What is claimed is:

1. A data security protection method, wherein the method is applied to a protection module disposed at a target device, the target device is a storage device or an intermediate device, and the intermediate device is used for connecting a computer device with the storage device, wherein the method comprises:
sending split disk capacity parameters of a target split disk in the storage device to the computer device in response to a capacity reading instruction of the computer device, so that the computer device only identifies the target split disk, wherein the target split disk is a split disk selected based on the target device or selected based on other devices communicating with the target device;
modifying operation addresses corresponding to a data interaction instruction to target sector addresses corresponding to the split disk capacity parameters of the target split disk in response to the data interaction instruction sent by the computer device;
performing data read/write according to the target sector addresses.

2. The data security protection method of claim 1, wherein before sending split disk capacity parameters of a target split disk in the storage device to the computer device in response to a capacity reading instruction of the computer device, the method further comprises:
selecting a split disk as the target split disk in response to a user's selection operation through an interaction device on the target device; or
taking a split disk indicated by a split disk selection instruction as the target split disk in response to the split disk selection instruction sent by a specifying device, wherein the specifying device communicates with the protection module through near-field communication or remote communication, and the specifying device is different from the computer device; or
taking a split disk indicated by a split disk selection instruction as the target split disk in response to a split disk selection instruction sent by the computer device; or
taking a split disk corresponding to password information in a verification instruction as the target split disk in response to the verification instruction sent by the computer device.

3. The data security protection method of claim 1, wherein the target split disk does not overlap with sector addresses of other split disks in the storage device.

4. The data security protection method of claim 1, wherein before sending split disk capacity parameters of a target split disk in the storage device to the computer device in response to a capacity reading instruction of the computer device, the method further comprises:
splitting the sector address range of the storage device to obtain a plurality of split disks based on a preset disk splitting strategy, wherein the target disk is one of the plurality of split disks, and the preset disk splitting strategy comprises a preset quantity of split disks or preset sector addresses of split disks.

5. The data security protection method of claim 4, wherein splitting the sector address range of the storage device to obtain a plurality of split disks based on a preset disk splitting strategy comprises:

reading basic information of and storage space of the storage device, and dividing the sector address range to obtaining a plurality of split disks based on the preset disk splitting strategy and the basic information, wherein the basic information comprises a total number of sectors and a number of bytes per sector; or

generating at least one image file in the storage space of the storage device, and dividing the storage space of the storage device to obtain a plurality of split disks according to the address ranges respectively corresponding to the image file, wherein the storage space comprises one or more of local storage space based on the storage device and storage space networked with the protection module.

6. The data security protection method of claim 1, wherein the data interaction instruction is an instruction based on the SCSI transmission protocol or the UFI command block protocol, and instruction parameters of the data interaction instruction comprise instruction read-write type, or instruction read-write address, or read-write status of the storage device, or total number of formattable blocks, or the last logical block address, or the number of single-sector bytes, or the maximum number of logical units, or device information.

7. The data security protection method of claim 1, further comprises:

sending a target hardware characteristic parameter to the computer device in response to a hardware characteristic parameter request instruction sent by the computer device, wherein the hardware characteristic parameter comprises a vendor identification, or a device identification, or a device attribute, or a class used by an interface, or an endpoint attribute, or a transmission rate, or an electrical demand, or other hardware characteristic parameters expressed with character string other than the above hardware characteristic parameters, and the hardware characteristic parameters corresponding to different split disks are different.

8. The data security protection method of claim 1, further comprises:

modifying operation addresses corresponding to the sector read/write instruction to target sector addresses in the split disk capacity parameters of a target file in response to the sector read/write instruction corresponding to the target file sent by the computer device, and performing data read/write according to the target sector address.

9. The data security protection method of any one of claims 1 to 8, wherein modifying operation addresses corresponding to the sector read/write instruction to target sector addresses in the split disk capacity parameters of a target file in response to the sector read/write instruction corresponding to the target file sent by the computer device comprises:

judging whether the operation address corresponding to the data interaction instruction conforms to access control rules in response to the data interaction instruction sent by the computer device;

modifying the operation addresses to the target sector addresses in the target split disk if the operation address corresponding to the data interaction instruction conforms to the access control rules.

10. The data security protection method of any one of claims 1 to 8, wherein performing data read/write according to the target sector address comprises:

forwarding the data interaction instruction after modifying the operation addresses to the target sector addresses to the storage device, and receiving data corresponding to the target sector addresses returned by the storage device,

and returning the read data, read status or write status to the computer device; or
forwarding the data interaction instruction after modifying the operation addresses to the target sector addresses to the storage device, and receiving data corresponding to the target sector addresses returned by the storage device, and modifying data of the target sector addresses according to content modification rules, and returning the read data, read status or write status to the computer device.

11. The data security protection method of any one of claims 1 to 8, further comprises:
in read-only mode, returning read-only status parameter of the storage device to the computer device if the data interaction instruction is a parameter reading request, and not responding to the data interaction instruction if the data interaction instruction is a write instruction; or
in specific file mode, the data interaction instruction is an instruction for at least one specific file in the storage device, and the operation type of the instruction is a read type, a write type, or a read and write type; or
in blank file mode, the data interaction instruction is an instruction for at least one blank file automatically created and/or manually created in the storage device, and the operation type of the instruction is a write type or a read and write type; or
in sector limited mode: the data source specified in the sector limited mode is at least one specific sector range in the storage device, and the specified operation type is a read type, a write type, or a read-write type.
file type restriction mode, the data interaction instruction is an instruction for at least one specific type of file in the storage device, and the operation type of the instruction is a read type, a write type, or a read and write type; or
in encryption write mode, the data interaction instruction is an instruction for data in at least one first sector range in the storage device, and the operation type of the instruction is a write type, or a read and write type; or
in decryption readout mode, the data interaction instruction is an instruction for data in at least one second sector range in the storage device, at least one second file, and/or at least one type of file, and the operation type of the instruction is a read type;
in manual confirmation mode, the data interaction instruction is an instruction for data in at least one third sector range in the storage device, at least one third file and/or at least one type of file, and the operation type of the instruction is a read and write type; or
in logical split disk mode, the data interaction instruction is an instruction for at least one split disk in the storage device, and the operation type of the instruction is a read type, a write type, or a read and write type.

12. A data security protection method, wherein the method is applied to server-side connected communicatively with target device that is provided with protection module, the target device is a networked storage device or an intermediate device, and the intermediate device is connected communicatively with a computer device, wherein the method comprises:
sending split disk capacity parameters of a target split disk in the server-side to the computer device in response to a capacity reading instruction of the computer device, so that the computer device only identifies the target split disk, wherein the target split disk is a split disk selected based on the target device or selected based on other devices communicating with the target device;
performing read/write on the target sector addresses in response to the data interaction instruction forwarded by the target device; the target sector address is a target sector address corresponding to the target disk capacity parameter

that is modified by modifying the operation address corresponding to the data interaction instruction based on the data interaction instruction sent by the computer device.

13. The data security protection method of claim 12, wherein before sending split disk capacity parameters of a target split disk in the server-side to the computer device, the method further comprises:
determining all split disks corresponding to the target device according to the identification information of the target device, and all the split disks are used for the target device or other devices communicating with the target device to select the target split disk.

14. A intermediate device, comprising:
a first port for connecting a computer device;
a second port for connecting a storage device;
a protection module which is connected between the first port and the second port and is used for implementing the steps of the data security protection method of any one of the above claims 1 to 11.

15. The intermediate device of claim 14, further comprises:
a communication component, which is connected with the protection module, and is used for networking so as to connect the protection module with the storage module on the cloud or server side, and when responding to the data interaction instruction, sending the data interaction instruction to the storage module on the network side, so that the storage module reads and/or writes corresponding data based on the data interaction instruction.

16. A device system, comprising:
a computer device;
a storage device; and
an intermediate device of claim 14 or 15.

17. A storage device, comprising:
a first port for connecting a computer device;
a protection chip for implementing the steps of the data security protection method of the data security protection method of any one of the above claims 1 to 11;
a control chip connected with the first port through the protection chip;
a storage chip connected with the control chip, which is used for performing storage management on data in storage space under the control of the control chip.

18. A storage device, comprising:
a first port for connecting a computer device;
a control chip on which a protection module is deployed for implementing the steps of the data security protection method of any one of the above claims 1 to 11;
a storage chip connected with the first port through the control chip, which is used for performing storage management on data in storage space under the control of the control chip.

19. A storage device, comprising:
a first port for connecting a computer device;
a control chip connected with a first port, which is used for generating corresponding control instructions based on the data interaction instructions sent by the computer device;
a storage chip connected with the control chip;
wherein, a protection module is deployed on the storage chip for processing control instructions sent by the control chip by adopting the steps of the data security protection method of any one of the above claims 1 to 11.

20. A server-side, comprising:
a first port for connecting a target device, wherein the target device is a networked storage device or an intermediate device;
a control chip connected with a first port, which is used for generating corresponding control instructions based on the data interaction instructions forwarded by the target device;
a storage chip connected with the control chip;
wherein, the storage chip is used for processing control instructions sent by the control chip by adopting the steps of the data security protection method of the above claim 12 or 13.

21. A computer-readable storage medium, on which a computer program is stored, and the steps in the data security protection method of any one of claims 1 to 13 are implemented when the computer program is executed by a processor.