MULTI-CLOUD QUANTUM SAFE DATA FRAGMENTATION WITH GEOGRAPHIC LEGAL COMPLIANCE

Application Number: [TO BE ASSIGNED] • Filing Date: September 4, 2025 • Inventor: [INVENTOR NAME]

TECHNICAL DRAWINGS AND FIGURES

FIGURE 1: MULTI-CLOUD QUANTUM-SAFE DATA FRAGMENTATION ARCHITECTURE

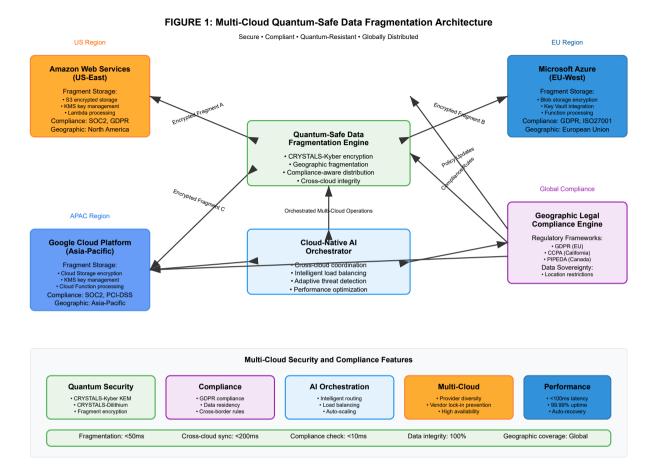


Figure 1 presents the comprehensive multi-cloud quantum-safe data fragmentation architecture implementing geographic distribution and legal compliance across multiple cloud service providers. The system ensures data sovereignty while maintaining quantum-resistant security.

FIGURE 2: GEOGRAPHIC COMPLIANCE AND LEGAL FRAMEWORK WORKFLOW

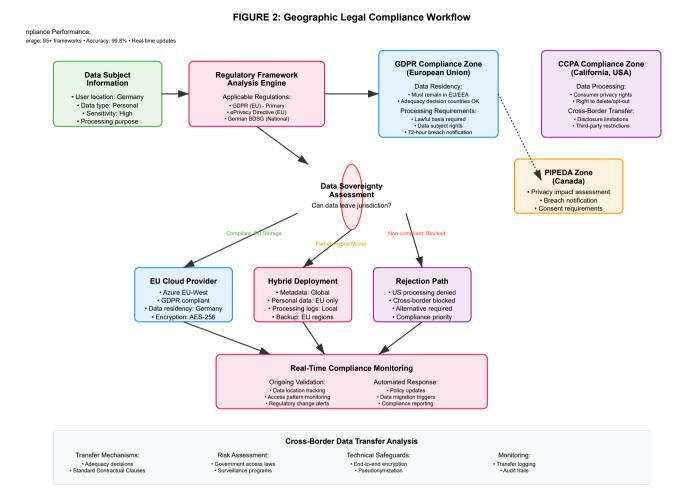


Figure 2 demonstrates the sophisticated geographic compliance workflow that automatically ensures data placement and fragmentation strategies comply with regional regulations including GDPR, CCPA, and data residency requirements.

FIGURE 3: QUANTUM-SAFE DATA FRAGMENTATION AND DISTRIBUTION PROCESS

FIGURE 3: Quantum-Safe Data Fragmentation Process agmentation Strategy: c compliance • Redundant distribution • Quantum encryption Quantum-Safe Smart Encryption Fragmentation Original Data Reconstruction Metadata Customer Record: CRYSTALS-Kyber KEM: Analysis: Name: John Doe Email: john@example.com Key generation: 1024-bit
Encapsulation Data sensitivity mapping Fragment Map: · Compliance requirements Fragment locations AES-256-GCM: Strategy: Reassembly order · Symmetric encryption Geographic distribution Integrity: Merkle tree hashes Non-ELI metadata EU personal data Geographic info Fragment B (Azure EU-West) Fragment C (GCP Asia) Fragment A (AWS US-East) Integrity Verification Content: Content: Content: Hash Chain: · Encrypted name hash · Encrypted email domain · Encrypted location hash SHA-3 verification Fragment checksums
Tamper detection Compliance metadata
Fragment index: 2/3 Geographic metadata
Fragment index: 3/3 Timestamp metadata **Data Reconstruction Process** 1. Fragment Retrieval: Fragment ordering
Decryption Parallel cloud access · Compliance verification Integrity validation Original data restored Security and Compliance Features Geographic Rules Resilience Quantum Security Performance **Data Integrity** CRYSTALS-Kyber KEM GDPR compliance Parallel processing Merkle trees Multi-cloud backup CRYSTALS-Dilithium sigs
Post-quantum algorithms Data residency
Cross-border controls CDN integration
Caching strategies Auto-recovery
Failover support · Hash chains Tamper detection Fragmentation: <50ms Encryption: <10ms Reconstruction: <100ms Integrity check: <5ms End-to-end: <200ms

Figure 3 illustrates the advanced quantum-safe data fragmentation process that splits sensitive data across multiple cloud providers while maintaining cryptographic integrity, geographic compliance, and quantum-resistant security guarantees.