REPORT

In today's ubiquitous computing world, which is driven by IOT devices and creates data every nanosecond. This digital realm is currently experiencing systemic shift in sheer, unparalleled surge in data generation and its subsequent consumption. This is where edge computing comes in hand. It's a paradigm which strategically aliens computers and storage capabilities of the computer closer to the data origin. Edge computing doesn't replace the cloud data but it actually works alongside adding a super-fast extension that brings processing closer to where data is created, so things can happen faster and there is less time delay.

Efficient Resource scheduling is a key to make edge computing successful. It's about how tasks are managed across different levels i.e. device, edge server and the cloud to manage goals like speed, energy saving and reliability. This report is based on the survey "Resource Scheduling in Edge Computing." By Luo el al. We explore different performance measures like latency and energy saving, and apply them in real world application like cities, healthcare and connected vehicles. It also gave an overview on how tasks are offloaded, how resources are shared and how different methods particularly centralized and distributed are used to make a system run smoothly.

How do inter-operability and cyber security challenges affect edge deployment matrix in healthcare?

Impact of Cybersecurity and Interoperability Challenges on Edge Deployment in Healthcare

1. System-Level Security Risks

The edge system is pretty vulnerable to attack and it highlights the inherent vulnerability of multi-layered edge architectures to attack. When it comes to healthcare context there are significant risk of patient data and potentially leading to data integrity issues. This vulnerability would stringent security protocols and increase the complexity and cost of the deployment. When the attackers gain access to this data could lead to significant problems such an incorrect diagnoses plan.

These measures are essential for protecting patient data complexity and increases the costs of deploying this system. Regulations like HIPAA (Health Insurance Portability and Accountability Act) strict guidance on how data can be handled. While Multi-layered edge architectures offer many benefits.so these challenges must be carefully managed to protect patient data and to ensure compliance with regulations.

Cybersecurity at the Service Level:

In cybersecurity at service level it's all about building the trust and ensuring that only the right people can get access to the sensitive information. It means that every medical device and edge node essentially the small computing units that process data needs to be properly authenticated and authorized before they can handle any patient information.

If these trust mechanisms are missing, it opens the door to unauthorized access or even tampering with health records. This not only puts patient data at risk but also makes the entire edge deployment much more dangerous and potentially against regulations.

However, implementing these safeguards adds extra layers of complexity to the deployment process. It requires careful planning and resources to ensure that everything is secure, which can be a challenge for healthcare organizations already facing numerous demands. In short, while these security measures are vital for protecting patient data, they also complicate the way healthcare systems are set up and managed.

Interoperability (Inferred Challenge):

it's important to note that many studies assume data can be accessed easily and without trust concerns. This is risky for sensitive patient information in healthcare, as any leakage during transmission or processing can have serious consequences. Techniques like encryption and anonymization are crucial, but they can also introduce computational overhead and complexity, potentially slowing down edge deployments.

Interoperability is a key challenge in edge computing. With multiple devices and layers involved, ensuring that different systems can communicate effectively is often difficult. In healthcare, this can lead to fragmented data and inefficient workflows, making it harder for providers to access and share information. Consequently, integrating and scaling edge solutions that rely on diverse data sources becomes a significant hurdle, which can negatively affect patient care.

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

Latency is crucial in healthcare, similar to how connected and autonomous vehicles (CAVs) require quick data processing for safety. Real-time monitoring, emergency responses, and critical diagnostics all depend on timely data to ensure patient safety.

The "Smart Health" section emphasizes the importance of using edge resources for fast medical data processing, which helps reduce operational costs. Energy consumption is also vital, as smart health devices need to minimize energy use to extend battery life, allowing wearables and remote monitoring tools to function longer without frequent recharges.

Cost-effectiveness is highlighted as a key benefit of edge-assisted medical systems, helping healthcare providers save money. While security and privacy aren't explicitly listed as performance indicators, they are essential for protecting patient data and ensuring the trustworthiness of edge solutions.

Lastly, although "accuracy" isn't directly mentioned, it is critical for patient diagnostics. Intelligent computing and data analysis at the edge must deliver accurate results, making accuracy an implied but vital performance metric in healthcare.

What benchmarks are used to measure the reliability of edge AI algorithms in patient diagnostics? Also discuss the importance of matrix such as latency, throughput, accuracy of diagnostics obtained reliability, complier standards and cost effectiveness

Latency: Low latency is crucial in-patient diagnostics, especially for critical conditions like continuous glucose monitoring and cardiac event detection. Delays in diagnosis can lead to serious outcomes. Edge AI helps reduce latency by processing data closer to the source, avoiding time-consuming cloud trips. The document highlights latency as a key performance indicator in healthcare applications.

Throughput: Throughput measures how much data can be processed in a given time. In healthcare, high throughput is essential for managing large volumes of patient data and multiple diagnostic requests simultaneously. The document mentions the need for robust computing capabilities at the edge, supporting high throughput.

Accuracy of Diagnostics: Accuracy is the most critical metric in patient diagnostics. The effectiveness of edge AI depends on the reliability of its results, as misdiagnoses can have severe consequences. Benchmarks typically compare AI outputs against confirmed clinical diagnoses. The document emphasizes the goal of edge computing as producing accurate and reliable results.

Reliability: Reliability refers to the consistency and trustworthiness of the AI system over time and under varying conditions. It includes handling noisy data and system failures. The document stresses the importance of enhancing system robustness and implementing intrusion detection strategies, which are vital for reliability in healthcare.

Compliance Standards: Compliance with regulations like HIPAA and GDPR is essential in healthcare. Edge AI solutions must adhere to standards for data privacy and security. The document underscores the importance of compliance in healthcare data management.

Cost-Effectiveness: While not a direct technical metric, cost-effectiveness is crucial for the adoption of edge AI in healthcare. This includes deployment, operation, and maintenance costs. The document identifies cost as a key performance indicator, noting that edge-assisted medical systems can lead to significant savings for healthcare providers.