CLAIMS

What is claimed is:

1. A data control method for a zero-trust security container, comprising:

generating a zero-trust security policy based on a scenario;

building a data pool for a zero-trust security container;

adopting the zero-trust security policy for data to be in or out of the data pool, wherein admission or egress is allowed for the data to be in or out of the data pool only after the data is verified based on the zero-trust security policy; and

hierarchically isolating data in the data pool into multiple data domains based on the zero-trust security policy, wherein the data is isolated into the multiple data domains by a source of the data, a role of a data reading party, and a role of a data writing party; and

verifying, for data to be read from the data pool, a source of the data, a role of a data writing party provided by a data reading party, and a role of a data reading party provided by the data reading party; and

egressing data whose source, role of the data writing party, and role of the data reading party are verified.

2. The method according to claim 1, wherein the zero-trust security policy comprises trusting none of data reading/writing parties.

3. The method according to claim 2, wherein the zero-trust security policy comprises the following:

verifying a source for data to be written to the data pool; and

admitting data whose source is verified, wherein the admitted data is labeled with a source label.

4. The method according to claim 2, wherein the zero-trust security policy comprises the following:

verifying a source and a role of a data writing party for data to be written to the data pool; and

admitting data whose source and role of a data writing party are verified, wherein the admitted data is labeled with a source label and a role label of the data writing party.

5. The method according to claim 1, wherein the hierarchically isolating data in the data pool into multiple data domains comprises isolating the data into the multiple data domains by sensitive data and runtime data; and

wherein corresponding protection levels are set for the multiple data domains.

6. A data control system for a zero-trust security container, comprising:

a zero-trust policy module, configured to generate a zero-trust security policy based on a scenario;

a data pool building module, configured to build a data pool for a zero-trust security container;

a zero-trust verification module, configured to adopt the zero-trust security policy for data to be in or out of the data pool, wherein admission or egress is allowed for the data to be in or out of the data pool only after the data is verified based on the zero-trust security policy; and

a data isolation module, configured to hierarchically isolate data in the data pool into multiple data domains based on the zero-trust security policy, wherein the data is isolated into the multiple data domains by a source of the data, a role of a data reading party, and a role of a data writing party; and

the zero-trust verification module being further configured to verify, for data to be read from the data pool, a source of the data, a role of a data writing party provided by a data reading party, and a role of a data reading party provided by the data reading party; and

the zero-trust verification module being further configured to egress data whose source, role of the data writing party, and role of the data reading party are verified.

7. The system according to claim 6, wherein the zero-trust security policy comprises trusting none of data reading/writing parties.

8. The system according to claim 7, wherein the zero-trust security policy comprises the following:

verifying a source for data to be written to the data pool; and

admitting data whose source is verified, wherein the admitted data is labeled with a source label.

9. The system according to claim 7, wherein the zero-trust security policy comprises the following:

verifying a source and a role of a data writing party for data to be written to the data pool; and

admitting data whose source and role of a data writing party are verified, wherein the admitted data is labeled with a source label and a role label of the data writing party.

10. The system according to claim 6, wherein the data isolation module is further configured to isolate the data into the multiple data domains by sensitive data and runtime data.

11. The system according to claim 6, wherein corresponding protection levels are set for the multiple data domains.

12. A computer-readable storage medium that stores an instruction, wherein when the instruction is executed, a machine is enabled to perform the method according to any one of claims 1 to 5.