VELLORE INSTITUTE OF TECHNOLOGY, CHENNAI

BECE351E - INTERNET OF THINGS (IoT)

NAME : RAHUL KARTHIK .S

REG. NO : 21BEC1851

DATE : 08.07.23

① Select any one use case scenario and explain with neat diagrams about how edge computing can be used in that application?

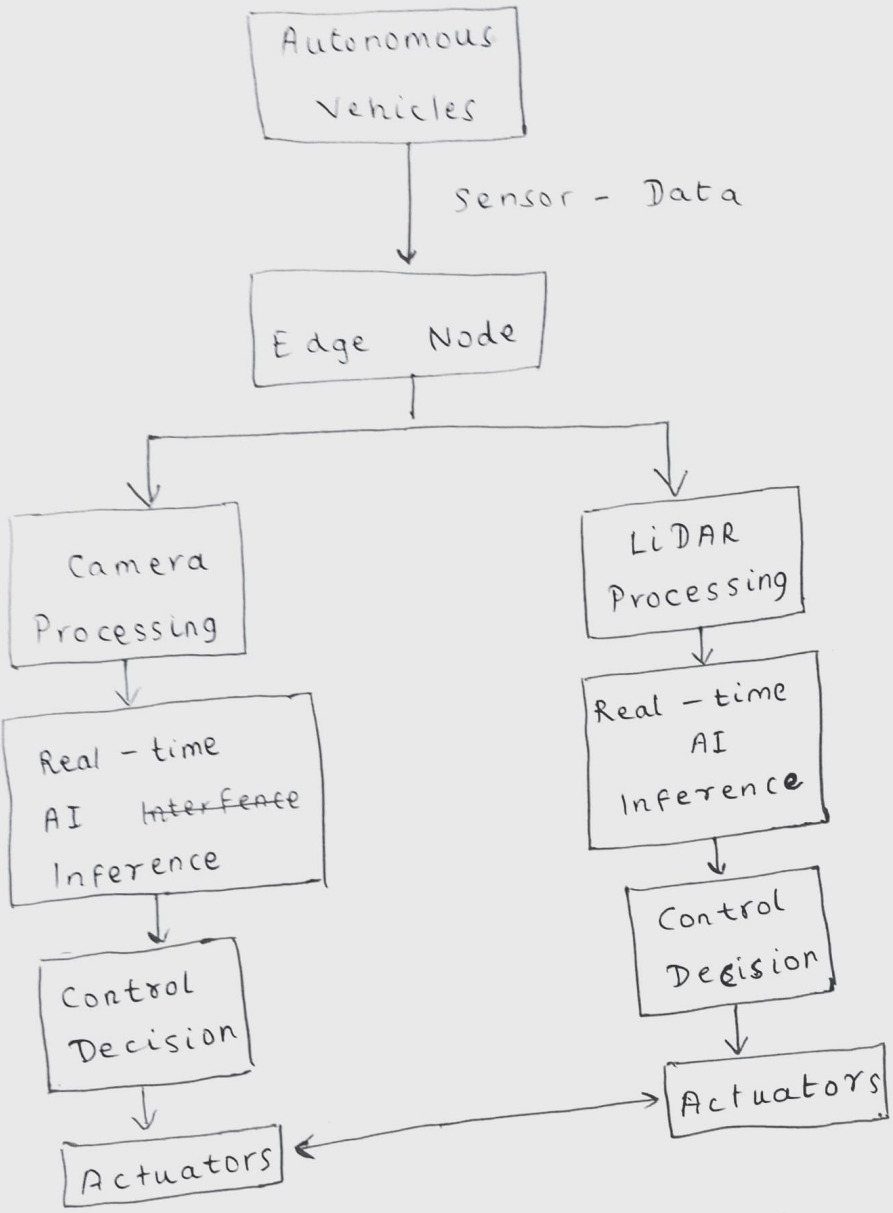
A: One of the use case scenario where edge computing can be applied is in the context of autonomous vehicles. Edge computing can significantly enhance the capabilities and efficiency of autonomous vehicles by enabling faster processing, reduced latency, and improved real-time decision making.

In an autonomous vehicle system, there are various sensors and cameras that continuously capture and generate a

massive amount of data, including video streams, LiDAR point clouds, and GPS information. Traditionally, this data would be sent to centralized cloud server for processing, which can introduce significant latency due to the round-trip communication and processing time. This latency can hinder the vehicle's ability to make immediate decisions, especially in critical situations that require real-time responses.

However by levaraging edge computing, the processing and decision-making tasks can be moved closer to the source of data generation, which in this case is autonomous vehicles itself. This involves deploying edge nodes, also known as edge-devices or edge servers, directly within the vehicles or at the network edge, such as road-side infrastructure or nearby data center. These edge nodes are capable of performing computations on the incoming data in real-time.

Let's consider a simplified diagram in an autonomous vehicle scenario:



In this diagram, the autonomous vehicle captures data from various sensors such as cameras and LiDAR. The data is then processed locally at the edge node, which can perform tasks like image and point cloud processing.

The processed data is then fed into real-time AI inference models, which analyze and interpret the data to make critical control decisions.

By performing these computations at the edge, the latency associated with sending the data to a remote cloud server is minimized. This allows the vehicles to respond rapidly to changing road conditions, obstacles, or other vehicles, ensuring a safe and efficient autonomous driving experience.

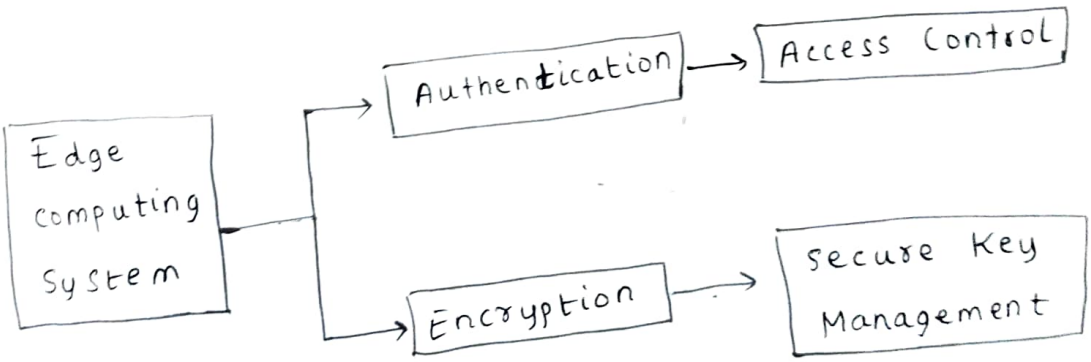
Edge computing in autonomous vehicles also enables localized decision-making, as the edge nodes can process data even when the vehicles is in an area with limited or no network connectivity. This ensures that the vehicles can continue operating ~~and~~ autonomously even in scenarios where a reliable cloud connection may not be available.

Overall, the use of edge computing in autonomous vehicles offers significant advantages in terms of reduced latency, improved real-time decision-making, and enhanced autonomy. It enables autonomous vehicles to operate more efficiently and effectively, paving the way for safer and more reliable transportation systems.

② With neat diagram explain the various security threads that are possible and steps to mitigate it.

A: 1. Unauthorized Access:

It refers to an attacker gaining unauthorized entry to the edge computing system, compromising data integrity and confidentiality. To mitigate this threat, the following steps can be taken:



- **Authentication**: Implement robust authentication mechanisms to ensure only authorized users or devices can access the edge computing system.

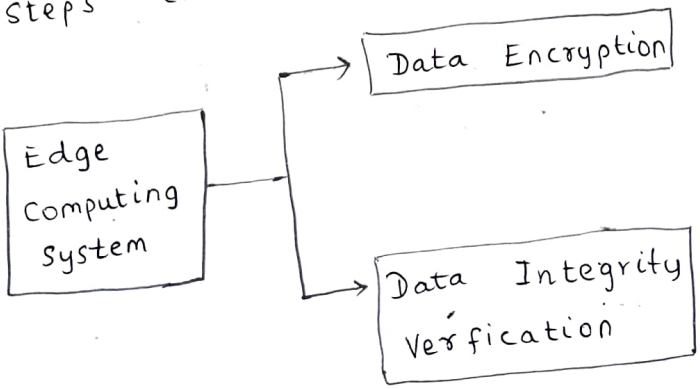
- **Access Control**: Employ access control policies to restrict access rights and permissions based on user's roles and privileges.

- **Encryption**: Encrypt data both at rest and in-transit to prevent unauthorized access to sensitive information.

- **Secure Key Management**: Implement secure key management practices to safeguard encryption keys.

2. **Data Privacy and Integrity**:

It involves unauthorized modification or disclosure of sensitive data. To mitigate these threats, the following steps can be taken:

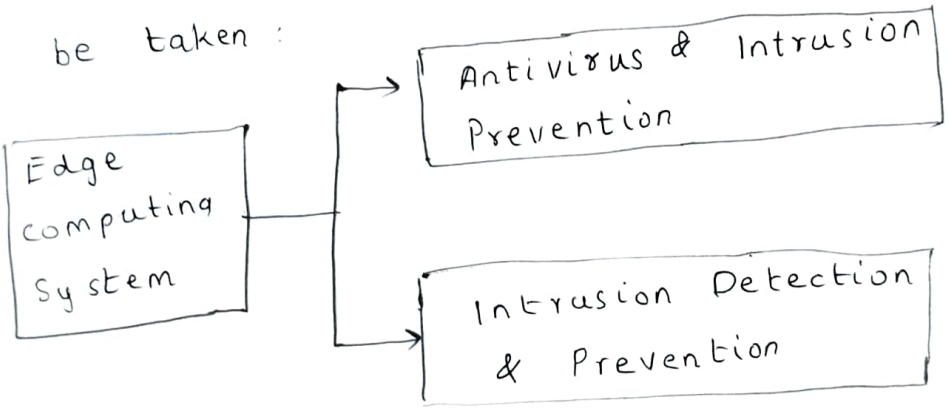


- **Data Encryption**: Encrypt data at rest and during transmission to protect it from unauthorized access.

- **Data Integrity Verfication**: Implement mechanisms, such as checksums or digital signatures, to verify the integrity of data and detect any unauthorized modifications.

3. **Malware and Intrusions**:

It pose a significant threat to edge computing systems. To mitigate these risks, the following steps can be taken:

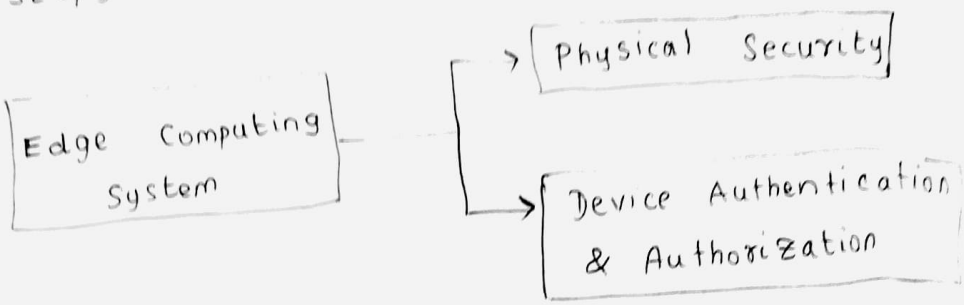


- **Antivirus and Intrusion Prevention**: Deploy antivirus and intrusion prevention systems to detect and prevent malware infection and unauthorized intrusions

- Intrusion Detection utilize intrusion detection system to identify any malicious activities or anomalies within the edge computing environment.

4. Physical Security:

Physical security threads include unauthorized physical access to edge computing devices or infrastructure. To mitigate these threads, the following steps can be taken



- Physical Security Measures :. Implement physical security measures, such as access control systems, surveillance cameras, and secure facilities, to prevent unauthorized physical access to edge computing devices.

- Devices Authentication and Authorization: Utilize device authentication and authorization mechanisms to ensure that only trusted and authorized devices can connect to edge computing system.