NAME:AMUDA RANTI

ROLE: CLOUD SECURITY ENGINEER

TASK: CLOUD DATA ENCRYPTION IMPLEMENTATION USING AWS KMS

I led the implementation of a cloud data encryption strategy using AWS Key Management Service (KMS) to secure sensitive data at rest and in transit. This experience demonstrates my ability to apply encryption best practices, enforce compliance with industry standards, and enhance data security within a cloud environment.

Project Scope & Key Responsibilities

1. Securing Data at Rest with AWS KMS

Deployed AWS KMS Customer Managed Keys (CMKs) for centralized encryption management.

Implemented server-side encryption (SSE-KMS) across:

Amazon S3 (default encryption and bucket policies)

Amazon RDS databases with automated key rotation

Amazon EBS volumes for encrypted EC2 instances

Enforced IAM-based access controls to limit decryption permissions.

2. Securing Data in Transit

Enforced TLS 1.2+ encryption to secure communication channels.

Applied KMS-integrated encryption for:

API Gateway and Lambda functions

Data transmission between AWS services (S3, RDS, EC2)

VPN tunnels using AWS Site-to-Site VPN with IPSec

Validated encryption settings using AWS Config Rules and security policies.

3. Compliance, Monitoring & Auditing

Enabled AWS CloudTrail to log key usage and access attempts.

Integrated AWS Security Hub to assess compliance with encryption policies.

Configured Amazon CloudWatch Alarms to detect unauthorized key access.

Business Impact & Key Outcomes

- Strengthened Data Security – Ensured end-to-end encryption for critical cloud data.
- Regulatory Compliance – Met security requirements for GDPR, HIPAA, and PCI DSS.
- Improved Access Control – Implemented strict IAM-based key management policies.
- Enhanced Visibility – Enabled monitoring and alerting for key access activities.
- Demonstrated Cloud Security Expertise – Showcased hands-on experience with AWS KMS and encryption best practices.

- AWS KMS configuration details, including key policies and access controls.
- Documentation of encryption implementation for S3, RDS, and EBS.
- TLS encryption setup and verification steps for data in transit.
- CloudTrail logs and compliance reports from AWS Security Hub.

This experience highlights my ability to architect and implement secure cloud encryption strategies, reinforcing my expertise in cloud security and compliance