Step 1: Project Plan (Week 1)

Data Defenders_Capstone Project

Define project goals, scope, target audience, and success metrics.

- **Goal:** Secure financial data using AWS KMS and CloudHSM.
- **Scope:** Secure financial data at rest and in transit within the AWS cloud environment.
- **Target Audience:** Financial Data Security Professionals.
- **Success Goals**: Achieve a notable reduction, at least 15%, in the likelihood of data breaches and ensure strict compliance with financial data privacy regulations such as the General Data Protection Regulation (GDPR) or Payment Card Industry Data Security Standard (PCI-DSS). Create a thorough 10-week sprint plan delineating specific tasks and milestones for each phase, including data encryption implementation, compliance audits, and staff training.

Step 2: Requirements Document (Week 1-2)

Required Document- Deliverable 1

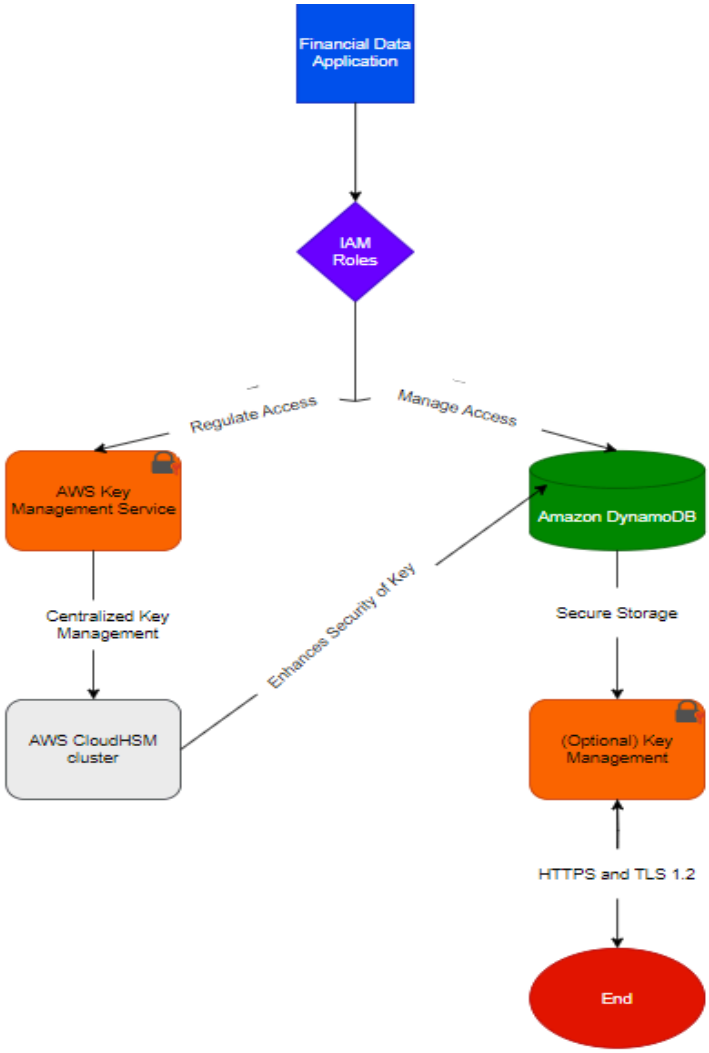
Identify and classify sensitive patient data into high and low sensitivity categories. Define specific data elements within each category.

High Sensitivity Data	**Low Sensitivity Data**
1. Account Numbers	1. Customer Names
2. Personal Identification Information (PII)	2. Contact Information
3. Transaction Amounts	3. Transaction Dates
4. Investment Portfolio Details	4. Product or Service Details
5. Income Statements	5. Account Opening Dates
6. Tax Identification Numbers (TIN)	6. Transaction Descriptions
7. Account Balances	7. Payment History
8. Loan Details	8. Transaction References
9. Financial Statements	9. Account Status (e.g., active, closed)
10. Securities Holdings	10. User Preferences

Step 3: Architecture Design (Week 2)

Visualize the architecture with the following components:

- Utilize KMS for centralized key management ensuring robust encryption.
- Implement a CloudHSM cluster to fortify the security of high-sensitivity data keys.
- Utilize DynamoDB for secure storage of financial data.
- Establish IAM roles to regulate access to KMS keys and DynamoDB tables, ensuring strict control over data access.
- Optionally, integrate key management middleware such as HashiCorp Vault for comprehensive encryption key management.
- Enforce secure communication protocols like HTTPS and TLS 1.2 or higher to safeguard data during transmission.



This visual architecture illustrates the flow of data and the integration of various components:

- Financial data application interacts with IAM roles to regulate access.
- IAM roles manage access to KMS for centralized key management.
- KMS is utilized for robust encryption of financial data.
- A CloudHSM cluster enhances the security of high-sensitivity data keys.
- DynamoDB serves as secure storage for financial data.
- Optionally, key management middleware such as HashiCorp Vault can be integrated for comprehensive encryption key management.
- Secure communication protocols like HTTPS and TLS 1.2 or higher ensure data transmission security.

10 Week Sprint Schedule

Sprint Week	Deliverables	Due Date
Sprint 1: (Week 1-2)	• Assign roles and responsibilities to the team. • Create users using IAM to work collaboratively. • GitHub Repository • Define project goals. • Create an outline of how to achieve that goal. • Identify what platforms will be used. • Team understands the concept of CloudHSM and AWS KMS. • Create High-Level Architecture Diagram	Monday, April 15 - Wednesday, May 1, 2024
Sprint 2: (Week 3-4): Secure Key Management with AWS KMS (Week 3-4	**KMS Key Management (Week 3)** • Create two CMKs in KMS: • KMS_Low_Sensitivity: Encrypts low-sensitivity data. • KMS_High_Sensitivity: Stored in CloudHSM for heightened security. • Implement key rotation every 30-90 days for enhanced security. **IAM Policies (Week 3)** • Develop IAM policies for precise access control: • Restrict access based on user roles. • Follow the principle of least privilege.	Monday, April 29 - Wednesday, May 15, 2024

Sprint Week	Deliverables	Due Date
	KMS Integration (Week 4) ● Configure server-side encryption for DynamoDB tables: ● Select KMS_Low_Sensitivity for low-sensitivity data. ● Choose KMS_High_Sensitivity for high-sensitivity data.	
Sprint 3 (Week 5-6): Enhanced Security with AWS CloudHSM (Week 5-6)	**CloudHSM Deployment & Configuration (Week 5)** Note: Deploying a CloudHSM cluster incurs additional costs compared to standard KMS keys. Evaluate your security needs and budget before proceeding. 1. Start creating a CloudHSM cluster in your VPC. 2. Choose HSM instance type based on workload and security needs. 3. Select Availability Zone(s) in your VPC for optimal performance. **Configuration Steps:** ● Decide backup policy for data recovery. ● Consider creating partitions for multi-tenant deployments. ● Specify VPC subnets and configure security groups. ● Initialize HSM following on-screen instructions.	Monday, May 13 - Wednesday, May 29, 2024

Sprint Week	Deliverables	Due Date
	Additional Considerations: ● Refer to AWS CloudHSM documentation for detailed instructions. ● Note cluster endpoint and relevant configuration details for KMS integration.	
Sprint 4: (Week 7-8) Securing Data in Transit with KMS	**Secure Communication Setup (Week 7)** Configure your financial data application and any related services handling sensitive data to utilize robust transport protocols such as HTTPS or TLS 1.2 or higher for all communication. Enforce the adoption of these protocols within your application's codebase and explore implementing certificate validation to guarantee secure connections. **KMS Integration with Key Management Middleware (Optional) (Week 7-8)** This step, though optional, adds depth to your security strategy. If opting for key management middleware (e.g., HashiCorp Vault), follow your middleware's integration guidelines.	Monday, May 27 - Wednesday, Jun 12, 2024

Sprint Week	Deliverables	Due Date
	Typically, this involves configuring the middleware to link with AWS KMS, handling the retrieval and usage of encryption keys for your application's data in transit.	
Sprint 5: (Week 9-10) Monitoring & Auditing (Week 9-10):	**KMS CloudTrail Integration (Week 9)** Enable CloudTrail logging for KMS to track all key usage activity, including key creation, deletion, rotation, and unauthorized access attempts. Configure CloudTrail to deliver logs to an S3 bucket within your account for centralized storage and analysis. **Security Automation for Key Management (Week 9)** Develop automated security checks using AWS Lambda functions to monitor KMS activity logs for suspicious patterns. Examples of suspicious patterns could include excessive key access attempts from unauthorized sources or unusual usage patterns for specific KMS keys. Configure Lambda functions to trigger alerts or notifications upon detecting suspicious activity, enhancing security measures for financial data management.	Monday, June 10 - Wednesday, Jun 26, 2024

Sprint Week	Deliverables	Due Date
	Penetration Testing & Security Validation (Week 9-10) - Perform penetration testing on your data encryption strategy to uncover potential vulnerabilities. - Engage qualified security professionals or use AWS services like Amazon Inspector for testing. - Resolve any vulnerabilities found during testing to enhance overall security. **Knowledge & Handover Package (Week 10)**	