# Secret Management in Managed Kubernetes Services

**Santosh Pai [1], & Srinivasa. R. Kunte [2]**

[1] Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
Orcid ID: 0000-0002-5053-1673; E-Mail ID: g.santoshpai@gmail.com

[2] Research Professor, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
Orcid ID: 0000-0002-5062-1505; E-Mail ID: kuntesrk@gmail.com

**Area of the Paper:** Computer Science.
**Type of the Paper:** Case Study.
**Type of Review:** Peer Reviewed as per |C|O|P|E| guidance.
**Indexed In:** OpenAIRE.
**DOI:** https://doi.org/10.5281/zenodo.7875023
**Google Scholar Citation:** IJCSBE

**How to Cite this Paper:**

Pai, S., & Kunte, S. R., (2023). Secret Management in Managed Kubernetes Services. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7*(2), 130-140. DOI: https://doi.org/10.5281/zenodo.7875023

**International Journal of Case Studies in Business, IT and Education (IJCSBE)**
A Refereed International Journal of Srinivas University, India.

Crossref DOI: https://doi.org/10.47992/IJCSBE.2581.6942.0263

Paper Submission: 18/12/2023
Paper Publication: 29/04/2024

# Secret Management in Managed Kubernetes Services

**Santosh Pai [1], & Srinivasa. R. Kunte [2]**

[1] Research Scholar, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
Orcid ID: 0000-0002-5053-1673; E-Mail ID: g.santoshpai@gmail.com

[2] Research Professor, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India,
Orcid ID: 0000-0002-5062-1505; E-Mail ID: kuntesrk@gmail.com

## ABSTRACT

**Purpose:** *Security and Privacy risks are increasing in the industry. Managed Kubernetes services help organizations to deploy micro service in the cloud. Securing the Secrets used by micro service applications in the cloud is a crucial topic. This paper studies how managed Kubernetes service industry secures the application Secrets in the cloud.*

**Design/Methodology/Approach**: *This study includes various Kubernetes service providers in the industry. The documentation available in the provider website and the published whitepapers are used to understand the Secret management technology.*

**Findings/Result:** *Software applications and their data are protected in managed cloud services using Secret keys. Across service providers, there is a trend and a common approach in managing the Secrets. External or remote services integration is an improvement area for the providers. Operators have the responsibility of protecting Secrets and ensuring it does not leak out.*

**Originality/Value:** *This paper studies the efforts of different vendors to protect the micro service Secrets. This ensures that the organization's critical assets are protected as per regulations and do not lead to financial losses. Cloud misconfiguration is one of the most common mistakes leading to security attacks, the knowledge of vendor's features helps to configure the cloud services securely.*

**Paper Type:** *Case study*

**Keywords:** Cyber Security, Secrets, Managed Kubernetes, SWOC analysis.

## 1. INTRODUCTION :

For many years, the software industry created monolithic software. Monolithic software usually involves application logic of all different functionalities implemented in the same large software. This approach works for small software. Complexities increase as the products get bigger. Maintaining complex software is one of the biggest challenges for organizations. Updating the software requires recompiling the entire product and deploying the same in the customer network.

Micro services architecture [1] solved the complexities of maintaining monolithic software. They break the monolith software into smaller applications [2]. This approach simplifies software maintenance. A potential issue in one micro service does not impact other micro service. This creates high cohesion and low coupling between the micro services.

Linux kernel provides capabilities for software isolation. In 2013, the concept of Containerization became popular [3]. It uses the isolation features offered by the Linux Kernel. Containerization helped organizations to realize micro service architecture. Google created Kubernetes to orchestrate the Containerized solution in 2014 [4]. Kubernetes automates the deployment, scaling, and management of micro service applications. It allowed aggregating micro services into a logical unit known as a Pod. Cloud Native Computing Foundation has maintained Kubernetes since 2016 [5].

With the advancement in Cloud and Web technologies, Kubernetes became one of the most popular platforms to host micro services [6] [7]. Organizations had to create a data center of physical or virtual machines to host Kubernetes. Managed Kubernetes allows businesses to host their micro services in the cloud without Capital Expenditures. Companies can concentrate on building applications to solve their

customer's problems. The managed Kubernetes service is responsible for hosting the application and providing the services.

A typical Pod includes one or more containerized micro services. Pods communicate with each other to share data. Adding a security layer for such communications requires credentials that the Pods use to negotiate a secure protocol. These credentials are called Secrets. A Secret can be a simple username and password, API Key, Access Tokens, or Private Key. Since Pods and their containers use the file system of the host operating system, storing the Secrets in the file system is not a secure solution.

This paper will explore how managed Kubernetes services secure the Secrets used by the micro services.

## 2. RELATED WORKS :

Google Scholar engine provides articles published on managed Kubernetes Services. Keywords such as ‘managed Kubernetes Secrets’, ‘managed Kubernetes’, ‘Azure Kubernetes Service Secret’, ‘Operating Azure Kubernetes Service’, and 'Google Kubernetes Engine Secret' filter the articles. Articles focused on managed Kubernetes published between 2014 to 2022 are filtered and reviewed. Table 1 summarizes the literature review.

**Table 1:** Contribution to the study of managed Kubernetes Services

| S. No | Focus | Contribution | References |
|---|---|---|---|
| 1. | Containerization | Kubernetes allows deploying and updating Secrets without re-creating the application image. | Shah & Dubaria, (2019). [8] |
| 2. | Secret management | With the help of an external Secret manager Open-source project, it was possible to integrate Kubernetes with the AWS Secret manager and Hashicorp Vault Secret manager. | Jurvanen, (2021). [9] |
| 3. | Secret management | There is software available to centralize the Secret management in an organization. The Secret injections feature of Kubernetes allows easy Secret management for organizations. | Blomqvist et al., (2021). [10] |
| 4. | Secret management | Kubernetes Secrets are stored as plaintext by default. It is recommended to use a Secret manager to encrypt the Secrets. | Shamim et al., (2020). [11] |
| 5. | Application deployment | Organizations can use Helm charts to configure Secrets in Kubernetes along with other application configurations | Gokhale et al., (2021). [12] |
| 6. | Performance Verification | Utilization of managed Kubernetes services did not directly impact the application's performance. The performance depended on the choice of cloud service resources. | Ferreira, & Sinnott, (2019). [13] |
| 7. | Azure Kubernetes Service | Azure Kubernetes Service provides support for Kubernetes Secrets to store confidential information. | Buchanan et al., (2020). [14] |
| 8. | Azure Kubernetes Service | By configuring the Azure Kubernetes Service correctly, it is possible to avoid cross-tenant service access. | Giangiulio & Malmberg, (2022). [15] |
| 9. | Container Orchestration | Kubernetes is a prevalent orchestration tool. Open Shift has the most Secret features for applications and cluster management. | Malviya, & Dwivedi, (2022). [16] |
| 10. | Performance Verification | All cloud platforms provided more than seventy percent accuracy | Opara et al., (2022). [17] |

## 3. RESEARCH GAP :

Current studies on Secret management in Kubernetes are limited to open-source Kubernetes solutions. Studies on the managed Kubernetes services are limited. In this paper, we focus our analysis on Secret management in managed Kubernetes services provided by different vendors.

## 4. RESEARCH AGENDA :

The paper has the following agenda for studying managed Kubernetes services in the cloud:
1. What is the default storage used for Secrets?
2. How managed Kubernetes services support Secret encryption?
3. Which managed Kubernetes Services can integrate Secret management services?
4. What are the strengths, weaknesses, opportunities, and challenges of secret management in managed Kubernetes services?

## 5. OBJECTIVES OF THE STUDY :

1. To study the default storage used by the managed Kubernetes services to store the Secrets
2. To analyse the Secret encryption strategy used by different managed Kubernetes service providers
3. To study the list of Secret management services that integrate with managed Kubernetes services
4. To perform SWOC analysis of Secret management solutions in managed Kubernetes services

## 6. METHODOLOGY :

The data required for this study is captured via journals, articles, and official documentation of the cloud service providers. Technical blogs from the internet are also used where necessary. Official documentation from the service providers served as one of the primary sources, as it provided up-to-date information about current design of the Secret Management in Kubernetes.
SWOC analysis is performed to study Secret management in Kubernetes managed services. Services listed in Table 2 are considered for the study using publicly available documentation [18-23].

**Table 2:** Managed Kubernetes services available in the market

| S. No | Service Name | Cloud Provider Name | Year of global availability | References |
|---|---|---|---|---|
| 1. | Amazon Elastic Kubernetes Service | Amazon Web Services | 2018 | Barr, (2018). |
| 2. | Azure Kubernetes Service | Microsoft | 2018 | Burns, (2018). |
| 3. | Google Kubernetes Engine | Google | 2014 | Google Cloud, (2014). |
| 4. | IBM Cloud Kubernetes Service | IBM | 2018 | Rosen, (2018). |
| 5. | Oracle Container Engine for Kubernetes | Oracle | 2018 | Oracle, (2018). |
| 6. | Alibaba Container Service for Kubernetes | Alibaba | 2015 | Tang et al., (2019). |

**Source**: Author

Google Kubernetes Service was the first to launch the managed Kubernetes service in 2014, followed by Alibaba Service for Kubernetes. In 2018, other significant vendors launched managed Kubernetes services. As of 2021, 90% of Kubernetes users use managed Kubernetes services [24].

## 7. DEFAULT SECRET MANAGEMENT IMPLEMENTATION :

**Open-source Kubernetes Secret management**
A typical application deployed in Kubernetes operates by connecting with external services and databases. The applications need Secrets to authenticate to others in Kubernetes and outside the Kubernetes cluster. A simple Secret is a username and password combination. The Secret can be an API Key or a token. The format and content of the Secret are specific to the application. Kubernetes

stores Secrets in a local database known as *etcd*. The Secrets are stored in plaintext in the database, and no access control is applied at the granular level.

Kubernetes recommends some measures to secure the application Secrets [25]. Enabling Secret encryption at rest [26] encrypts the plaintext Secrets in the *etcd*. This ensures data at rest for all Secrets stored in *etcd*. Different encryption providers are supported to allow encryption using different algorithms. There is a problem with this approach as it does not protect against the compromise of the key used for encrypting the Secrets when attackers access the Host node. The key is stored in a file on the host. Table 3 indicates the default storage location for the Secrets in the managed Kubernetes services [27-32].

**Table 3:** Default Secret store used in the managed Kubernetes services

| S. No | Service Name | Default Secret Store | Reference |
|---|---|---|---|
| 1. | Amazon Elastic Kubernetes Service | *etcd* | Amazon Web Services, (2022). |
| 2. | Azure Kubernetes Service | *etcd* | Microsoft, (2022) |
| 3. | Google Kubernetes Engine | *etcd* | Google, (2022). |
| 4. | IBM Cloud Kubernetes Service | *etcd* | IBM, (2022). |
| 5. | Oracle Container Engine for Kubernetes | *etcd* | Oracle, (2022). |
| 6. | Alibaba Container Service for Kubernetes | *etcd* | Alibaba Cloud, (2022). |

**Source**: Author

## 8. SECRET ENCRYPTION IMPLEMENTATION :

This section will identify the Secret encryption implementation supported by managed Kubernetes service providers. We use the attributes listed in Table 4 to study the supported features.

**Table 4:** Attributes for Secret encryption study

| S. No | Attribute Name | Attribute Value and Description |
|---|---|---|
| 1. | Default encryption type | No encryption - The application is responsible for all encryptions. By default, there is no encryption provided.<br><br>Disk encryption - storage volume is encrypted by the service.<br><br>Envelope encryption - Secrets are encrypted by the service using a user-provided key / managed key. |
| 2. | Envelope Encryption Support | Not supported - The service does not implement Envelope encryption.<br><br>Supported - Service supported the Envelope encryption. The user should enable it.<br><br>Default - Service supports Envelope encryption by default. |
| 3. | Encryption Key Ownership | Service Managed - Cloud service providers are responsible for the encryption key's lifecycle.<br><br>User Managed - Cloud service expects the service user to manage the Key lifecycle. |

**Source**: Author

The managed Kubernetes services are studied using the attributes in Table 4. The results of the study are detailed in Table 5.

**Table 5:** Secret encryption feature details

| S. No | Service Name | Default encryption type | Envelope Encryption Support | Envelope Encryption Key Ownership |
|---|---|---|---|---|
| 1. | Amazon Elastic Kubernetes Service | Disk encryption | Supported | Service Managed |
| 2. | Azure Kubernetes Service | Disk encryption | Supported | Service Managed |
| 3. | Google Kubernetes Engine | Disk encryption | Supported | Service Managed |
| 4. | IBM Cloud Kubernetes Service | Disk encryption | Supported | Service Managed |
| 5. | Oracle Container Engine for Kubernetes | Disk encryption | Supported | Service Managed |
| 6. | Alibaba Container Service for Kubernetes | Disk encryption | Supported | Service Managed |

**Source:** Author

Kubernetes allows an additional layer of encryption known as Envelop encryption [33]. Envelop encryption will enable Secrets to be stored encrypted in *etcd*. This is an extra layer of defense on top of disk encryption. The Secrets in the *etcd* are encrypted using the Kubernetes generated Secret key. This Kubernetes generated Secret key is encrypted using the user provided Customer Master Key. Users can manage CMK using AWS KMS.

Amazon Elastic Kubernetes Service stores the Secrets in *etcd* using AWS volumes. The disks where these volumes are stored are, by default, encrypted by AWS [34], [27]. There is no user intervention needed here. Support for Envelope encryption is provided by implementing the encryption provider [35] interface of Kubernetes.

Azure Kubernetes Service or AKS uses a fully managed data store for the *etcd* backend. This ensures Secrets are encrypted at rest using disk encryption. AKS provides options to encrypt Secrets stored in the *etcd* using Envelope encryption [36]. The encryption works similarly to AWS EKS by using a key hierarchy. AKS uses the AES-256 algorithm for encryption. User's keys are stored in Azure Key Vault and shared with AKS workloads using the KMS plugin.

There is an additional option to create a Private Key Vault, passing the Secrets between Kubernetes and Key Vault over an Azure private communication link. This reduces the risk of public exposure and attack surface [37]. Google cloud provides encryption of Secrets using multiple layers of hardware and software controls [29]. GKE uses *etcd* to store the Secrets and default encrypted at the disk level. An optional application layer encryption is supported [38].

IBM Kubernetes service also uses *etcd* as the default store for Secrets. Using a KMS provider, the service allows users to bring their key for Envelope encryption. Oracle Container Engine for Kubernetes and Alibaba Container Service for Kubernetes provide similar Envelope encryption and default Volume encryption features.

## 9. KEY MANAGEMENT INTEGRATION SUPPORT :

An External Key Management Service is a service outside the managed Kubernetes cluster that can be used to manage the Secrets used by the applications in the Kubernetes cluster. This section details the external Secret management integration support of the managed Kubernetes services. Table 6 lists different integrations supported by the managed Kubernetes services [36], [39], [40-43].

**Table 6:** Secret management service integrations

| S. No | Kubernetes Service Name | Key Management Service Name | References |
|---|---|---|---|
| 1. | Amazon Elastic Kubernetes Service | AWS Secret Manager | Amazon Web Services, (2022) |

| | | | |
|---|---|---|---|
| 2. | Azure Kubernetes Service | Azure Key Vault | Microsoft, (2022) |
| 3. | Google Kubernetes Engine | Cloud KMS | Google, (2022) |
| 4. | IBM Cloud Kubernetes Service | IBM Key Protect for IBM Cloud, Hyper Protect Crypto Services | IBM, (2022) |
| 5. | Oracle Container Engine for Kubernetes | Oracle Cloud Infrastructure Vault service | Oracle, (2022) |
| 6. | Alibaba Container Service for Kubernetes | Key Management Service | Alibaba Cloud, (2022) |

**Source**: Author

The Kubernetes service in Table 6 and their corresponding Key Management Services belong to the same cloud provider. For example, Cloud KMS and Google Kubernetes Engine are from Google Cloud vendors. Integrating AWS Secret Manager or any other Key Management service with Google Kubernetes Engine is impossible.

Most cloud provider documentation indicated limitations when using the Key management services to encrypt the Secrets. Once enabled, Envelope encryption cannot be disabled during the lifetime of the Kubernetes cluster. Disabling the Envelope encryption is not allowed. IBM Kubernetes Engine service does not allow IP filtering features when using Key management service [44].

## 10. SWOC ANALYSIS OF SECRET MANAGEMENT SOLUTION :

SWOC analysis [45] provides current situation, and a fair comparison with competitions. It is used to identify next steps to improve the performance [46]. Data backup security and cloud computing security are considered one of the top challenges in using Amazon Web Service storage solutions [47]. Encryption of the data at rest and the data at transit are highly reliable solutions to protect the data in Cloud. Secrets are the basic elements that enable encryption algorithms. Strength of the encryption depends on the strength of the Secrets used. Kubernetes Secret management solutions are studied to understand the current Strengths, Weaknesses, Opportunities, and Challenges. The analysis is provided in Table 7.

**Table 7:** The SWOC Analysis of Secret management solutions

| | |
|---|---|
| Strengths of Secret management | • Secrets are stored in encrypted disk by default<br>• Envelop encryption is supported to customize Secret encryption<br>• Manual Secret management is avoided, and reduced human intervention<br>• Centralized secret management avoids need for local storage of the sensitive data<br>• Secret rotation is provided by the service provider |
| Weakness of Secret management | • Compromise of the Secret database *etcd* by an attacker could leak the Secrets<br>• Cloud misconfiguration could lead to poor management of the Secrets<br>• Insider attacks on the cloud provider services leak the secrets to cloud provide employees<br>• Secrets could be shared to Cloud provider's third party |
| Opportunities of Secret management | • Integration with third party Secret management solutions<br>• Standardization of the Secret management in cloud to allow compatibility between cloud providers |
| Challenges of Secret management | • Ensuring Secrets are secured at rest and during transfer |

| | |
|---|---|
| | • Ensuring Access control mechanisms on the Secrets for external and internal attackers in the Kubernetes service provider organization<br>• Complying to regulations and standards to help the Secret management consumers achieve the compliance<br>• Shifting to strong encryption algorithms and retiring weak encryption algorithm while maintaining the compatibility with existing Secrets<br>• Creating awareness about secure cloud configurations options for Secret management to cloud administrators |

## 11. FINDINGS :

This section lists the findings of the research.
1. Managed Kubernetes services use default *etcd* database to store the Secrets
2. Disks used to store the *etcd* data are encrypted at rest by default
3. Envelope encryption is supported by all managed Kubernetes services
4. Applications deployed in a cloud cannot use the Key management service of another cloud service provider
5. Kubernetes stores a cached entry of Data Encryption Keys when the Secret manager is configured

## 12. SUGGESTIONS :

Based on this study, we have the following suggestions.
1. Managed Kubernetes service provides essential security for Secrets by default using disk encryption
2. For critical Secrets, cloud users shall enable Envelope encryption to enhance the Secret encryption levels
3. Cost estimation of using the Envelope encryption shall be done to balance the security and asset value of the Secrets

## 13. SUMMARY AND CONCLUSION :

Managed Kubernetes services help organizations to deploy their micro service applications in the cloud without managing the data center infrastructure. The service providers have implemented different security features to protect the confidentiality of the application's Secrets. Additional features to support the Key management service of different cloud service providers would help re-use Secrets across the cloud. Overall, the current Secret management in managed Kubernetes services across vendors is sufficiently secure. It provides confidence for cloud users to deploy applications that use sensitive data to communicate with external services. Documentation in the cloud provider websites is comprehensive and helps the cloud administrators to configure the cloud with minimal effort.

## REFERENCES :

[1] Larrucea, X., Santamaria, I., Colomo-Palacios, R., & Ebert, C. (2018). Microservices. *IEEE Software*, *35*(3), 96-100. Google Scholar↗ CrossRef/DOI↗

[2] The Twelve Factors. https://12factor.net/. Accessed on on 15-Dec-2022.

[3] Dua, R., Raja, A. R., & Kakadia, D. (2014). Virtualization vs containerization to support paas. *IEEE International Conference on Cloud Engineering*, 610-614. Google Scholar↗ CrossRef/DOI↗

[4] Vayghan, L. A., Saied, M. A., Toeroe, M., & Khendek, F. (2018). Deploying microservice based applications with kubernetes: Experiments and lessons learned. *IEEE 11th international conference on cloud computing*, 970-973. Google Scholar↗ CrossRef/DOI↗

[5] Kubernetes project. https://www.cncf.io/projects/kubernetes/ . Accessed on 15-Dec-2022.

[6] Hardikar, S., Ahirwar, P., & Rajan, S. (2021). Containerization: Cloud Computing based Inspiration Technology for Adoption through Docker and Kubernetes. *Second International*

*Conference on Electronics and Sustainable Communication Systems (ICESC)*, 1996-2003. Google Scholar↗ CrossRef/DOI↗

[7] Trihinas, D., Tryfonos, A., Dikaiakos, M. D., & Pallis, G. (2018). Devops as a service: Pushing the boundaries of microservice adoption. *IEEE Internet Computing, 22*(3), 65-71. Google Scholar↗ CrossRef/DOI↗

[8] Shah, J., & Dubaria, D. (2019). Building modern clouds: using docker, kubernetes & Google cloud platform. *IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* 184-189. Google Scholar↗ CrossRef/DOI↗

[9] Using AWS Secrets Manager with Kubernetes, https://www.theseus.fi/bitstream/handle/10024/511401/Jurvanen_Karl-Juhan.pdf?sequence=3 , Accessed on 15-Dec-2022.

[10] Secrets Management in a Multi-Cloud Kubernetes Environment, https://www.utupub.fi/bitstream/handle/10024/151776/Secrets_Management_in_a_Multi_Cloud_Kubernetes_Environment_pdf-a.pdf?sequence=1 , Accessed on 15-Dec-2022.

[11] Shamim, M. S. I., Bhuiyan, F. A., & Rahman, A. (2020). Xi commandments of kubernetes security: A systematization of knowledge related to kubernetes security practices. *IEEE Secure Development*, *1* (1), 58-64. Google Scholar↗ CrossRef/DOI↗

[12] Gokhale, S., Poosarla, R., Tikar, S., Gunjawate, S., Hajare, A., Deshpande, S., Gupta, S., & Karve, K. (2021). Creating Helm Charts to ease deployment of Enterprise Application and its related Services in Kubernetes. *International Conference on Computing, Communication and Green Engineering (CCGE)*, 1-5. Google Scholar↗ CrossRef/DOI↗

[13] Ferreira, A. P., & Sinnott, R. (2019). A performance evaluation of containers running on managed kubernetes services. *IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 199-208. Google Scholar↗ CrossRef/DOI↗

[14] Buchanan, S., Rangama, J., & Bellavance, N. (2020). Operating Azure Kubernetes Service. *Introducing Azure Kubernetes Service*, *1*(1), 101-149. Google Scholar↗ CrossRef/DOI↗

[15] Testing the Security of a Kubernetes Cluster in a Production Environment, https://www.diva-portal.org/smash/get/diva2:1700029/FULLTEXT01.pdf, Accessed on 15-Dec-2022.

[16] Malviya, A., & Dwivedi, R. K. (2022). A Comparative Analysis of Container Orchestration Tools in Cloud Computing. *9th International Conference on Computing for Sustainable Global Development (INDIACom)*, 698-703. Google Scholar↗ CrossRef/DOI↗

[17] Opara, E., Wimmer, H., & Rebman, C. M. (2022). Auto-ML Cyber Security Data Analysis Using Google, Azure and IBM Cloud Platforms. *International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1-10. Google Scholar↗ CrossRef/DOI↗

[18] Amazon EKS – Now Generally Available, https://aws.amazon.com/blogs/aws/amazon-eks-now-generally-available/, Accessed on 15-Dec-2022.

[19] Azure Kubernetes Service (AKS) GA – New regions, more features, increased productivity, https://azure.microsoft.com/en-in/blog/azure-kubernetes-service-aks-ga-new-regions-new-features-new-productivity/, Accessed on 15-Dec-2022.

[20] Kubernetes Release, https://cloud.google.com/kubernetes-engine/docs/release-notes-archive#november_4_2014, Accessed on 15-Dec-2022.

[21] IBM Cloud Container Service is now IBM Cloud Kubernetes Service, https://www.ibm.com/cloud/blog/announcements/ibm-cloud-container-service-now-ibm-cloud-kubernetes-service, Accessed on 15-Dec-2022.

[22] Oracle Container Engine for Kubernetes, https://docs.oracle.com/en-us/iaas/releasenotes/changes/6f1aeeb9-3adb-4e2f-a88e-9960790a94f4/, Accessed on 15-Dec-2022.

[23] Demystifying Kubernetes as a service – How Alibaba cloud manages 10,000s of Kubernetes clusters, https://www.cncf.io/blog/2019/12/12/demystifying-kubernetes-as-a-service-how-does-alibaba-cloud-manage-10000s-of-kubernetes-clusters/, Accessed on 15-Dec-2022.

[24] 10 trends in real world container use, https://www.datadoghq.com/container-report-2021/, Accessed on 15-Dec-2022.

[25] Secrets, https://kubernetes.io/docs/concepts/configuration/secret/, Accessed on 15-Dec-2022.

[26] Encrypting Secret Data at Rest, https://kubernetes.io/docs/tasks/administer-cluster/encrypt-data/, Accessed on 15-Dec-2022.

[27] Amazon EKS clusters, https://docs.aws.amazon.com/en_us/eks/latest/userguide/clusters.html, Accessed on 15-Dec-2022.

[28] Security concepts for applications and clusters in Azure Kubernetes Service (AKS), https://learn.microsoft.com/en-us/azure/aks/concepts-security, Accessed on 15-Dec-2022.

[29] Default encryption at rest, https://cloud.google.com/docs/security/encryption/default-encryption, Accessed on 15-Dec-2022.

[30] Protecting sensitive information in your cluster, https://cloud.ibm.com/docs/containers?topic=containers-encryption#encrypt_ov, Accessed on 15-Dec-2022.

[31] Encrypting Kubernetes Secrets at Rest in Etcd, https://docs.oracle.com/en-us/iaas/Content/ContEng/Tasks/contengencryptingdata.htm, Accessed on 15-Dec-2022.

[32] Use KMS to encrypt Kubernetes Secrets, https://www.alibabacloud.com/help/en/container-service-for-kubernetes/latest/professional-kubernetes-clusters-use-kms-to-encrypt-kubernetes-secrets, Accessed on 15-Dec-2022.

[33] Encrypting Secret Data at Rest, https://kubernetes.io/docs/tasks/administer-cluster/encrypt-data/, Accessed on 15-Dec-2022.

[34] Using EKS encryption provider support for defense-in-depth, https://aws.amazon.com/blogs/containers/using-eks-encryption-provider-support-for-defense-in-depth/, Accessed on 15-Dec-2022.

[35] Using a KMS provider for data encryption, https://kubernetes.io/docs/tasks/administer-cluster/kms-provider/, Accessed on 15-Dec-2022.

[36] Add Key Management Service (KMS) etcd encryption to an Azure Kubernetes Service (AKS) cluster, https://learn.microsoft.com/en-us/azure/aks/use-kms-etcd-encryption, Accessed on 15-Dec-2022.

[37] Integrate Key Vault with Azure Private Link, https://learn.microsoft.com/en-us/azure/key-vault/general/private-link-service?tabs=portal, Accessed on 15-Dec-2022.

[38] Envelope encryption, https://cloud.google.com/kubernetes-engine/docs/how-to/encrypting-secrets#envelope_encryption, Accessed on 15-Dec-2022.

[39] Use AWS Secrets Manager secrets in Amazon Elastic Kubernetes Service, https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_csi_driver.html, Accessed on 15-Dec-2022.

[40] Secrets encryption at application layer, https://cloud.google.com/kubernetes-engine/docs/how-to/encrypting-secrets#limitations, Accessed on 15-Dec-2022.

[41] Key Management Services, https://cloud.ibm.com/docs/containers?topic=containers-encryption#kms, Accessed on 15-Dec-2022.

[42] Overview of Vault in Oracle Cloud Infrastructure, https://docs.oracle.com/en-us/iaas/Content/KeyManagement/Concepts/keyoverview.htm, Accessed on 15-Dec-2022.

[43] Creating Secrets in Alibaba Cloud, https://www.alibabacloud.com/help/en/key-management-service/latest/create-a-secret, Accessed on 15-Dec-2022.

[44] Managing allowed IP settings, https://cloud.ibm.com/docs/key-protect?topic=key-protect-manage-allowed-ip#manage-allowed-ip-instance-policy, Accessed on 15-Dec-2022.

[45] Aithal, P. S., & Kumar, P. M. (2015). Applying SWOC analysis to an institution of higher education. *International Journal of Management, IT and Engineering*, *5*(7), 231-247. Google Scholar↗ CrossRef/DOI↗

[46] Aithal, P. S. (2017). Industry Analysis– The First Step in Business Management Scholarly Research. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, *1*(1), 1-13. Google Scholar↗ CrossRef/DOI↗

[47] Priyadarshini, P., & Veeramanju, K. T., (2022). A Systematic Review of Cloud Storage Services-A Case Study on Amazon Web Services. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, *6*(2), 124-140. CrossRef/DOI↗

*******