# Proposal: Building AI CI/CD Orchestrating Agents with Zero-Trust Principles, Least-Privilege Execution, and Secure Secret Handling

## 1. Introduction

The integration of Artificial Intelligence (AI) into Continuous Integration and Continuous Deployment (CI/CD) pipelines is emerging as a transformative approach to modern software engineering. AI agents acting as CI/CD orchestrators can optimize build, test, and deployment processes by dynamically adapting to project contexts. However, the security risks associated with AI-driven automation remain underexplored. This proposal aims to address these gaps by designing and implementing AI CI/CD orchestrating agents based on zero-trust principles, least-privilege execution, and secure secret handling.

## 2. Problem Statement

Existing CI/CD orchestration systems, whether rule-based or AI-enhanced, typically operate with broad privileges and limited security constraints. This creates vulnerabilities in the event of compromised credentials, malicious code injections, or flawed AI decision-making. The absence of zero-trust enforcement and fine-grained privilege control increases the attack surface and undermines the reliability of the deployment process.

## 3. Objectives

1. Develop an AI-powered CI/CD orchestrator capable of adaptive pipeline optimization.  
2. Integrate zero-trust access control and least-privilege execution into AI-driven automation.  
3. Implement secure secret management and credential rotation mechanisms.  
4. Evaluate the system’s security resilience and performance in real-world scenarios.

## 4. Research Questions

1. How can zero-trust principles be effectively embedded in AI-based CI/CD orchestration?  
2. What are the optimal methods for implementing least-privilege execution in automated DevOps pipelines?  
3. How can secure secret handling be integrated without compromising orchestration efficiency?  
4. What security vulnerabilities are most relevant to AI-driven CI/CD systems, and how can they be mitigated?

## 5. Methodology

The research will follow a design-science methodology, combining theoretical security models with practical implementation and testing. The proposed AI orchestrator will be built using reinforcement learning or large language model (LLM)-based planning capabilities, with a focus on modular, policy-driven security enforcement. Evaluation will be conducted through simulated attack scenarios and performance benchmarking.

## 6. Expected Contributions

1. A novel AI-driven CI/CD orchestration framework incorporating zero-trust principles.  
2. A secure secret handling and rotation protocol for automated DevOps environments.  
3. Empirical evaluation of AI orchestration under adversarial and real-world conditions.  
4. A roadmap for secure AI integration into DevOps workflows.