ROHINI
COLLEGE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)
Approved By AICTE & Affiliated to Anna University
NBA Accredited for All Eligible B.E/B.Tech Programs | NAAC Accredited with A+ Grade
Near Anjugramam - Kanyakumari Main Road, Palkulam, Variyoor P.O.-629401, Kanyakumari Dist, Tamil Nadu.

DEPARTMENT OF BIOMEDICAL ENGINEERING

VI Semester

24BM501 BIOMEDICAL DEVICE DESIGN

UNIT- III WEARABLE, IoT AND AI-ENABLED MEDICAL DEVICES

Syllabus: UNIT III - WEARABLE, IoT AND AI-ENABLED MEDICAL DEVICES: Internet of Medical Things (IoMT), Wearable Healthcare Technologies, Smart Health Monitoring Devices, AI and Machine Learning in Medical Devices.

Contents of this Unit:

Section	Topic	Figures
3.1	Internet of Medical Things (IoMT)	3.1 - 3.7
3.2	Wearable Healthcare Technologies	3.8 - 3.12
3.3	Smart Health Monitoring Devices	3.13 - 3.18
3.4	AI and Machine Learning in Medical Devices	3.19 - 3.26
3.5	Unit Summary, 2-mark questions and 16-mark question bank	-

Learning outcome: After studying this unit the student should be able to explain the architecture and communication technologies of IoMT, describe the working principles of wearable and smart monitoring devices with block diagrams, and discuss the role, evaluation, regulation and challenges of AI/ML in medical devices.

3.1 Internet of Medical Things (IoMT):

3.1.1 Introduction and Definition

The **Internet of Things (IoT)** is a network of physical objects ("things") that have sensors, embedded software and network connectivity so that they can collect and exchange data over the internet without human intervention. When the same idea is applied to healthcare, medical devices, wearables, hospital equipment, software applications and

Definition: IoMT is a connected infrastructure of medical devices, software applications and healthcare systems that communicate with each other over wired and wireless networks to **sense, collect, transmit, store, analyse and act upon** health-related data, so that care can be delivered remotely, continuously, accurately and at lower cost.

health-information systems become "smart" connected things. This connected healthcare ecosystem is called the **Internet of Medical Things (IoMT)**. It is also known as **Healthcare IoT (H-IoT)** or **Smart Healthcare**.

In a conventional system, a patient's data is recorded only when the patient visits a clinic. In IoMT, data such as heart rate, blood pressure, oxygen saturation and glucose is captured **continuously** in the patient's home, workplace or hospital bed and sent automatically to the care team. The doctor therefore moves from **episodic care** to **continuous, proactive and personalised care**.

3.1.2 Need for IoMT

- **Rising burden of chronic diseases:** Diabetes, hypertension, heart disease and COPD need life-long monitoring that cannot be done by occasional hospital visits.
- **Ageing population:** Elderly people living alone need fall detection, medication reminders and emergency alerts.
- **Shortage of doctors and rural access:** In countries like India, specialists are concentrated in cities. IoMT and telemedicine bring expertise to villages.
- **Cost reduction:** Early detection and home monitoring reduce hospital admissions, readmissions and length of stay.
- **Technology push:** Low-cost MEMS sensors, ultra-low-power wireless chips (Bluetooth Low Energy), cloud computing and AI have made connected devices affordable.
- **Pandemic experience:** COVID-19 showed the value of contact-free monitoring (remote pulse oximetry, tele-consultation) and reduced exposure of health workers.

3.1.3 Difference between IoT and IoMT

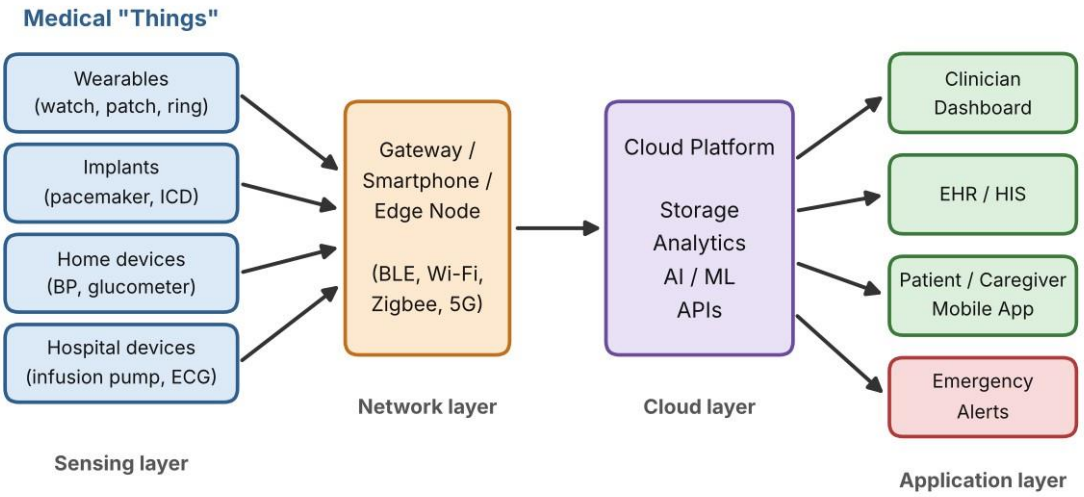
Parameter	General IoT	IoMT
Application domain	Smart home, industry, agriculture, transport	Healthcare, hospitals, patient care, clinical research
Data type	Environmental / machine data	Sensitive personal health information (PHI)
Criticality	Failure usually causes inconvenience	Failure may cause injury or death (life-critical)
Regulation	Few regulations	Strict: CDSCO / FDA / CE-MDR, IEC 60601, ISO 13485
Security & privacy	Moderate	Very high: HIPAA, GDPR, India DPDP Act 2023
Reliability / latency	Tolerant to short delays	Needs high reliability and low latency (alarms, pumps)
Interoperability	Vendor-specific protocols common	Needs HL7 FHIR, DICOM, IEEE 11073 for EHR integration
Examples	Smart bulb, smart meter	Smart insulin pump, connected ECG patch, smart infusion pump

3.1.4 Architecture of IoMT

The overall working of IoMT is shown in Fig. 3.1. Medical "things" at the patient end send data through a gateway (smartphone, bedside hub or router) to a cloud platform. The cloud stores and analyses the

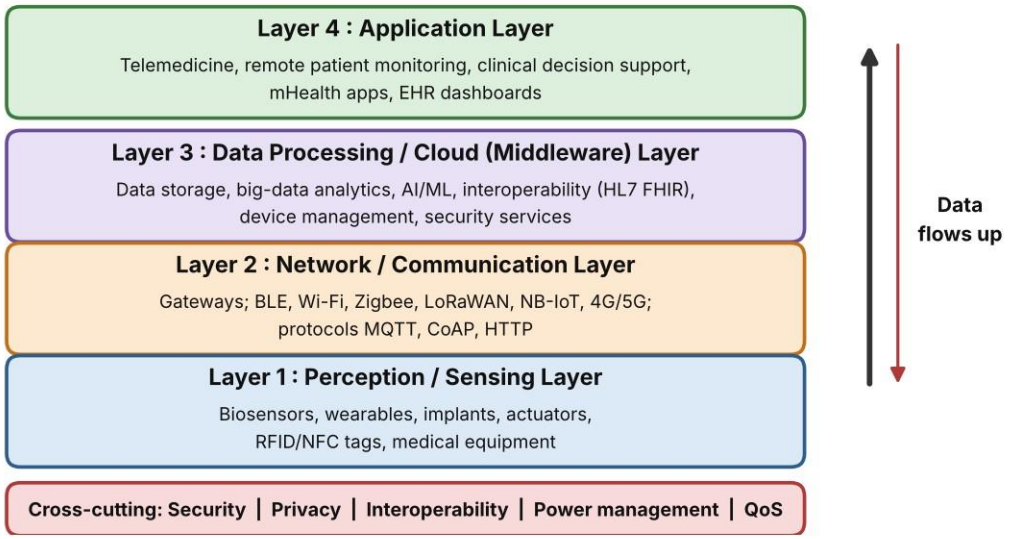
data and delivers information to clinicians, caregivers and patients through dashboards, mobile applications and electronic health record (EHR) systems.

Fig. 3.1 Overview of the Internet of Medical Things (IoMT)



A widely used reference model divides IoMT into **four layers** (Fig. 3.2). Each layer has a clear job, and security and interoperability run across all layers.

Fig. 3.2 Four-Layer Architecture of IoMT



➢ Layer 1 - Perception / Sensing Layer

✓ Contains all the physical devices that interact with the human body or the clinical environment: biosensors (ECG, PPG, temperature, glucose, respiration), wearables, implants, RFID/NFC tags and actuators such as infusion pumps and ventilators.

- ✓ Functions: sensing, signal conditioning, analogue-to-digital conversion, basic local processing and identification of the device/patient.

➢ Layer 2 - Network / Communication Layer

- ✓ Transfers data from devices to the processing layer. Uses short-range links (BLE, Zigbee, NFC, Wi-Fi) between sensors and gateway and long-range links (4G/5G, NB-IoT, LoRaWAN, broadband) from gateway to cloud.
- ✓ Application protocols such as **MQTT, CoAP and HTTP/REST** carry the messages; gateways translate between protocols.

➢ Layer 3 - Data Processing / Cloud (Middleware) Layer

- ✓ Stores huge volumes of patient data in secure databases and data lakes; performs analytics, AI/ML inference, rule-based alerting and trend analysis.
- ✓ Provides device management (registration, firmware over-the-air update), identity management and interoperability services (HL7 FHIR APIs).

➢ Layer 4 - Application Layer

- ✓ Delivers services to end users: remote patient-monitoring dashboards for doctors, mobile apps for patients, tele-consultation, clinical decision support, hospital management systems, insurance and research portals.

3.1.5 Components of an IoMT System

- ❖ **Medical sensors and devices:** biosensors and wearables that measure vital signs and biochemical markers; implantable devices such as pacemakers.
- ❖ **Actuators:** devices that act on the patient, for example smart insulin pumps, infusion pumps, drug-delivery patches, ventilators and neuro-stimulators.
- ❖ **Gateway / edge node:** smartphone or bedside hub that collects data from many sensors, filters it, converts protocols and forwards it securely.
- ❖ **Connectivity:** wireless and wired networks (Section 3.1.6).
- ❖ **Cloud / data centre:** storage, computing, AI engines and APIs.
- ❖ **Software and user interfaces:** dashboards, mobile apps, alarm systems, EHR and hospital information system (HIS) integration.
- ❖ **Security and identity services:** encryption, authentication, consent management and audit trails.

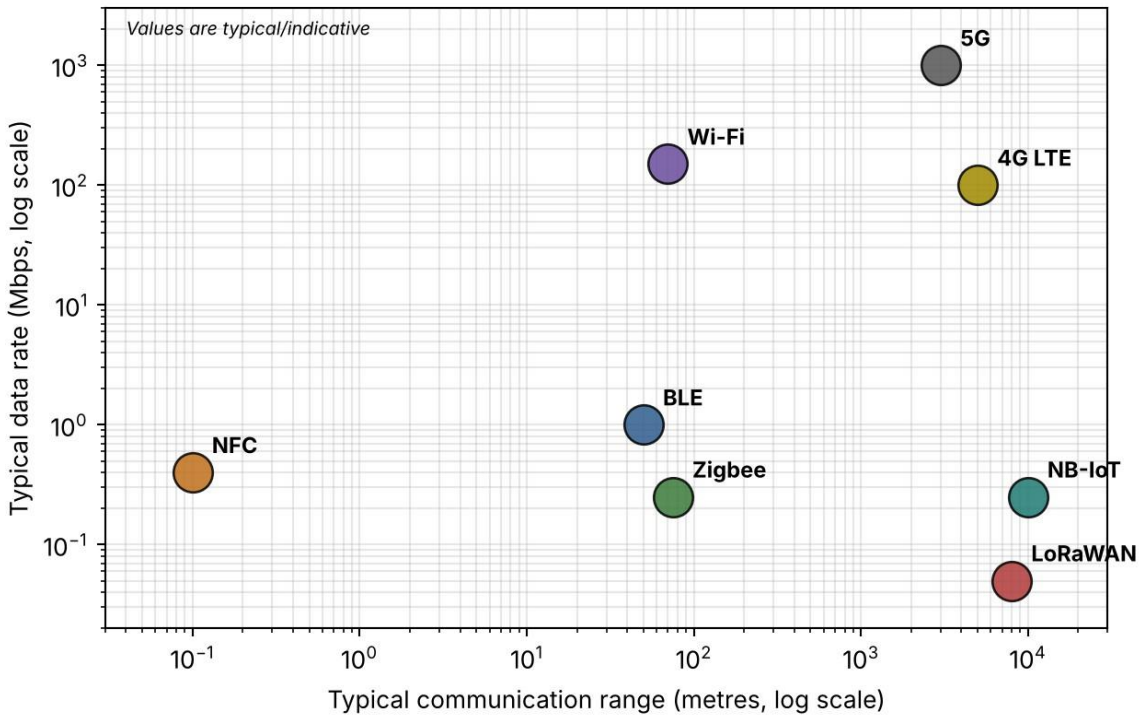
3.1.6 Communication Technologies and Protocols in IoMT

Choice of communication technology is a trade-off between **range, data rate, power consumption and cost**. Implants and small wearables need ultra-low power, whereas imaging devices need high bandwidth.

Technology	Typical range	Data rate	Power	Typical medical use
NFC	< 10 cm	106-424 kbps	Very low	Device pairing, patient ID, glucose sensor read-out

Technology	Typical range	Data rate	Power	Typical medical use
Bluetooth Low Energy (BLE)	10-100 m	1-2 Mbps	Very low	Wearables, BP cuffs, glucometers, ECG patches
Zigbee (IEEE 802.15.4)	10-100 m (mesh)	250 kbps	Low	Hospital sensor networks, ward monitoring
Wi-Fi (IEEE 802.11)	30-100 m	Up to Gbps	High	Bedside monitors, imaging, infusion pumps
MICS / MedRadio (402-405 MHz)	2-5 m	Low	Very low	Communication with implants (pacemakers, ICDs)
LoRaWAN	2-15 km	0.3-50 kbps	Very low	Rural monitoring, asset tracking
NB-IoT / LTE-M	Up to 10 km	~ 250 kbps	Low	Remote patient devices, smart inhalers
4G / 5G	Cellular	100 Mbps - Gbps	High	Ambulance telemetry, tele-surgery, high-quality video

Fig. 3.4 Range vs Data-Rate of Wireless Technologies Used in IoMT



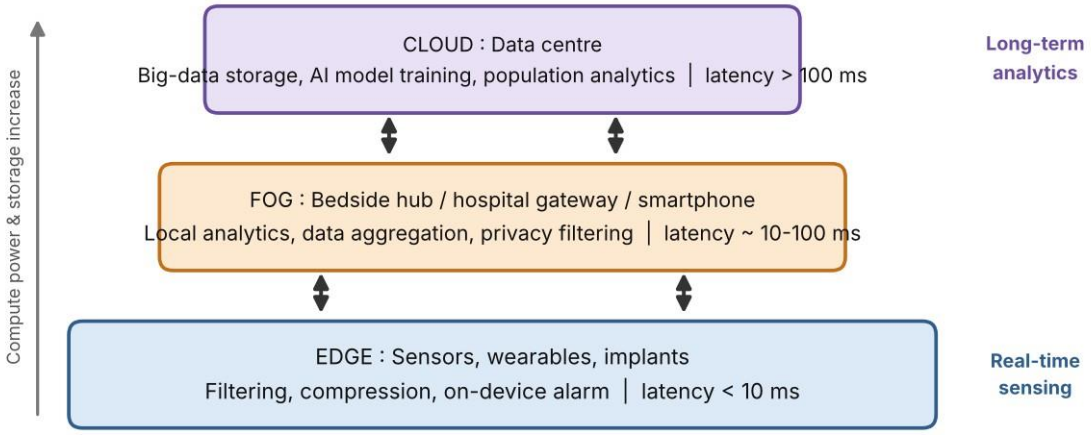
➢ Application-layer and messaging protocols

- **MQTT (Message Queuing Telemetry Transport):** lightweight publish/subscribe protocol over TCP; a sensor "publishes" a vital sign to a topic and subscribed applications receive it. Suitable for low-bandwidth links.
- **CoAP (Constrained Application Protocol):** RESTful protocol over UDP designed for constrained devices; similar to HTTP but with much lower overhead.
- **HTTP/HTTPS (REST APIs):** commonly used between smartphone apps and cloud servers.
- **AMQP / DDS:** reliable messaging used in hospital back-end systems and real-time device integration.

3.1.7 Edge, Fog and Cloud Computing in IoMT

Sending all raw data to a distant cloud causes delay, uses bandwidth and raises privacy concerns. Modern IoMT therefore distributes computing across three tiers (Fig. 3.5).

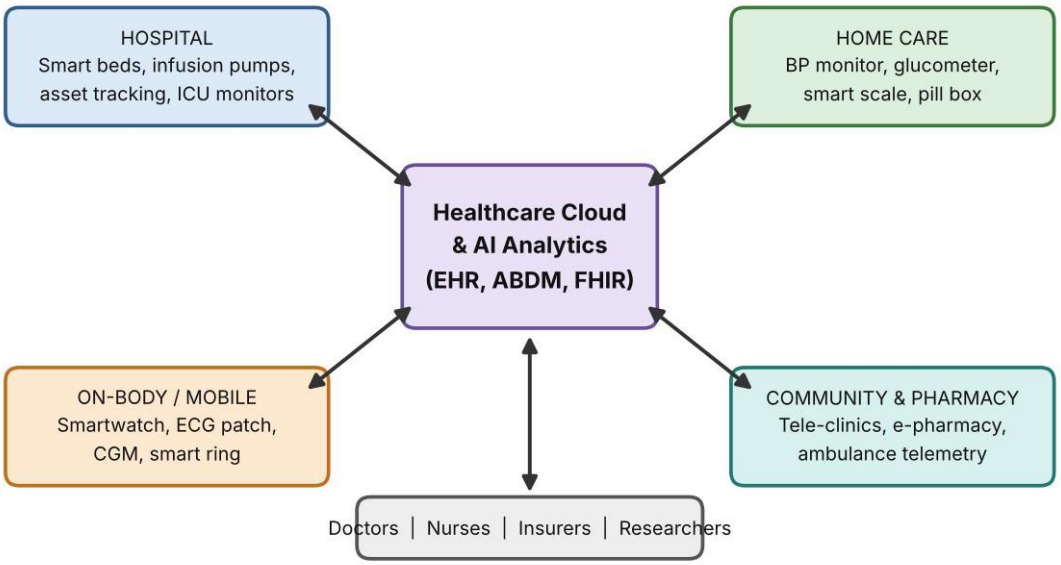
Fig. 3.5 Edge - Fog - Cloud Computing in IoMT



- **Edge computing:** processing inside the sensor, wearable or implant. Example: a smartwatch detecting an irregular pulse locally and sounding an alert within milliseconds, even without internet.
- **Fog computing:** an intermediate layer such as a bedside hub, hospital gateway or smartphone. It aggregates data from many sensors, applies local analytics and removes identifying details before upload.
- **Cloud computing:** elastic storage and heavy computing for long-term records, population-level analytics and training of AI models.

3.1.8 Categories of IoMT Devices and the IoMT Ecosystem

Fig. 3.3 IoMT Ecosystem: Care Settings Connected through the Cloud

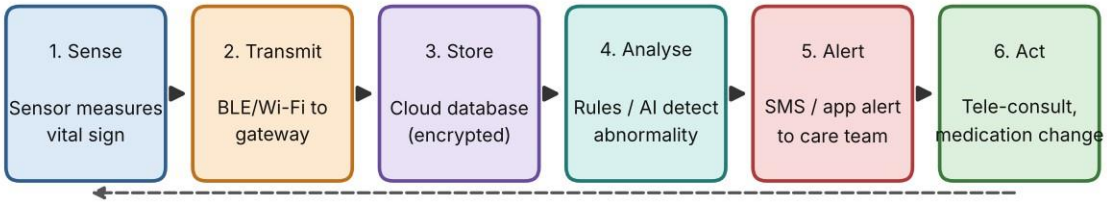


- **Wearable IoMT:** smartwatches, fitness bands, ECG patches, smart rings, CGM sensors worn on the body.
- **Implantable IoMT:** pacemakers, implantable cardioverter-defibrillators (ICD), neuro-stimulators, cochlear implants with wireless telemetry.
- **In-hospital (stationary) IoMT:** smart infusion pumps, connected ventilators, patient monitors, smart beds, imaging systems (CT/MRI) and RFID asset tracking.
- **Home / ambient IoMT:** connected BP monitors, weighing scales, glucometers, smart pill dispensers, fall-detection sensors, sleep mats.
- **Community IoMT:** tele-clinics, mobile health vans, e-pharmacy, ambulance telemetry and public-health surveillance.

3.1.9 Remote Patient Monitoring (RPM) Workflow

Remote patient monitoring is the most important application of IoMT. The workflow of RPM is shown in Fig. 3.7. A sensor measures a vital sign, the data is transmitted to a gateway and cloud, analysed by rules or AI, and if a value crosses a threshold an alert is sent to the care team who can then intervene by tele-consultation or change in medication. The updated plan is sent back to the patient, completing a closed feedback loop.

Fig. 3.7 Remote Patient Monitoring (RPM) Workflow



3.1.10 Applications of IoMT

- **Chronic disease management:** continuous glucose monitoring for diabetes, home BP monitoring for hypertension, weight and fluid monitoring for heart failure.
- **Smart hospitals:** real-time location of equipment and staff by RFID/BLE tags, smart infusion pumps linked to the EHR (dose error reduction), smart beds that detect patient movement and pressure-ulcer risk.
- **Telemedicine and tele-ICU:** remote specialists view live vital signs of ICU patients in rural hospitals.
- **Medication adherence:** smart pill boxes, smart inhalers and ingestible sensors record when a dose is taken and remind the patient.
- **Emergency and ambulance care:** vitals and ECG are streamed from the ambulance so that the cardiology team is ready on arrival.
- **Elderly care and ambient assisted living:** fall detection, wandering alerts, activity pattern analysis.
- **Surgery and rehabilitation:** robot-assisted surgery, tele-rehabilitation with motion sensors.
- **Cold-chain monitoring:** IoT temperature loggers protect vaccines and blood products during storage and transport.
- **Public health surveillance:** aggregated anonymised data helps in early detection of outbreaks.

➢ Indian examples

- ✓ **e-Sanjeevani:** national telemedicine service of the Government of India for doctor-to-patient and doctor-to-doctor consultation.
- ✓ **Ayushman Bharat Digital Mission (ABDM):** builds a national digital health ecosystem with ABHA (health ID), health-facility registries and interoperable health records based on open standards such as HL7 FHIR.

3.1.11 Interoperability and Standards

A major goal of IoMT is that devices and software from different manufacturers should exchange data meaningfully. This is called **interoperability**. It has three levels: technical (connectivity), syntactic (common data format) and semantic (common meaning, e.g. SNOMED CT, LOINC codes).

Standard	Purpose
HL7 v2 / HL7 FHIR	Exchange of clinical and administrative data between healthcare applications; FHIR uses modern web APIs (REST/JSON).
DICOM	Storage and transfer of medical images (X-ray, CT, MRI, ultrasound).
ISO/IEEE 11073 (PHD)	Plug-and-play communication between personal health devices (BP monitor, pulse oximeter, glucometer) and managers.
Continua Design Guidelines (PCHAlliance)	Interoperability guidelines for personal connected-health devices.
IEC 80001-1	Risk management of IT networks that incorporate medical devices.
IEC 60601 series / ISO 13485 / ISO 14971	Safety of electrical medical equipment / quality management / risk management of medical devices.
IEC 62304	Software life-cycle processes for medical device software.

3.1.12 Security, Privacy and Regulatory Aspects

Because IoMT devices handle sensitive data and some of them (pacemakers, insulin pumps) can directly affect patient safety, security is a primary design requirement. A well-known example is the 2017 firmware update issued for about 465,000 pacemakers after a cybersecurity vulnerability was identified, and the 2017 WannaCry ransomware attack that disrupted hospitals of the UK National Health Service.

Fig. 3.6 Security Threats and Countermeasures in IoMT

THREATS	LAYER	COUNTERMEASURES
Tampering, cloning, firmware attack, battery-drain attack	Device layer	Secure boot, signed firmware, tamper-resistant hardware
Eavesdropping, man-in-the-middle, replay, DoS / DDoS	Network layer	TLS/DTLS, AES-128/256, VPN, mutual authentication
Data breach, ransomware, insider misuse, SQL injection	Cloud layer	Encryption at rest, RBAC, audit logs, backups, SIEM
Weak passwords, phishing, API abuse, malware in apps	Application layer	Multi-factor auth, API gateway, secure coding, consent mgmt

➢ Major threats

- ✓ Unauthorised access and data theft (identity theft, selling of medical records).
- ✓ Man-in-the-middle and eavesdropping on wireless links; replay attacks.
- ✓ Denial-of-service attacks that make life-critical devices unavailable.
- ✓ Ransomware on hospital networks; malware on legacy devices that cannot be patched.
- ✓ Physical tampering, device cloning and insecure firmware updates.

➢ Security measures

- ✓ **Encryption** of data in transit (TLS/DTLS) and at rest (AES-256); secure key management.
- ✓ **Authentication and access control:** multi-factor authentication, role-based access, device certificates.
- ✓ **Secure boot and signed over-the-air (OTA) updates** to keep firmware trusted and patched.
- ✓ **Network segmentation / zero-trust architecture** to isolate medical devices from the general hospital network.
- ✓ **Privacy by design:** data minimisation, anonymisation / de-identification, patient consent management, audit logs.
- ✓ **Blockchain** can provide tamper-proof audit trails and patient-controlled data sharing.

➢ Laws and regulations

✓ **HIPAA** (USA) and **GDPR** (European Union) protect health information; **Digital Personal Data Protection (DPDP) Act, 2023** and the Information Technology Act, 2000 apply in India; ABDM has its own health-data management policy.

✓ Medical-device regulators (**CDSCO** under the Medical Devices Rules, 2017 in India; **US FDA**; **EU MDR**) require manufacturers to show cybersecurity risk management as part of device approval.

3.1.13 Advantages and Challenges of IoMT

Advantages	Challenges / Limitations
Continuous real-time monitoring and early warning	Data security, privacy and cyber-attack risk
Better access to care in remote areas	Lack of interoperability between vendors
Reduced hospital visits, readmission and cost	Battery life and power limitations of devices
Personalised treatment based on patient data	Data accuracy, false alarms and alarm fatigue
Fewer medication and human errors	Regulatory complexity and certification cost
Huge data for AI-based research and prediction	Network reliability and digital divide; high initial cost
Improved patient engagement and self-care	Ethical issues: consent, data ownership, liability

3.1.14 Future Trends in IoMT

- **5G / 6G connectivity** with ultra-low latency for tele-surgery and real-time remote care.
- **Edge AI and TinyML** so that devices make decisions locally and protect privacy.
- **Digital twins** of patients and organs for simulation of treatment before it is applied.
- **Federated learning and blockchain** for privacy-preserving data sharing.
- **Internet of Bodies (IoB):** ingestible, implantable and e-skin devices connected to the network.
- **Generative AI assistants** that summarise IoMT data for doctors and patients.