

TRUSTED DEPLOYMENT OF APPLICATION CONTAINERS
IN CLOUD DATA CENTERS

ABSTRACT

Systems, apparatuses and methods may provide for establishing a hardware-based chain of trust in a computing system and extending the hardware-based chain of trust to a container manager and a containerized application on the computing system. Additionally, the containerized application may be checked for its trust and security while it is launched, via the container manager, on the computing system. In one example, extending the hardware-based chain of trust includes conducting a pre-boot measurement of the container manager, a root of trust measurement agent, and one or more packages associated with the containerized application, and verifying the pre-boot measurement of the platform/host and the application itself prior to the containerized application being launched.

Fig. 3A