A Zero Trust-Driven Framework for Mitigating Access Control Misconfigurations in Multi-Cloud Environments

Vishal Gowda V, Harshad K Reddy

Vellore Institute of Technology, Vellore, India

Project Introduction & Objectives

Problem Statement

Access control misconfigurations in multi-cloud environments are cited in nearly 90% of cloud security breaches, including overly permissive IAM policies, unsecured storage buckets, and lateral privilege escalations.

Project Objective

Develop a Zero Trust-driven framework that integrates Infrastructure-as-Code (IaC) auditing, continuous monitoring of runtime configurations, and automatic policy remediation to secure cloud-native environments.

Our approach combines infrastructure template scanning, real-time policy auditing, and automated remediation to address limitations in visibility, compliance, and control across dynamic, heterogeneous multi-cloud infrastructures.

Literature Survey (1/2)

Recent studies (2020 and beyond) have focused on mitigating cloud access misconfigurations using dynamic access control, Zero Trust, and Infrastructure-as-Code scanning:

Base Paper: Federated Zero Trust Architecture using Artificial Intelligence

Proposes a federated model for Zero Trust enhanced with AI, enabling adaptive decision-making and stronger authentication across distributed environments.

Cloud Service Misconfigurations: Emerging Threats

Explores common misconfigurations in cloud services and highlights how they lead to enterprise breaches, along with mitigation strategies.

Unified Framework for Securing Cloud-Native Storage

Introduces a unified approach to secure multi-cloud storage buckets, preventing data leaks caused by misconfigured access policies.

Literature Survey (2/2)

Zero-Trust Based Dynamic Access Control

Proposes a Zero Trust-driven adaptive model to dynamically adjust access policies in cloud infrastructures.

Security Issues in Multi-Cloud

Provides a comprehensive review of security challenges in multi-cloud environments, including identity sprawl, policy conflicts, and compliance issues.

Cloud Native Network Security Architecture

Suggests a Zero Trust-aligned security framework to strengthen network security in cloud-native systems.

Implementing Dynamic Confidential Computing

Suggests a Zero Trust-based confidential computing model to continuously monitor and mitigate security threats across cloud environments.

These studies from IEEE, Elsevier, and Springer provide the foundation for our research approach.

Research Gap

Lack of Real-Time Responsiveness

Existing mechanisms detect misconfigurations only after the fact through periodic audits and static scans.

Limited Context-Awareness

Many IAM tools don't dynamically adapt to changing contexts such as workload variations or ephemeral resources.

Absence of Automatic Remediation

Most systems detect misconfigurations but require manual remediation, which is slow and prone to errors.

Fragmented Multi-Cloud Security

Cloud providers offer separate monitoring tools, lacking a unified mechanism for handling misconfigurations across multi-cloud setups.

Weak Integration of Zero Trust

Few implementations focus on access control misconfigurations like IAM over-permissioning and lateral privilege escalation.

Lack of IaC-Aware Security

Many solutions do not integrate Infrastructure-as-Code auditing into security frameworks.

Architecture Diagram

Our Zero Trust-driven framework integrates IaC auditing, continuous monitoring, and automatic policy remediation across multi-cloud environments, enforcing least-privilege access dynamically.

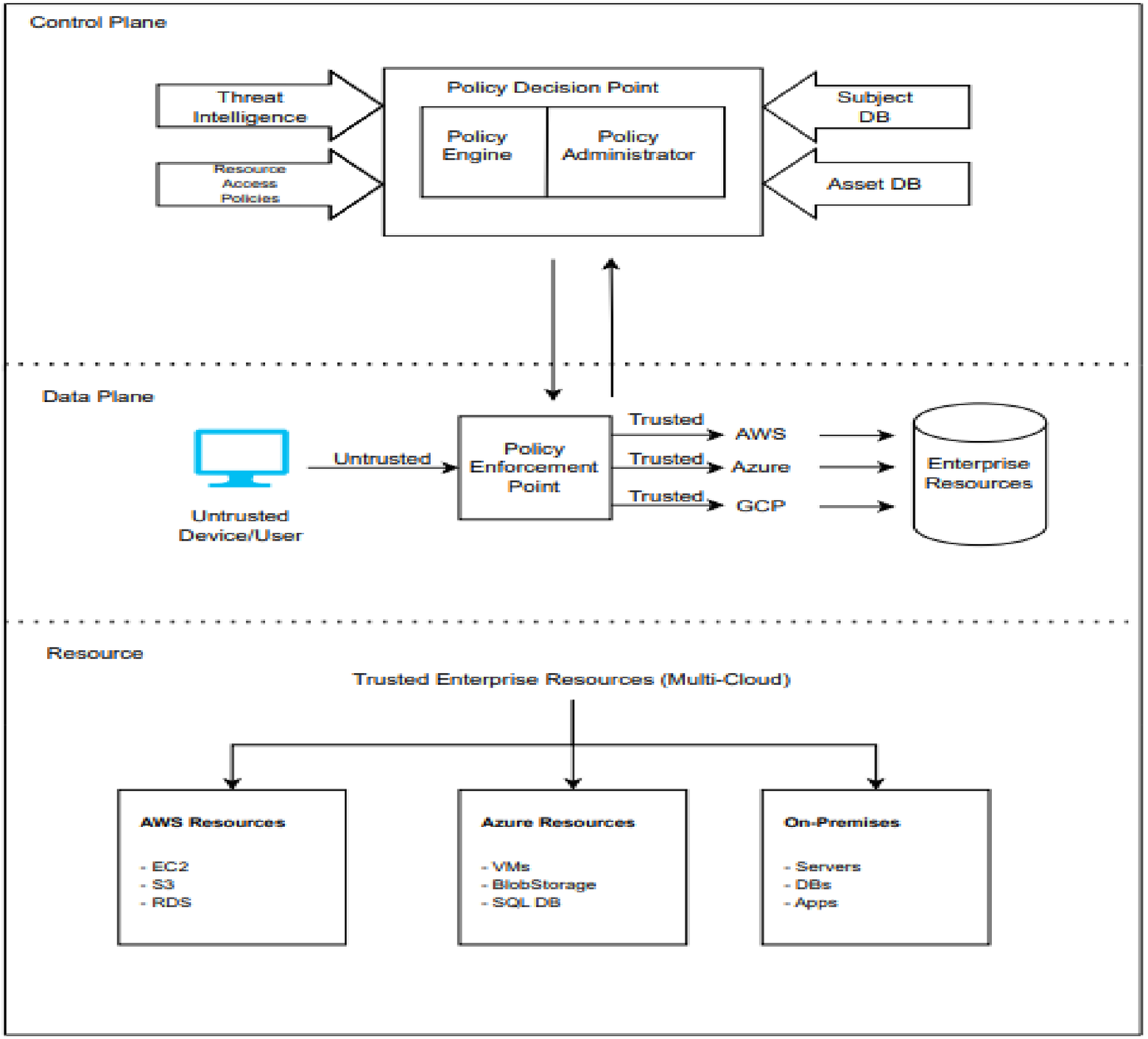
Hardware & Software Specifications

Hardware Requirements

- Processor: Intel i5/i7 or AMD Ryzen 5/7, ≥ 2.5 GHz
- Memory: 8 GB minimum (16 GB recommended)
- Storage: 256–512 GB SSD
- Network: Stable broadband ≥ 20 Mbps

Software Requirements

- OS: Windows 10/11
- Languages: Python, FastAPI/Flask
- IaC: Terraform, CloudFormation
- Containers: Docker, Kubernetes
- Cloud: AWS, Azure, GCP
- Zero Trust: OPA, Gatekeeper, Cloud Custodian
- Monitoring: CloudTrail, Prometheus, Grafana


Control Plane
Threat Intelligence
Resource Access Policies
Policy Decision Point
Policy Engine
Policy Administrator
Subject DB
Asset DB
Data Plane
Untrusted Device/User
Untrusted
Policy Enforcement Point
Trusted
AWS
Trusted
Azure
Trusted
GCP
Enterprise Resources
Resource
Trusted Enterprise Resources (Multi-Cloud)
AWS Resources
- EC2
- S3
- RDS
Azure Resources
- VMs
- BlobStorage
- SQL DB
On-Premises
- Servers
- DBs
- Apps

Module Split-up

IAM Monitoring Module

Detect overly permissive policies, unsecured storage, and privilege escalations

IaC Auditing Module

Prevent misconfigurations at deployment stage

Policy Decision Point

Evaluate access requests against security policies

Policy Enforcement Point

Enforce PDP decisions before allowing access

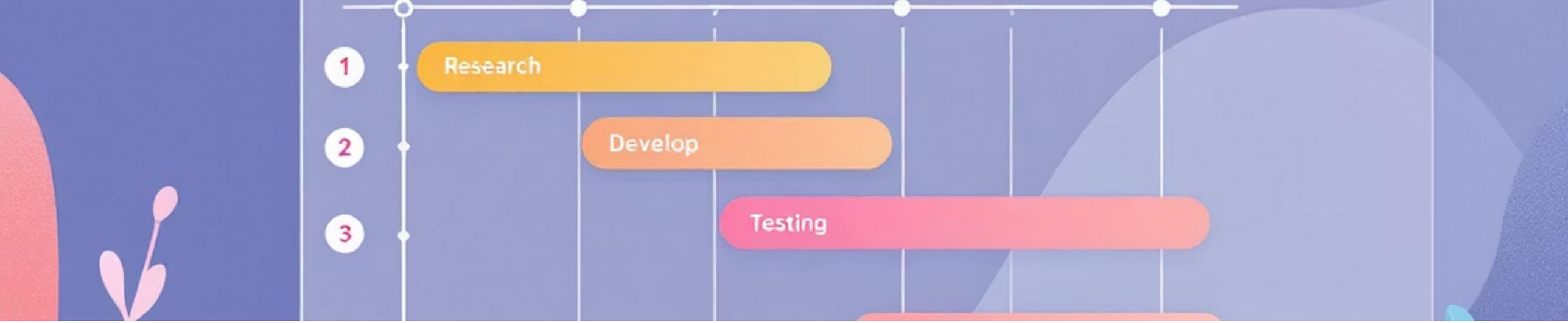
Remediation Module

Fix misconfigurations automatically

Monitoring & Logging

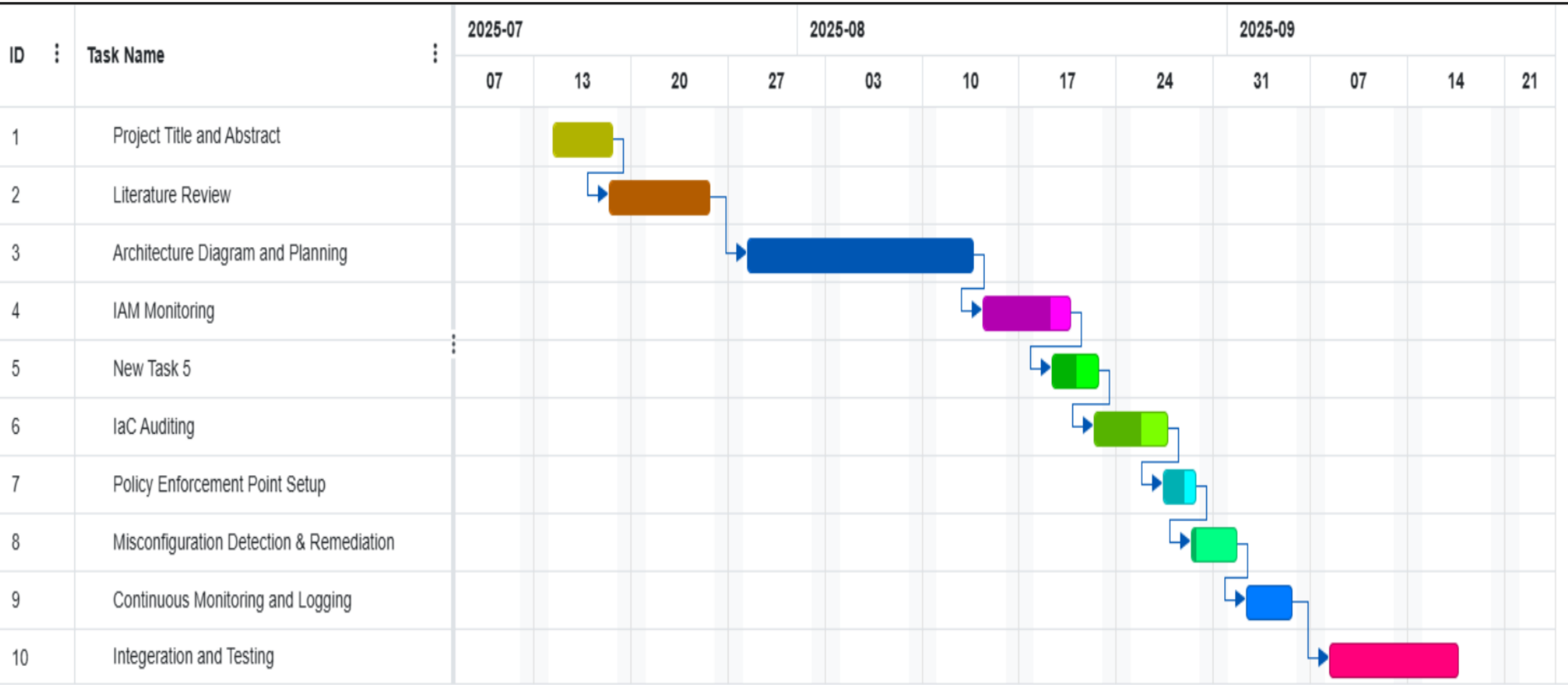
Provide visibility and feedback loops

The Multi-Cloud Resource Layer represents the actual enterprise resources protected by Zero Trust across AWS, Azure, GCP, and on-premises environments.



Gantt Chart & Timeline

The project implementation follows a structured timeline with parallel development of modules and integration phases to ensure timely completion and thorough testing.


ID
Task Name
2025-07
2025-08
2025-09
07
13
20
27
03
10
17
24
31
07
14
21
1
Project Title and Abstract
2
Literature Review
3
Architecture Diagram and Planning
4
IAM Monitoring
5
New Task 5
6
IaC Auditing
7
Policy Enforcement Point Setup
8
Misconfiguration Detection & Remediation
9
Continuous Monitoring and Logging
10
Integeration and Testing

Key Takeaways

Zero Trust Integration

Our framework applies Zero Trust principles specifically to access control misconfigurations, addressing a critical gap in cloud security.

Multi-Cloud Unification

Provides a unified approach to security across AWS, Azure, and GCP environments, eliminating fragmented security monitoring.

Automated Remediation

Implements automatic policy remediation to fix overly permissive policies without human intervention, reducing response time.

By combining IaC auditing with runtime monitoring in a single security loop, our framework enables proactive prevention of access control misconfigurations while maintaining usability and performance.