CephVault: A Secure Key Management System for Ceph

Subhabrata Rana, Fatemeh Khoda Parast, Kenneth B. Kent
Faculty of Computer Science, University of New Brunswick
Brett Kelly
45Drives
{srana1, fkhoda, ken}@unb.ca, bkelly@45drives.com

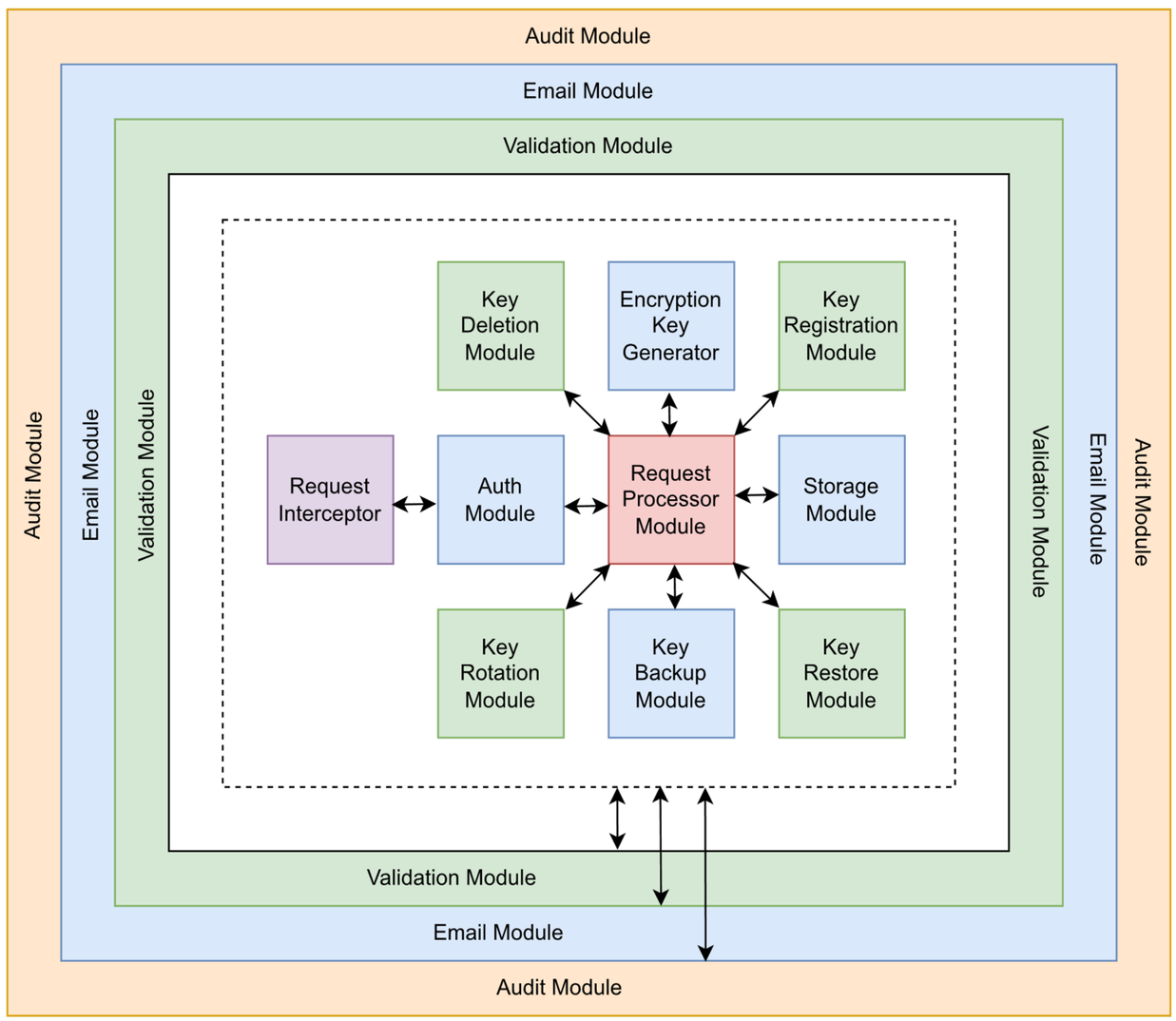
Background

- Ceph is a distributed storage system.
- Provides software-defined unified storage solutions.
- Supports object, block, and file storage.
- Massively scalable, high-performing, highly available without any single-point of failure.
- Serves as a cloud and enterprise cluster storage solution.
- Cost effective as it runs on the available commodity hardware.

Problem Statement

- Ceph lacks native object encryption.
- Ceph offers software encryption of the disk level, but objects themselves are not encrypted.
- Ceph does not support highly secure encryption schemes.
- Ceph does not have a reliable Key Management System (KMS).

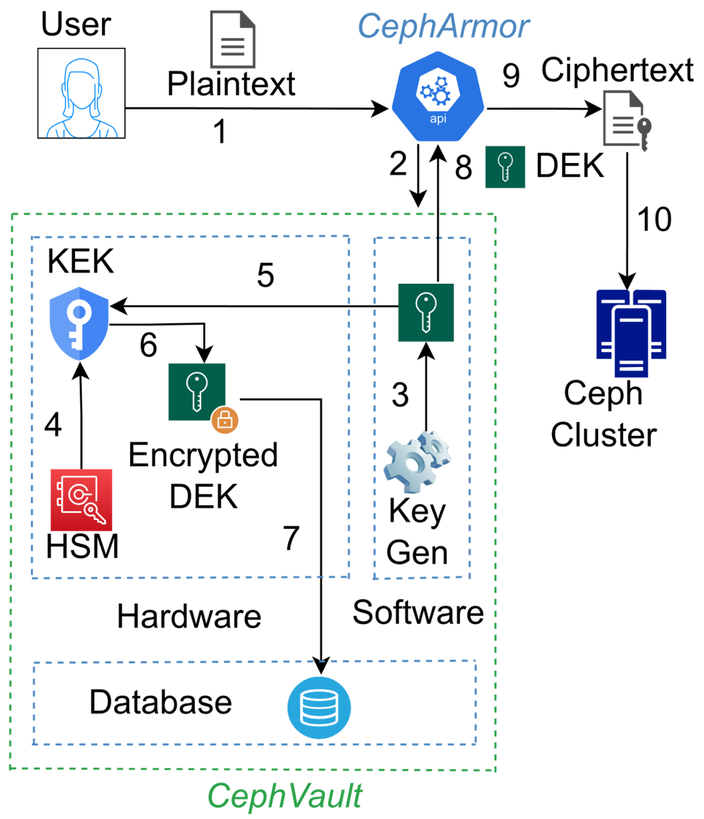
CephVault Architecture



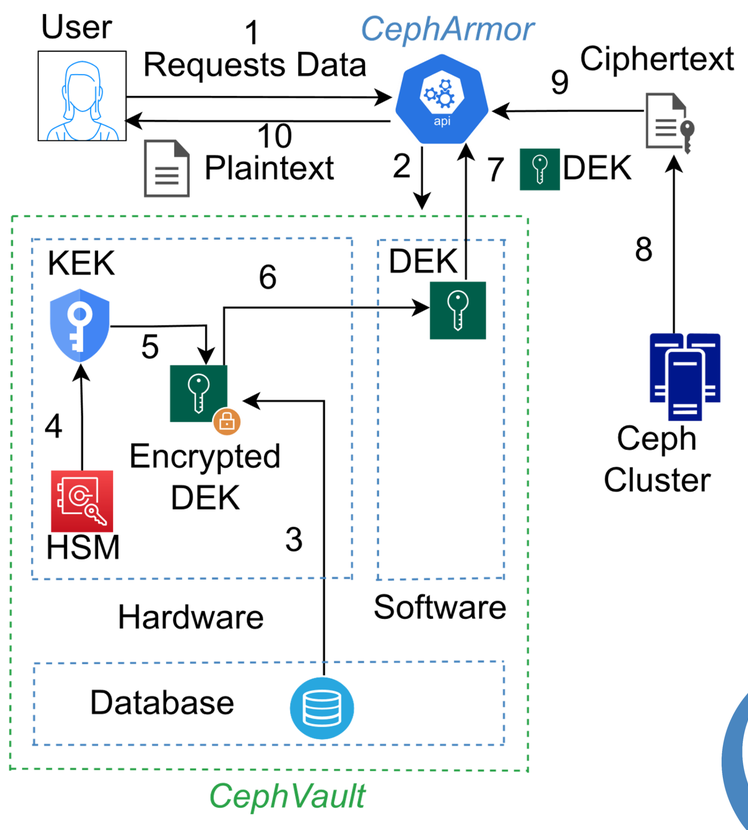
Proposed Solutions

- *CephArmor*, a lightweight API to provide encryption schemes.
- Flexibility to select various secure encryption schemes and modes.
- *CephVault,* a secure, reliable, scalable KMS for *CephArmor.*
- *CephVault* supports entire KMS lifecycle.

CephVault Encryption Operations



CephVault Decryption Operations



CAS–Atlantic