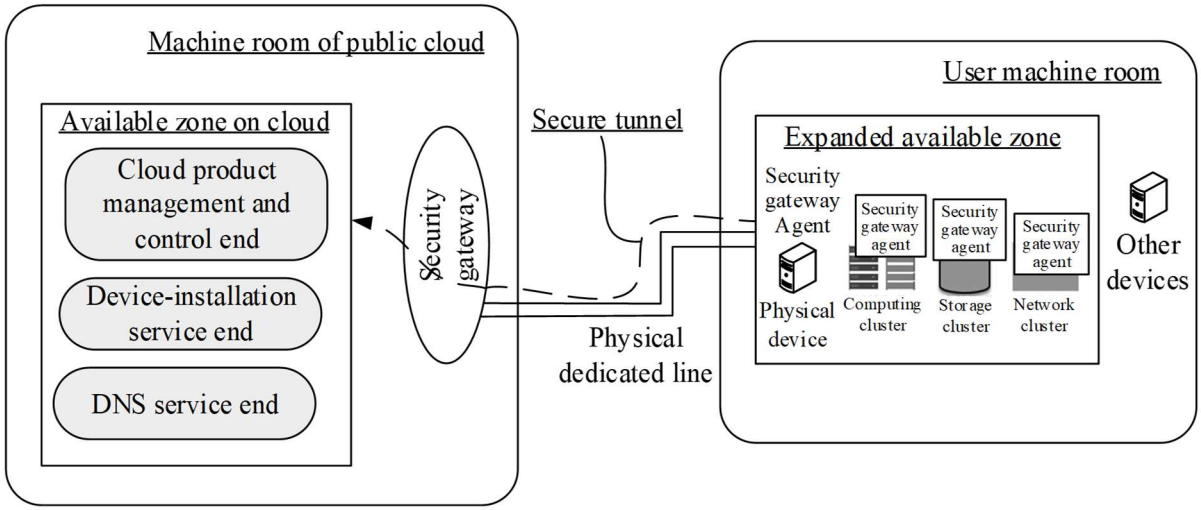

Machine room of public cloud
Available zone on cloud
Cloud product management and control end
Device-installation service end
DNS service end
Security gateway
Secure tunnel
Physical dedicated line
User machine room
Expanded available zone
Security gateway Agent
Physical device
Security gateway agent
Computing cluster
Security gateway agent
Storage cluster
Security gateway agent
Network cluster
Other devices

FIG. 1

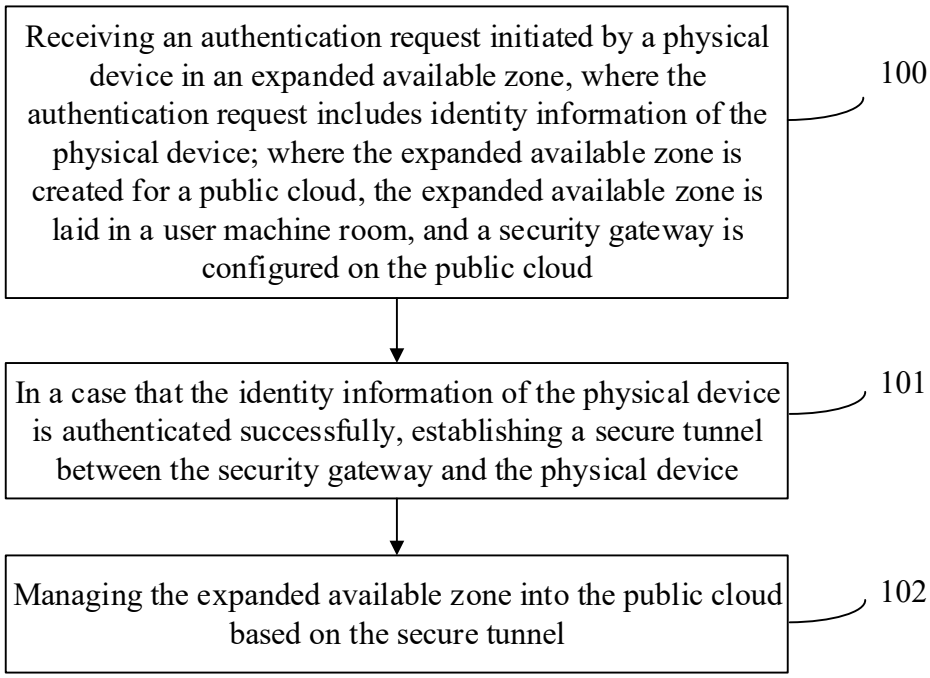

Receiving an authentication request initiated by a physical device in an expanded available zone, where the authentication request includes identity information of the physical device; where the expanded available zone is created for a public cloud, the expanded available zone is laid in a user machine room, and a security gateway is configured on the public cloud
100
In a case that the identity information of the physical device is authenticated successfully, establishing a secure tunnel between the security gateway and the physical device
101
Managing the expanded available zone into the public cloud based on the secure tunnel
102

FIG. 2

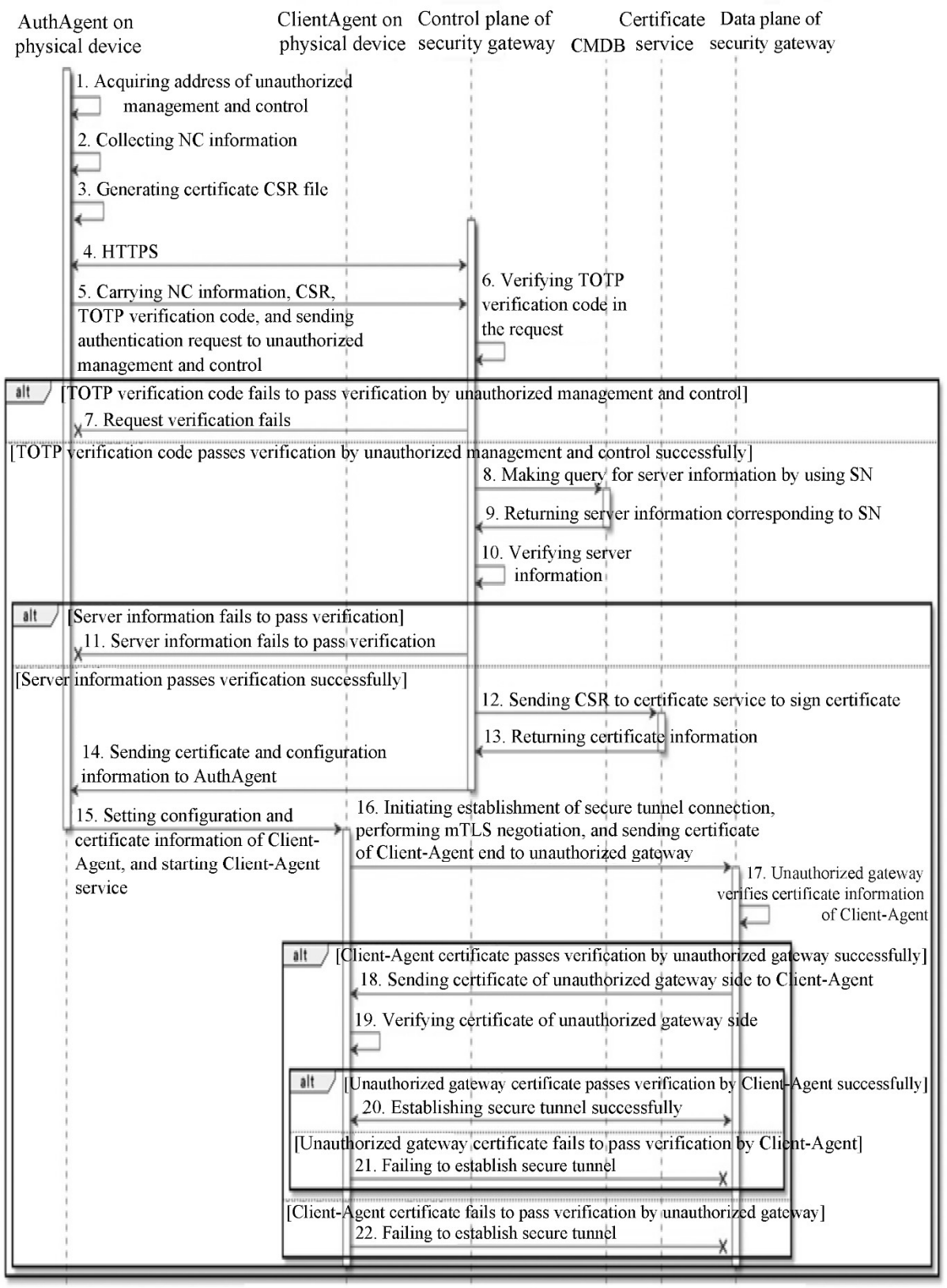

AuthAgent on physical device
ClientAgent on physical device
Control plane of security gateway
Certificate CMDB service
Data plane of security gateway
1. Acquiring address of unauthorized management and control
2. Collecting NC information
3. Generating certificate CSR file
4. HTTPS
5. Carrying NC information, CSR, TOTP verification code, and sending authentication request to unauthorized management and control
6. Verifying TOTP verification code in the request
alt
[TOTP verification code fails to pass verification by unauthorized management and control]
7. Request verification fails
[TOTP verification code passes verification by unauthorized management and control successfully]
8. Making query for server information by using SN
9. Returning server information corresponding to SN
10. Verifying server information
alt
[Server information fails to pass verification]
11. Server information fails to pass verification
[Server information passes verification successfully]
12. Sending CSR to certificate service to sign certificate
13. Returning certificate information
14. Sending certificate and configuration information to AuthAgent
15. Setting configuration and certificate information of Client-Agent, and starting Client-Agent service
16. Initiating establishment of secure tunnel connection, performing mTLS negotiation, and sending certificate of Client-Agent end to unauthorized gateway
17. Unauthorized gateway verifies certificate information of Client-Agent
alt
[Client-Agent certificate passes verification by unauthorized gateway successfully]
18. Sending certificate of unauthorized gateway side to Client-Agent
19. Verifying certificate of unauthorized gateway side
alt
[Unauthorized gateway certificate passes verification by Client-Agent successfully]
20. Establishing secure tunnel successfully
[Unauthorized gateway certificate fails to pass verification by Client-Agent]
21. Failing to establish secure tunnel
[Client-Agent certificate fails to pass verification by unauthorized gateway]
22. Failing to establish secure tunnel

FIG. 3

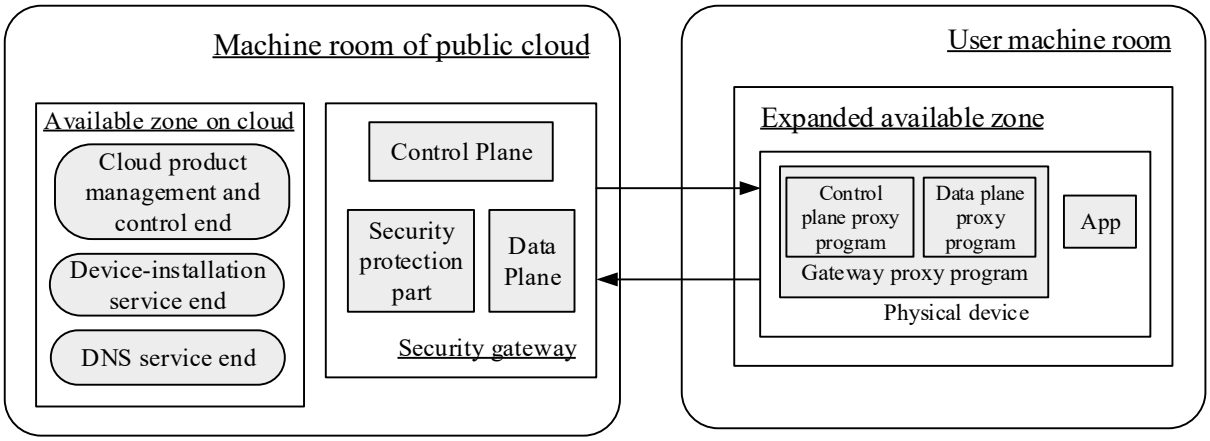

Machine room of public cloud
Available zone on cloud
Cloud product management and control end
Device-installation service end
DNS service end
Control Plane
Security protection part
Data Plane
Security gateway
User machine room
Expanded available zone
Control plane proxy program
Data plane proxy program
App
Gateway proxy program
Physical device

FIG. 4

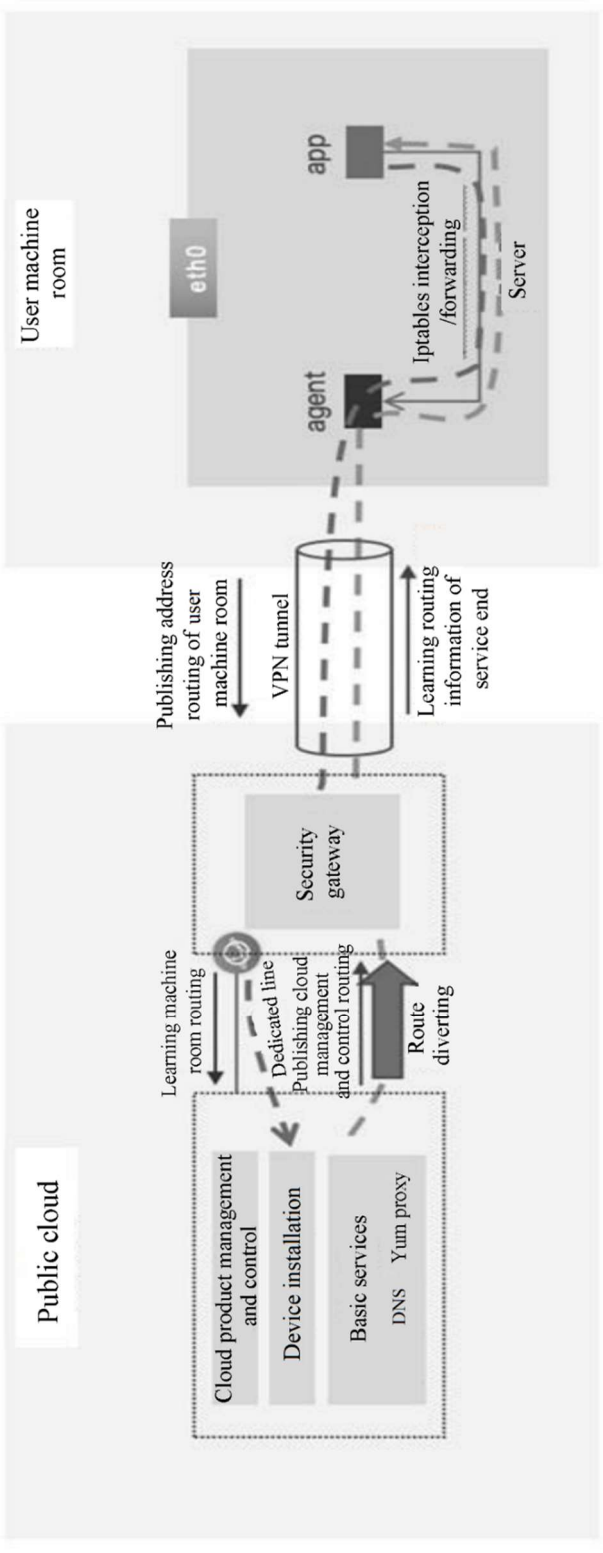

User machine room
eth0
app
agent
Iptables interception /forwarding
Server
Publishing address routing of user machine room
VPN tunnel
Learning routing information of service end
Public cloud
Security gateway
Learning machine room routing
Dedicated line
Publishing cloud management and control routing
Route diverting
Cloud product management and control
Device installation
Basic services
DNS
Yum proxy

FIG. 5

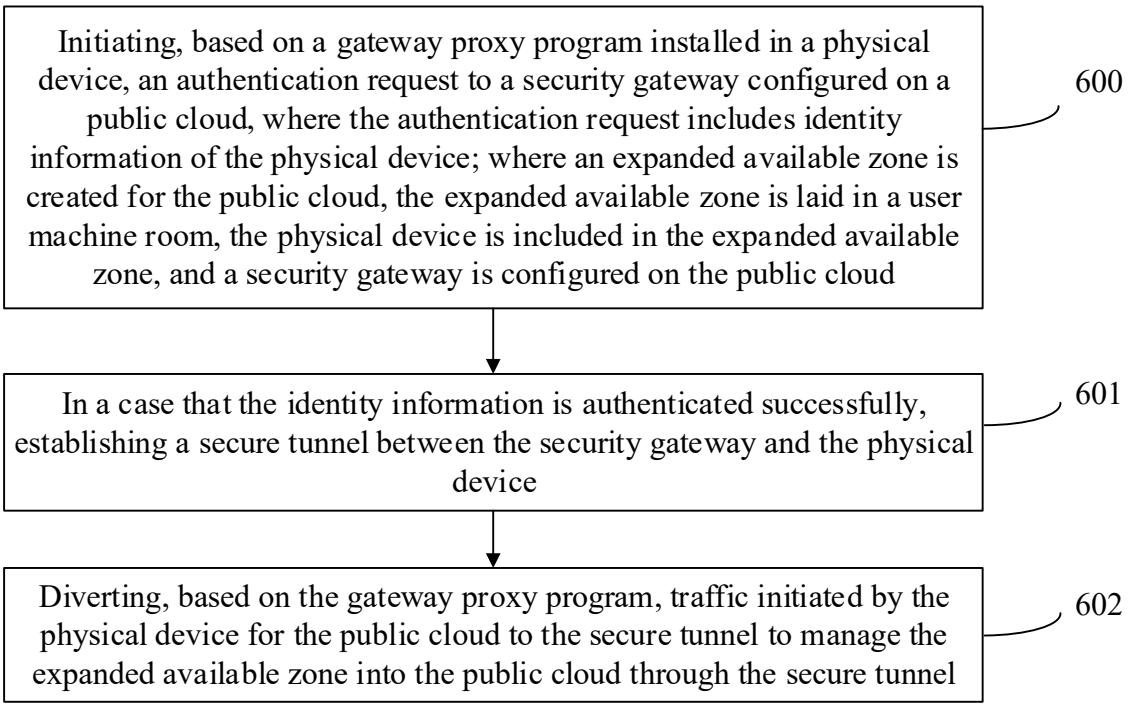

Initiating, based on a gateway proxy program installed in a physical device, an authentication request to a security gateway configured on a public cloud, where the authentication request includes identity information of the physical device; where an expanded available zone is created for the public cloud, the expanded available zone is laid in a user machine room, the physical device is included in the expanded available zone, and a security gateway is configured on the public cloud
600
In a case that the identity information is authenticated successfully, establishing a secure tunnel between the security gateway and the physical device
601
Diverting, based on the gateway proxy program, traffic initiated by the physical device for the public cloud to the secure tunnel to manage the expanded available zone into the public cloud through the secure tunnel
602

FIG. 6

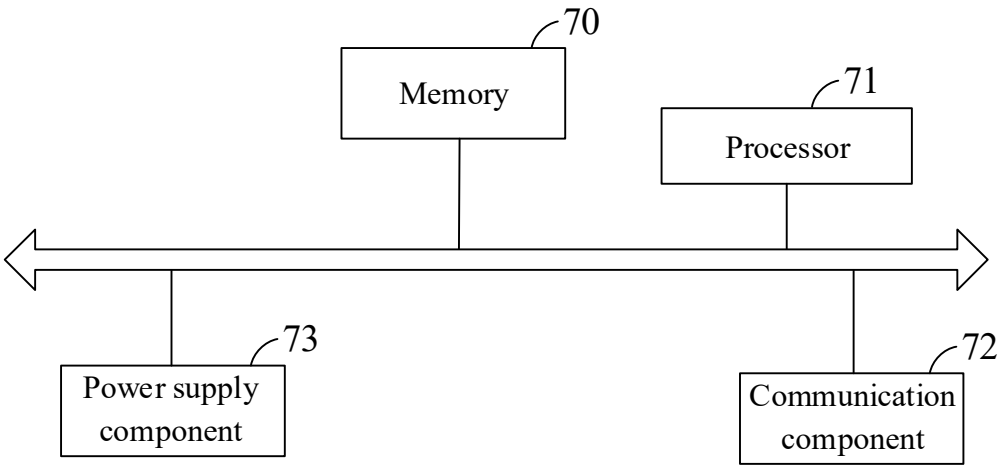

70
Memory
71
Processor
73
Power supply component
72
Communication component

FIG. 7

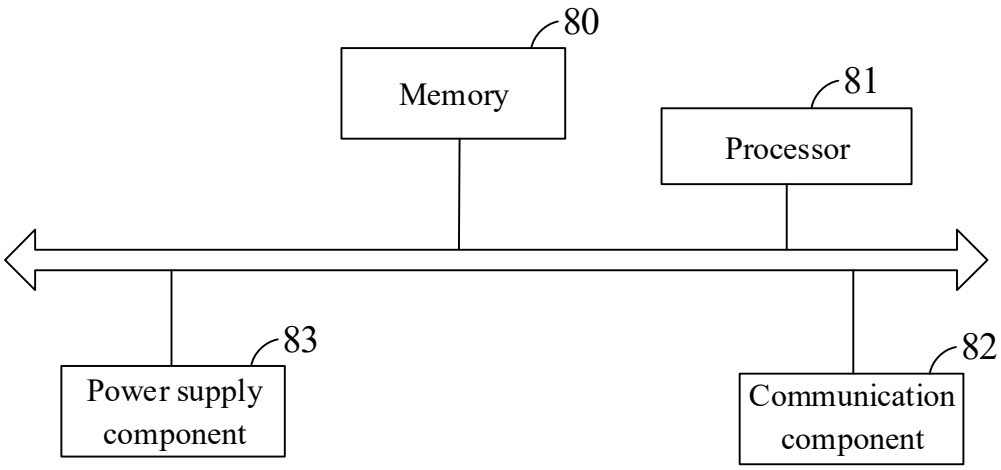

80
Memory
81
Processor
83
Power supply component
82
Communication component

FIG. 8

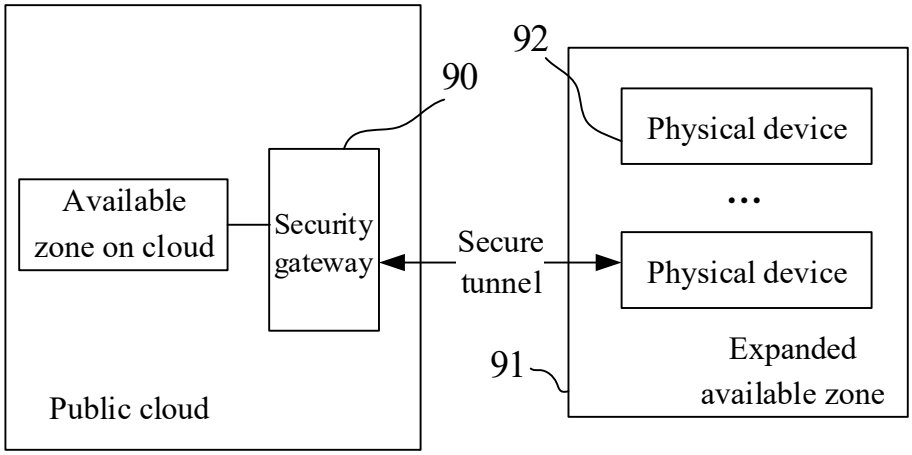

92
90
Physical device
Available zone on cloud
Security gateway
Secure tunnel
Physical device
91
Expanded available zone
Public cloud

FIG. 9