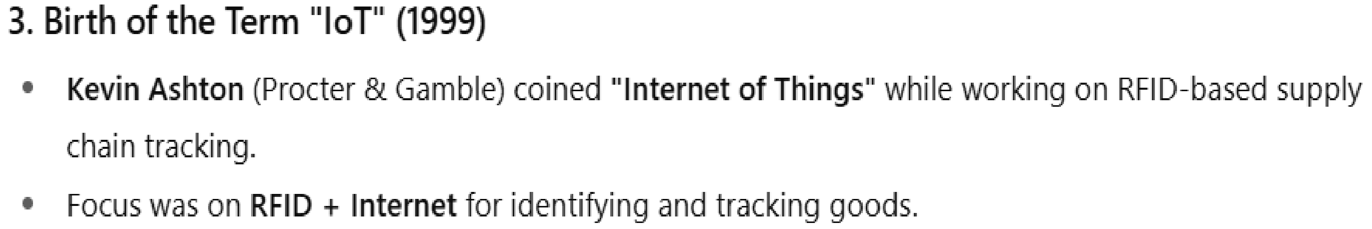
1. Pre-IoT Era (Before 1980s)

- **Concept Stage** – Ideas of *interconnected devices* existed but no real tech to support it.
- Examples:
  - **Telegraph (1830s)** → early long-distance machine communication.
  - **Remote controls** & **wired sensors** in industries.



2. Early Foundations (1980s–1990s)

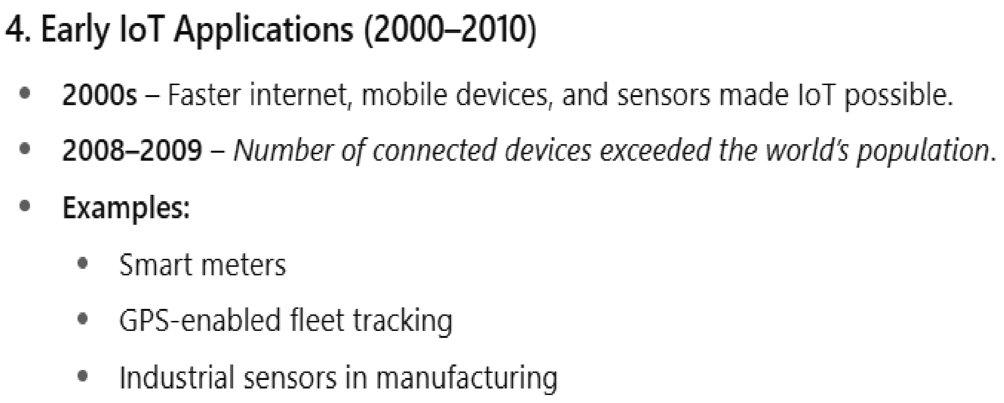
- **1982** – First “smart” device: *Coca-Cola vending machine* at Carnegie Mellon University, connected to the internet to report stock & temperature.
- **1990** – John Romkey created an *internet-connected toaster*.
- Networks like **M2M (Machine-to-Machine)** emerge in industrial automation.
- Wireless tech (RFID, Wi-Fi) begins appearing.



3. Birth of the Term "IoT" (1999)

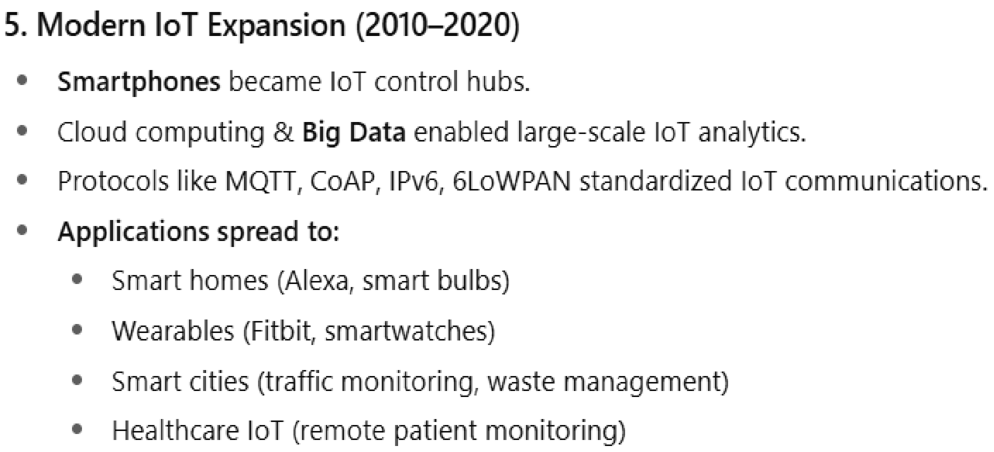
- **Kevin Ashton** (Procter & Gamble) coined **"Internet of Things"** while working on RFID-based supply chain tracking.
- Focus was on **RFID + Internet** for identifying and tracking goods.

Evolution of IoT



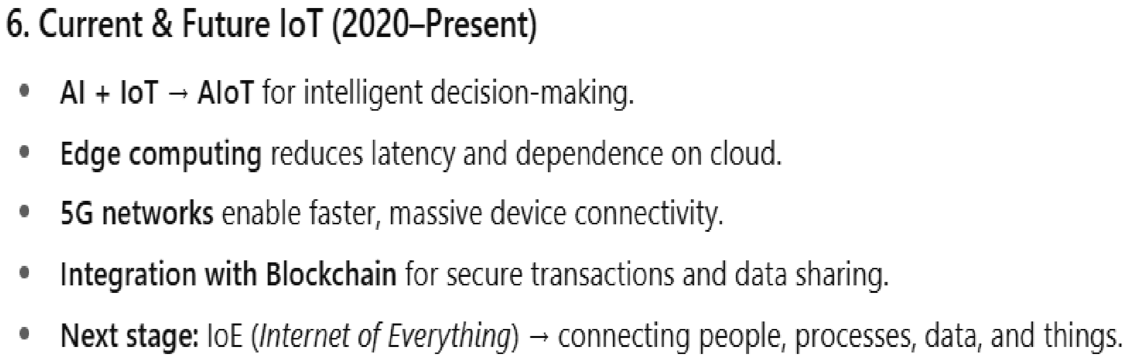
4. Early IoT Applications (2000–2010)

- **2000s** – Faster internet, mobile devices, and sensors made IoT possible.
- **2008–2009** – *Number of connected devices exceeded the world's population*.
- **Examples:**
  - Smart meters
  - GPS-enabled fleet tracking
  - Industrial sensors in manufacturing



5. Modern IoT Expansion (2010–2020)

- **Smartphones** became IoT control hubs.
- Cloud computing & **Big Data** enabled large-scale IoT analytics.
- Protocols like MQTT, CoAP, IPv6, 6LoWPAN standardized IoT communications.
- **Applications spread to:**
  - Smart homes (Alexa, smart bulbs)
  - Wearables (Fitbit, smartwatches)
  - Smart cities (traffic monitoring, waste management)
  - Healthcare IoT (remote patient monitoring)



6. Current & Future IoT (2020–Present)

- **AI + IoT → AIoT** for intelligent decision-making.
- **Edge computing** reduces latency and dependence on cloud.
- **5G networks** enable faster, massive device connectivity.
- **Integration with Blockchain** for secure transactions and data sharing.
- **Next stage:** IoE (*Internet of Everything*) → connecting people, processes, data, and things.

Applications of IoT

1. Smart Lighting
2. Water management
3. Smart tourism
4. Smart Parking
5. Waste management
6. Self driven cars
7. IoT retail shops
8. Air quality management

Characteristics of IoT

- ❑ Intelligence - incorporation of Artificial Intelligence for responding intelligently during device integration.
- ❑ Connectivity - connecting multiple devices through network useful for object level integration.
- ❑ Security - IoT devices are exposed to security risks.
- ❑ Scalability - many devices connected daily to IoT network causing enormous expansion and data handling.
- ❑ Dynamic & Self adapting - dynamic to adopt shifting circumstances and flexible to adopt various environment – light adjustment in morning, afternoon, & night.
- ❑ Architecture - no uniform architecture. capable of accepting goods from different manufactures.

IoT Stack / Architecture

- Different technologies, applications, standards utilized to construct an IoT application referred to IoT technology stack. It includes everything needed to create application, send data and provide notification and other useful insights.
- Dividing IoT solution into 5 layers

1. **Device Hardware:** Physical sensors, Raspberry Pi, Arduino and Actuators.
2. **Device Software**: Software defined hardware phrase is enabled by device software. Software enables different application with single device. This layer is important because it connects hardware to cloud and decides how much functionality will be in hardware and cloud. This layer is divided into 2 layers:

   a. **Device OS** – depending on complexity of IoT solution, type of device OS will be needed. Deciding factors for OS selection are whether real time processing essential, sort of I/O support needed,

   b.**Device Application**- It works above OS . Useful for data collection, cloud streaming, analytics, local control etc.

3. **Communication-** covers network protocols for connection establishment
4. **Cloud platform-**data gathering and management.
5. **Cloud application**

Layer 1 – Device Hardware

- "Things" in IoT = devices that connect the real and online worlds; form the first IoT layer.
- Determine if the product is already a connected device or needs added sensors/communication to become one.
- Primary purpose: data gathering — hardware depends on what type and amount of data is required.
- Minimal data needs → single sensor.
- Complex data needs → multiple sensors, strong CPU, local storage, industrial computers.
- Must consider price, size, ease of deployment, and maintenance when selecting hardware.

Layer 1 – Device Hardware

- Examples:
- Compact devices (e.g., smartwatches) → limited space, use System-on-Chip (SoC).
- More complex solutions → embedded computers like Raspberry Pi, Arduino, BeagleBone.
- Advanced industrial solutions → tiny RIO, PXI for high computing demands.

- Each hardware choice differs in cost, size, battery life, and application.

Layer 2 – Device Software

- Responsible for transforming hardware into a “smart device”.
- Enables software-defined hardware.
- Allows:
- - Remote software updates
- - Real-time analytics
- - Cloud communication

Layer 2a-Device OS

- Operates close to hardware.
- Enables real-time processing & I/O support.
- Examples:
- - Linux
- - Brillo (Android-based)
- - Windows Embedded
- - VxWorks

Layer 2b-Device Applications

- Operates above Device OS.
- Offers specialized functionality (e.g., data collection, analytics).
- Example Use Case:
- - Wind turbine monitor
- - Accelerometer samples vibration
- - Sends only relevant alerts to cloud

Layer 3 – Communication

- Responsible for data exchange.
- Termed as “connectivity”.
- Varies by sector and device type.
- It decides individual sensor will have connection establishment for data transfer or combined aggregated data will be transferred through one link.

Layer 4 – Cloud platform

- It is important for data gathering and management. Data is transmitted to cloud via different devices depending on kind and volume of data generated by solution.

IoT Challenges

- Challenges in IoT Security
- Challenges in IoT Design
- Challenges in IoT Deployment

Challenges in IoT Security

The Internet of Things (IoT) faces a variety of obstacles, especially in security and design.

1. Lack of encryption: Encryption is often missing in IoT devices, making them vulnerable to hacking and data breaches.

2. Lack of testing and updating: Rapid development without adequate testing leads to unpatched vulnerabilities in many IoT devices.

3. Malware and ransomware: With increasing devices, threats grow. Malware encrypts data, retaining access to users' vital information.

4. Botnet targeting cryptocurrency: IoT botnets threaten data privacy and open crypto markets. Blockchain security is improving, but app development remains a weak link.

Challenges in IoT Design

1. Limitation of battery life: Small chips demand higher power. Larger displays increase power needs despite compact device sizes.

2. Increased cost and time to market: Cost is a constraint. Designers must optimize costs and reduce design time to meet market demands.

3. System Security: The adoption of cryptographic techniques and security protocols is needed to construct and execute embedded systems that are reliable, resilient, and secure.

All embedded system components must be secured using a variety of methods from prototype to implementation.

Challenges in IoT Deployment

1)Connectivity – Reliable network links between devices, apps, and cloud platforms are essential. Weak connections hinder monitoring and data processing.

2)Cross-platform capability – IoT apps must be compatible with the latest technologies and have balanced hardware/software features to ensure smooth operation.

3)Data collection & processing – Effective storage, processing, security, and privacy of IoT data require careful planning.

4)Skill shortage – Skilled professionals are vital to overcoming IoT deployment issues and ensuring successful application development.

Conclusion

- IoT is transforming industries and daily life.
- Offers automation, efficiency, and insights.
- Challenges must be addressed for sustainable growth.
- Future trends: AI integration, Edge Computing, 6G.

IoT Architecture for Smart Cities

- **1. Perception Layer (Sensing & Actuation)**
- **Purpose:** Capture real-world data and take actions.
- **Components:**
  - **Sensors:**
    - Environmental: Temperature, humidity, air quality (PM2.5, CO_2)
    - Traffic: Vehicle counters, speed detectors, road condition sensors
    - Utilities: Water flow meters, smart electricity meters, waste bin fill sensors
    - Public safety: CCTV cameras, gunshot detectors, flood level sensors
  - **Actuators:**
    - Traffic lights, street light dimmers, water pumps, automatic gates

IoT Architecture for Smart Cities

- **2. Network Layer (Data Transmission)**
- **Purpose:** Move data from devices to processing units securely and efficiently.
- **Technologies:**
  - **Short-range:** Zigbee, BLE, Wi-Fi, LoRaWAN (low power, wide area)
  - **Long-range:** 4G/5G, NB-IoT, LTE-M
  - **IoT Protocols:** MQTT, CoAP, AMQP, HTTP/REST
  - **Networking Support:** IPv6, 6LoWPAN for low-power devices

IoT Architecture for Smart Cities

- **3. Edge Layer (Local Processing)**
- **Purpose:** Process data near the source to reduce latency.
- **Components:**
  - Edge gateways or micro data centers
  - Raspberry Pi / Industrial IoT gateways for protocol translation & data aggregation
  - AI/ML inference at edge (e.g., detecting traffic congestion from camera feed in real-time)

IoT Architecture for Smart Cities

- **4. Data Processing Layer (Cloud & Big Data)**
- **Purpose:** Heavy processing, storage, and analytics.
- **Technologies:**
  - Cloud Platforms: AWS IoT Core, Azure IoT Hub, Google Cloud IoT
  - Big Data Tools: Apache Kafka, Spark, Hadoop
  - Databases: NoSQL (MongoDB, Cassandra), Time-series DB (InfluxDB)

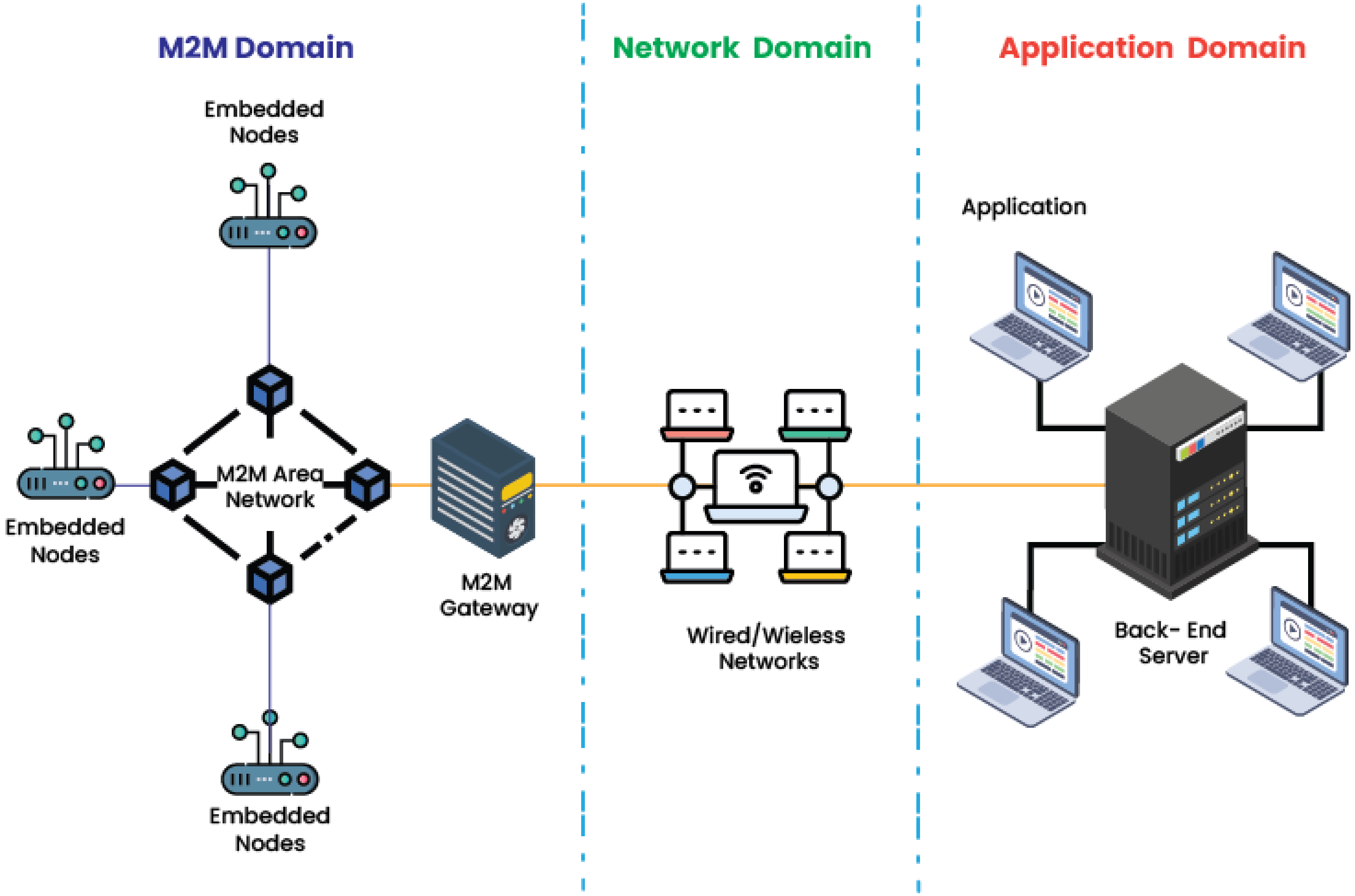
IoT Architecture for Smart Cities

- **5. Application Layer (User Interaction)**
- **Purpose:** Provide insights, dashboards, and control mechanisms.
- **Features:**
  - City management dashboard
  - Mobile apps for citizens (real-time bus tracking, pollution levels, emergency alerts)
  - AI-powered predictions (traffic rerouting, energy optimization)

IoT Architecture for Smart Cities

- **6. Security Layer (Cross-Layer)**
- **Purpose:** Secure the entire ecosystem.
- **Measures:**
  - Device authentication & authorization
  - Data encryption (TLS/SSL)
  - Intrusion detection
  - Blockchain for tamper-proof transactions

Machine 2 Machine Communication



M2M Technology (Machine-to-Machine Technology)

M2M Technology (Machine-to-Machine Technology) refers to the direct communication between two or more devices or machines without human intervention. It enables devices to exchange data and perform actions based on that data automatically.

M2M is a type of communication where machines (devices, sensors, or systems) talk to each other using a network (wired or wireless), enabling automation and remote monitoring/control.

Key Components:

- Sensors or Devices – Collect real-time data (e.g., temperature, pressure).
- Network – Transfers data (e.g., cellular, Wi-Fi, Ethernet).
- Data Processing Unit / Platform – Analyzes the data.
- Actuators/Controllers – Trigger actions based on data analysis.
- M2M Software – For analytics, visualization, alerts, and remote commands.

How It Works:

- A sensor detects a condition (e.g., a machine gets too hot).
- The sensor sends the data via a network.
- The system processes this data.
- The system decides an action (e.g., shut down the machine).
- The command is executed — all automatically.

Aspect	M2M (Machine-to-Machine)	IoT (Internet of Things)	IoE (Internet of Everything)
Definition	Communication between machines without human input	Network of connected devices that share data	Broader concept: IoT + people + processes + data
Focus	Device-to-device communication	Device-to-device + cloud + analytics	Integration of people, process, data, and things
Human Involvement	No (fully automated communication)	Minimal (for monitoring or control)	Yes (people are integral to decision-making)
Connectivity	Point-to-point or closed networks	IP-based, internet-enabled, often cloud-based	Internet + context-aware systems
Technology Used	Cellular, wired, proprietary protocols	Wi-Fi, Bluetooth, ZigBee, MQTT, cloud platforms	AI, Big Data, Cloud, IoT, Analytics, Machine Learning
Data Usage	Data used for direct control/feedback	Data used for analysis, automation, optimization	Data is used to drive intelligent business actions
Scope	Narrow (specific machine functions)	Broader (network of devices/systems)	Broadest (includes everything: devices, people, data)
Example	Vending machine alerts supplier when low	Smart home controlling lights, AC remotely	Smart city optimizing traffic based on real-time data

IoT 2.0

IoT 2.0 refers to the **evolved, smarter, more secure, and integrated version** of the original IoT (Internet of Things). It addresses the limitations of traditional IoT (1.0) and brings **intelligence, interoperability, automation, and scalability** to a much higher level.

IoT 2.0

Feature	IoT 1.0	IoT 2.0
Focus	Device connectivity	Intelligent, autonomous ecosystems
Data Processing	Mostly cloud-based	Edge + cloud + AI-driven
Intelligence	Reactive (basic monitoring/control)	Proactive (predictive, self-healing systems)
Interoperability	Limited, proprietary protocols	Open standards, seamless device integration
Security	Basic, often patchy	Built-in, end-to-end, AI-based threat detection
Scalability	Challenging as devices increase	Designed for massive scale (billions of devices)
Architecture	Cloud-centric	Distributed (Edge, Fog, Mesh networks)
User Involvement	Manual interaction required	Automation + contextual decision-making
Example	Smart light turns on via app	Light auto-adjusts brightness based on presence, time, and mood

Key Features of IoT 2.0:

Edge & Fog Computing: Data processed locally for faster, real-time decision-making.

AI & Machine Learning: Devices learn from patterns and make decisions autonomously.

5G & Beyond: Ultra-fast, low-latency connectivity supports massive IoT deployments.

Security by Design: AI-driven threat detection, blockchain, and secure boot.

Digital Twins: Virtual replicas of physical assets for simulation and monitoring.

Self-Healing Networks: Systems detect and fix issues without human input.

Interconnected Ecosystems: Cross-domain integration (smart home + healthcare + city).