

CLAIMS

1. A method for accessing shared sensitive information in a managed container environment, the method comprising:

accessing, by each worker node in a plurality of worker nodes, shared sensitive application data located in a secure enclave within the plurality of worker nodes using a data encryption key;

protecting, by each worker node in the plurality of worker nodes, the data encryption key of each respective worker node using a sealing key that is unique to the secure enclave on a respective worker node;

establishing a first worker node in a cluster;

generating, by the first worker node, the data encryption key; generating, by the first worker node, a first sealing key unique to the secure enclave on the first worker node for protecting the data encryption key;

performing, by the first worker node, remote attestation with a second worker node in the cluster in response to creation of the second worker node in the cluster; and

providing, by the first worker node, a copy of the data encryption key to the second worker node upon successful performance of the remote attestation.

2. The method of claim 1 further comprising: generating, by the second worker node, a second sealing key unique to the secure enclave on the second worker node for protecting the data encryption key by encrypting the data encryption key using the second sealing key.

3. A system for accessing shared sensitive information in a managed container environment, the system comprising:

a plurality of worker nodes, wherein:

each worker node in the plurality of worker nodes accesses shared sensitive application data located in a secure enclave within the plurality of worker nodes using a data encryption key;

each worker node in the plurality of worker nodes protects the data encryption key of each respective worker node using a sealing key that is unique to the secure enclave on a respective worker node;

a first worker node is established in a cluster;

the first worker node generates the data encryption key;

the first worker node generates a first sealing key unique to the secure enclave on the first worker node for protecting the data encryption key;

the first worker node performs remote attestation with a second worker node in the cluster in response to creation of the second worker node in the cluster; and

the first worker node provides a copy of the data encryption key to the second worker node upon successful performance of the remote attestation.

4. The system of claim 3, wherein: the second worker node generates a second sealing key unique to the secure enclave on the second worker node for protecting the data encryption key by encrypting the data encryption key using the second sealing key.

5. A computer program product for accessing shared sensitive information in a managed container environment, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by a set of processors to cause the set of processors to perform a method comprising:

accessing, by each worker node in a plurality of worker nodes, shared sensitive application data located in a secure enclave within the plurality of worker nodes using a data encryption key;

protecting, by each worker node in the plurality of worker nodes, the data encryption key of each respective worker node using a sealing key that is unique to the secure enclave on a respective worker node;

establishing a first worker node in a cluster;

generating, by the first worker node, the data encryption key;

generating, by the first worker node, a first sealing key unique to the secure enclave on the first worker node for protecting the data encryption key;

performing, by the first worker node, remote attestation with a second worker node in the cluster in response to creation of the second worker node in the cluster; and

providing, by the first worker node, a copy of the data encryption key to the second worker node upon successful performance of the remote attestation.

6. The computer program product of claim 5 further comprising: generating, by the second worker node, a second sealing key unique to the secure enclave on the second worker node for protecting the data encryption key by encrypting the data encryption key using the second sealing key.

7. A computer-implemented method for cryptographic key orchestration, the computer-implemented method comprising:

generating, by a set of processors, a first worker node with a first key orchestration agent in a cluster of an open source container orchestration framework;

generating, by the set of processors, using the first key orchestration agent of the first worker node, a data encryption key;

retrieving, by the set of processors, using the first key orchestration agent, a sealing key of the first key orchestration agent from a secure enclave of the first worker node; and

sealing, by the set of processors, using the sealing key of the first key orchestration agent, the data encryption key.

8. The computer-implemented method of claim 7 further comprising:

determining, by the set of processors, whether a container has been created in the first worker node; and

responsive to the set of processors determining that a container has been created in the first worker node, performing, by the set of processors, using the first key orchestration agent, local attestation with the container to establish authenticity of the container.

9. The computer-implemented method of claim 8 further comprising:

determining, by the set of processors, whether the container is trusted based on the local attestation; and

responsive to the set of processors determining that the container is untrusted based on the local attestation, denying, by the set of processors, access to the data encryption key by the container.

10. The computer-implemented method of claim 9 further comprising:

responsive to the set of processors determining that the container is trusted based on the local attestation, sharing, by the set of processors, using the first key orchestration agent, the data encryption key with the container;

encrypting, by the set of processors, using the data encryption key shared with the container, data corresponding to a workload of the container; and

storing, by the set of processors, an identifier of the first worker node and the data encryption key sealed with a unique sealing key of the container in a shared database.

11. The computer-implemented method of claim 7 further comprising:

generating, by the set of processors, a second worker node with a second key orchestration agent within the cluster; and

performing, by the set of processors, using the second key orchestration agent of the second worker node, remote attestation with the first key orchestration agent of the first worker node to establish authenticity of the second key orchestration agent.

12. The computer-implemented method of claim 11 further comprising:

determining, by the set of processors, whether the second key orchestration agent is trusted based on the remote attestation; and

responsive to the set of processors determining that the second key orchestration agent is untrusted based on the remote attestation, denying, by the set of processors, access to the data encryption key of the first key orchestration agent by the second key orchestration agent.

13. The computer-implemented method of claim 12 further comprising:

responsive to the set of processors determining that the second key orchestration agent is trusted based on the remote attestation, sharing, by the set of processors, using the first key orchestration agent of the first worker node, the data encryption key of the first key orchestration agent with the second key orchestration agent;

retrieving, by the set of processors, using the second key orchestration agent, a unique sealing key of the second key orchestration agent from a secure enclave of the second worker node; and

sealing, by the set of processors, using the unique sealing key of the second key orchestration agent, the data encryption key.

14. The computer-implemented method of claim 7, wherein sensitive application data is only shared among trusted containers, even when containers move within the cluster.

15. The computer-implemented method of claim 14, wherein the sensitive application data is protected in any form of storage.

16. A computer program product for cryptographic key orchestration, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by a set of processors to cause the set of processors to perform a method comprising:

generating, by the set of processors, a first worker node with a first key orchestration agent in a cluster of an open source container orchestration framework;

generating, by the set of processors, using the first key orchestration agent of the first worker node, a data encryption key;

retrieving, by the set of processors, using the first key orchestration agent, a sealing key of the first key orchestration agent from a secure enclave of the first worker node; and

sealing, by the set of processors, using the sealing key of the first key orchestration agent, the data encryption key.

17. The computer program product of claim 16 further comprising:

determining, by the set of processors, whether a container has been created in the first worker node; and

responsive to the set of processors determining that a container has been created in the first worker node, performing, by the set of processors, using the first key orchestration agent, local attestation with the container to establish authenticity of the container.

18. The computer program product of claim 17 further comprising:

determining, by the set of processors, whether the container is trusted based on the local attestation; and

responsive to the set of processors determining that the container is untrusted based on the local attestation, denying, by the set of processors, access to the data encryption key by the container.

19. The computer program product of claim 18 further comprising:

responsive to the set of processors determining that the container is trusted based on the local attestation, sharing, by the set of processors, using the first key orchestration agent, the data encryption key with the container;

encrypting, by the set of processors, using the data encryption key shared with the container, data corresponding to a workload of the container; and

storing, by the set of processors, an identifier of the first worker node and the data encryption key sealed with a unique sealing key of the container in a shared database.

20. The computer program product of claim 16 further comprising:

generating, by the set of processors, a second worker node with a second key orchestration agent within the cluster; and

performing, by the set of processors, using the second key orchestration agent of the second worker node, remote attestation with the first key orchestration agent of the first worker node to establish authenticity of the second key orchestration agent.

21. The computer program product of claim 20 further comprising:

determining, by the set of processors, whether the second key orchestration agent is trusted based on the remote attestation; and

responsive to the set of processors determining that the second key orchestration agent is untrusted based on the remote attestation, denying, by the set of processors, access to the data encryption key of the first key orchestration agent by the second key orchestration agent.

22. The computer program product of claim 21 further comprising:

responsive to the set of processors determining that the second key orchestration agent is trusted based on the remote attestation, sharing, by the set of processors, using the first key orchestration agent of the first worker node, the data encryption key of the first key orchestration agent with the second key orchestration agent;

retrieving, by the set of processors, using the second key orchestration agent, a unique sealing key of the second key orchestration agent from a secure enclave of the second worker node; and

sealing, by the set of processors, using the unique sealing key of the second key orchestration agent, the data encryption key.