國立中山大學 COLLEGE OF ENGINEERING, NSYSU 工學院 聯合專題競賽與展示

資訊工程學系
Department of Computer Science and Engineering

第 18 組：楊志璿　　　　指導老師：范俊逸 教授

健康資訊交換系統中之容器安全

摘要

This research proposes a mechanism to enforce the system call a specific policy in the container, which is deployed in runtime. This policy is designed for the FHIR healthcare data exchange standard's container, which could guarantee the FHIR server does not have unsupported behavior and takes almost zero overhead. Recently, many companies use containers to run their microservices since containers could make their hardware resources be used efficiently. And the newest healthcare data exchange standard FHIR has been implemented in a container by IBM, Microsoft, and Firebase. The deployment of FHIR in a container is a trend in the digital world. However, containers are not sandboxes. Containers are just isolated processes. Therefore, if hackers or malicious software could sneak into the container that would be a new cyber attacking surface in nearly future.

動機

There are many applications using IBM's FHIR server as the base component of the EHR (Electronic Health Records) system to communicate with the other various databases. Take it for example that the NextCloud's EHR service, Taipei Veterans General Hospital, and AWS Cloud are using the FHIR server in a container for subroutine service.

NextCloud is an open-source and self-hosted productivity platform for users. Many people caring about their privacy issues distrust the FAANG (Facebook, Amazon, Apple, Netflix, Google), so they are using NextCloud to keep their privacy on their own. Therefore, they are eager to have a secure EHR system for their PHR.

架構

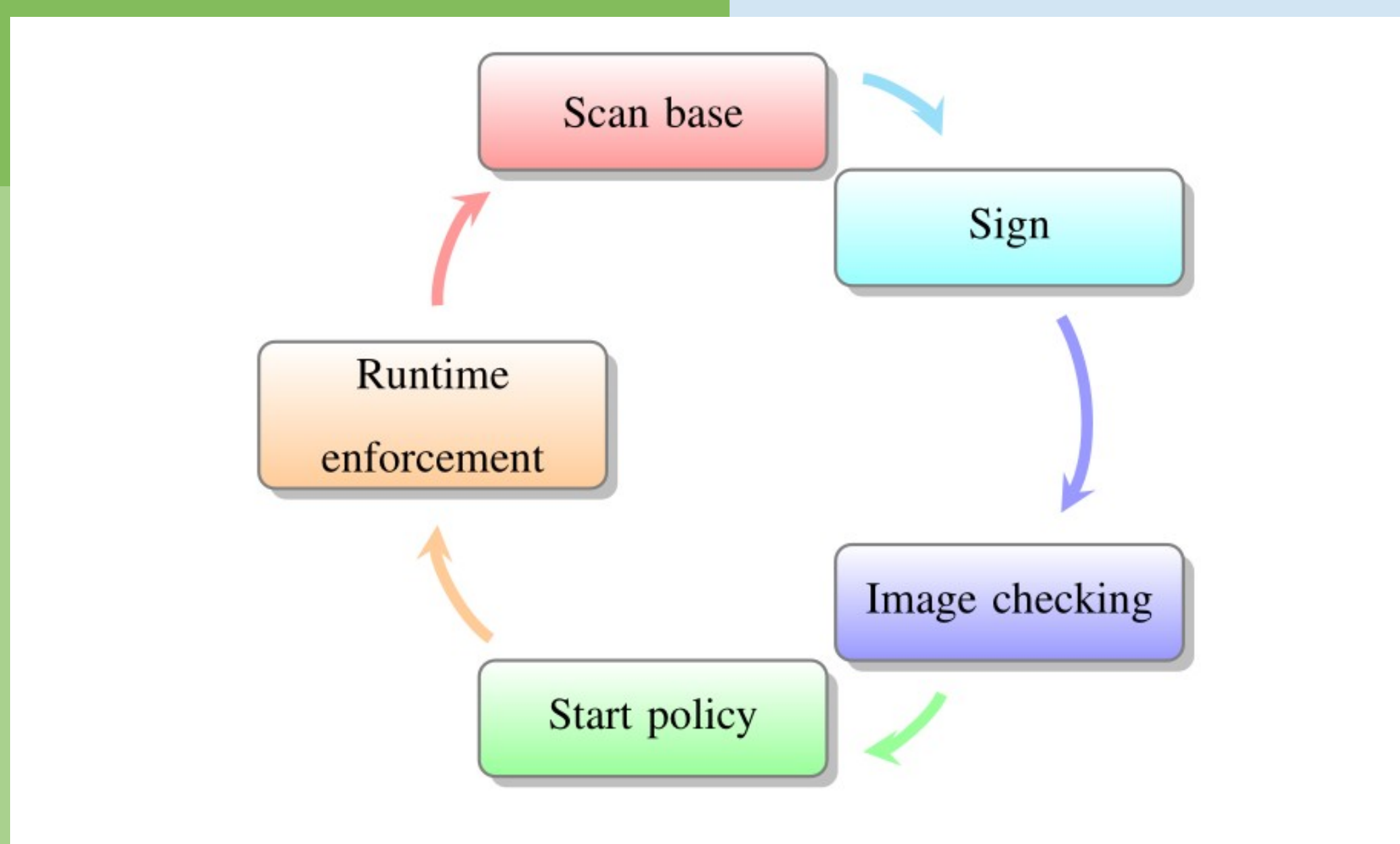

Figure 4.1: Contiguous Integration and Contiguous Deployment

未來與展望

We can see the comparison results in virtual machine and container are significantly indifferent order of time-consuming. There is no exist the gVisor's result is because the gVisor was not able to launch the IBM/FHIR server system, which is the target in our research. We also expect the gVisor might run faster significantly than the virtual machine, however, our target cannot be launched successfully in gVisor's sandbox.

This architecture can make sure the container is secure in build time and runtime. However, it might have some false negative cases occurrence. If we can use LSTM or some machine learning models in kernel, we might have a better balance of the statistical power trade-off.

成果展示

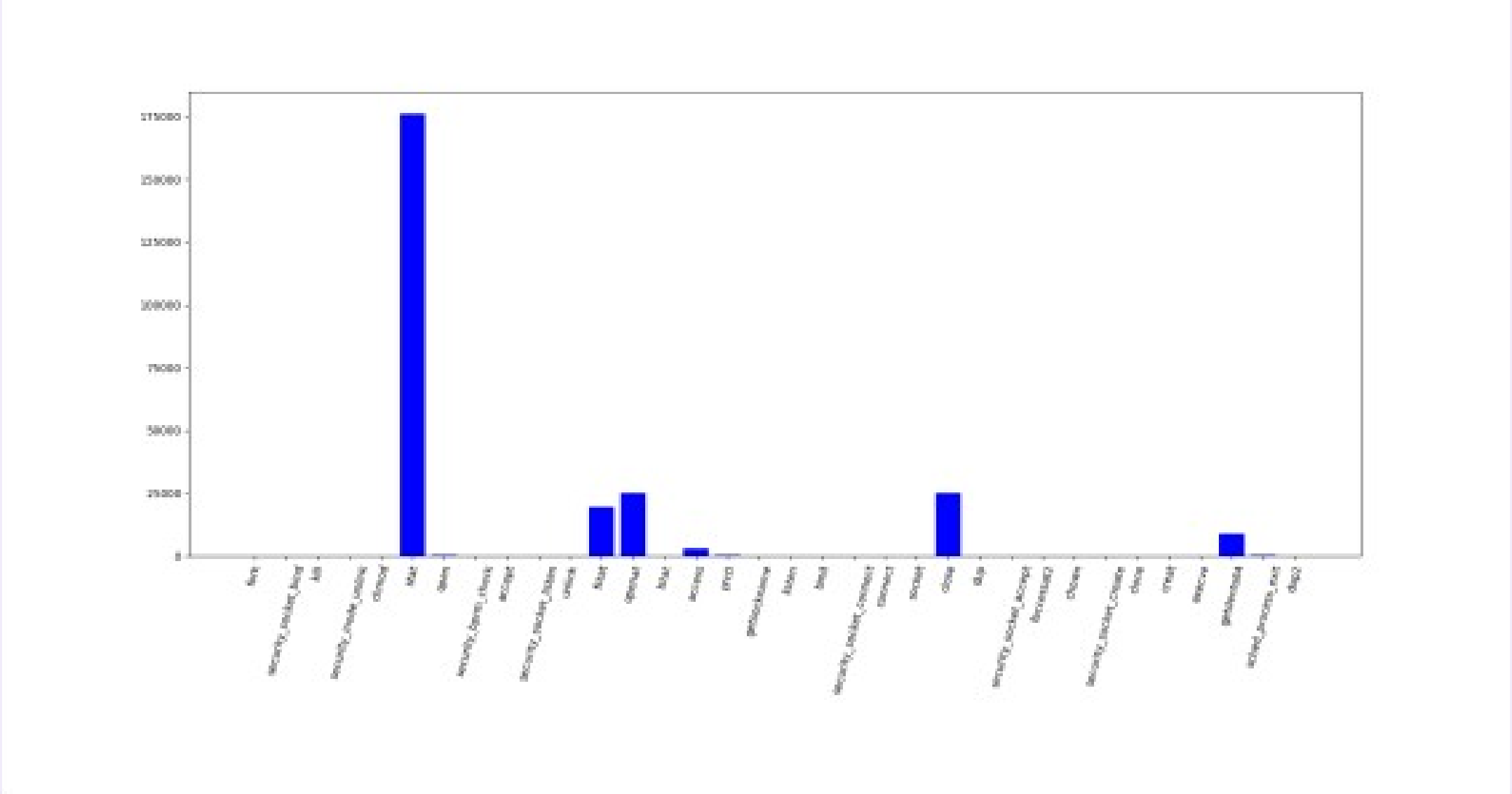

Figure 5.1: All the system calls which the FHIR called times

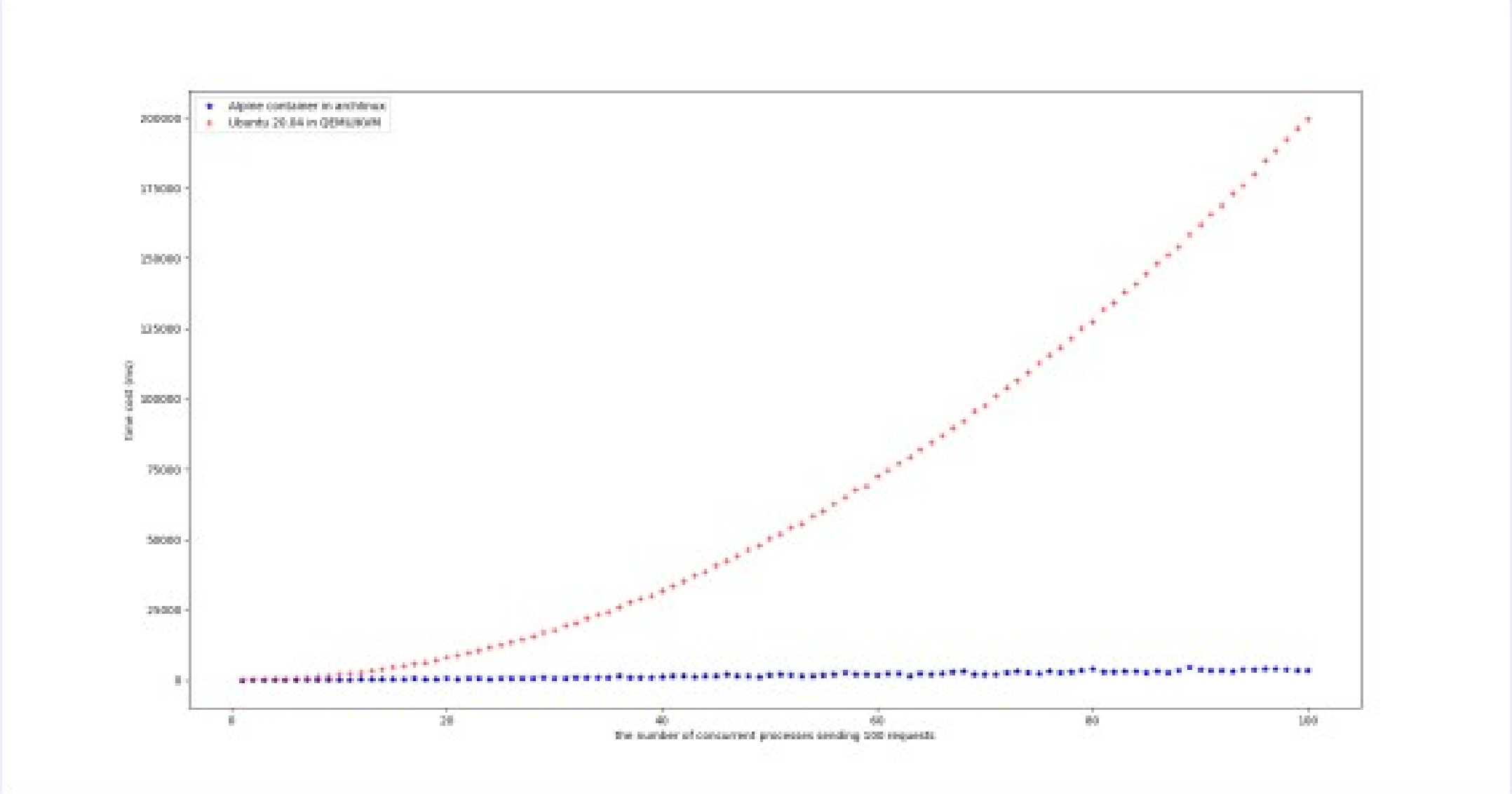

Figure 5.2: Concurrent processes transporting time