1. How do interoperability and cyber-security challenges affect edge deployment metrics in healthcare?

Edge deployement metrics to be monitored in time-critical healthcare environments are Throughput , Latency , System Uptime , Diagnostic accuracy , Bandwidth usage , Privacy Compilation and Fault Tolerance , Since healthcare is a time sensitive department where every extra calculation done by the system which doesn’t update the current situation on the patient is a Redundancy that has to be prevented but when it comes to cyber security and interoperability where synchronisation of IOT edge devices and securing these edge devices from external control to preventing misdiagnosis are crucial since every mistake can lead to the loss of a life

The thing layer (e.g., end devices like body area networks or CAVs) often consists of diverse devices with varying computational capacities and service goals. This heterogeneity introduces significant interoperability challenges, especially when coordinating data formats, protocols, and task types across devices. In healthcare, this can directly impact deployment efficiency, as inconsistent device behaviour leads to suboptimal resource allocation and complicates task scheduling.

These inconsistencies across the system level can cause an increase in latency preventing proper interoperability between the iot devices Also, the lack of standardization in how medical data is processed, stored, and transmitted across edge and cloud systems reduces system reliability and QoS (Quality of Service).

On the Cyber Security side , healthcare iot are very sensitive additional computation and additional security measure have to be incorporated into the iot putting higher demand on their through put and bandwidth during usage this may also affect their latency metric due to the additional computational demand , since these edge nodes are trying to offload the computational capability to local nodes they have to be incorporated with extensive security protocols to prevent ransom attacks

The need to encrypt, authenticate, and securely transmit data adds latency and increases energy consumption — two critical metrics in edge environments. These constraints are particularly problematic in time-sensitive healthcare applications like real-time diagnostics or remote surgery support. Without robust and efficient security frameworks, the edge system becomes vulnerable to data leaks, breaches, and denial-of-service attacks, all of which degrade uptime, availability, and system trustworthiness.

In conclusion interoperability and cyber security are deeply involved in success of edge computing in healthcare department

2. Which performance indicators are crucial to capture edge computing's impact on healthcare, latency, and accuracy?

Latency :- In scenarios involving smart icus , health vitals monitoring systems where the calculation and alerting the responsible nurse or doctor is necessary , Latency proves to be a very crucial metric since relaying this data to the cloud and expecting a response is lengthier than processing these locally .

Energy Consumption :- This metric can boost edge computings impact on healthcare since hospitals run on generators during power cuts this edge based computings lower power consumption compared to cloud relay of information is greatly beneficial even in lower power situations .

Cost also matters. Edge systems must balance performance gains with resource expenditure, including the cost of bandwidth, computing power, and energy. Healthcare systems often work within budget constraints, so cost-effectiveness becomes an important metric.

(QOS) and (QOE) also matter since a Doctor receiving real time vitals of his patients and a patient receiving real time results of his condition ensures a consistent service and minimal lag.

These performance metric are crucial for edge computings impact on healthcare sector

3. What benchmarks are used to measure the reliability of edge AI algorithms in patient diagnostics?

- Also discuss the importance of metrics like latency, throughput, accuracy of diagnostics, uptime, reliability, compliance with privacy standards, and cost effectiveness.

Reliability on edge ai models for healthcare sector depends on multiple factors like technical performance , operational reliability , security threshold , financial viability

1. Latency :- The delay between data capture and inference output is a vital benchmark. In patient diagnostics, edge AI must deliver results fast enough to support real-time intervention. This is especially relevant for scenarios like cardiac monitoring, where delays can result in life-threatening consequences. The survey emphasizes how local processing at edge servers or gateways can significantly reduce round-trip communication delays.
2. Throughput: This measures the volume of tasks (e.g., diagnostic queries) the system can process per unit of time. For hospitals managing hundreds of patients and devices, a high-throughput edge AI system ensures timely diagnosis at scale, without backlogging critical tasks.
3. Accuracy : In diagnostics accuracy in non negotiable and requires minimal clincal standards to be passed , however with the minimal amount of computation available on the edge node it might be hard to run heavy code with out loss of precision rather selective offloading may help compute with the limited computing power
4. Uptime: Diagnostic systems must be continuously available, particularly in 24/7 care settings like ICUs or ambulatory care units. Any downtime impacts both patient safety and operational efficiency. Edge systems can improve uptime by offloading tasks adaptively or leveraging nearby edge nodes in a redundant configuration.
5. Reliability: It is of utmost necessary as correctness and consistency of output is crucial at all times even under changing bandwidth , network , increased workload precise output is necessary
6. Compliance with privacy standards : Edge Computing offers great privacy since the data is processed locally rather sending it to cloud risking data duplication ,etc.
7. Cost Effectiveness : Diagnostic AI must justify their value but the cost varies based on the task assigned but it can be deduced that it will be cheaper since the tasks are being performed locally rather than outsourcing , Metrics like cost per diagnostic return on infrastructure inference are checked .