Project Report on

Secure Web System Architecture With DevOps Integration

Submitted by

Damini Dhenge (250244223015)
Priyanka Gotkhinde (250244223016)
Neha Pakhare (250244223036)
Vandana Shinde (250244223055)

Under the guidance of

Mr. Sandeep Walvekar

In partial fulfillment of the award of Post Graduate Diploma in

IT Infrastructure, Systems and Security

(PG-DITISS)

Sunbeam Institute of Information Technology,

Pune (Maharashtra)

PG-DITISS -2025

DECLARATION

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed**.**

Place: Pune

Date:

Damini Dhenge	**Priyanka Gotkhinde**	**Neha Pakhare**	**Vandana Shinde**
(250244223015)	**(250244223016)**	**(250244223036)**	**(250244223055)**

CERTIFICATE

This is to certify that the project report entitled **"Secure Web System Architecture With DevOps Integration"**, submitted by **Damini Dhenge** is the Bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Mr. Sandeep Walvekar
Guide

Mr. Vishal Salunkhe
Course Coordinator

Mr. Nitin Kudale

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

CERTIFICATE

This is to certify that the project report entitled **"Secure Web System Architecture With DevOps Integration"**, submitted by **Priyanka Gotkhinde** is the Bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Mr. Sandeep Walvekar

Guide

Mr. Vishal Salunkhe

Course Coordinator

Mr. Nitin Kudale

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

CERTIFICATE

This is to certify that the project report entitled **"Secure Web System Architecture With DevOps Integration"**, submitted by **Neha Pakhare** is the Bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Mr. Sandeep Walvekar

Guide

Mr. Vishal Salunkhe

Course Coordinator

Mr. Nitin Kudale

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

CERTIFICATE

This is to certify that the project report entitled **"Secure Web System Architecture With DevOps Integration"**, submitted by **Vandana Shinde** is the Bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Mr. Sandeep Walvekar

Guide

Mr. Vishal Salunkhe

Course Coordinator

Mr. Nitin Kudale

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

APPROVAL CERTIFICATE

This Project II report entitled **"Secure Web System Architecture With DevOps Integration"** by **Damini Dhenge (250244223015)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner: _____

(Signature)

_____

(Name)

APPROVAL CERTIFICATE

This Project II report entitled **"Secure Web System Architecture With DevOps Integration "** by **Priyanka Gotkhinde (250244223016)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner: _____

(Signature)

_____

(Name)

APPROVAL CERTIFICATE

This Project II report entitled **"Secure Web System Architecture With DevOps Integration"** by **Neha Pakhare (25024422303)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner: _____

(Signature)

_____

(Name)

APPROVAL CERTIFICATE

This Project II report entitled **"Secure Web System Architecture With DevOps Integratio"** by **Vandana Shinde (250244223055)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner: _____

(Signature) _____

(Name)

CONTENTS

ABSTRACT

In the modern era of cloud-native applications, ensuring automation, scalability, and security is critical to delivering reliable web services. This project focuses on designing and implementing a secure and automated web system by integrating DevOps practices with container orchestration, real-time monitoring, threat detection, and alert management.

The core of the architecture leverages Kubernetes as the orchestration platform, enabling automated deployment, scaling, and management of containerized web applications. Jenkins pipelines are used to implement Continuous Integration and Continuous Deployment (CI/CD), ensuring efficient, automated testing and delivery workflows.

To strengthen the system's security, a De-Militarized Zone (DMZ) network architecture is implemented, creating an isolated buffer zone between the internal infrastructure and external access. An advanced Intrusion Detection and Prevention System (IDS/IPS) using Suricata is deployed to actively monitor and block malicious traffic.

The project integrates the Wazuh Security Information and Event Management (SIEM) platform to provide comprehensive threat detection, log analysis, and security event correlation. Real-time system monitoring and visualization are achieved using Prometheus for metrics collection and Grafana for graphical dashboards and alerting.

Additionally, a Mail Server is configured to send automated security alerts and notifications, while centralized logging and backup mechanisms are established to ensure data integrity, reliability, and quick recovery during incidents.

By combining container orchestration, automated CI/CD pipelines, layered security defenses, and real-time monitoring, this project delivers a resilient, secure, and maintainable infrastructure for modern web application deployment.

1. INTRODUCTION

In the ever-evolving landscape of web technologies, deploying, managing, and securing web applications has grown increasingly complex. To meet modern demands for scalability, automation, and security, organizations are shifting toward cloud-native architectures integrated with DevOps practices and advanced monitoring solutions. This project presents a secure and automated web system architecture that leverages container orchestration, CI/CD pipelines, and a layered security approach to efficiently host, manage, and protect a web application environment.

At the core of this architecture is Kubernetes, used for orchestrating containerized applications to ensure high availability, scalability, and self-healing capabilities. The deployment pipeline is automated using Jenkins, implementing Continuous Integration and Continuous Delivery (CI/CD) for fast and reliable code updates without human intervention.

To strengthen the system's defenses, a DMZ (Demilitarized Zone) is configured to isolate the internal network from external threats. The deployment also integrates Suricata, a powerful Intrusion Detection and Prevention System (IDS/IPS), for real-time inspection and blocking of malicious traffic.

For centralized threat detection and log analysis, Wazuh SIEM is incorporated, enabling administrators to monitor security events and compliance metrics across the infrastructure. Prometheus and Grafana are employed for system health monitoring and real-time visualization of performance metrics, offering insights into server load, resource usage, and network behavior.

An alerting system is established using a configured mail server, which notifies administrators of critical issues or intrusions. In addition, centralized logging and regular backups are implemented to ensure data integrity, quick recovery, and audit readiness.

To demonstrate this architecture in action, the project uses a simple Flask-based web application connected to a MariaDB backend. This application is deployed within Kubernetes and managed through the Jenkins CI/CD pipeline. The system is actively monitored and protected using the integrated tools, ensuring high performance, availability, and security

1.1 Applications

- E-Commerce Platforms: Online stores and e-commerce platforms require reliable web server deployments to handle high traffic loads, ensure seamless user experiences, and protect sensitive customer data.

- Finance and Banking Systems: In the finance sector, security and performance are critical. Web server deployment with CI/CD ensures that updates to financial applications are rigorously tested and deployed smoothly.

- Gaming and Entertainment Platforms: Online gaming and entertainment platforms need scalable web server deployments to handle sudden surges in user activity. CI/CD enables game updates and feature releases without disrupting user experiences. Nagios monitoring guarantees the availability of gaming services, while the Snort IDS safeguards against cheating and hacking attempts.

1.2 Project Plan

Table: Activities Details

Sr. No.	ACTIVITY	WEEK			
		1	2	3	4
1	Project group formation				
2	Project work to be started in respective labs				
3	First review with PPT presentation				
4	Design Use-Case view as per project				
5	Design Block diagram as per project				
6	Second review with PPT presentation				
7	Selection				
8	Final review with PPT presentation				
9	Implementation coding as per project				
10	Testing, Troubleshooting with different techniques				
11	Created Soft copy of project and then final hardcopy				

2. LITERATURESURVEY

Paper 1: A Qualitative Study of DevOps Usage in Practice

Authors: Floris Erich, C. Amrit & M. Donevan

This paper discusses how organizations apply DevOps principles to accelerate software delivery while maintaining quality. Through a literature review and interviews with six organizations, the study finds that adopting DevOps helps improve deployment speed, team collaboration, and system stability. Most organizations reported positive outcomes with only minor challenges during implementation.

Relation to Project:

This project applies DevOps practices by integrating Jenkins for continuous integration and delivery and Kubernetes for automated orchestration. These tools align directly with the practices discussed in the paper and support the project's goal of achieving fast, automated, and reliable application deployments.

Paper 2: DevOps – A New Approach to Cloud Development & Testing

Author: Dhaya Sindhu Battina

This study explores the merging of DevOps and cloud computing, emphasizing the role of automation in developing and deploying scalable cloud-native applications. It outlines how DevOps accelerates development in cloud environments by enabling continuous testing, delivery, and infrastructure-as-code.

Relation to Project:

Our project implements a cloud-ready architecture using Kubernetes clusters, CI/CD via Jenkins, and infrastructure automation. The insights from this paper reinforce the benefits of automating workflows and explain why DevOps is essential for maintaining agility and performance in modern cloud deployments.

Relation to Project:

Although Snort is mentioned, our project uses Suricata, a high-performance IDS/IPS tool with similar functionality. It provides real-time network traffic analysis and intrusion prevention. Combined with Wazuh

Paper 3: Review Paper on Suricata and Its Applications in Network Security

Authors: Adapted from community and research contributions around Suricata.

This paper presents a comprehensive review of Suricata, a high-performance Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Network Security Monitoring (NSM) engine developed by the Open Information Security Foundation (OISF). It discusses how Suricata operates with multi-threading capabilities, supports various protocols (HTTP, TLS, FTP, SMB, etc.), and offers deep packet inspection and file extraction.

SIEM and a DMZ network setup, our project implements a layered security approach as inspired by the concepts reviewed in this paper.The system is designed to provide a **secure, automated, and highly observable web infrastructure** by integrating modern DevOps and cybersecurity tools. The design focuses on scalability, reliability, and proactive threat detection and response.

2.1 Overall Architecture

The project follows a **modular microservices architecture** hosted on a Kubernetes cluster to manage containerized services efficiently. Each component of the system performs a distinct function and communicates over a secured network.

2.2 Key Components

a. Kubernetes Orchestration

- Used as the core platform to deploy and manage containers.
- Supports **auto-scaling**, **load balancing**, and **self-healing** of services.
- Ensures isolated and secure service environments.

b. Jenkins CI/CD Pipeline

- Automates the **build, test, and deployment** process.
- Integrates with GitHub for continuous integration.

- Ensures consistent and error-free deployments across environments.

c. DMZ Network Layer

- A **Demilitarized Zone (DMZ)** is implemented to isolate external-facing services (like the web server) from the internal network.
- Adds an **extra layer of security** between the internet and critical internal resources.

d. Suricata IDS/IPS

- Acts as an **Intrusion Detection and Prevention System**.
- Monitors network traffic and blocks or alerts on suspicious behavior.
- Deployed at the network boundary for real-time threat detection.

e. Wazuh SIEM

- Integrated as a **Security Information and Event Management (SIEM)** system.
- Collects logs from all critical services including Suricata, Jenkins, Kubernetes, and the OS.
- Performs **log analysis, threat detection**, and **compliance monitoring**.

f. Prometheus and Grafana

- Prometheus collects system and application **metrics**.
- Grafana visualizes these metrics through **real-time dashboards**.
- Alerts are configured to notify on performance degradation or suspicious system behavior.

g. Mail Server

- Configured to send **alert notifications** to system administrators.
- Supports **SMTP-based email delivery** of system logs and alerts.

3. SYSTEM DEVELOPMENT AND DESIGN

3.1 Proposed System

The system is designed to provide a **secure, automated, and highly observable web infrastructure** by integrating modern DevOps and cybersecurity tools. The design focuses on scalability, reliability, and proactive threat detection and response.

3.2 Overall Architecture

The project follows a **modular microservices architecture** hosted on a Kubernetes cluster to manage containerized services efficiently. Each component of the system performs a distinct function and communicates over a secured network.

3.3 Key Components

a. Kubernetes Orchestration

- Used as the core platform to deploy and manage containers.
- Supports **auto-scaling**, **load balancing**, and **self-healing** of services.
- Ensures isolated and secure service environments.

b. Jenkins CI/CD Pipeline

- Automates the **build, test, and deployment** process.
- Integrates with GitHub for continuous integration.
- Ensures consistent and error-free deployments across environments.

c. DMZ Network Layer

- A **Demilitarized Zone (DMZ)** is implemented to isolate external-facing services (like the web server) from the internal network.
- Adds an **extra layer of security** between the internet and critical internal resources.

d. Suricata IDS/IPS

- Acts as an **Intrusion Detection and Prevention System**.
- Monitors network traffic and blocks or alerts on suspicious behavior.
- Deployed at the network boundary for real-time threat detection.

e. Wazuh SIEM

- Integrated as a **Security Information and Event Management (SIEM)** system.
- Collects logs from all critical services including Suricata, Jenkins, Kubernetes, and the OS.
- Performs **log analysis, threat detection**, and **compliance monitoring**.

f. Prometheus and Grafana

- Prometheus collects system and application **metrics**.
- Grafana visualizes these metrics through **real-time dashboards**.
- Alerts are configured to notify on performance degradation or suspicious system behaviour.

g. Mail Server

- Configured to send **alert notifications** to system administrators.
- Supports **SMTP-based email delivery** of system logs and alerts.

h. Backup and Logging

- Centralized logging is maintained using Wazuh and Prometheus.
- A backup mechanism is configured to ensure **data resilience and recovery** in case of failure.

3.4Flow chart

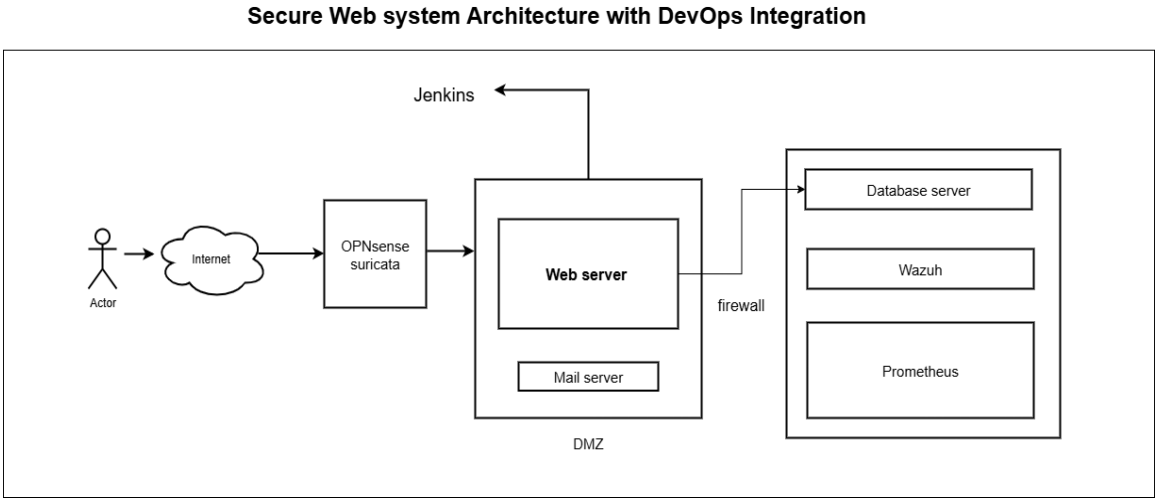


Figure: Flowchart

3.5 Technology used

3.5.1Git

Git is a distributed version control system (VCS) designed to manage source code history and facilitate collaborative software development.

Key features of Git:

Distributed Architecture: Unlike centralized version control systems, Git is distributed. Each developer has a complete copy of the repository, including its entire history. This allows for offline work, faster operations, and improved resilience.

Branching and Merging: Git makes it easy to create branches, which are separate lines of development. Developers can work on features, bug fixes, or experiments in their own branches without affecting the main codebase. Merging branches back together is relatively simple and allows for collaborative development.

Commit History: Git maintains a detailed history of changes to the codebase. Each change is represented by a commit, which includes information about who made the change, when it was made, and what was changed. This commit history provides a clear view of the evolution of the project.

Fast and Efficient: Git is designed for speed and efficiency. Most operations are local, as the repository resides on the developer's machine. This results in rapid commits, branching, and merging.

Collaboration: Git enables effective collaboration among developers. Multiple developers can work on different branches simultaneously, and changes can be shared

by pushing them to a remote repository. Pull requests or merge requests facilitate the process of reviewing and integrating changes from different contributors.

3.5.2 Web Server (Flask Application)

A web server is deployed using the Flask framework to provide a lightweight and flexible front-end for user interaction and data visualization.

Key features of the Web Server include:

- **Lightweight Framework:** Built with Flask, a micro web framework in Python known for its simplicity and speed.
- **REST API Support:** Offers secure endpoints to interact with backend services and databases.
- **Alert Integration:** Displays real-time security events and alerts fetched from Wazuh , Prometheus, and other monitoring tools.
- **User Authentication:** Basic login system implemented to restrict unauthorized access to sensitive dashboards.
- **Modular Design:** Easy to scale and integrate with future security components.

3.5.3 Database Server (MariaDB)

MariaDB is used as the relational database management system to store logs, alert data, configuration settings, and audit trails.

Key features of the Database Server include:

- **SQL-Based Storage:** Supports efficient querying of structured data including logs and system events.
- **Secure Connections:** Database access is restricted using credentials and IP-based filtering.
- **Data Retention Policies:** Implements data aging and archival strategies to optimize storage.
- **Integration Ready:** Works seamlessly with Flask, Jenkins, Wazuh, and Alert manager for data storage and retrieval.

- **Backup and Restore:** Periodic backups ensure data availability and integrity in case of system failure.

3.5.4 Kubernetes (Container Orchestration)

Kubernetes is an open-source platform designed to automate the deployment, scaling, and operation of application containers.

Key features of Kubernetes include:

- **Automated Rollouts and Rollbacks:** Supports controlled deployment of updates and automatic rollback in case of failures.
- **Self-Healing:** Automatically restarts failed containers, replaces dead nodes, and reschedules workloads.
- **Service Discovery and Load Balancing:** Exposes applications via stable network endpoints and balances traffic between pods.
- **Horizontal Scaling:** Automatically scales applications up or down based on load or resource usage.
- **Namespace Isolation:** Segregates environments and improves security by isolating workloads.

3.5.5Jenkins

Jenkins is an open-source automation server that facilitates the continuous integration and continuous delivery (CI/CD) of software projects. It helps automate various tasks related to building, testing, and deploying applications, making the development and release process more efficient and reliable.

Key features of Jenkins:

Continuous Integration: Jenkins automates the process of integrating code changes from multiple contributors into a shared repository. It triggers builds whenever code is committed, allowing developers to identify and fix integration issues early.

Automated Builds: Jenkins can automatically build projects from source code repositories. It supports various build tools, languages, and platforms, making it versatile for different types of projects.

Extensibility: Jenkins can be extended through a wide range of plugins that provide additional functionalities. Plugins are available for source code management, build tools, testing frameworks, and deployment options.

Pipeline as Code: Jenkins uses a domain-specific language called Groovy to define build pipelines as code. This enables you to define complex workflows that include build, test, and deployment stages in a version-controlled script.

Continuous Delivery: Jenkins supports continuous delivery by automating the deployment process after successful builds. It can deploy applications to different environments, such as development, staging, and production.

Distributed Builds: Jenkins can distribute builds across multiple machines, allowing for parallel builds and improved build performance. This is particularly useful for large and resource-intensive projects.

3.5.6 Prometheus (Monitoring & Metrics Collection)

Prometheus is an open-source monitoring and alerting toolkit used to collect real-time metrics from services and infrastructure.

Key features of Prometheus include:

- **Time-Series Data Collection:** Captures time-series data through exporters or custom instrumentation.

- **Alert manager Integration:** Sends alerts to communication platforms (like email or Slack) when specific conditions are met.
- **Powerful Query Language (PromQL):** Enables deep data analysis and metric queries.
- **Lightweight and Scalable:** Can run in containerized environments and scale with Kubernetes.
- **Integration with Grafana:** Works seamlessly with Grafana for advanced visualization

3.5.7 Grafana (Dashboard & Visualization)

Grafana is a popular open-source analytics and visualization platform. It is used in this project to visualize data collected from Prometheus and Wazuh.

Key features of Grafana include:

- **Custom Dashboards:** Create interactive dashboards to monitor system performance, resource utilization, and application health.
- **Real-Time Visualization:** Displays real-time data with flexible charting and graphing tools.
- **Multi-Source Support:** Integrates with various data sources like Prometheus, Elasticsearch, Wazuh, etc.
- **Alerting System:** Allows setting threshold-based alerts that trigger notifications on system anomalies.
- **User Access Management:** Supports access control for multi-user environments.

3.5.8 Wazuh (SIEM Platform)

Wazuh is an open-source Security Information and Event Management (SIEM) tool used for log analysis, intrusion detection, file integrity monitoring, and compliance reporting.

Key features of Wazuh include:

- **Log Collection and Analysis:** Collects logs from endpoints, Suricata, Jenkins, and other tools; parses and analyzes them for threats.

- **Intrusion Detection:** Detects malicious activities through rules and behavior-based detection techniques.
- **File Integrity Monitoring (FIM):** Monitors changes to important files to detect unauthorized modifications.
- **Security Alerts and Notifications:** Sends alerts for suspicious activities, login anomalies, and system vulnerabilities.
- **Integration with Elasticsearch and Kibana:** Provides powerful search and visualization capabilities.

3.5.9 Suricata (IDS/IPS)

Suricata is an open-source, high-performance Intrusion Detection and Prevention System (IDS/IPS) designed for deep packet inspection and real-time network threat detection. It is used in this project to secure the system from malicious activities and ensure robust network-level defense.

Key features of Suricata include:

- **Real-Time Intrusion Detection and Prevention:** Suricata inspects packets and applies signature-based detection to identify known threats.
- **Protocol Awareness:** Understands and analyzes protocols like HTTP, DNS, TLS, FTP, and SMB for detecting protocol-specific threats.
- **Multi-threading:** Offers high performance through parallel processing, making it scalable for modern high-speed networks.
- **Alert and Log Generation:** Generates detailed alerts and logs for security events, which are later forwarded to SIEM for analysis.
- **File Extraction and MD5 Checks:** Allows extraction of files from network traffic and checks file integrity using hashes.

3.3.12 Mail Server (Alert Notification)

A mail server is configured in the system to ensure timely delivery of alerts and system notifications to administrators.

Key features of Mail Server include:

- **SMTP Configuration:** Supports sending emails over a secured channel using SMTP protocols.
- **Alert Forwarding:** Integrates with Wazuh, Suricata, Prometheus Alert manager, and Jenkins to send alert emails.
- **Custom Alert Rules:** Alerts are filtered and routed based on severity or event type.
- **Reliable Delivery:** Ensures alerts reach designated recipients promptly for quick action.

3.5.10 OpenSence

3.5.9 OPNSence (Open-Source Firewall & Routing Platform)

OPNsense is an open-source, FreeBSD-based firewall and routing platform that provides enterprise-grade security features for network protection, monitoring, and traffic management. It is often used for perimeter defense, VPN services, and network segmentation.

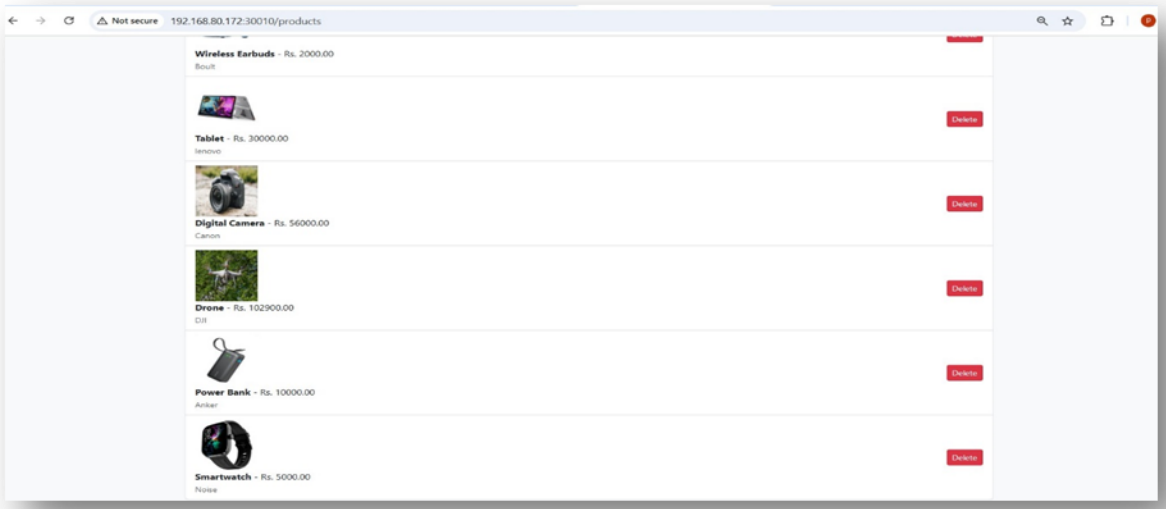
Key features of OPNsense include:

- **Firewall & Traffic Filtering:** Uses stateful packet inspection (SPI) and customizable rules to control inbound and outbound network traffic.
- **VPN Support:** Offers IPsec, OpenVPN, and WireGuard for secure remote connections and site-to-site VPNs.
- **Intrusion Detection & Prevention (IDS/IPS):** Integrates with Suricata to detect and block malicious traffic in real time.
- **Web Proxy & Content Filtering:** Supports Squid and category-based filtering to control web access and block harmful websites.
- **High Availability & Failover:** Provides CARP (Common Address Redundancy Protocol) for redundancy, ensuring minimal downtime.
- **Traffic Shaping & QoS:** Manages bandwidth allocation to optimize performance for critical applications.

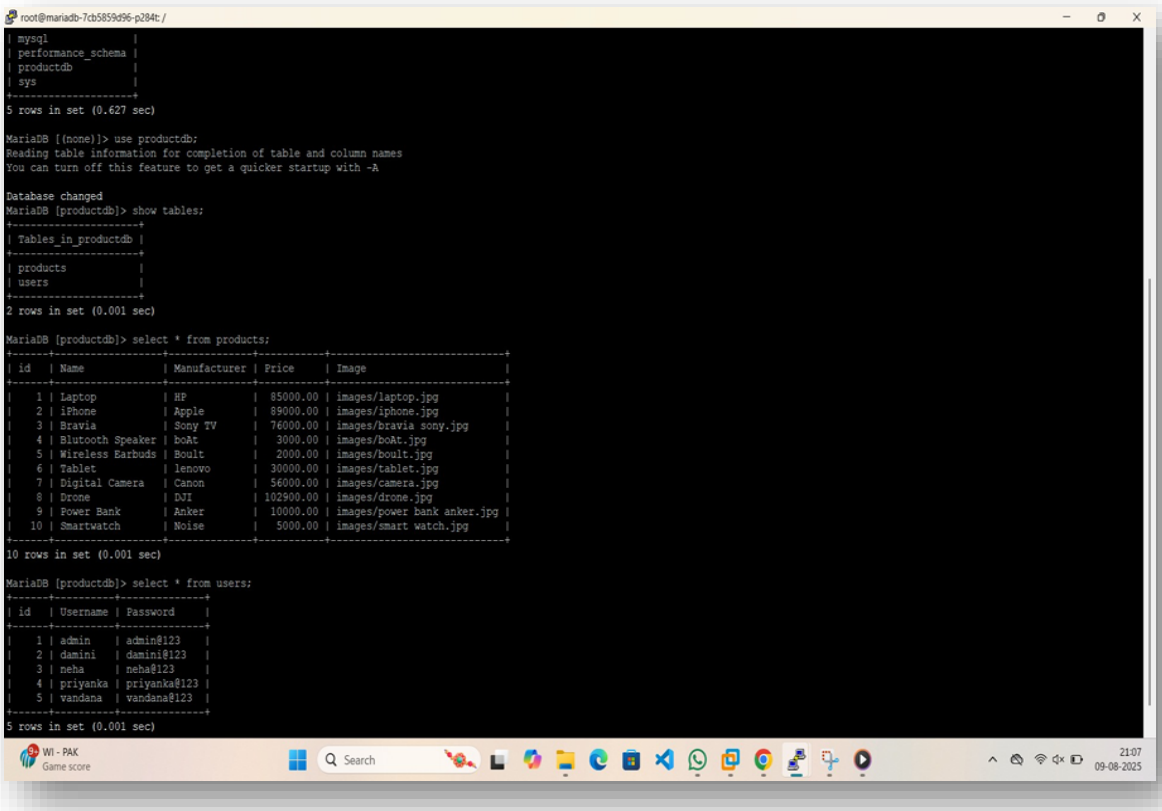
- **Integration with Reporting Tools:** Works with tools like Elasticsearch, Grafana, and Zabbix for monitoring and visual analytics.

4) Project Output

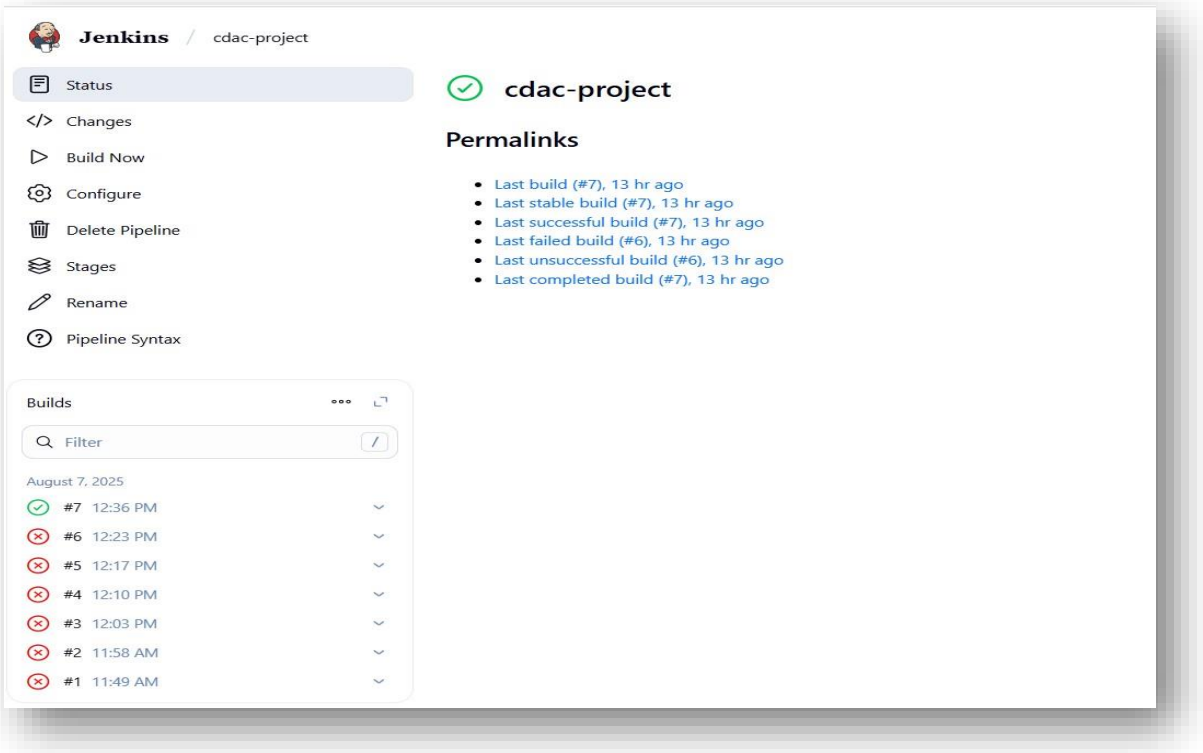
4.1 web application



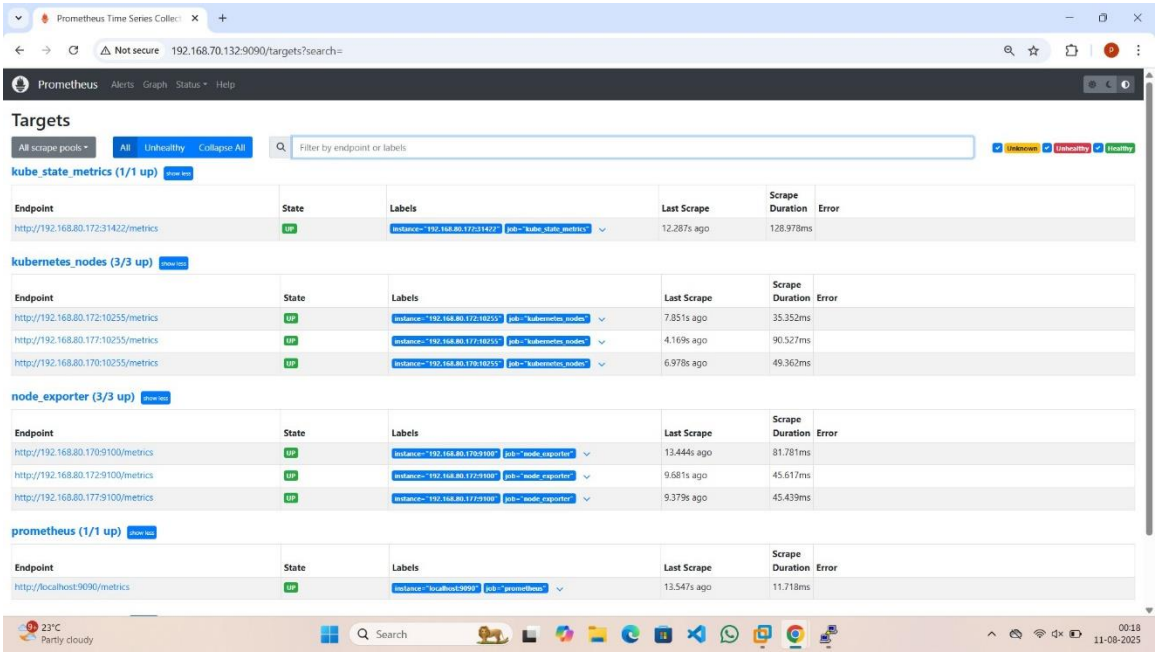
4.2 Database



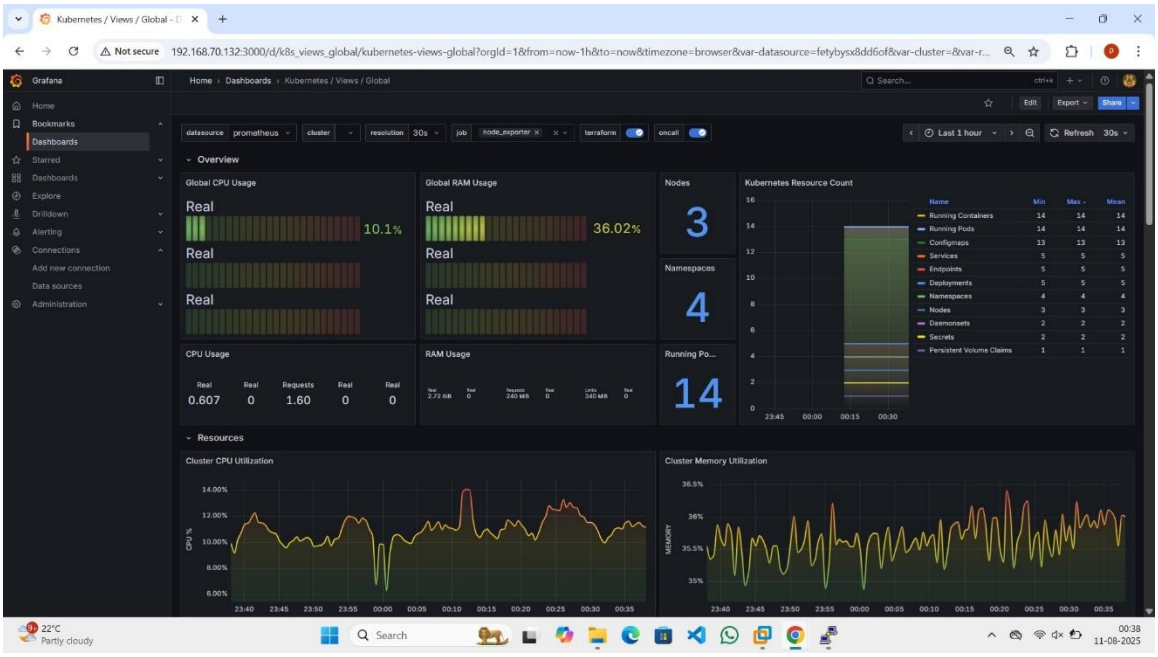
4.3 Jenkins



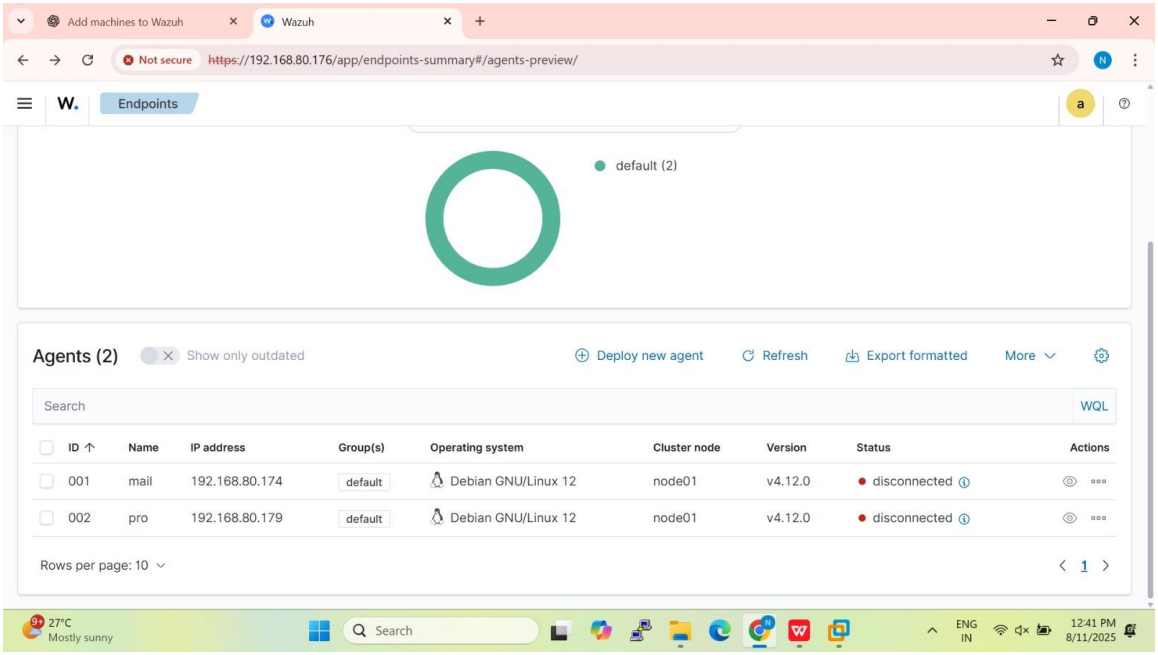
4.4 Prometheus



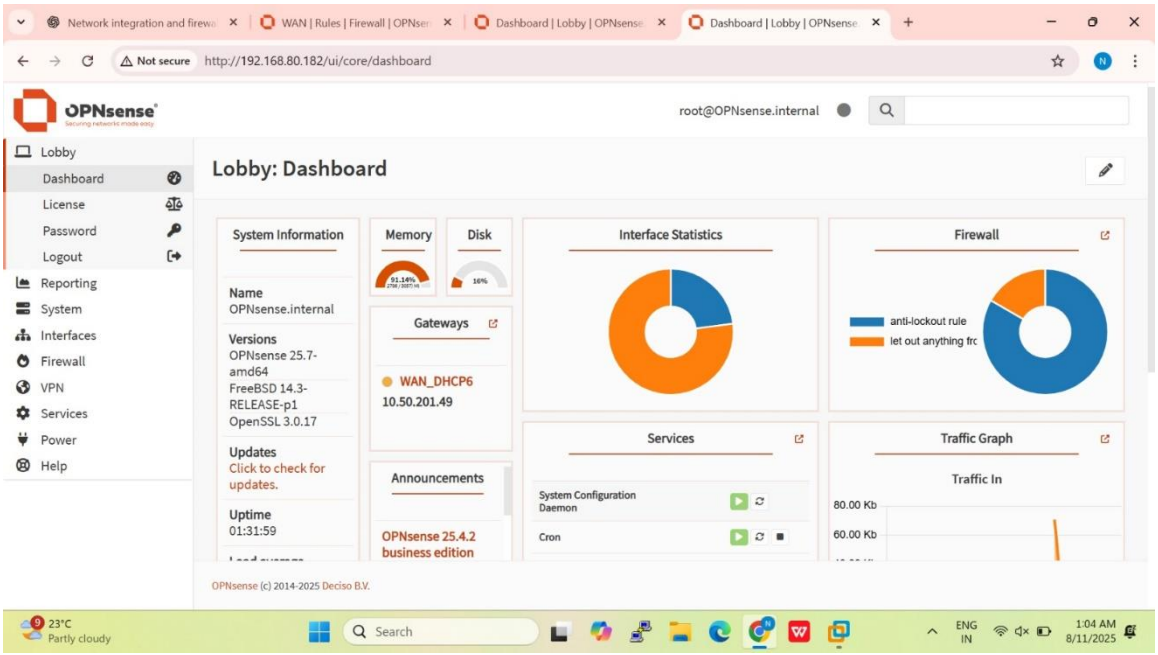
4.5 Grafana



4.6 Wazuh



4.7 OpenSence



5. CONCLUSION

5.1 Conclusion

This project focuses on designing and deploying a secure web system architecture, integrated with DevOps practices to bring together automation, scalability, and security. By using Kubernetes along with a Jenkins CI/CD pipeline, the system supports smooth application deployment and continuous delivery. Security is strengthened through Suricata IDS/IPS and a DMZ network layer, while Wazuh SIEM helps in detecting threats in real time and analyzing logs. With Prometheus and Grafana, I was able to keep proactive track of system health, and a configured mail server ensures that important alerts are delivered right on time. Centralized logging and backup processes add an extra layer of resilience, making the overall architecture dependable and ready for real-world production environments.

5.2 Future Scope

The proposed system can be further enhanced by integrating **Zero Trust Architecture** to ensure that no user or system is implicitly trusted, with every access request validated based on identity, device health, and context. Security can be reinforced through **Multi-Factor Authentication (MFA)**, requiring multiple verification methods to minimize credential theft risks.

For proactive threat mitigation, **AI/ML-driven threat detection** and **runtime protection** using Falco can be implemented to monitor container and host behavior in real time, identifying suspicious activity such as unauthorized processes or unexpected file changes.

The **CI/CD pipeline** can be secured by adding **SonarQube** for Static Application Security Testing (SAST) to detect vulnerabilities in code prior to deployment, and **OWASP ZAP** for Dynamic Application Security Testing (DAST) to uncover exploitable issues during runtime.

Finally, **Suricata** can be integrated with **live threat intelligence feeds** to automatically update detection rules with the latest attack signatures, ensuring advanced intrusion prevention against evolving threats.

REFERENCES

Paper 1: - A Qualitative Study of DevOps Usage in Practice

Author: Floris Erich, C. Amrit & M. Daneva

Paper 2: - Devops, A New Approach To Cloud Development & Testing

Author: Dhaya Sindhu Battina

Paper 3: Review Paper on Suricata and Its Applications in Network Security

Authors: Adapted from community and research contributions around Suricata.