IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 8, August 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308138|

Key to the Cloud: A Review of Amazon Web Services, Azure, and Google Cloud Platform Key Management Systems

Varadharaj Varadhan Krishnan

Independent Researcher, Washington, USA

ABSTRACT: In this paper, various features, security protocols, use cases, and challenges associated with each of the three main key management servers are made available. The paper also offers insights to help organizations select the best solution for their needs. Through a comparative analysis, the paper highlights the strengths and limitations of each of the services and provides a guideline tool for decision-making. The goal of this paper is to assist organizations in making informed decisions about their public cloud key management security strategy and ensure that they can effectively protect sensitive data while meeting compliance requirements and optimizing operational efficiency.

KEYWORDS: Key Management System, AWS KMS, Azure Key Vault, GCP KMS, Cloud Security, Data Security.

I. INTRODUCTION

Amazon Web Services, the pioneer in public cloud infrastructure as a service, turned 18 this year (2024). In the last 15 years, cloud computing has emerged as a digital transformation vehicle for various businesses and has become an integral part of modern Information Technology (IT) infrastructure [1][8]. Today, most organizations have at least some parts of their IT infrastructure in the public cloud, if not for the majority of their IT footprint. With the growth in more digital applications and systems moving to the public cloud and being built natively in the public cloud, data security and cloud security becomes imperative. Key Management Systems (KMS) play a vital role in data security in the cloud. Key Management Services (KMS) go beyond encryption by including rotation, secure storage, and access control. In environments like the public cloud, with data spread across various services and storage options and accessed by different users, applications like KMS help maintain strict security measures and comply with regulations. Without a strong KMS system in place, organizations face risks like data breaches, non=compliance, as well as potential financial and reputational harm [1][2]. The purpose of this paper is to review the KMS solutions offered by the top three cloud service providers, namely Amazon Web Services Key Management Service (AWS KMS), Azure Key Vault, and Google Cloud Platform Key Management Service (GCP KMS). Organizations using AWS, Azure., or GCP tend to use the native key management solution as well. Hence, a significant number of organizations are using these Cloud Service Provider (CSP) provided key management solutions. The aim of this review is to evaluate and compare the features, security protocols, practical applications, and operational challenges with these CSP's native key management solutions. By doing that, the paper aims to provide insights to help organizations choose the correct KMS solution for their cloud security requirements and be aware of any deficiencies and feature gaps. Clearly understanding these gaps can help organizations build systems or other controls to address them and thereby maintain a secure public cloud footprint.

II. OVERVIEW OF KEY MANAGEMENT SERVICES

A Key Management Service (KMS) is a software system that provides capabilities to securely manage cryptographic keys used for encryption and decryption of data [2]. In the context of the public cloud, KMS provides capabilities like creating, storing, managing, and using cryptographic keys within a cloud environment. KMS also provides automation for various stages of a key management lifecycle. They are vital to most modern organizations to make sure critical cryptographic keys are handled securely. The core capabilities of a KMS typically include [4][5][6].

1. Key Generation: Creation of a new key or key pair for data encryption, decryption, digital signatures, and other cryptographic functions.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308138|

2. Key Storage: Securely store keys. Ensure keys are secured at rest; most often, a Hardware Security Module (HSM) is used for that.
3. Key Rotation: Periodically rotate keys.
4. Access Control: Managing permissions and policies governing usage specifying who can access the keys and for what purposes. This guarantees that authorized individuals can utilize the keys.
5. Key Auditing and Monitoring: Monitoring usage activities for compliance and security monitoring objectives, like detecting unauthorized access.
6. Key Destruction: Securely revoking and eliminating keys that are no longer required or have been compromised [3][8][10]

The significance of Key Management Service (KMS) in cloud security cannot be emphasized enough. As businesses transfer more of their data and applications to the cloud, ensuring the confidentiality, integrity, and availability of this data becomes crucial. KMS plays a role in securing data in cloud environments through these methods [7]. Data Encryption: KMS facilitates the encryption of data both at rest and in transit. By managing the keys required for encryption, KMS ensures that sensitive data remains safeguarded even if the encrypted data is intercepted or accessed by unauthorized individuals. Compliance with Regulations: Many industries are bound by guidelines concerning data protection and encryption, such as GDPR, HIPAA, and PCI DSS. KMS assists organizations in meeting these regulations by offering the tools and controls to manage encryption keys while complying with relevant standards. Access Management: KMS empowers organizations to enforce strict access controls on who can access encryption keys. This reduces the risk of unauthorized access and prevents potential data breaches.

Key management practice has its roots in ancient times. It is not new and not something specific to the public cloud. CSPs provide KMS solutions to help organizations operate securely in the public cloud. Amazon unveiled its Key Management Service (KMS) offering in 2013; prior to that, customers had been relying on management systems tailored for on-premise setups, which were not well suited for the cloud environment [9]. Amazon's KMS empowered users to handle keys for both Amazon services and their own applications, whether they were operating on-premises or in the cloud. Following suit, Microsoft introduced Azure Key Vault, which has similar functionalities. These services have since evolved to encompass not encryption keys but password connection strings and other confidential information. Google also entered the scene with its key management service launch in 2017, further diversifying the landscape.

III. SHARED RESPONSIBILITY MODEL

In cloud, security is a shared responsibility between the CSP and the Customer. The shared responsibility model articulates the security obligations of each party, understanding this model is important for cloud customers, primarily to know what they are responsible for and act on it. Figure 1 shows an Illustration of Shared Responsibility Model from Microsoft [11].

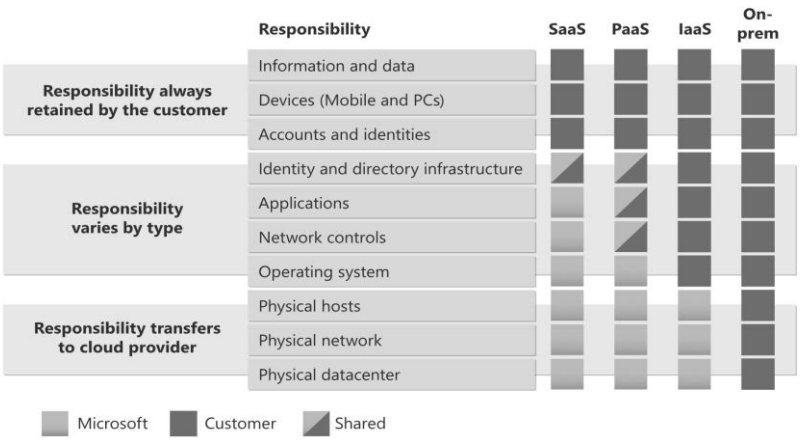

Figure 1 Public Cloud Shared Responsibility Model [11]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308138|

Amazon Web Services describes the shared responsibility model as "Security of the Cloud" and "Security in the Cloud." AWS is responsible for ensuring the security of the cloud environment, which involves safeguarding all the underlying components, such as hardware, software, networking, and facilities that support AWS services. On the other hand, customers hold the responsibility for maintaining security within the cloud. This can vary depending on the specific services customers use. When it comes to Infrastructure as a Service (IaaS) offerings like Amazon EC2, customers need to take care of security configurations, operating system management, and updating applications. For services like Amazon S3 and DynamoDB, AWS handles the infrastructure aspect while customers are tasked with managing their data securely through encryption measures and implementing access controls using Identity and Access Management tools. The shared responsibility model clarifies that although cloud providers provide the infrastructure and tools needed for data security, the responsibility for protecting data lies with the customer. This underscores the role a Key Management Service (KMS) plays in cloud security.

IV. COMPARATIVE ANALYSIS

Each of the three KMS services offer a range of features for all stages of the key management lifecycle. However, they differ in their specific features, integration options, supported technical standards and service maturity with respect to integration with other cloud native services offered the KMS provider. Table 1 outlines the key features of each service and compares it with other cloud KMS service [3-8][13-20].

Feature	AWS KMS	Azure Key Vault	Google Cloud KMS
Service Name	AWS Key Management Service (KMS)	Azure Key Vault	Google Cloud Key Management Service (KMS)
Primary Use Cases	Encryption and decryption of data, management of cryptographic keys	Management of keys, secrets, and certificates	Management of cryptographic keys and encryption/decryption
Key Types Supported	Symmetric and Asymmetric keys	Symmetric and Asymmetric keys	Symmetric and Asymmetric keys
Integrated Services	AWS S3, AWS EBS, AWS RDS, AWS Lambda, etc.	Azure Storage, Azure SQL Database, Azure VM, etc.	Google Cloud Storage, Google Compute Engine, BigQuery, etc.
Key Rotation	Automatic and manual	Automatic and manual	Automatic and manual
Key Import/Export	Key import supported; export restricted	Key import supported; export restricted	Key import supported; export restricted
HSM Support	AWS CloudHSM integration available	Azure Dedicated HSM	Cloud HSM, External Key Manager (EKM)
Compliance and Certifications	FIPS 140-2, SOC, PCI-DSS, HIPAA, FedRAMP	FIPS 140-2, SOC, PCI-DSS, HIPAA, FedRAMP	FIPS 140-2, SOC, PCI-DSS, HIPAA, FedRAMP
Key Access Control	AWS IAM, Key Policies	Azure RBAC, Access Policies	Google Cloud IAM, Key Policies
Logging and Monitoring	AWS CloudTrail, AWS CloudWatch	Azure Monitor, Azure Security Center	Cloud Audit Logs, Google Cloud Monitoring
Backup and Recovery	Automatic, integrated with AWS Backup	Automatic, integrated with Azure Backup	Automatic, integrated with Google Cloud Backup
Secret Management	Integrated with AWS Secrets Manager	Built-in secret management	Integrated with Google Cloud Secret Manager
Hybrid and Multi-Cloud Support	AWS Outposts, AWS Snowball, multi-cloud key management	Azure Arc, Azure Stack, multi-cloud key management	Anthos, multi-cloud key management

Table 1 AWS KMS vs. Azure Key Vault vs. GCP KMS Feature Comparison

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308138|

Table 2 shows a comparison of supported technical standards and limits [3-8][13-20].

Feature	AWS KMS	Azure Key Vault	Google Cloud KMS
Key Storage	Appliance (Software + Hardware)	Appliance* (Software)	Appliance (Software + Hardware)
FIPS 140-2 Level	Level 2	Level 2	Level 1
Key Types	Symmetric and Asymmetric	Asymmetric	Symmetric and Asymmetric
BYOK (Bring Your Own Key)	AES 256-bit wrapped by RSA 2048-bit	RSA wrapped by AES and RSA-OAEP	AES 256-bit wrapped by RSA 3072-bit
Symmetric Key Length	256-bit AES	None	256-bit AES
Asymmetric Key Length	2048-bit, 3072-bit, 4096-bit RSA	2048-bit, 3072-bit, 4096-bit RSA	2048-bit, 3072-bit, 4096-bit RSA
Encryption Modes	AES-GCM, RSA-OAEP	AES-GCM, RSA-OAEP	RSA PKCS#1v1.5, RSA-OAEP
Plain-text size limit	4KB	0.25KB	64KB
Signature Modes	• RSA-PSS • RSA PKCS#1v1.5 • ECDSA with P-256 • ECDSA with P-384 • ECDSA with P-512 • ECDSA with SECP-256k1	• RSA-PSS • RSA PKCS#1v1.5 • ECDSA with P-256 • ECDSA with P-384 • ECDSA with P-512 • ECDSA with SECP-256k1	• RSA-PSS • RSA PKCS#1v1.5 • ECDSA with P-256 • ECDSA with P-384
Key Capabilities	• AWS Managed Service • Encryption/Decryption • Sign/Verify • Auditing • REST APIs	• Support Customer Managed Keys • Support tokens, passwords, certificates, API keys, and other secrets • Encryption/Decryption • Sign/Verify • Key Vault logging • REST APIs	• Support Customer Managed Keys • Encryption/Decryption • Sign/Verify • Auditing • REST APIs

Table 2 AWS KMS vs. Azure Key Vault vs. GCP KMS Technical Standards Comparison

V. CHALLENGES AND CONSIDERATIONS

Although services such as AWS KMS, Azure Key Vault, and GCP KMS offer a baseline capability for data encryption and security, they also pose certain challenges that every organization should address. Complexity of Key Management: Handling keys across cloud platforms can be complex, especially for organizations operating in multi-cloud or hybrid setups. Ensuring the rotation, secure storage, and effective management of keys across multiple services needs significant administrative oversight and technical proficiency. Security Concerns: Despite the strong security posture and control maintained by the cloud service provider, cloud KMS solutions are always susceptible to misconfigurations via human mistakes that could result in unauthorized access to sensitive keys and encrypted information. It is critical to configure correct access permissions and continuously monitor them to ensure only authorized users and services have access to the secret stores in the KMS systems. Compliance and Regulatory Obligations: Various industries and government agencies have their own compliance mandates regarding data protection and encryption. Adhering to these requirements can pose a challenge in environments where data is spread across multiple regions with varying regulations. Aligning KMS solutions with these frameworks needs both a good understanding of the framework and technical proficiency to convert the requirements laid out in the framework to actual implementation.

When transitioning between Key Management Service (KMS) platforms or incorporating KMS solutions into existing systems, several factors should be considered. Key Compatibility: One of the challenges in migrating between KMS

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308138|

platforms is to make sure that cryptographic keys can be easily moved and are compatible across systems. Since each cloud provider has their own KMS setup, compatibility issues may arise, leading to the need for data decryption and re-encryption. Interoperability: Integrating a KMS with applications and services can be complex sometimes, especially if there are significant differences between the old and new KMSs. Organizations must verify that the new KMS seamlessly integrates with their current applications and data storage solutions without causing disruptions. Data Integrity: During migration, there's a risk of downtime or data integrity problems if the migration process isn't well planned and executed. Organizations' plans for moving data should incorporate testing, backup strategies, and backup plans to ensure data security and accessibility during the transition. Vendor Lock-In: Transitioning KMS providers can be complex due to the nature of cloud services. Organizations need to consider the advantages of migration versus the risks of being tied to one vendor's platform, which might restrict flexibility and raise long-term expenses. Organizations need to assess these aspects when selecting and implementing a KMS solution to ensure it aligns with their future requirements. Strategic planning, awareness of constraints, and informed decisions are essential to address these challenges and optimize the benefits of cloud KMS solutions.

VI. CONCLUSION

Organizations adopt public cloud for agility, scalability, and overall reduced cost, but it also presents new challenges in data privacy and security. Organizations should analyze and clearly define their data privacy requirements, obligations to external agencies, and regional laws regarding data security before adopting public cloud technologies. Key Management Systems (KMS) play a critical role in achieving meeting those requirements by securely managing cryptographic keys and transiently complying with various standards. The effectiveness of a KMS in a public cloud environment depends on how the cloud controls are used to protect the keys, especially for cases like BYOK (Bring Your Own Key). Organizations should intentionally design controls to mitigate the threats they think they have with moving sensitive data into the cloud; they should evaluate their existing key and to-be key management systems against their privacy and security goals. In this paper, we have reviewed and detailed the differences between the top three cloud-native KMS solutions available in the market and address the challenges and considerations organizations should have before they choose a KMS solution. The information and insights shared in the paper should serve as a guiding light for organizations that are evaluating a new cloud-based KMS solution.

REFERENCES

1. Encryption Consulting. AWS KMS vs. Azure Key Vault vs. GCP KMS. Encryption Consulting. https://www.encryptionconsulting.com/aws-kms-vs-azure-key-vault-vs-gcp-kms/
2. Mahesh, S. (2013). Data classification: The foundation for achieving information security. In S. Mahesh (Ed.), Information security management handbook (pp. 1-16). Springer. https://link.springer.com/chapter/10.1007/978-1-4614-9278-8_1
3. Amazon Web Services. AWS Key Management Service: Overview. AWS Documentation. https://docs.aws.amazon.com/kms/latest/developerguide/overview.html
4. Microsoft. Basic concepts - Azure Key Vault. Microsoft Learn. https://learn.microsoft.com/en-us/azure/key-vault/general/basic-concepts
5. Google Cloud. Key Management Service documentation. Google Cloud Documentation. https://cloud.google.com/kms/docs/key-management-service
6. Amazon Web Services. Cryptographic details for AWS KMS. AWS Documentation. https://docs.aws.amazon.com/kms/latest/cryptographic-details/intro.html
7. Amazon Web Services. Cryptographic operations in AWS KMS. AWS Documentation. https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html#cryptographic-operations
8. Entro Security. (2023). Comparison of key management solutions: Google, AWS, Microsoft. https://entro.security/blog/comparison-key-management-solutions-google-aws-microsoft/
9. Mahesh, S. (2013). Data classification: The foundation for achieving information security. In S. Mahesh (Ed.), Information security management handbook (pp. 1-16). Springer. https://link.springer.com/chapter/10.1007/978-1-4614-9278-8_1
10. Cloud Security Alliance. (2017). Key management when using cloud services. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services
11. Microsoft. Shared responsibility in the cloud. Microsoft Learn. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 8, August 2024

|DOI: 10.15680/IJIRSET.2024.1308138|

12. Biryukov, A., & Lysyanskaya, A. (2016). Cryptographic systems in cloud environments. Proceedings of the ACM Conference on Computer and Communications Security, 10, 138-147. https://dl.acm.org/doi/abs/10.1145/2909067.2909068
13. Microsoft. About keys - Azure Key Vault. Microsoft Learn. https://learn.microsoft.com/en-us/azure/key-vault/keys/about-keys
14. Microsoft. Azure Key Vault - Key management. Microsoft Learn. https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management
15. Microsoft. Azure Managed HSM overview. Microsoft Learn. https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/overview
16. Microsoft. About secrets - Azure Key Vault. Microsoft Learn. https://learn.microsoft.com/en-us/azure/key-vault/secrets/about-secrets
17. Google Cloud. Client-side encryption with Key Management Service. Google Cloud Documentation. https://cloud.google.com/kms/docs/client-side-encryption
18. Google Cloud. Digital signatures with Key Management Service. Google Cloud Documentation. https://cloud.google.com/kms/docs/digital-signatures
19. Google Cloud. Key Management Service: Protecting data. Google Cloud Documentation. https://cloud.google.com/kms/docs/key-management-service#protecting-data
20. Google Cloud. Protection levels in Key Management Service. Google Cloud Documentation. https://cloud.google.com/kms/docs/protection-levels

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details