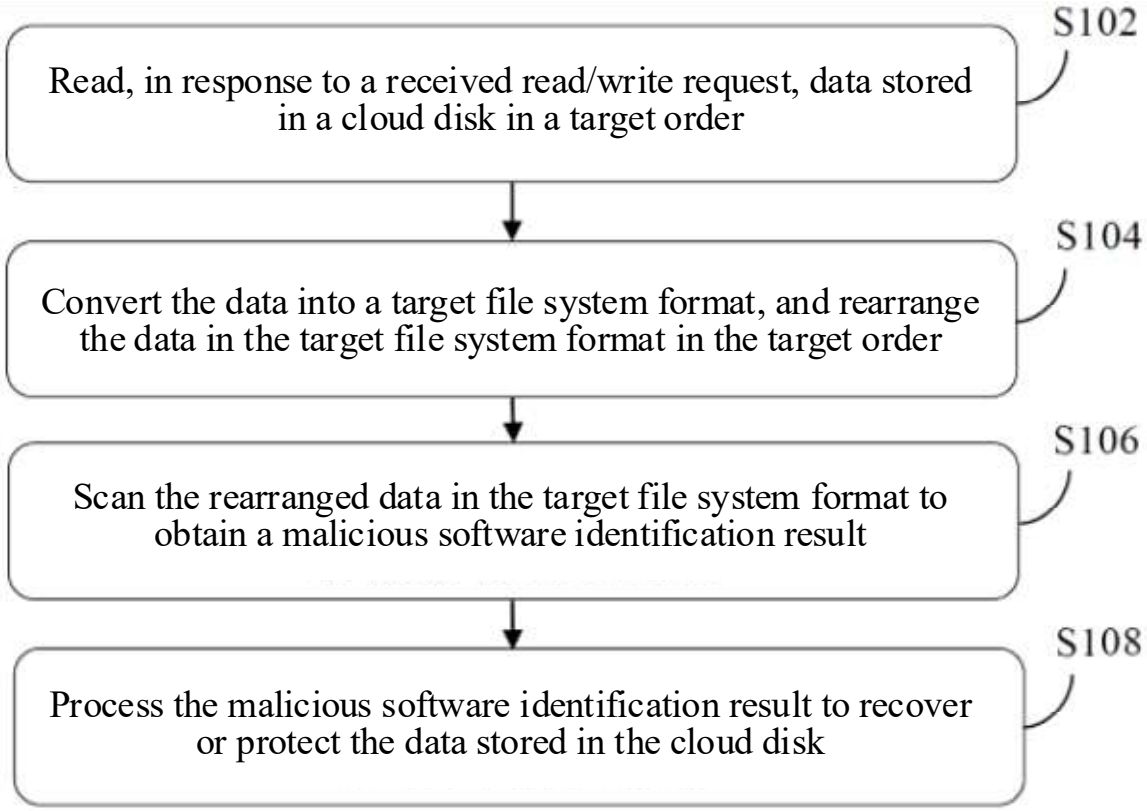

S102
Read, in response to a received read/write request, data stored in a cloud disk in a target order
S104
Convert the data into a target file system format, and rearrange the data in the target file system format in the target order
S106
Scan the rearranged data in the target file system format to obtain a malicious software identification result
S108
Process the malicious software identification result to recover or protect the data stored in the cloud disk

FIG. 1

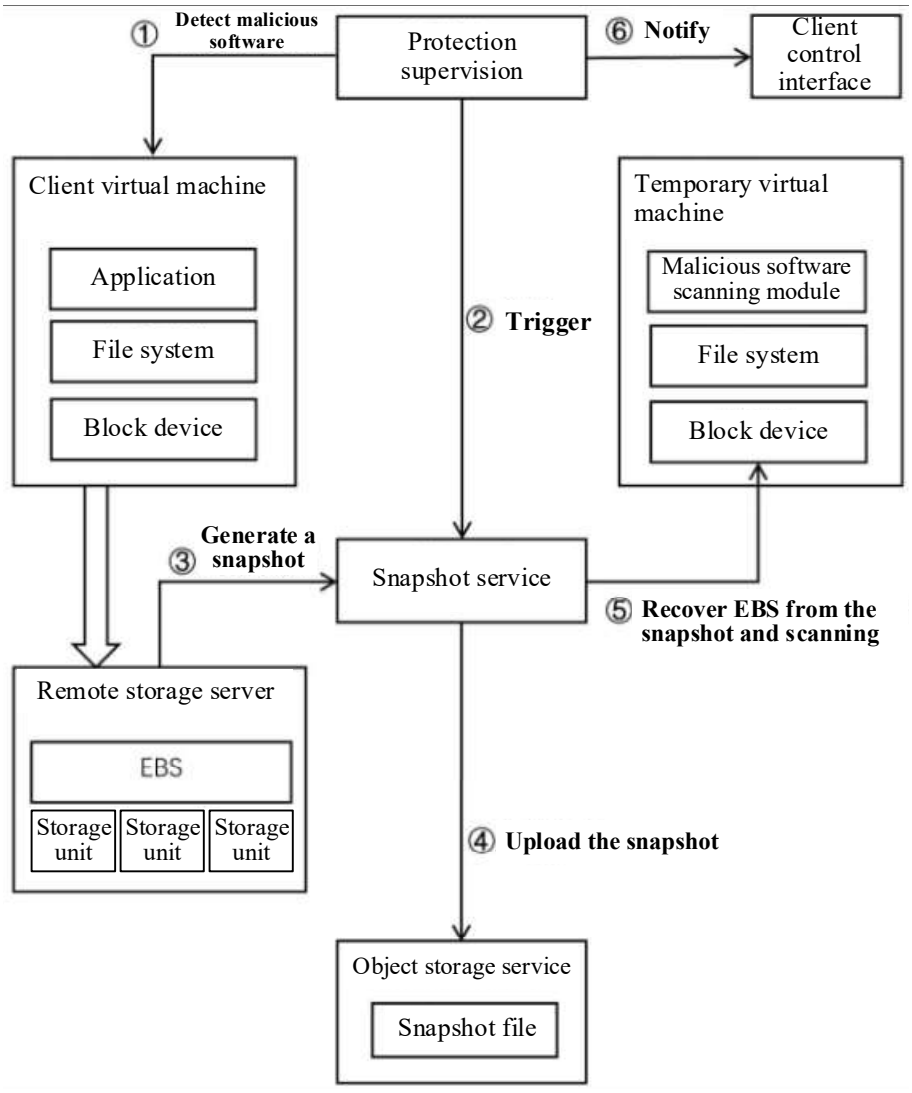


FIG. 2

Rule 91,
08.05.2024

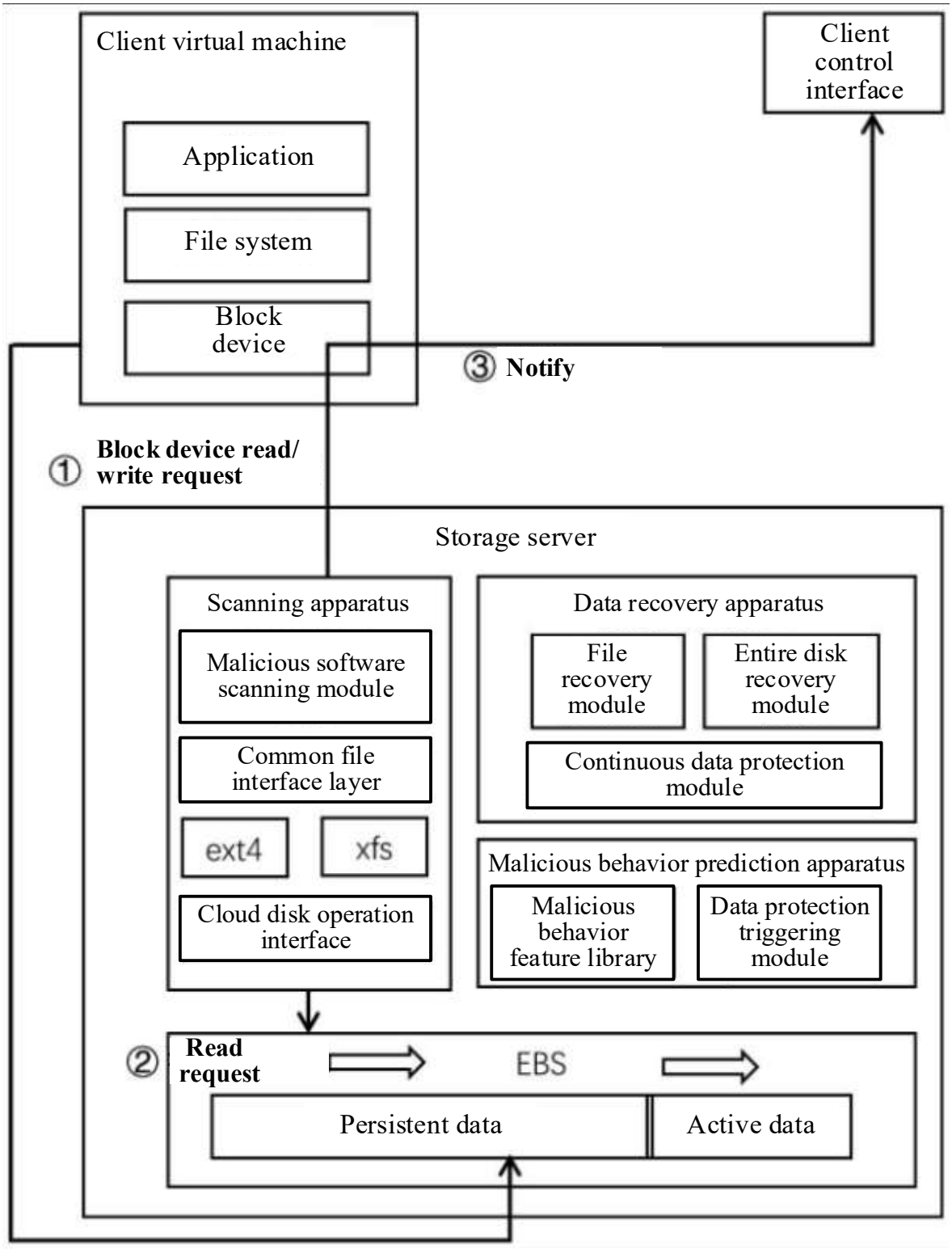

Client virtual machine
Application
File system
Block device
Client control interface
③ Notify
① Block device read/ write request
Storage server
Scanning apparatus
Malicious software scanning module
Common file interface layer
ext4
xfs
Cloud disk operation interface
Data recovery apparatus
File recovery module
Entire disk recovery module
Continuous data protection module
Malicious behavior prediction apparatus
Malicious behavior feature library
Data protection triggering module
② Read request
EBS
Persistent data
Active data

FIG. 3

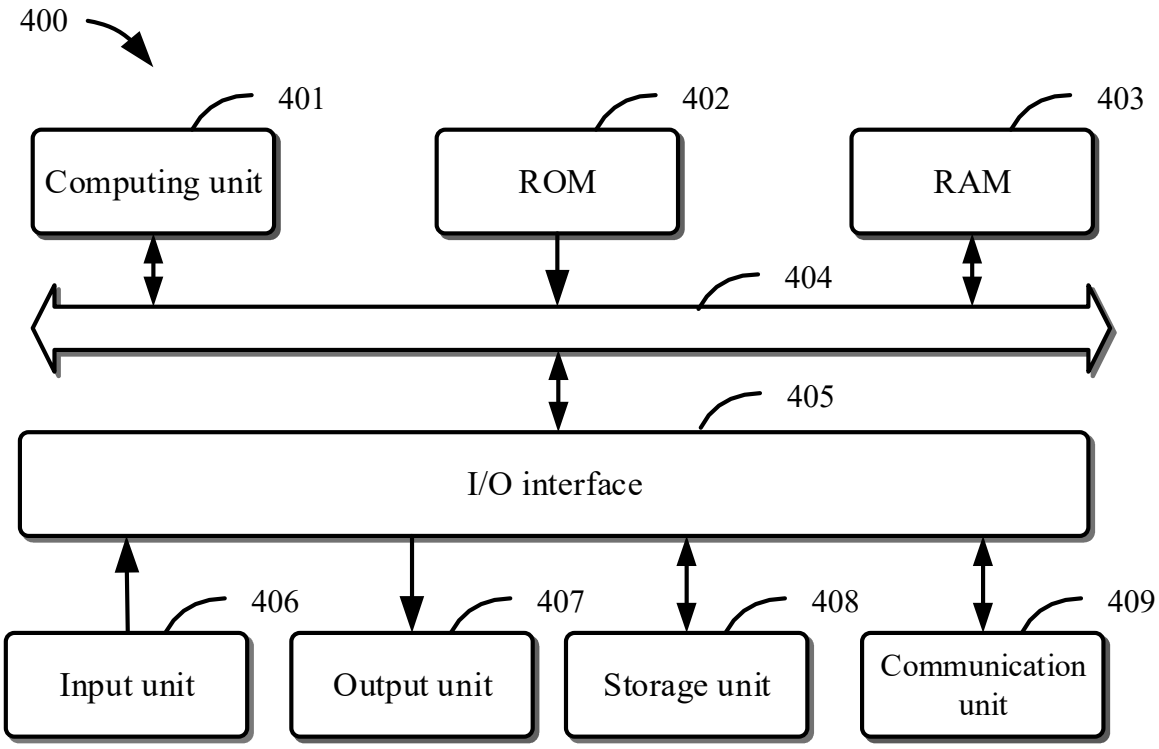

400
401
Computing unit
402
ROM
403
RAM
404
405
I/O interface
406
Input unit
407
Output unit
408
Storage unit
409
Communication unit

FIG. 4

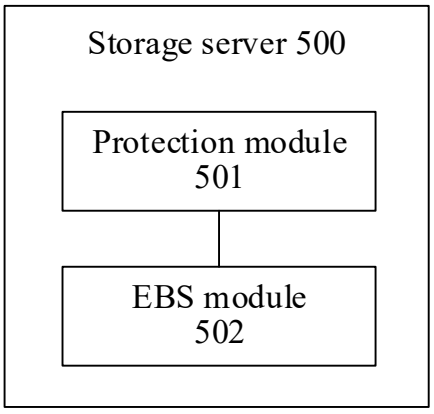

Storage server 500
Protection module 501
EBS module 502

FIG. 5