**Thesis Title:** On Detecting Malicious Code Injection by Monitoring Multi-level Container Activities

**Submitted By,**

1705013 - Md. Olid Hasan Bhuiyan

1705034 - Souvik Das

**Supervised By,**

Dr. Md. Shohrab Hossain

**Abstract**

In recent years, cloud-native applications are widely hosted and managed through containerized environments due to their unique benefits, such as lightweight, portable, cost-efficient. In spite of their benefits and popularity, the security of such environments is very often questioned as evidenced by recent attacks. Among which, attackers are frequently using malicious code injection to breach systems and steal sensitive data from a containerized environment. However, there is no existing solution to efficiently detect malicious code injection in container applications. In this paper, we fill in this gap and propose a multi-level monitoring-based approach, where we monitor container activities at both system call level as well as orchestrator level. Thus, our approach can detect malicious code injection attacks in containers by distinguishing between their expected and unexpected behavior from various system call characteristics (e.g., sequence, frequency, etc.) along with activities through log files. We implement and evaluate our approach for Kubernetes, a major container orchestrator.