Kubernetes has gained widespread adoption as the leading platform for container orchestration, offering scalability and resilience for modern applications. Within Kubernetes, pods are critical components that host containers, but their security is highly dependent on configurations defined in YAML files. Misconfigurations in these files frequently introduce security vulnerabilities, exposing pods to potential attacks. This study investigates the configuration parameters that facilitate such attacks, focusing on their combinatorial effects.

Through our investigation, we identified 10 critical attack vectors including container escape, Docker-in-Docker attacks, privilege escalation via misconfigured host-level access (hostNetwork, hostPID), and cross-pod compromise scenarios. To address the combinatorial nature of these vulnerabilities, we developed an innovative analysis tool employing pairwise testing methodology.

We evaluated the tool’s effectiveness by comparing it with five existing static analysis tools, measuring performance using precision and recall metrics. Our results reveal that existing tools frequently miss vulnerability patterns that emerge from parameter interactions, while our approach achieves more comprehensive coverage.

This work makes three key contributions: (1) a systematic analysis of configuration-driven attack surfaces in Kubernetes pods, (2) an advanced testing framework using pairwise combinatorial methods, and (3) empirical validation showing significant improvements over current security analysis tools. Our findings provide both immediate practical benefits for security practitioners and important insights for future Kubernetes hardening techniques.