ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Comparative Analysis of Native Secrets Management Services

Rameshbabu Lakshmanasamy

Senior Data Engineer, Jewelers Mutual Group, USA

ABSTRACT

Secrets management means storing, accessing, and managing secrets, including API keys, passwords, encryption keys, certificates, etc. It has a vital role in current Information Technology infrastructure since it ensures that private information is well protected from access by other people and hackers. Proper secret handling lowers data exposure, and adherence to security regulations is vital for businesses that run their applications in the cloud environment. The rationale for this comparative analysis is to provide the companies with the information needed to assess the capabilities and drawbacks of each native secrets management solution. In this way, these services are compared based on such parameters as feature, price, usability, and security, which helps organizations and companies to make correct decisions according to their business conditions and capacities, thus increasing the safety level of the organizations.

***Corresponding author**

Rameshbabu Lakshmanasamy, Senior Data Engineer, Jewelers Mutual Group, USA.

Received: November 13, 2024; **Accepted:** November 20, 2024; **Published:** November 29, 2024

Keywords: Secrets Management, GCP Secrets Manager, AWS Secrets Manager, Azure Key Vault

Introduction

Three major cloud providers—Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)—offer native secrets management services: AWS Secrets Manager, Azure Key Vault, and Google Secret Manager are included to represent Cloud Service Providers. These solutions allow organizations to effectively protect and process their sensitive information within their cloud environments, including encryption, rights management, and auditing functionalities [1].

Overview of Each Secrets Management Service

AWS Secrets Manager

AWS Secrets Manager is an AWS service that provides secure storage and management of Secrets, such as keys, passwords, and credentials, of any database. It discourages users from obtaining secrets by hard-coding them in the code, putting them in one place, and controlling access to them. One outstanding property is that secret updates can be performed automatically without affecting services that this supports: Amazon RDS, Redshift, etc.

To enable smooth integration, AWS Secrets Manager supports services like EC2, ECS, and lambda, while secrets on rest accepted use AWS KMS and are defined by the user. AWS IAM is user and Access Control and AWS CloudTrail can give this detailed auditing if needed [2]. It also enables secret versioning and lifecycle, in other words, to manage updates without any issues.

Azure Key Vault

Azure Key Vault is a service hosted in the Azure Cloud that securely manages cryptographic essential secrets and certificates. It stores all the primary data, such as IDs and credentials, several passwords, API keys, and connection strings [3]. This mainly covers essential creation and storage, whereas the Hardware Security Module supports and stores essential creation. The service also addresses certificate management, including issuance, renewal, and their overall lifecycle.

Azure Key Vault is easily interoperable with other Azure services, such as Azure AD, Azure DevOps, and Azure App Service, which enhance the security of managing secrets and keys. Benefits include tight integration with Azure AD for identity management and the use of HSM-based security to meet compliance, which is achieved by automating previously manual certificate management.

Google Secret Manager

Google Secret Manager is an infrastructure service that securely stores organizes, and retrieves information such as API keys, passwords, and certificates. Described for use specifically on Google Cloud Platform (GCP), it focuses on flexibility, security, and compatibility with other GCP services [4]. The highlighted features include versioning, where users can set and track different secret versions for easy updates and rollback, as this provides stability in the event of changes. Specifically, Google Cloud IAM is used for access control in the system; it grants and revokes somewhat granular, role-based access to secrets.

Data protection involves data encryption at rest and in transit, while Google handles encryption keys. Users can also decide to provide their keys, which will be used in encryption (BYOK) to enhance their usage. Google Secret Manager also works well with similar services such as Google Kubernetes Engine (GKE), App Engine, and Cloud Functions to facilitate access to secrets in the cloud application [5]. Furthermore, audit logging is tied to Google Cloud Audit Logs, which helps shed light on secret access and use.

Feature Comparison

Security and Encryption

AWS Secrets Manager stores secrets at rest in AWS KMS and in transit in TLS. The service is SOC 2, ISO 27001, and PCI DSS compliant. You can disable the service's managed keys and use its customer-managed keys for more customization instead.

Azure Key Vault also supports encryption of data both at rest and in-transit, and has available to it HSM-backed keys for the highest level of security. It has facilities for user-defined keys and is SOC 2, ISO 27001 & FIPS 140-2 compliant.

In Google Secret Manager, data is shielded using Google-generated keys or customer-generated keys (BYOK) and TLS for the data in transit. The company has compliance standards that include SOC 2, ISO 27001, and GDPR compliance.

All three services provide high-security measures, including strong encryption and security certification. Organizations can choose from among the list depending on the infrastructure, compliance, and security measures they require.

Access Control and Identity Management

The steps related to the implementation of access control guarantee that only the required subject can access the secret, which is very important for security.

AWS Secrets Manager also operates with AWS Identity and access management systems, providing precise RBAC and enabling scalable control of privileges for AWS Secrets Manager. For the secrets, users can set up precise permissions depending on the individual, a group or a service that needs to access those secrets. AWS Identity and Access Management has flexibility designed into it through IAM roles and policies that can be used to manage consolidated and filtered access to resources across accounts and services [6].

RBAC is also used by Azure Key Vault, where Azure Active Directory serves as the source. It allows for defining the role of definite identities, which dictates permission levels regarding secrets within the vault—who is allowed to use, admin, or modify them. The integration with Azure AD ensures that the organization can utilize the existing identity management frameworks, thus making work easy when setting up permissions.

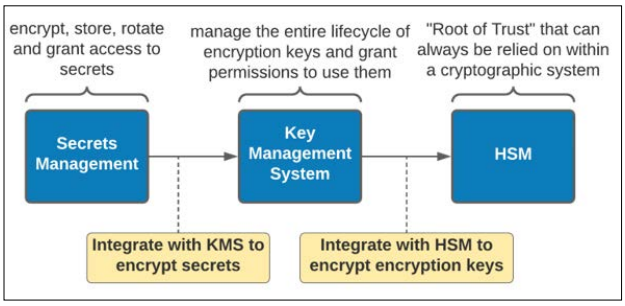
GSM assigns roles from the Cloud Identity and Access Management service for defining access rights to secrets. IAM-based permissions offer a permission granularity level in which users set permissions (read, write, administrative, etc.) on the identity [6]. This close coupling of the GCP service guarantees that only the endorsed services or people can access or modify secrets.

Backup and Recovery

The Secrets Manager helps maintain multiple versions of a secret and can quickly revert to a prior version if needed. Some of its features are related to lifecycle management—such as the automatic removal of old versions—and can help organizations control secrets during their lifecycle.

The next feature is that Azure Key Vault allows storing different versions of secrets and, if necessary, revert to a previous version. The user or a program can delete such information; however, there is a chance to restore information deleted within a specified time limit. This feature allows you to fix the documents and is good if you delete something by mistake; it does not let you deviate from the main track.

Google Secret Manager also has versioning built in so not only can you update secrets to their current version but you can see previous versions and even restore to a prior version of the secret. If needed, secrets can be erased by hand, and the service offers tools for managing the life cycle of secrets for removing unused ones [2].



Pricing Models and Cost Comparison

AWS Secrets Manager Pricing

AWS Secrets Manager charges are based on two main components: encryption specialization and APIs. The basic subscription tier costs $12 per month per secret, plus up to 30,000 API calls per month. Any other request is extra chargeable. For instance, from October 2024, AWS demands $0.40 for each secret in a month and $.005 for each 1000 API operations over 30000. With AWS, for example, there is a free tier where you can store up to thirty secrets for the first thirty days free, and this is good for evaluating small applications.

Nevertheless, the costs can quickly skyrocket for high-traffic workloads, especially when working with many secrets or constantly making many API calls. AWS also allows users to subscribe to savings plans and reserved instance pricing. Users with relatively fixed workloads may find this a way to save significant money.

Azure Key Vault Pricing

Azure Key Vault's pricing model includes costs for secret storage, key management, and HSM-backed operations, with standard and premium tiers. Secret storage also allows for charging per operation, with primary operations having low tariffs, making it affordable to organizations with moderate security needs. The more secure version, which includes keys backed up with HSM, costs more than the standard one. Except for other costs, request fees are charged on every specific operation. Usually, it is $0.03 for 10000 operations. The pricing structure allows deriving standard and premium tiers as needed, but depending on HSM-backed keys can be highly costly if high-security requirements exist [7].

Google Secret Manager Pricing

Google Secret Manager follows a simple pricing model, where you are charged based on the number of secrets stored and the number of API calls made. Secrets processing costs $ about 0.06 per active secret version per month, and API requests cost $ 0.03 per 10,000 operations. Google also offers a free version that offers ten actively managed secret versions and allows up to 10,000 monthly operations, suitable for small applications or a staging environment [8]. Google's business model is pretty straightforward regarding pricing, overall costs, and invoicing. Nonetheless, the facility cost per operation tends to be much higher in large-scale implementation due to the high frequency of utilization of secrets.

Comparative Analysis

Comparing the pricing structure of these services, AWS Secrets Manager is more economical for small to medium workloads primarily because it has a simple pricing plan and a free tier of operation, offering a believable quantity of operations before you are charged. Nevertheless, it becomes rather expensive in an environment characterized by a large number of calls, in which case extra charges will be applicable for API services.

Depending on an organization's embrace of Azure services, Azure Key Vault may be more attractive since it allows for choosing between standard and premium tiers. Tier mixing flexibility can be utilized to bring down the costs, but for those who need to leverage HSM-backed security, it might be costly to go to Azure premium service [9]. Another disadvantage is that Azure's pay-per-operation model may place additional costs to interact with the secrets frequently.

According to the Google Secret Manager, the price is simple and prevents bill shock, which makes it suitable for smaller project users and developers. Being a free tier, it is also ideal for testing & small projects. However, constantly querying the API can be expensive for large environments competing with services such as AWS and Azure without some of the added security functionalities being a priority.

Integration Capabilities

Native Integration with Cloud Services

AWS Secrets Manager interworks tightly with AWS services like AWS Lambda, Amazon EC2, Amazon RDS, AWS ECS, and more. This helps provide secure, automated, machinable access to secrets used in applications deployed on these services without baking them into the applications. AWS Secrets Manager directly associates secrets with application deployments, making workflows smoother and more secure.

Specifically, Azure Key Vault integrates directly with Azure DevOps, AKS, and Azure App Service, which means secure secrets apply to available CI/CD pipelines and virtual and cloud-native applications. Managing access through identity relies on Azure AD for authentication and provides a streamlined application for secret access in the Azure environment.

Google Secret Manager seamlessly works with Google Kubernetes Engine (GKE), Google Cloud Functions, and App Engine so secrets for GCP-native applications can be accessed securely [6]. This allows developers to avoid the cardinal mistake of hard-coding secrets, making security easy to manage and the management overhead low.

Third-Party Tool Integration

All three services, AWS Secrets Manager, Azure Key Vault, and Google Secret Manager, are extensible with other third-party secrets management services to accommodate additional functionality. Kubernetes Secrets, HashiCorp Vault, and all these services can be utilized in tandem with AWS, Azure, and other providers, which allows organizations to manage secrets and credentials centrally across different cloud environments or internally on the company's infrastructure.

In the same context, Google Secret Manager works with other tools such as Terraform for infrastructure as code and HashiCorp Vault for secrets management. This flexibility is particularly appropriate in deploying programs where multiple clouds are involved and require a single solution for secret management.

	Secret Manager	HashiCorp Vault	Berglas
Key/Value Storage	Yes	Yes, default API support for up to 32MB	Yes, limited to 64GiB
Secrets Rotation	No	Yes	No
Password Generation	No	Yes	No
Infrastructure as Code Integration	Yes	Yes	Yes

Cross-Platform Considerations

Securing and syncing multiple credentials related to any multi-cloud or hybrid cloud architecture is more essential. All three services provide strong APIs that enable the use of secrets and interaction with other tools or services running on a different cloud. Failures in security policies can occur for numerous reasons; having tools like HashiCorp Vault that can connect to AWS, Azure, and Google Cloud protect areas that were once openly accessible to predefined specifications towards both secrets and security policies can be implemented [7].

Conclusion

In the case of AWS Secrets Manager, Azure Key Vault, and Google Secret Manager, each of them offers certain benefits. AWS Secrets Manager is the best in integrating and having auto-rotating features for managers for those most into AWS services and products. However, this increases costs depending on the traffic needed. Regarding security solutions, Azure Key Vault is robust and integrates well with Azure AD, but the price could be more straightforward. Hailed for simplicity and no extra hidden fees, Google Secret Manager is fluttery for startups and small to medium-scale businesses in the GCP domain. Thus, the solution largely depends upon specific requirements from security or integration points of view, pricing models, or compliance requirements.

References

1. Arcolini D (2023) Full Lifecycle API Management: Microgateway Infrastructural Pattern adopting Kong Gateway. Doctoral dissertation, Polytechnic of Turin https://webthesis.biblio.polito.it/29360/.
2. Dotson C (2023) Practical Cloud Security. O'Reilly Media, Inc https://books.google.com/books?hl=en&lr=&id=2GTbEAAAQBAJ&oi=fnd&pg=PP1&dq=Comparative+Analysis+of+Native+Secrets+Management+Services++AWS+Secrets+Manager,+Azure+Key+Vault,+and+Google+Secret+Manager,&ots=zapUf8v7o1&sig=MHWqm8Boe7EtE-nX-OcK1NgM0N8.
3. Hamid M (2023) Advanced Secret Handling in Kubernetes Application with HashiCorp Vault. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1836909.
4. Mwikya J, Karani J, Obura J (2022) Secure Management of Encryption Keys for Small and Medium Enterprises in Africa: A Comparative Study. 5th KyU International conference https://www.researchgate.net/profile/James-Reuben-5/publication/360342471_Secure_management_of_encryption_keys_for_small_and_medium_enterprises_in_Africa_A_comparative_study/links/627130433a23744a726006ba/Secure-management-of-encryption-keys-for-small-and-medium-enterprises-in-Africa-A-comparative-study.pdf.
5. Ots K (2021) Azure Security Handbook. Apress https://link.springer.com/content/pdf/10.1007/978-1-4842-7292-3.pdf.
6. Somasundaram P (2024) Unified Secret Management Across Cloud Platforms: A Strategy for Secure Credential Storage and Access. International Journal of Computer Engineering & Technology 5-12.
7. Li H, Evans D (2017) Horcrux: A password manager for paranoids. arXiv preprint https://arxiv.org/abs/1706.05085.

8. Maxwell R (2024) Azure Arc Systems Management: Governance and Administration of Multi-cloud and Hybrid IT Estates. Springer Nature https://books.google.com/books?hl=en&lr=&id=4ekXEQAAQBAJ&oi=fnd&pg=PR5&dq=Comparative+Analysis+of+Native+Secrets+Management+Services++AWS+Secrets+Manager,+Azure+Key+Vault+Google+Secret+Manager,&ots=6BwFCwNRMd&sig=ERdagweQnvdF4qBJOBOtaYq7hUM.

9. Sailakshmi V (2021) Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud. St. Clous State University https://repository.stcloudstate.edu/msia_etds/112/. https://repository.stcloudstate.edu/msia_etds/112/.