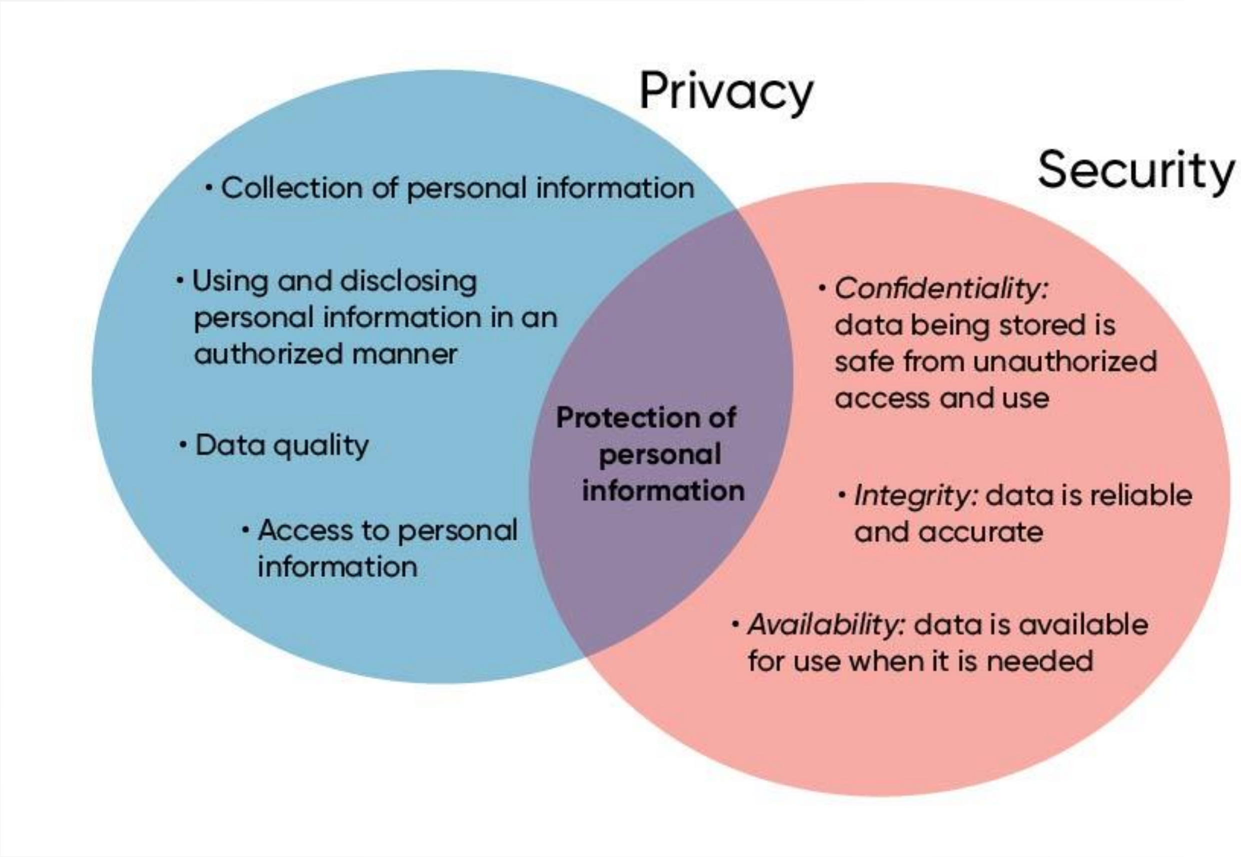
EDGE SECURITY

Click to add subtitle

TERMINOLOGY



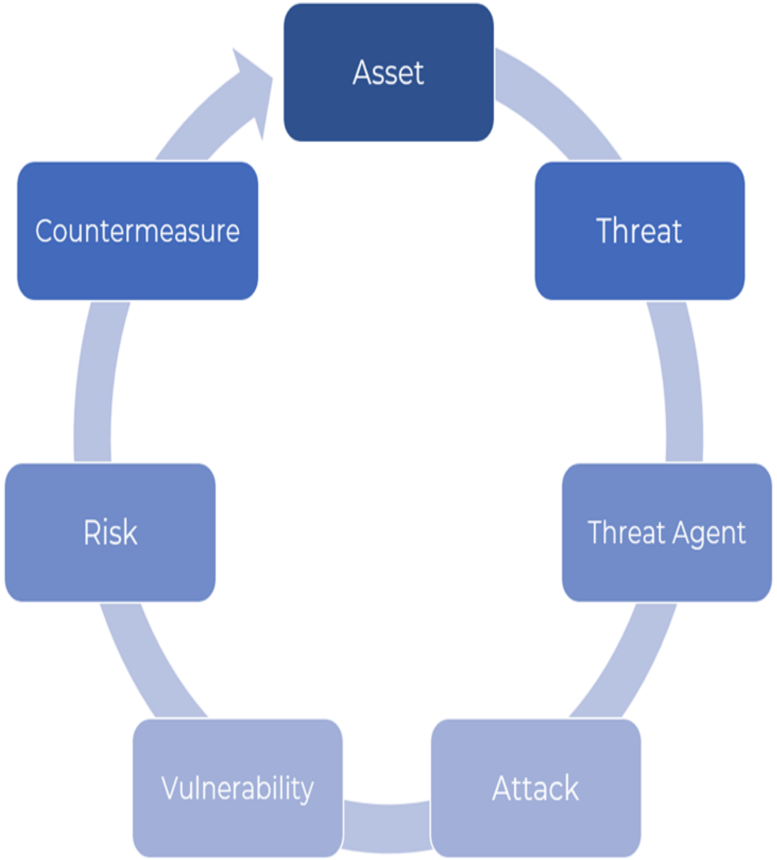
Privacy

- Collection of personal information
- Using and disclosing personal information in an authorized manner
- Data quality
- Access to personal information

Protection of personal information

Security

- *Confidentiality:* data being stored is safe from unauthorized access and use
- *Integrity:* data is reliable and accurate
- *Availability:* data is available for use when it is needed



Asset

Threat

Threat Agent

Attack

Vulnerability

Risk

Countermeasure

//* IBM Z Day
//* open | on | secure

TERMINOLOGY

1. **Asset:** Something of value to a business that needs protection, such as files, intellectual property, hardware, or employees.
2. **Threat:** A potential event that could damage, alter, or destroy an asset. Threats can be malicious (e.g., hacking), accidental (e.g., human error), or natural (e.g., earthquakes).
3. **Threat Agent:** A person or system that causes harm to an asset. Examples include hackers or systems used in attacks like DDoS.
4. **Attack:** The actual damage, destruction, alteration, or theft of an asset. Attacks can be malicious (e.g., cyberattacks) or accidental (e.g., spilling water on a laptop).
5. **Vulnerability:** A weakness or lack of a safeguard that threat agents exploit. Vulnerabilities can be due to flaws in programming, security lapses, or social engineering.
6. **Risk:** The likelihood of something bad happening (accidental or malicious). Risks can be mitigated by implementing safeguards or countermeasures.

EDGE COMPUTING

Why did we come up with Edge Computing??

- **Improving Performance** and **Reducing Processing Latency**.
- **Reducing costs associated with data transfer** to centralized locations.
- **Addressing technical challenges** such as data movement, management, processing, and storage.
- **Enhancing data governance, privacy, and compliance**, which are difficult to manage when relying solely on centralized data centers.

What’s wrong now??

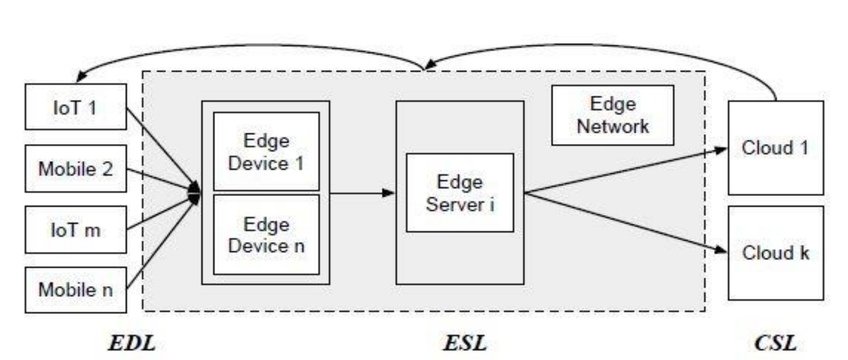
- **Security challenges** across multiple fields
- **A lack of holistic approaches** to security
- **Emerging security challenges** at the domain boundaries
- **Issues with compatibility and redundancy** when we have domain-specific security solutions
- **Privacy and regulatory compliance challenges** because of geo-location and the diverse nature of edge computing deployments.

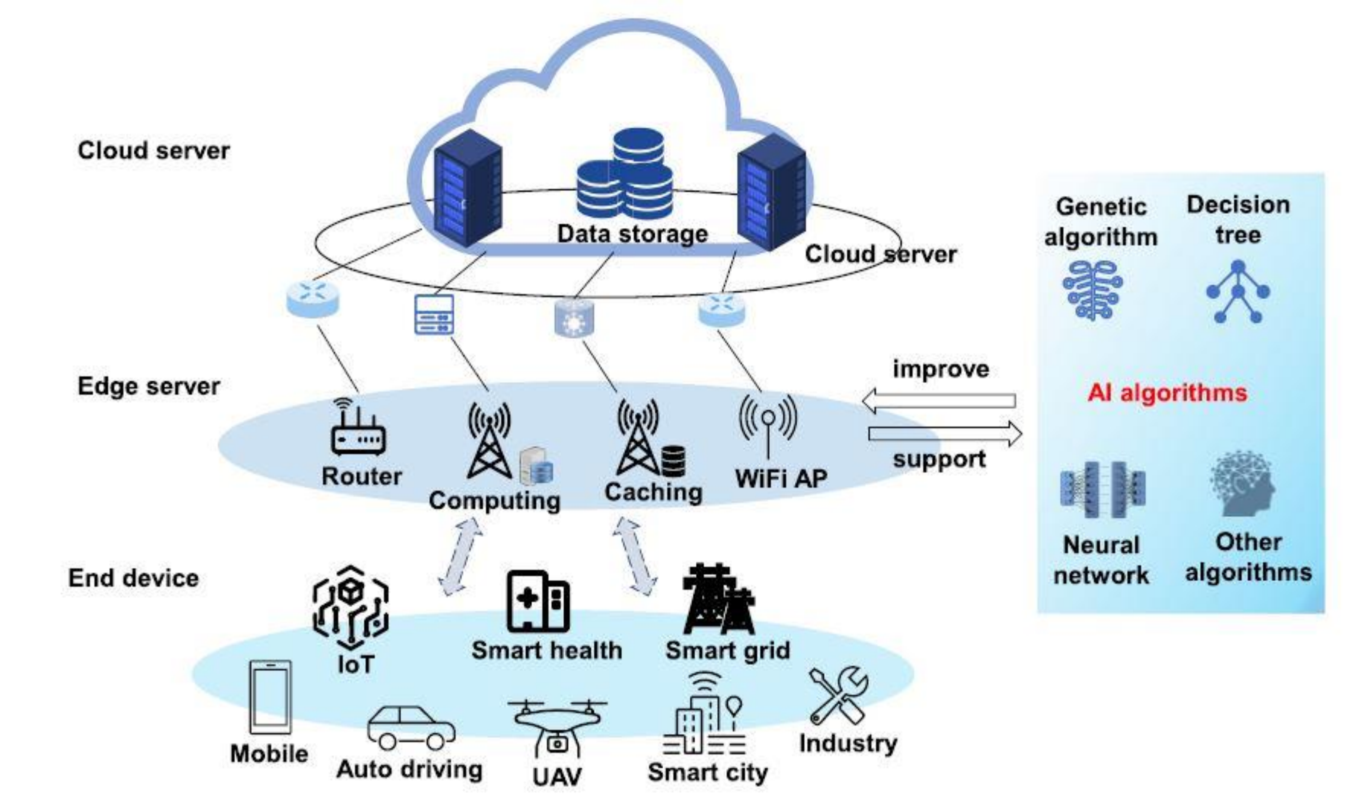
THE GENERAL ARCHITECTURE OF EDGE COMPUTING

The **Edge Device Layer (EDL)** consists of IoT and mobile devices that perform field tasks like sensing, actuating, and controlling, often using microcontroller

The **Edge Server Layer (ESL)** handles core computing functions such as authentication, computation, data analytics through a hierarchical setup.

The **Cloud Service Layer (CSL)** hosts cloud servers and data centers for high-level operations and extensive data storage, complementing EDL and ESL.





SECURITY CHARACTERISTICS OF EDGE COMPUTING

1. **Weaker computation power:** Compared to a cloud server, the computation power of an edge server is relatively weaker
2. **Large volume of interconnected devices:** Edge devices are typically interconnected, so a small intrusion can have a more significant impact if the attack is spread and propagated among devices.
3. **Heterogeneous device form factors:** The heterogeneity of devices poses extreme challenges when designing general solutions to potential threats and issues.
4. **Unavailability of security features:** Due to different form factors and diverse of platforms, desired security features are not always available on specific edge computing platforms
5. **Maintaining the quality of service:** Any security measurements should try to maintain the original quality of service (QoC) (e.g., availability and real-time)

SECURITY ISSUES ON THE NETWORK EDGE

- **DoS Attacks (Denial of Service):** Overloading a device or server to make it unavailable.

A DDoS attack uses hijacked IoT devices to flood a server with traffic, causing it to crash.

- **Malware:** Malicious software that damages or steals data from devices.

Malware infects a smart home camera, stealing private footage and sending it to attackers.

- **Poisoning Attacks:** Introducing false data to corrupt AI or machine learning models.

Malicious data in a federated learning system causes the global AI model to make wrong predictions.

PRIVACY ISSUES ON THE NETWORK EDGE

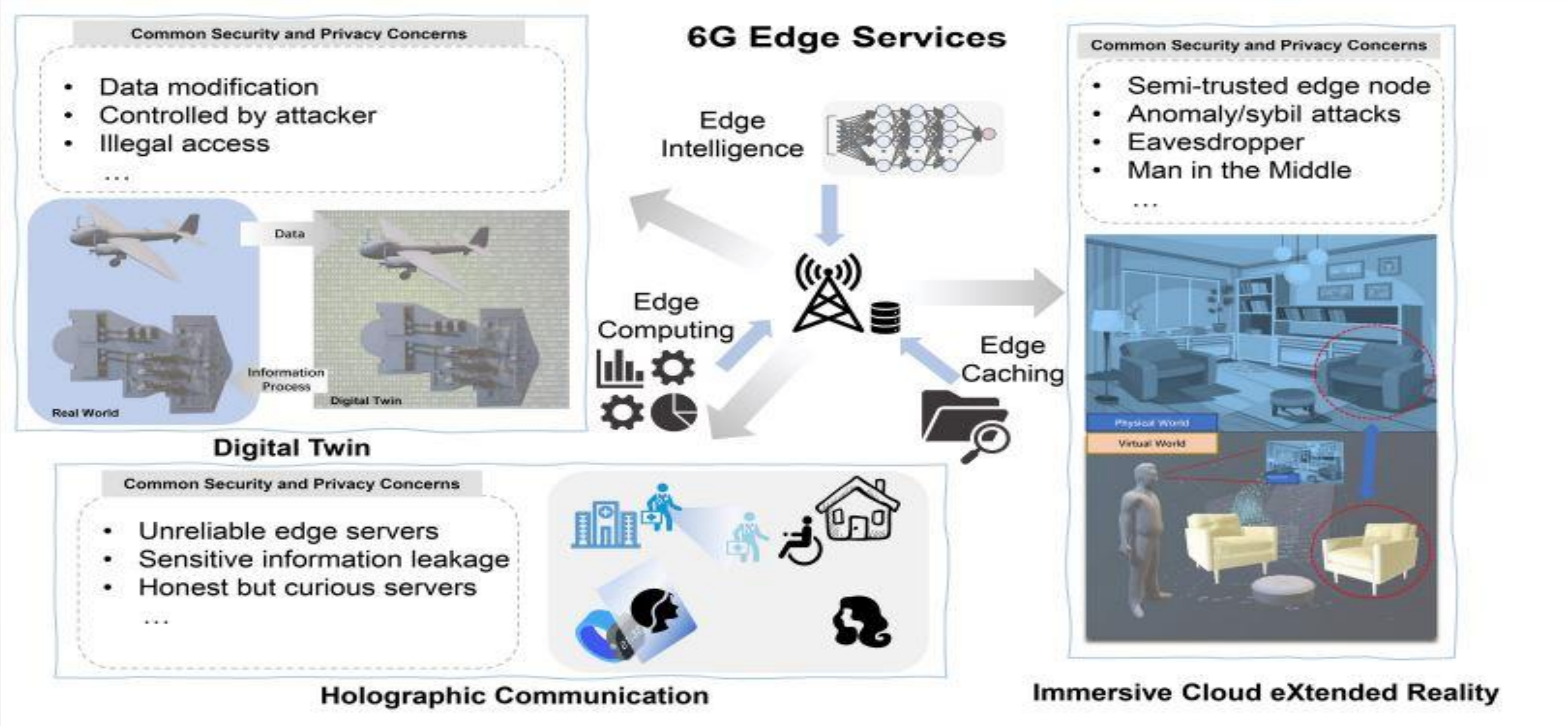
- **Eavesdropping:** Malicious actors can intercept sensitive data (e.g., personal, financial) transmitted by IoT devices, which are often too resource-constrained to use strong encryption.

Eavesdropping on video data for blackmail or exploiting weak signals from devices like wearable sensors.

- **Abuse of Data Access:** Weak security on edge servers and unclear data-sharing mechanisms can lead to unauthorized data access. This is further complicated by the risk of honest service providers using private data for unintended purposes.
- **Unreliable Participants:** Collaborative edge systems, such as those used in 6G networks, may involve untrustworthy participants who could steal data during processing.

Privacy can be improved through reliable server selection, data encryption, and access control mechanisms. Privacy protection strategies like Differential Privacy (DP) and homomorphic encryption help mitigate these risks by anonymizing or securing data during processing.

6G AND EDGE TECHNOLOGIES USE CASES



6G AND EDGE TECHNOLOGIES

Advances in 6G and Edge Technologies

1. **Edge Computing and Caching:** Edge computing and caching reduce latency, bandwidth usage, and risks of large-scale data breaches or service disruptions while enhancing privacy and security.
2. **Edge Intelligence:** Incorporating AI at the network edge enables adaptive, automated management and local processing of machine learning models, reducing the need for centralized data sharing.

Security and Privacy Requirements for 6G Edge Services

1. **Generality:** Both end devices and service providers must be authenticated and reliable to prevent attacks, data tampering, and privacy leakage. Communication on the edge must also be protected against eavesdropping.
2. **Diversity:** Different technologies and providers demand tailored solutions that balance protection levels with energy and resource efficiency
3. **Cooperation:** Edge servers must collaborate securely to handle large tasks, as failures or malicious actions from one participant can compromise the system.
4. **High Cost-Efficiency:** Security measures must minimize processing and energy overhead due to limited resources on edge devices. Efficient solutions are critical to support IoT, IIoT, and latency-sensitive services in 6G environments.

TECHNIQUES TO ENHANCE SECURITY AND PRIVACY ON 6G NETWORK EDGE: FL

1. **Privacy Preservation:** FL protects sensitive data by keeping it local and using techniques like Differential Privacy (adding noise) and Homomorphic Encryption (encrypted parameters during transmission).
2. **Applications:** It enables secure intrusion detection systems, private data processing (e.g., healthcare, smart parking), and personalized content caching/recommendation without compromising privacy.
3. **Mitigating Threats:** FL resists poisoning attacks with participant verification methods and integrates blockchain to ensure data integrity and reliability.
4. **Challenges Addressed:** Adaptive aggregation and transfer learning tackle communication bottlenecks and performance issues.

TECHNIQUES TO ENHANCE SECURITY AND PRIVACY ON 6G NETWORK EDGE: BLOCKCHAIN

1. **Decentralized Ledger:** Transactions verified/stored by multiple users without a central authority.
2. **Traceable Blocks:** New blocks contain previous values/timestamps for secure verification.

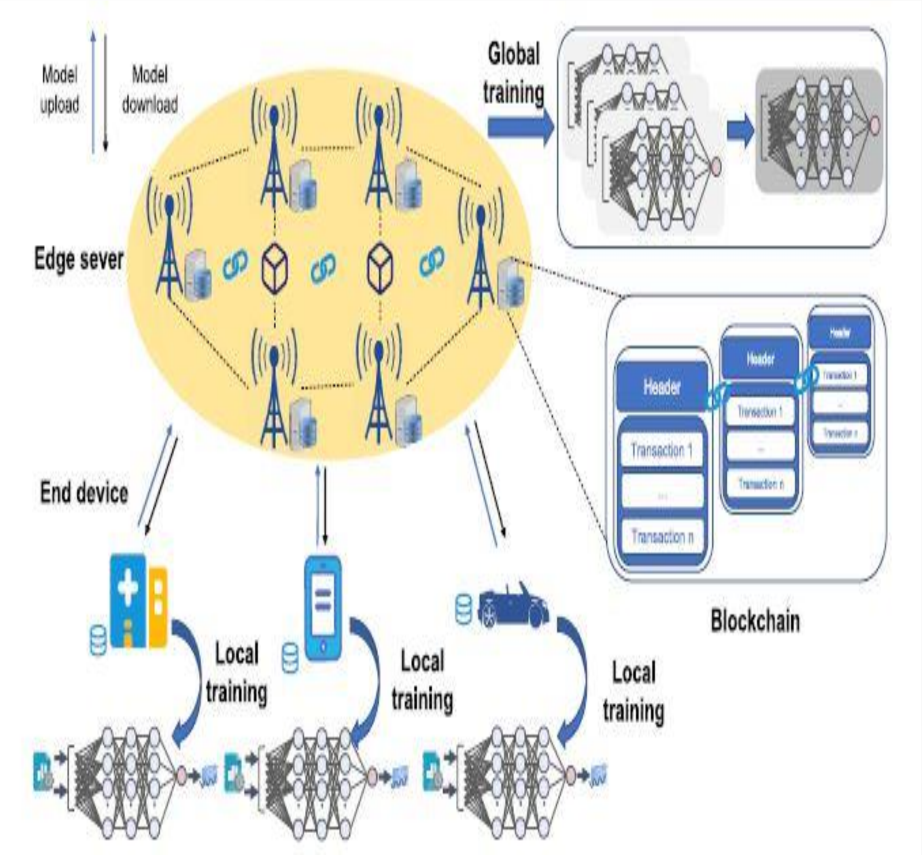
Applications

1. **IoT, Smart Driving, Edge Caching:** Blockchain secures data storage, transmission, and usage.
2. **Federated Learning (FL):** Counters Byzantine attacks, ensures traceability, and verifies local models.

Limitations and Solutions

High Costs (PoW): Blockchain's computation/energy demands cause latency.

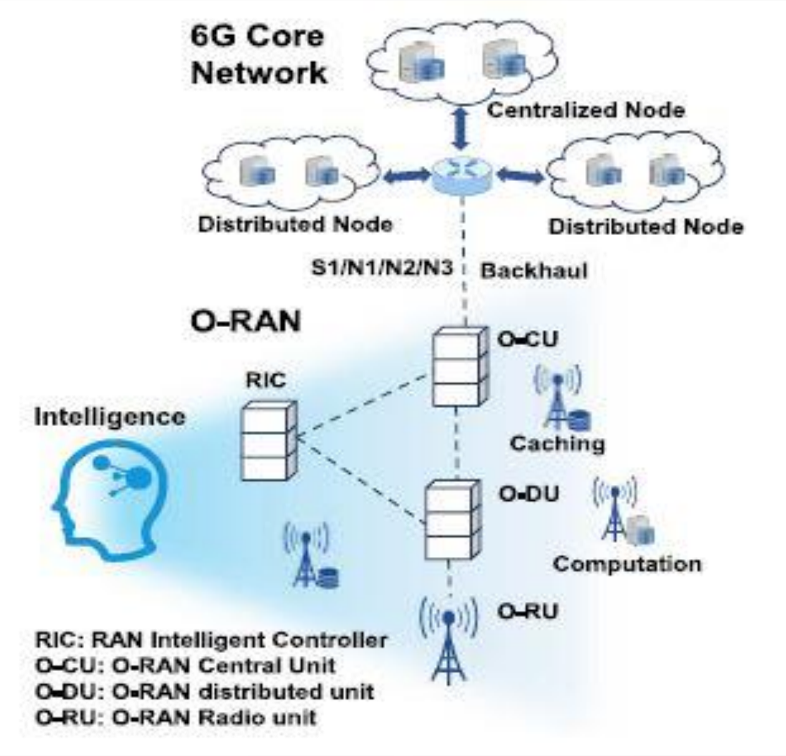
Advanced Architectures: Hierarchical systems and acyclic graphs mitigate latency issues.



TECHNIQUES TO ENHANCE SECURITY AND PRIVACY ON 6G NETWORK EDGE: ORAN

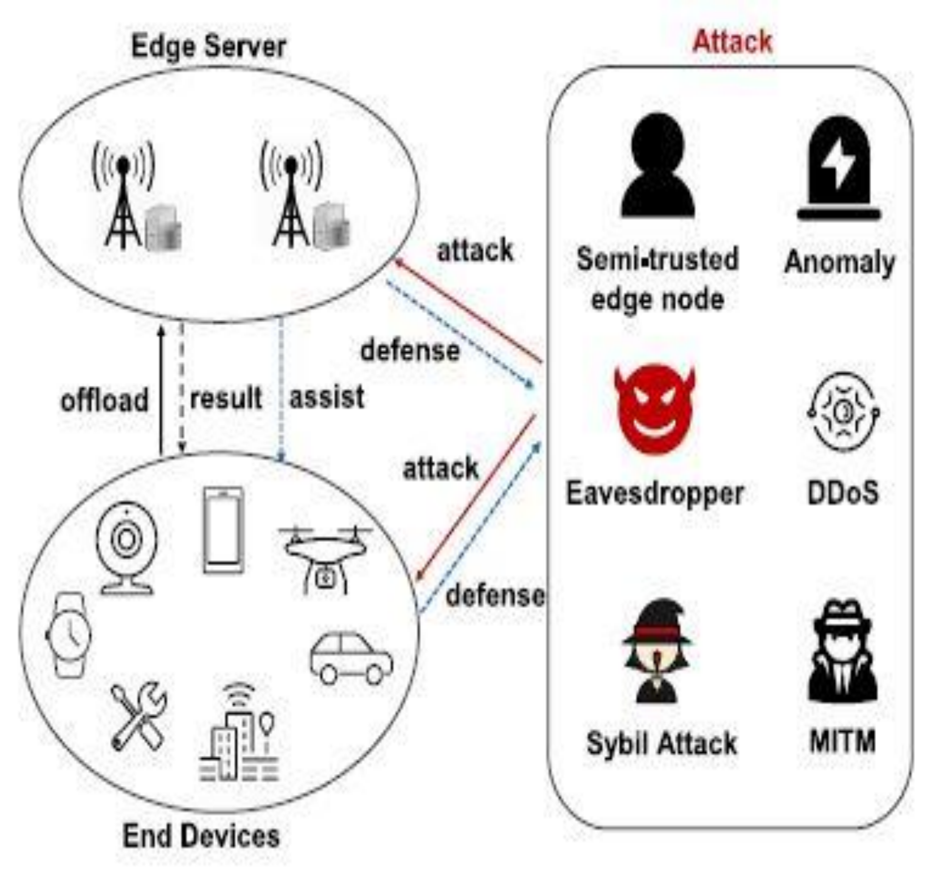
O-RAN, developed to improve flexibility using SDN and NFV, separates network software and hardware to enable AI-driven network automation. O-RAN Network Functions, and O-Cloud platforms for edge computing, caching, and intelligence.

1. **Role in Edge Services:** Low-latency edge services, including edge computing, caching, and intelligence, enabling self-organizing networks (SONs) for automatic configurations and optimizations.
2. **Security Challenges:** While O-RAN increases flexibility, it introduces vulnerabilities like weak authentication, insecure interfaces, and AI-based threats (e.g., poisoning attacks). Defense mechanisms include Zero Trust Architecture and blockchain integration for secure data tracking.



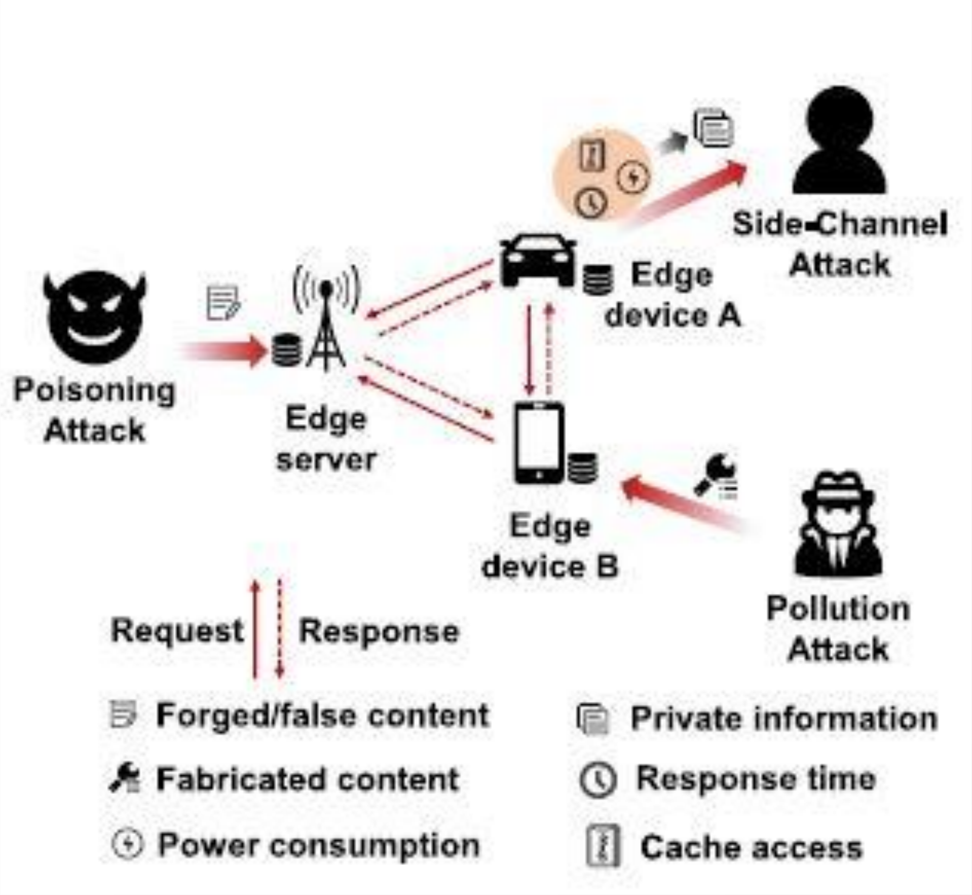
SECURITY AND PRIVACY IN EDGE COMPUTING

1. **Authentication Improvements:** Lightweight authentication strategies are crucial for IoT devices. Complex tasks like encryption and key generation can be offloaded to edge servers, with emerging solutions such as machine learning (ML) and blockchain improving security.
2. **Lightweight Encryption:** Traditional encryption methods are too resource-intensive for edge scenarios. New techniques, like proxy re-encryption, shift encryption tasks to edge servers, reducing device overhead. Blockchain is also used for secure data access.
3. **Intrusion Detection Systems (IDS):** Edge computing enables efficient IDS for detecting attacks on IoT devices, vehicular networks, and edge servers. Techniques like federated learning and LSTM autoencoders help detect anomalies, with a growing focus on protecting edge servers from attacks.



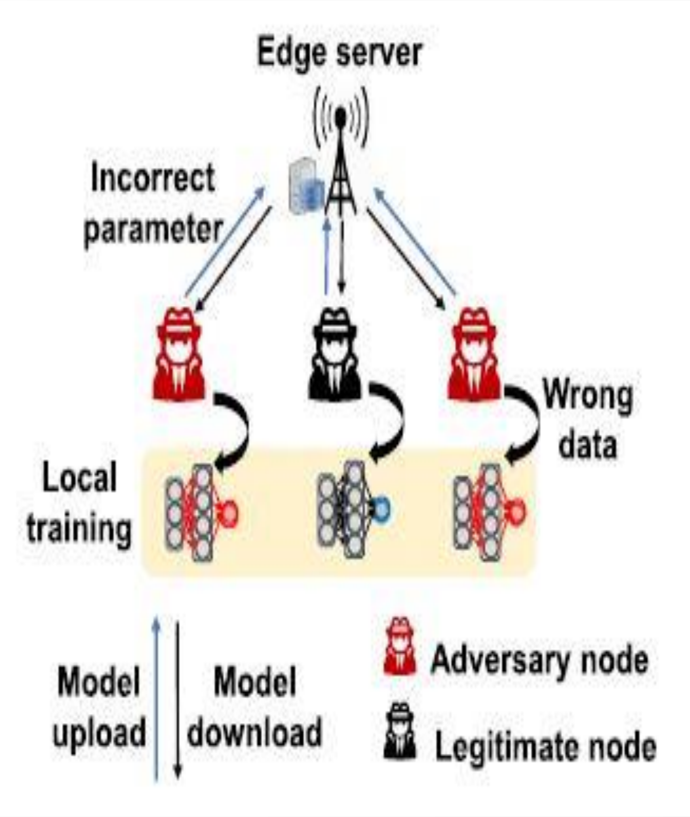
SECURITY AND PRIVACY IN EDGE CACHING

1. **Caching Placement:** Ensuring the security of cached content involves selecting reliable edge servers and using techniques like blockchain to verify content validity. Game theory is also used to optimize content placement based on trust and security.
2. **Content Storage:** Protecting cached data requires authentication and encryption. Methods like Attribute-Based Encryption (ABE) and blockchain are used to ensure the privacy of data in edge networks. Techniques like Federated Learning (FL) help predict content popularity without compromising user privacy.
3. **Content Delivery:** Secure content delivery involves safeguarding against eavesdropping and unauthorized access. Techniques include physical-layer security, access control based on encryption policies, and blockchain for tamper detection. Additionally, coding methods, such as network coding, are used to prevent unauthorized content decryption.



SECURITY AND PRIVACY IN EDGE INTELLIGENCE

1. **Anomaly Detection:** Edge intelligence uses AI to detect network anomalies by analyzing data from end devices, improving attack detection and identifying threats like flooding, probes, and malware.
2. **Malware Detection:** AI models, such as multi-kernel SVM and deep learning, are used for detecting malware in IoT networks and preventing the spread of harmful data across edge and cloud layers.
3. **Collaborative Learning and Countermeasures:** Edge intelligence enables distributed AI model training without exposing data. Blockchain and DRL enhance security by verifying model updates and ensuring node reliability.
4. **Security Threats and Countermeasures:** Edge networks face new AI-driven security risks. Solutions like identity-based cryptography and federated data cleaning help protect against malicious nodes and data corruption.
5. **Privacy Concerns and Countermeasures:** Edge intelligence aids privacy by processing data locally, but challenges remain during collection and transmission.



TRADE-OFF BETWEEN SECURITY/PRIVACY AND QOS

1. **Security vs. Latency:** Offloading computation tasks reduces energy cost but increases latency.
2. **Security vs. Energy Consumption**: Energy harvesting IoT devices must balance security measures like encryption with energy limitations to avoid draining resources.
3. **Security vs. Computational Overhead:** Attribute-based encryption (ABE) for data protection adds computational overhead due to encryption and key management.
4. **Security vs. QoS:** Encryption in IoT networks may reduce throughput and increase delays, affecting the overall service quality.
5. **Security vs. Accuracy in AI/ML Models:** Dropout in AI models enhances robustness against attacks but reduces accuracy, affecting model performance.

TRADE-OFF BETWEEN SECURITY/PRIVACY AND QOS

6. Security/Privacy vs. Accuracy in Federated Learning: Differential privacy and homomorphic encryption in Federated Learning can lower training accuracy by limiting data use.

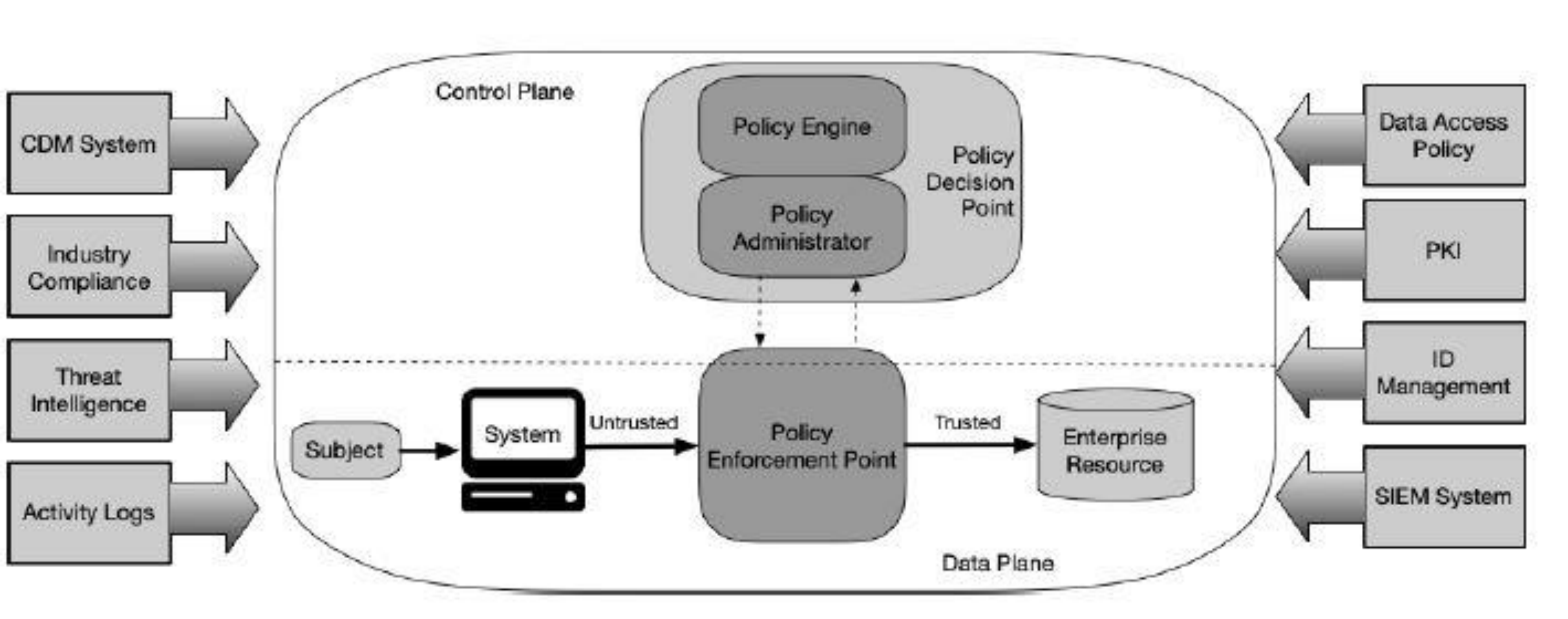
7. Lightweight Security in Resource-Constrained Networks: In edge networks, lightweight security solutions are needed to avoid overloading resource-constrained devices while still ensuring protection.

8. Trade-off in IoT/IoT Network: IoT networks must balance strong security protocols with the need for efficient performance due to resource constraints.

TRADE-OFF BETWEEN SECURITY/PRIVACY AND QOS: SOLUTIONS

1. **Optimization Models:** Multi-objective models balance security and QoS requirements (e.g., Integer Linear Programming).
2. **Lightweight Security:** Protocols that reduce resource consumption while providing adequate protection.
3. **Task Offloading:** Security tasks are offloaded to edge servers or nearby devices to optimize resource use.
4. **Blockchain/Digital Twins:** Enhances security without significant cost or performance degradation.

ZERO TRUST ARCHITECTURE: LOGICAL COMPONENTS



THE QUIZ

WITH THE POWER
OF KNOWLEDGE
– FOR THE WORLD