JioCloud

Managed Hardware Security Module

Overview

JioCloud's Managed HSM (Hardware Security Module) delivers enterprise-grade cryptographic security without the complexity of owning and managing hardware. Built on FIPS 140-2 Level 3 certified HSMs, it ensures secure key generation, storage, and lifecycle management for sensitive workloads. Designed to meet the demand of regulated industries, the service offers high availability, scalability, and compliance—empowering organizations to protect data, digital identities, and transactions with confidence.

Key Features

- **Certified cryptographic core**
  Protect keys and operations with FIPS 140-2 Level 3 certified HSMs.
- **Seamless API integration**
  Connect easily using PKCS#11, JCE, CSP/CNG for apps, databases, and identity systems.
- **Role-based access control**
  Separate duties with Crypto Officer and Security Officer roles.
- **High availability clusters**
  Maintain uninterrupted service with clustering and automatic failover.
- **Centralized key management**
  Oversee keys from creation to retirement with full audit trails.
- **Tamper-proof security**
  All operations stay within physically secure, tamper-resistant boundaries.
- **Cloud-native scalability**
  Provision capacity elastically to meet workload spikes.
- **Multi-tenant isolation**
  Provide logical separation for teams, apps, or business units.

JioCloud

Benefits

- **Scalability**
  Scale key operations and clusters on-demand for fluctuating workloads.
- **Security**
  Hardware-backed protection with FIPS-certified assurance against physical and logical threats.
- **Integration**
  Plug into existing commercial applications such as PKI, IAM, IoT, SSL/TLS etc seamlessly.
- **Cost Efficiency**
  Reduce upfront expenditure of owning and managing dedicated HSM appliances.
- **Compliance Ready**
  Align with NIST, GDPR, HIPAA standards effortlessly.

Technologies Supported

- **Operating Systems:** Windows, Linux, Unix
- **APIs and Protocols:** PKCS#11, CSP/CNG, JCE, REST APIs
- **Cloud Integrations:** Jio Azure & On-Prem environments

Technical Specifications

Specification	Details
API Support	PKCS#11, CSP/CNG, JCE
Key Algorithms	RSA 2048, 3072,4096, AES, DES
Compliance	FIPS 140-2 Level 3

JioCloud

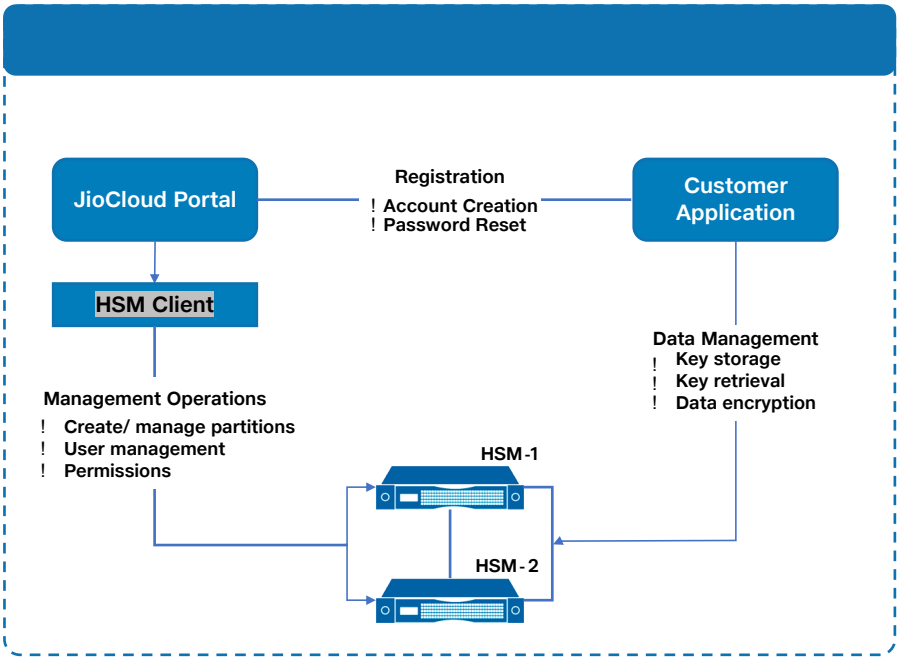
Architecture Diagram

A special purpose hardware based key storage that provides tamper resistant storage to secure keys

Store the master keys/ root keys

Secure Storage with FIPS 140-2 compliance

HSM client can access the HSM through CLI commands for management of HSM, Applications can access through proprietary or PKCS11 interface for data place



Use Cases

- **Financial services**
  Protect customer transactions and meet audit requirements with certified encryption.
- **Government and public sector**
  Keep citizen records and national identity systems safefor the long term.
- **Healthcare**
  Encrypt and safeguard patient data while staying aligned with HIPAA mandates.
- **Manufacturing**
  Ensure IoT devices and supply chain communication are both trusted and secure.
- **Cloud-native enterprises**
  Add cryptographic protection into apps and services quickly.
- **PKI and identity management**
  Support certificates, digital signatures, and secure identity frameworks.