

Securing Sensitive Data in a Financial Application with AWS KMS and Cloud HSM

Data Defenders

Takala, Awa, Jaelin, Mariana



Table of Content

- ★ Overview
- ★ Overview of AWS KMS
- ★ Overview of AWS Cloud HSM
- ★ Architecture Design
- ★ Implementation Steps
- ★ Best Practices for Data Security
- ★ DataDefender_AWS_Company_SecureUtility Solutions
- ★ Conclusion & Takeaways
- ★ References

OVERVIEW

Project Objective:

Design and implement a secure data encryption strategy utilizing AWS Key Management Service (KMS) and AWS Cloud HSM to safeguard sensitive data at rest and in transit within the AWS cloud environment. The project emphasizes ongoing security hygiene, key management practices, and provides a roadmap for future enhancements to ensure the long-term effectiveness of data protection in the cloud.

Project Goal:

Provide a robust and secure data encryption strategy within the AWS cloud environment to significantly reduce the risk of data breaches and improve overall data security posture.

Target Audience:


Cloud Security Architects,
Security Engineers, Data
Security Specialists



Overview of AWS KMS

AWS Key Management Service (KMS) is a highly available and scalable key management service that allows users to create and manage encryption keys. KMS makes it easy to protect sensitive data by providing a centralized and secure key management solution.

1. KMS supports customer-managed keys for custom encryption workflows
2. KMS integrates with other AWS services like **S3**, **DynamoDB**, and **RDS** for encrypted data storage
3. KMS provides secure key generation, storage, and management, with support for audit logging and key rotation

- S3: Scalable object storage (**hosting websites, storing media files**)
 - DynamoDB: NoSQL databases (**gaming, IoT, mobile apps**)
 - RDS: Managed relational databases (**e-commerce, content management, enterprise apps**)
- 

Encryption Key Management with AWS



1- Key Generation

AWS KMS allows you to create and manage your own encryption keys, ensuring full control over the lifecycle of your sensitive data.

2- Key Storage

KMS securely stores your keys in a highly available and durable service, protecting them from unauthorized access or tampering.

3- Key Usage

KMS provides a simple API for your applications to encrypt, decrypt, and re-encrypt data using your keys, without exposing the actual key material.

Comparison of AWS KMS and AWS Cloud HSM



AWS KMS

A managed key management service that allows you to create and control encryption keys. Offers software-based encryption with centralized key management.

AWS CLOUD HSM

A hardware security module (HSM) service that provides a dedicated, on-premises HSM appliance for securing cryptographic operations.

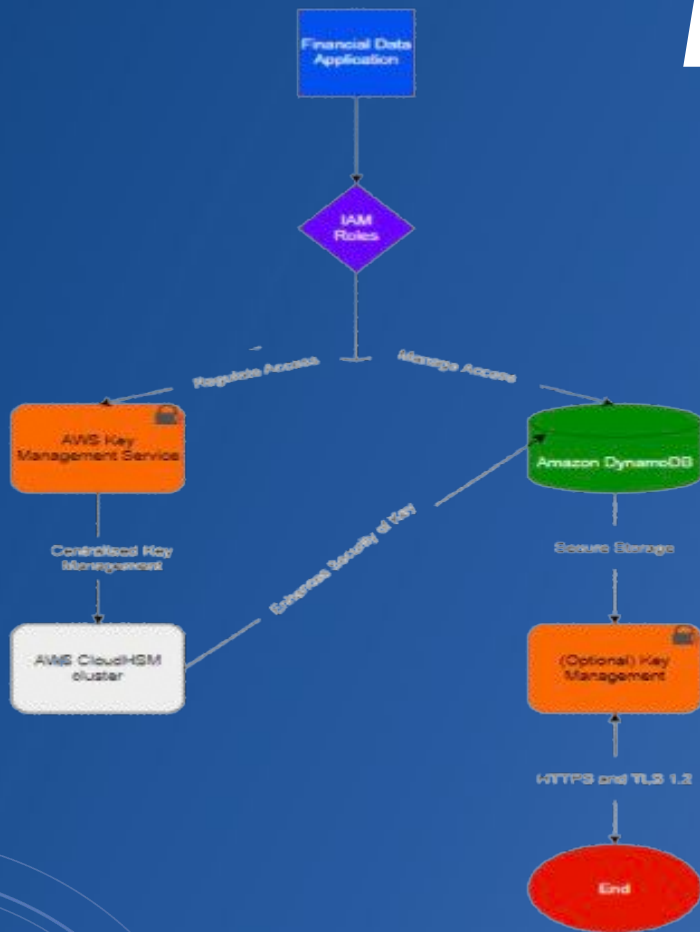
KEY DIFFERENCES

- KMS is software-based, Cloud HSM is hardware-based.
- Cloud HSM offers FIPS 140-2 Level 3 compliance for highly sensitive data
- Cloud HSM provides more control over encryption keys and operations
- KMS is easier to set up and manage, Cloud HSM requires more hands-on administration

USE CASES

KMS is well-suited for general-purpose encryption needs, while Cloud HSM is better for highly regulated industries with strict compliance requirements.

ARCHITECTURE DESIGN



- Financial app interacts with IAM for access.
- IAM manages KMS for key control.
- KMS encrypts financial data.
- Cloud HSM boosts key security.
- DynamoDB stores financial data securely.
- Optional: HashiCorp Vault for key management.
- Secure protocols (HTTPS, TLS 1.2+) ensure data safety.



IMPLEMENTATION STEPS

1

Identify Sensitive Data

Determine the critical data assets that require the highest level of protection, such as customer account details, transaction history, and financial statements.

2

Create KMS Key

Generate an encryption key using AWS KMS, which provides centralized control and auditing of your encryption keys.

3

Encrypt Data

Use the KMS key to encrypt sensitive data within your financial application before storing it in the cloud.

4

Leverage AWS Cloud HSM

Utilize AWS Cloud HSM, a hardware-based key storage solution, to manage the lifecycle of encryption keys and ensure the highest level of security

5

Integrate AWS KMS

Use AWS KMS to create customer-managed encryption keys and apply them to encrypt sensitive data at rest and in transit.

Best Practices for Securing Sensitive Data



Use Encryption at Rest and in Transit

Encrypt all sensitive financial data when it's stored and when it's sent over networks.

Use Hardware security Module (HSMs)

Use devices like AWS Cloud HSM to securely create, store, and manage encryption keys.

Enforce Strict Access Controls

Use strong identity and access management to limit who can access sensitive data.

Keep Detailed Logs and Monitor

Record and review detailed audit logs to detect and respond to suspicious activities or data breaches

Example

Use TLS for data in transit and AES-256 for data at rest.

Example

Store encryption keys in AWS Cloud HSM to keep them safe

Example

Implement role-based access control (RBAC) to ensure only authorized personnel can access sensitive data

Example

Use tools like AWS Cloud Trail to monitor access patterns and identify anomalies.



SecureUtility Solutions

SECUREUTILITY SOLUTIONS



secure data, EFFICIENT management**





SecureUtility Solutions

SECUREUTILITY SOLUTIONS



secure data, EFFICIENT Management**

SecureUtility Solutions is a leading provider of cloud-based management systems for utility companies worldwide. We specialize in ensuring the secure and efficient management of sensitive data, including customer information and operational details. Our robust security measures and protocols safeguard critical data against unauthorized access and breaches, providing utility companies with peace of mind and reliable service.





Comprehensive Utility Management Solutions

SECURE UTILITY SOLUTIONS



secure data, efficient management**

1

Customer Information Management

Securely manage customer account details, billing information, and contact preferences.

2

Operational Data Management

Efficiently handle meter readings, usage patterns, and maintenance schedules.

3

Asset Management

Track and maintain infrastructure, including power lines, substations, and equipment.

4

Billing and Payment Processing

Streamline billing, process payments securely, and manage customer accounts effectively.

5

Analytics and Reporting

Gain insights, identify trends, and make informed decisions to improve efficiency and customer service.



Multi-Layered Data Protection Approach

SECUREUTILITY SOLUTIONS



Secure data, EFFICIENT Management**

1

Encryption

Industry-standard encryption protocols for data at rest and in transit.

2

Access Control

Strict measures with role-based access control (RBAC) for authorized personnel.

3

Data Masking

Anonymization and obfuscation techniques for data sharing and testing.

4

Regular Security Audits

Proactive assessments to identify and address vulnerabilities.



Compliance Standards

SECURE UTILITY SOLUTIONS



secure data, EFFICIENT management**

GDPR Compliance

PCI-DSS Compliance

Adherence to
General Data
Protection
Regulation standards
for data privacy and
security.

Compliance with
Payment Card
Industry Data
Security Standard for
secure payment
processing.





Secure Communication Channels

SECURE UTILITY SOLUTIONS



secure data, EFFICIENT Management**

HTTPS and TLS 1.2+

Ensures encrypted data exchange between components, preventing unauthorized access and interception.

Private Networking

VPC and private subnets create isolated network environments for secure data transmission.

IAM and RBAC

Restricts access to sensitive resources through policies and role-based access control.



User Roles and Permissions

SECURE UTILITY SOLUTIONS



Secure Data, Efficient Management**

Role	Key Permissions	Description
Administrator	AWSKMSFullAccess, AWSCloudHSMFullAccess, IAMFullAccess	Oversees overall management and security of the AWS environment. Responsible for key creation, rotation, and management in AWS KMS and CloudHSM. Manages user permissions and roles through IAM.
Data Engineer	AWSKMSFullAccess, AWSCloudHSMFullAccess, AmazonS3FullAccess, AmazonRDSFullAccess	Implements and manages data encryption mechanisms. Creates and manages encryption keys, integrates with CloudHSM, and secures data in S3 and RDS. Focuses on ensuring data security across storage and database systems.



User Roles and Permissions

SECURE UTILITY SOLUTIONS



Secure Data, Efficient Management**

Role	Key Permissions	Description
Security Analyst	AWSKMSReadOnly, AWSCloudHSMReadOnly, CloudTrailReadOnlyAccess	Monitors and analyzes security events and compliance status. Has read-only access to AWS KMS, CloudHSM, and CloudTrail for generating reports, analyzing logs, and tracking API activity.
Developer	AWSKMSReadOnly, AmazonS3ReadOnlyAccess, AmazonRDSReadOnlyAccess	Focuses on application development and integration of security features. Has read-only access to KMS, S3, and RDS for testing encryption mechanisms, data storage, and database functionality.

Compliance
Officer

-AWSKMSReadOnly

-CloudTrailReadOnlyAccess

CONCLUSION

- **Protecting sensitive data** in financial applications is essential for **consumer trust** and **compliance**.
- By using **AWS KMS** and **Cloud HSM**, organizations can:
 - Implement **strong encryption**
 - Use advanced **key management**
- These steps **protect** the organization's most valuable **assets**.



TAKEAWAYS

- ★ **Prioritize end-to-end data encryption**
- ★ **Leverage hardware-based security** with Cloud HSM for highly sensitive data
- ★ **Enforce strict access controls**
- ★ **Maintain comprehensive logging and monitoring** to detect and respond to security incidents

A word cloud featuring the phrase "Thank You" in numerous languages and scripts. The words are arranged in a circular pattern, with "thank you" in large red letters at the center. Other prominent words include "gracias" in green, "danke" in blue, "merci" in orange, and "shukriya" in purple. The colors of the words vary, creating a vibrant and multicultural visual. The background is white, making the colorful text stand out.