SECURE KEY MANAGEMENT

CROSS –REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of and priority to U.S. Provisional Patent Application Ser. No. 62/421,835 filed on Nov. 14, 2016 and entitled “Secure Key Management,” which application is expressly incorporated herein by reference in its entirety.

BACKGROUND

Background and Relevant Art

[0001] Computers and computing systems have affected nearly every aspect of modern living. Computers are generally involved in work, recreation, healthcare, transportation, entertainment, household management, etc.

[0002] Further, computing system functionality can be enhanced by a computing systems' ability to be interconnected to other computing systems via network connections. Network connections may include, but are not limited to, connections via wired or wireless Ethernet, cellular connections, or even computer to computer connections through serial, parallel, USB, or other connections. The connections allow a computing system to access services at other computing systems and to quickly and efficiently receive application data from other computing systems.

[0003] Interconnection of computing systems has facilitated distributed computing systems, such as so-called "cloud" computing systems. In this description, "cloud computing" may be systems or resources for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services, etc.) that can be provisioned and released with reduced management effort or service provider interaction. A cloud model can be composed of various characteristics (e.g., on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service, etc.), service models (e.g., Software as a Service ("SaaS"), Platform as a Service ("PaaS"), Infrastructure as a Service ("IaaS"), and deployment models (e.g., private cloud, community cloud, public cloud, hybrid cloud, etc.).

[0004] In cloud computing systems, there is a cloud service provider and tenant customers. While the tenant customers desire to use the cloud computing system resources, these customers will generally not want individuals at the cloud service provider, e.g., cloud service provider employees or others having physical access to cloud service provider resources, to have access to the customer' s data. Thus, there is a desire by tenant customers for a third party to administer data without actually being able to view the data.

[0005] The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments described herein may be practiced.

What is claimed is :

1. A system comprising:

a compute fabric comprising a first plurality of hardware machines, each of the first plurality of hardware machines running a first management enclave and a tenant enclave, wherein for each of the first plurality of hardware machines the first management enclave is configured to provide one or more tenant keys into the tenant enclave; the tenant enclave corresponds to a protected area of an application address space for which access is prevented for any application code not resident in the tenant enclave; and the first management enclave corresponds to a protected area of an application address space for which access is prevented for any application code not resident in the first management enclave, except that the first management enclave is permitted to provide the one or more tenant keys to the tenant enclave; and

a key fabric comprising a second plurality of hardware machines, each of the second plurality of hardware machines running a second management enclave, wherein for each of the second plurality of hardware machines the second management enclave is configured to cause one or more encrypted tenant keys to be stored locally and exclusively on the second hardware machine, and wherein each of the first and second management enclaves run mutually approvable and authenticatable management enclave application code, thereby allowing tenant keys to be passed between management enclaves of different hardware machines in a trusted fashion by the management enclaves approving and authenticating management enclave application code.

2. The system of claim 1, wherein each of the first and second management enclaves run mutually approvable and authenticatable management enclave application code by running identical application code.

3. The system of claim 1, wherein each of the first and second management enclaves run mutually approvable and authenticatable management enclave application code by running different versions of a same application code that can be verified as different versions of the same application code..

4. The system of claim 3, wherein each of the first and second management enclaves are configured to verify different versions of the same application code by verifying an attestation certificate including an enclave attestation for a management enclave, wherein the enclave attestation comprises verifiable proof of a signing authority, verifiable proof of a signing authority declaration of what functionality application code has, and verifiable proof of a signing authority declared version of application code.

5. The system of claim 1, wherein each of the second management enclaves is configured to encrypt and decrypt tenant keys using a machine key for a machine on which each second management enclave is running.

6. The system of claim 1, wherein the system is configured to generate tenant keys.

7. The system of claim 1, wherein the system is configured to receive tenant keys from tenants.

8. A hardware machine comprising:

one or more hardware processors, comprising :

a tenant enclave which corresponds to a protected area of an application address space for which access is prevented for any application code not resident in the tenant enclave itself, except that keys can be provided by one or more management enclaves into the tenant enclave; and

a management enclave coupled to the tenant enclave, wherein the management enclave is configured to provide a key to the tenant enclave, and wherein the management enclave corresponds to a protected area of an application address space for which access is prevented for any application code not resident in the management enclave itself.

9. The hardware machine of claim 8, wherein the management enclave is configured to communicate with other management enclaves running mutually approvable and authenticatable application code such that tenant keys can be passed between management enclaves in a trusted fashion by management enclaves approving and authenticating management enclave application code.

10. The hardware machine of claim 9, wherein the management enclave is configured to communicate with other management enclaves running identical application code.

11. The hardware machine of claim 9, wherein the management enclave is configured to communicate with other management enclaves running different versions of a same application code that can be verified as different versions of the same application code.

12. The hardware machine of claim 11, wherein the management enclave is configured to verify different versions of the same application code by verifying an attestation certificate including an enclave attestation for a management enclave, wherein the enclave attestation comprises verifiable proof of a signing authority, verifiable proof of a signing authority declaration of what functionality application code has, and verifiable proof of a signing authority declared version of application code.

13. The hardware machine of claim 8, wherein the management enclave is configured to encrypt and decrypt tenant keys using a machine key for the hardware machine.

14. The hardware machine of claim 8, wherein the tenant enclave is configured to perform functions for a cloud service tenant, and wherein the management enclave is configured to provide a tenant key into the tenant enclave.

15. A method of securely managing tenants on a cloud system, the method comprising:

obtaining a tenant key; and

at a management enclave on a hardware machine in a compute fabric in a cloud service, providing the tenant key into a tenant enclave on the hardware machine, wherein the management enclave corresponds to a protected area of an application address space for which access is prevented for any application code not resident in the management enclave itself and a tenant enclave corresponds to a protected area of an application address space for which access is prevented for any application code not resident in the tenant enclave itself, except that the management enclave can provide keys to the tenant enclave, and wherein the tenant enclave is configured to perform functionality for a cloud service tenant.

16. The method of claim 15, wherein obtaining a tenant key comprises obtaining a tenant key from another management enclave running a version of a same application code as the management enclave by verifying that the another management enclave is running mutually approvable and authenticatable management enclave code such that the tenant keys can be passed between the management enclave and the another management enclave in a trusted fashion by the management enclave approving and authenticating management enclave code.

17. The method of claim 16, wherein verifying that the another management enclave is running mutually approvable and authenticatable application code comprises verifying that the another management enclave is running identical application code to application code being run by the management enclave.

18. The method of claim 16, wherein verifying that the another management enclave is running mutually approvable and authenticatable management enclave code comprises verifying that the another management enclave is running a different version of application code than the management enclave, but that can be verified as a different version of application code than the management enclave.

19. The method of claim 18, wherein verifying that the another management enclave is running a different version of the management enclave code comprises verifying an attestation certificate including an enclave attestation for the another management enclave, wherein the enclave attestation comprises verifiable proof of a signing authority, verifiable proof of a signing authority declaration of what functionality application code has, and verifiable proof of a signing authority declared version of application code.

20. The method of claim 15, wherein obtaining a tenant key comprises obtaining a tenant key from a cloud tenant.