If the main constraint is SCALE & DATA VOLUME
→ Cloud Computing
Cloud provides elastic infrastructure and pay-as-you-go pricing.
Suitable for massive IoT data ingestion and global workloads.
Enables storage, distributed processing, and on-demand resources.
Often relies on distributed systems and data partitioning to handle growth.
Limit: network latency and data processed by third parties.

If the system needs INTELLIGENCE (prediction, detection, analytics)
→ AI & ML in the Cloud
Cloud platforms provide CPUs, GPUs, TPUs and ML pipelines.
Pre-trained models and managed ML services allow large-scale deployment.
Cost-efficient experimentation and secure environments.
Well adapted to batch processing and large historical datasets.
Limit: latency and data privacy constraints.

If the main constraint is REAL-TIME & LOW LATENCY
→ Fog Computing
Processing is moved closer to IoT devices.
Fog nodes filter local data and react immediately.
Only relevant data is sent to the cloud for long-term analysis.
Reduces bandwidth usage and avoids round-trip delays to the cloud.
Goal: responses under 10 ms.

If the workload is EVENT-BASED & VARIABLE
→ Event-Driven Architecture + Serverless
Services communicate asynchronously via events.
Message brokers manage event streams.
Serverless enables automatic scaling and cost per event.
Particularly efficient for burst workloads and IoT-generated events.
Cloud Native preferred for agility and self-healing systems.

If the priority is RESILIENCE & AVAILABILITY
→ Cloud Disaster Recovery & Business Continuity
Strategy chosen based on RTO/RPO requirements:
Low criticality → Backup & Restore
Medium → Pilot Light
High → Warm Standby
Mission-critical → Active-Active
Cloud enables automation and multi-region recovery.
Higher availability implies higher operational and financial cost.

If the concern is SECURITY & REGULATORY COMPLIANCE
→ Apply Cloud Security & Compliance mechanisms
Shared Responsibility Model.
Zero Trust, encryption (AES, SSL/TLS), IAM & SSO.
Compliance with GDPR, DORA.
Be careful with provider jurisdiction (CLOUD Act vs GDPR).
Security must be integrated by design, not added afterward.

If the issue is SOVEREIGNTY & VENDOR LOCK-IN
→ Hybrid or Multicloud Strategy
Hybrid cloud keeps sensitive data under control.
Multicloud increases resilience and avoids dependency.
FinOps required to manage costs.
Adds architectural complexity but increases strategic flexibility.

If the system must be CONTEXT-AWARE & INVISIBLE
→ Pervasive Information Systems
Combines IoT devices, networks, cloud “brain”, and adaptive interfaces.
Enables autonomous, personalized services in real time.
Often combined with Fog + Cloud.
Relies heavily on context-awareness and continuous data collection.