**Abstract**:

The adoption of Docker and Kubernetes has increased along with the rising demand for container technologies. Recent technological assessments indicate that containers are now widely used. This sort of isolated environment's implementation and management pose concerns regarding the security of such systems. Our research attempts to identify risks in a container environment using various system call characteristics (name, frequency, sequence, etc.) and to differentiate between anticipated and unexpected behavior (possible threats).

**Motivation:**

From the perspective of the attacker, there are several ways to attack a container-based virtualization system, such as using virtualization to steal users' private data, initiating attacks by injecting malicious workload, or escalating the intrusion to numerous VM instances.

The CNCF Financial User Group released, in January 2020, documentation and outcomes of an in-depth threat modeling exercise performed against a generic Kubernetes cluster. Their work provided a detailed view of several attack paths by which an attacker could exploit configuration vulnerabilities within Kubernetes to achieve specific goals. Our work contributes to the mitigation of all the attack paths that finally leads to malicious code execution in container. [Figure here]

**Methodology:**

We classified these attack paths according to distinct detection mechanisms.

[Figure here]

Firstly, we simulated some attacks(XSS, CSRF, SQLi, RBAC attack, etc) that follow the aformentioned paths and for each path we experimented with our detection mechanisms. The benign and malicious behaviour are distinguished by analysing the names, freuquencies and sequences of system calls.

For the purpose of attack simulation, **Seed-Ubuntu** is used as virtual machine. To collect different parameters of system calls, sysdig and strace are used as reverse engineering tools. Kubernetes dashboard collects the log files for RBAC attack. And finally to implement Kubernetes in local machine, minikube is used.

**Research Outcome:**

Our research work assumes that each container has its own IDS(Intrusion Detection System) for ensuring scalability. Our detection mechanism shows high accuracy(92-97%) along with healthy precision and recall. It can be observed that frequency-based mechanism is more efficient but less accurate than sequence-based mechanism. For future work, there are many other paths for different kinds of attacks that can be classified and detected.