CLEARANCE OF BARE METAL RESOURCE TO TRUSTED STATE USABLE IN CLOUD COMPUTING

PRIORITY

The present application claims priority to U.S. provisional patent application Ser. No. 62/630,534, filed Feb. 14, 2018, which is incorporated by reference in its entirety.

BACKGROUND

[0001] Cloud computing typically involves the delivery of computing services, which may involve servers, storage, databases, networking, software, etc., over the Internet. Companies offering these computing services are called cloud providers and typically charge for cloud computing services based on usage.

[0002] Often, cloud providers use virtualization to implement a reusable pool of computing resources that can be assigned to different tenants. Virtualization is a technology that separates physical infrastructure to create various dedicated resources, such as virtual machines (VMs), that can run different instances of operating systems and applications on the same server. Using server virtualization, cloud providers can maximize the use of server resources and reduce the number of servers required. Also, VMs may run as separate, isolated units, thus providing fault and security isolation. Cloud providers may rely on virtualization technology to protect hardware from various intrusive attacks, such as attacks caused by firmware malware, bios-level hypervisor attacks, BIOS (basic input/output system)/firmware overwrite and denial of service attacks. Commonly, non-volatile memory modules on a system board are the target for such attacks, because targeting the non-volatile

What is claimed is:

1. A bare metal resource comprising:

a trusted portion including a first processing circuit, a clearance manager, and an image repository storing a known good basic input/output system (BIOS);; and

an untrusted portion including a second processing circuit and storage devices storing untrusted software that includes an accessible BIOS,

wherein, in response to a signal indicating that the bare metal resource is to be reassigned or that the bare metal resource has failed, the first processing circuit in the trusted portion is triggered by the signal to reboot the bare metal resource from the trusted portion and cause the clearance manager in the trusted portion to perform a clearance process on the untrusted portion to place the bare metal resource in a known good state prior to providing access to the bare metal resource, the clearance process including deleting data stored in the storage devices of the untrusted portion and restoring the accessible BIOS in the untrusted portion by replacing the accessible BIOS in the untrusted portion with the known good BIOS from the image repository of the trusted portion , and

in response to verifying that the clearance process has been completed, the second processing circuit in the untrusted portion reboots the bare metal resource from the untrusted portion using the restored accessible BIOS in the untrusted portion.

2. The bare metal resource of claim 1 , wherein the clearance process further includes, deleting the untrusted software, including the accessible BIOS, previously stored in the untrusted portion.

3. The bare metal resource of claim 1, wherein the clearance process further includes loading firmware from the image repository of the trusted portion into a storage device of the storage devices of the untrusted portion.

4. The bare metal resource of claim 1, wherein the clearance process further includes setting a state of a real-time clock to a valid default value.

5. The bare metal resource of claim 1, wherein

the untrusted portion is accessible by a new tenant via a network after the bare metal resource is rebooted from the untrusted portion.

6. The bare metal resource of claim 1, wherein the trusted portion and the untrusted portion are not simultaneously operational.

7. The bare metal resource of claim 5, wherein the bare metal resource is communicatively coupled to a trusted infrastructure device in a control plane of a cloud provider via an out-of-band channel, and

the bare metal resource is configured to receive the signal indicating that the bare metal resource is to be reassigned or that the bare metal resource has failed from the trusted infrastructure device to invoke the clearance process.

8. The bare metal resource of claim 7, wherein the bare metal resource is configured to receive a verification that the clearance process has been completed from the trusted infrastructure device via the out-of-band channel, after the trusted infrastructure device has verified that the clearance process is completed and the bare metal resource is in the known good state, to cause the bare metal resource to reboot from the untrusted portion.

9. The bare metal resource of claim 7, wherein the trusted infrastructure device runs a timer when the clearance process begins to determine whether the clearance process has been completed or is stalled.

10. The bare metal resource of claim 7, wherein the trusted infrastructure device is a rack controller, and the out-of-band channel comprises a wired connection between the rack controller and a connector on a system board of the bare metal resource.

11. A bare metal resource in a pool of computing resources, the bare metal resource comprising:

a trusted portion including a memory storing a clearance manager, an image repository storing a known good basic input/output system (BIOS), and a first processing circuit to execute the clearance manager, wherein the trusted portion is inaccessible to a new tenant;

an untrusted portion, accessible to the new tenant when the bare metal resource is assigned to the new tenant, including a second processing circuit and storage device storing untrusted software that comprises an accessible BIOS; and

a communication interface communicatively coupled to an external device,

wherein in response to receiving a first signal, from the external device, indicating that the bare metal resource is to be reassigned to the new tenant or that the bare metal resource has failed, the first processing circuit in the trusted portion is triggered by the first signal to reboot the bare metal resource from the trusted portion and cause the clearance

manager in the trusted portion to perform a clearance process on the untrusted portion to place the bare metal resource in a known good state prior to providing access to the bare metal resource , the clearance process including deleting data stored in the storage devices of the untrusted portion by a previous tenant and restoring the accessible BIOS in the untrusted portion by replacing the accessible BIOS in the untrusted portion with the known good BIOS from the image repository of the trusted portion, and

in response to verifying that the clearance process has been completed, the second processing circuit in the untrusted portion reboots the bare metal resource from the untrusted portion using the restored accessible BIOS in the untrusted portion.

12. The bare metal resource of claim 11, wherein the external device is a trusted infrastructure device of a cloud service provider.

13. The bare metal resource of claim 11, wherein the clearance process further includes deleting the untrusted software, including the accessible BIOS, previously stored in the untrusted portion.

14. The bare metal resource of claim 11, wherein the external device runs a timer to determine whether the clearance process has been completed or is stalled.

15. The bare metal resource of claim 11, wherein the external device is a rack controller communicatively coupled to the bare metal resource via an out-of-band channel, and wherein the out-of-band channel comprises a wired connection between the rack controller and a connector on a system board of the bare metal resource.

16. The bare metal resource of claim 11, wherein the trusted portion and the untrusted portion are not simultaneously operational.

17. The bare metal resource of claim 11, wherein the trusted portion and the untrusted portion are on a mother-board of the bare metal resource.

18. A method comprising:

receiving, from a trusted infrastructure device, a first signal indicating that a bare metal resource is to be reassigned or that the bare metal resource has failed;

in response to the first signal indicating that the bare metal resource is to be reassigned or that the bare metal resource has failed, causing a first processor in a trusted portion of the bare metal resource to reboot the bare metal resource from the trusted portion and causing a clearance manager in the trusted portion to perform a clearance process on an untrusted portion of the bare metal resource to place the bare metal resource in a known good state prior to providing access to the bare metal resource, wherein the clearance process includes deleting data stored in storage devices of the untrusted portion by a previous tenant and restoring an accessible basic input/output system (BIOS) in the untrusted portion by replacing the accessible BIOS in the untrusted portion with a known good BIOS from an image repository of the trusted portion of the bare metal resource; and

in response to verifying that the clearance process has been completed, causing a second processor in the untrusted portion of the bare metal resource to reboot the bare metal resource from the untrusted portion using the restored accessible BIOS in the untrusted portion.

19. The method of claim 18, wherein the trusted infrastructure device transmits a second signal to the bare metal resource indicating that the clearance process has been verified to be completed to cause the second processor to reboot the bare metal resource from the untrusted portion.

20. The method of claim 18, wherein the trusted infrastructure device runs a timer to determine whether the clearance process has been completed.