https://dx.doi.org/10.22161/ijaers.ncitsa.2025.24 ISSN: 2349-6495(P) | 2456-1908(O)

Deploying Docker-based EaaS in Kubernetes

Ms. Rama Bhardwaj[1] , Neha Khandelwal[2], Parth Chittora[3]

[1]Assistant Professor Department of Information Technology, Jaipur Engineering College & Research Centre, Jaipur
[2] Student Department of Information Technology, Jaipur Engineering College & Research Centre, Jaipur
Email:parthchittora.it25@gmail.com
[3]Student Department of Information Technology, Jaipur Engineering College & Research Centre, Jaipur
Email:nehakhandelwal.it25@gmail.com

Abstract— Modern networking frameworks like Kubernetes have advanced "as-a-service" models, including encryption. This paper presents an Encryption as a Service (EaaS) platform deployed on Kubernetes, featuring a Django-based web application for managing subscriptions and token-based encryption services. Clients use these tokens to perform secure data operations. The deployment includes essential services such as Nginx and a database, all containerized using Docker. Steps for building Docker images and configuring deployments are detailed, with testing conducted on local Minikube clusters and remote Kubernetes clusters via VPN. This work offers practical insights into building and simulating encryption services in scalable, real-world environments using Kubernetes, guiding researchers and developers aiming to implement secure, efficient cloud-native encryption platforms.
Keywords—Docker, Encryption as a Service, IoT, Kubernetes, NGINX

I. INTRODUCTION

The increasing adoption of scalable networking frameworks, such as Kubernetes, has significantly amplified the demand for secure and efficient encryption solutions, particularly in domains like the Internet of Things (IoT). Despite advancements in orchestration and containerization technologies, implementing Encryption as a Service (EaaS) remains a complex challenge. Developers and researchers often face difficulties in achieving seamless deployment, ensuring high service availability, and enabling secure communication between clients and service providers. These challenges are further complicated by the need to integrate essential components such as databases, load balancers, and web servers into the encryption framework.

Deploying Django-based applications on Kubernetes introduces additional complexities, especially in configuring supporting services like Nginx and databases to work together reliably. Docker-based containerization demands careful optimization for performance, scalability, and fault tolerance. Moreover, the deployment of such systems across both local (Minikube) and remote (VPN-connected) Kubernetes clusters adds another layer of difficulty in validating accuracy, availability, and responsiveness of encryption services.

Previous studies have explored encryption services using virtual machines and monolithic deployments, which often lack flexibility and scalability. Some approaches have utilized containerized architectures, but few have addressed the integration of Django-based web platforms with Kubernetes for encryption services. The need for a lightweight, scalable, and secure EaaS framework that can adapt to varied deployment environments remains largely unmet.

The purpose of this study is to design, implement, and evaluate an Encryption as a Service (EaaS) framework deployed on Kubernetes. The proposed system features a Django-based web application that manages user subscriptions and provides token-based access to encryption and decryption services. Supporting components such as Nginx and PostgreSQL are containerized using Docker and orchestrated within Kubernetes environments.

This research provides:

- A step-by-step guide to containerizing and deploying Django applications with encryption services
- Insights into building a modular and secure EaaS framework

https://dx.doi.org/10.22161/ijaers.ncitsa.2025.24 ISSN: 2349-6495(P) | 2456-1908(O)

- Performance evaluations in both local (Minikube) and remote (VPN-based) testbed deployments
- Practical solutions to common challenges in deploying real-world encryption services

II. EaaS IN MODERN CLOUD ARCHITECTURE

EaaS is vital in modern cloud architectures, securing data in transit and at rest across distributed systems like Kubernetes. It supports scalable, on-demand encryption for digital transactions, cloud storage, and communications. Benefits include dynamic scalability, reduced infrastructure costs, high availability through orchestration, and robust disaster recovery. Integrated with cloud-native tools, EaaS enhances data protection, operational resilience, and performance across sectors like finance, healthcare, and enterprise IT.

It also facilitates secure IoT deployments, protects sensitive workloads in hybrid and multi-cloud environments, and supports regulatory compliance. As cloud ecosystems grow, EaaS offers a modular, easily deployable solution that adapts to evolving security requirements and industry-specific needs.

III. CHALLENGES AND ETHICAL CONSIDERATIONS

Deploying EaaS on Kubernetes poses several challenges. Complex configuration of interdependent services like Django, Nginx, and PostgreSQL demands careful orchestration, environment setup, and domain expertise. Containerization introduces scalability, performance, and encryption efficiency hurdles, requiring precise tuning of Dockerfiles, environment variables, and Kubernetes clusters. Managing secure inter-service communication, persistent storage, and secrets handling further complicates deployment. Ensuring reliability across varied environments—local and remote—adds additional layers of complexity, with persistent issues in networking, resource limits, version control, and service consistency necessitating rigorous integration testing, observability improvements, and continuous performance monitoring.

IV. FUTURE PROSPECTS

While the current EaaS framework has demonstrated robust functionality, future work will emphasize production readiness and enhanced security. Key priorities include implementing advanced monitoring with real-time alerts, integrating honeypots for threat analysis, and adopting stronger authentication methods. Techniques like Moving Target Defense and virtual network embedding with machine learning will also be explored to optimize security and resource allocation. These efforts aim to elevate the framework's resilience, scalability, and applicability across industries requiring secure, cloud-native solutions.

V. CONCLUSION

This work presents the deployment of an Encryption as a Service (EaaS) framework on Kubernetes, demonstrating advantages in scalability, modularity, and secure communication—especially for IoT applications. Integration of Django, PostgreSQL, and Nginx within containerized environments showcased reliable performance during local testing. However, limitations remain in security and observability, with current tools suitable only for early-stage deployment. Future enhancements will target improved monitoring, real-time alerting, stronger authentication, and compliance with data protection laws. These advancements will broaden the framework’s applicability across security-critical domains and support its transition to production environments.

ACKNOWLEDGEMENTS

The author acknowledges the contributions of various open-source research initiatives and academic discussions that shaped the understanding of the EaaS presented in this paper. These resources provided valuable insights into containerization, cloud security practices, Kubernetes orchestration, and encryption frameworks. The collaborative nature of the open-source and academic communities continues to inspire future enhancements and innovation in secure cloud-native solutions.

https://dx.doi.org/10.22161/ijaers.ncitsa.2025.24 ISSN: 2349-6495(P) | 2456-1908(O)

REFERENCES

[1] Javadpour, A., Ja'fari, F., Taleb, T., Zhao, Y., Bin, Y., and Benzaid, C., Encryption as a Service for IoT: Opportunities, Challenges, and Solutions, IEEE Internet of Things Journal, 2023.

[2] Zhang, M., Cao, J., Sahni, Y., Chen, Q., Jiang, S., and Wu, T., EaaS: A Service-Oriented Edge Computing Framework Towards Distributed Intelligence, IEEE International Conference on Service-Oriented System Engineering (SOSE), 2022.

[3] Taleb, T., Boudi, A., Rosa, L., Cordeiro, L., Theodoropoulos, T., Tserpes, K., Dazzi, P., Protopsaltis, A.I., and Li, R., Toward Supporting XR Services: Architecture and Enablers, IEEE Internet of Things Journal, 2022.

[4] Benmerar, T.Z., Theodoropoulos, T., Fevereiro, D., Rosa, L., Rodrigues, J., Taleb, T., Barone, P., Tserpes, K., and Cordeiro, L., Intelligent Multi-Domain Edge Orchestration for Highly Distributed Immersive Services: An Immersive Virtual Touring Use Case, IEEE International Conference on Edge Computing and Communications (EDGE), 2023.

[5] Javadpour, A., Ja'fari, F., Taleb, T., and Benzaid, C., Enhancing 5G Network Slicing: Slice Isolation via Actor-Critic Reinforcement Learning with Optimal Graph Features, IEEE Global Communications Conference (GLOBECOM), 2023.