

METHOD OF PERFORMING SMART HYBRID ACCELERATION ON RESOURCES, DEVICE, MEDIUM AND APPARATUS

The present application claims priority to Chinese Patent Application No. 201710081627.8 filed to the China National Intellectual Property Administration on February 15, 2017 and entitled "METHOD AND DEVICE FOR PERFORMING SMART HYBRID ACCELERATION ON RESOURCES HAVING DIFFERENT SECURITY LEVELS", the disclosure of which is hereby incorporated by reference in its entirety.

Technical Field of the present invention

Embodiments of the present invention relate to but not limited to the communication field, and in particular to a method, device, medium and apparatus for performing smart hybrid acceleration on resources.

Background of the present invention

One of the challenges brought to the Content Delivery Network (CDN for short) by the security-oriented HTTP channel (Hyper Text Transfer Protocol over Secure Socket Layer, HTTPS) is how to cope with a huge increase in CPU load, particularly for the load on small files. This is because the Queries Per Second (QPS for short) of the small files is higher under the same bandwidth. The cost for acceleration by a hardware scheme (e.g., an acceleration card) is very high, but the requirements for performance cannot be satisfied by a pure software scheme (e.g., by CPU computation). A CDN server provides a variety of services. Since it is required to accelerate static resources, dynamic resource and the like, the resources having different security levels cannot be processed by the same standard. However, in most existing methods, a same HTTPS scheme is used for any type of resources. Consequently, an expensive hardware acceleration scheme is still used for resources having a lower security level. Apparently, it is unable to realize high cost performance.

Summary of the present invention

The following provides a general summary of the theme described in detail herein. The general summary is not intended to limit the protection scope of the appended claims.

In order to solve the above technical problem, the embodiments of the present invention provide a method, device, medium and apparatus for performing smart hybrid acceleration on resources.

An embodiment of the present invention provides a method for performing smart hybrid acceleration on resources, comprising steps of:

receiving a handshake request from a client terminal; determining whether the handshake request contains a self-defined resource extension field; if the handshake request does not contain any self-defined resource extension field, acquiring a target domain name to be connected by the client terminal in the handshake request, and determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; and, if the handshake request contains a self-defined resource extension field, determining, according to content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal, and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method.

The method for performing smart hybrid acceleration on resources is further featured by: the step of determining whether the handshake request contains a self-defined resource extension field comprises: determining whether a client hello message of the handshake request contains the self-defined resource extension field.

The method for performing smart hybrid acceleration on resources is further featured by: the step of determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises: performing acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and performing acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level; and

the step of determining, according to content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises:

in a case where the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when the resource level is a high security level, and performing acceleration processing by a software acceleration method when the resource level is a low security level;

or, in a case where the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when it is determined according to the resource type that the corresponding resource level is a high security level, and performing acceleration processing by a software acceleration method when it is determined according to the resource type that the corresponding resource level is a low security level, wherein the resource type includes a static resource type or a dynamic resource type.

An embodiment of the present invention provides a method for performing smart hybrid acceleration on resources, comprising steps of:

receiving a handshake request from a client terminal, acquiring, from the handshake request, a target domain name to be connected by the client terminal in the handshake request, and determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method;

or, receiving a handshake request from a client terminal, acquiring, from the handshake request, content in a self-defined resource extension field, determining, according to the content, a resource level of a resource accessed by the client terminal, and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method.

The method for performing smart hybrid acceleration on resources is further featured by:

the step of determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises:

performing acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and performing acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level; and

the step of determining, according to the content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises:

in a case where the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when the resource level is a high security level, and performing acceleration processing by a software acceleration method when the resource level is a low security level;

or, in a case where the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when it is determined according to the resource type that the corresponding resource level is a high security level, and performing acceleration processing by a software acceleration method when it is determined according to the resource type that the corresponding resource level is a low security level.

An embodiment of the present invention provides a device for performing smart hybrid acceleration on resources having different security levels, comprising:

a receiving module, configured to receive a handshake request from a client terminal;

a determination module, configured to determine whether the handshake request contains a self-defined resource extension field;

a first processing module, configured to: when the determination module determines that the handshake request does not contain any self-defined resource extension field,

acquire a target domain name to be connected by the client terminal in the handshake request and determine, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; and

a second processing method, configured to: when the determination module determines that the handshake request contains a self-defined resource extension field, determine, according to content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal and determine, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method;

wherein the receiving module and the determination module are positioned in a front-end apparatus, and the first processing module and the second processing module are positioned in a Content Delivery Network server or a non-CDN server; or, the receiving module, the determination module, the first processing module and the second processing module are all positioned in a CDN server or a non-CDN server.

The device for performing smart hybrid acceleration on resources is further featured by: the determination module is further configured to determine, according to the determination whether a client hello message of the handshake request contains a self-defined resource extension field, whether the handshake request contains a self-defined resource extension field.

The device for performing smart hybrid acceleration on resources is further featured by: the first processing module is further configured to perform acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and perform acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level; and

the second processing module is further configured to: when the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined that the resource level is a high security level, and perform acceleration

processing by a software acceleration method after it is determined that the resource level is a low security level; and, when the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined according to the resource type that the corresponding resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined according to the resource type that the corresponding resource level is a low security level.

An embodiment of the present invention provides a device for performing smart hybrid acceleration on resources having different security levels, applied to a Content Delivery Network server or a non-CDN server, comprising:

- a receiving module, configured to receive a handshake request from a client terminal; and

- a processing module, configured to: acquire, from the handshake request, a target domain name to be connected by the client terminal in the handshake request, and determine, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; or, acquire, from the handshake request, content in a self-defined resource extension field, determine, according to the content, a resource level of a resource accessed by the client terminal, and determine, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method.

The device for performing smart hybrid acceleration on resources is further featured by:

- the processing module is configured to: perform acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and perform acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level; the processing module is further configured to: when the content in the self-defined resource extension field is a resource level of a resource accessed by the

client terminal, perform acceleration processing by a hardware acceleration method after it is determined that the resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined that the resource level is a low security level; and, the processing module is further configured to: when the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined according to the resource type that the corresponding resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined according to the resource type that the corresponding resource level is a low security level.

An embodiment of the present invention provides a computer-readable storage medium stored with computer programs that, when executed by a processor, implement the steps of the method described above.

An embodiment of the present invention provides a computer apparatus, including a memory, a processor and computer programs that are stored on the memory and can be run on the processor, the processor implementing the steps of the method described above.

In the embodiments of the present invention, different acceleration methods are used for resources having different security levels, and the saved computation capacity of an acceleration card is applied to resources having higher security requirements, so that the cost performance and the utilization efficiency of edge nodes of a CDN are improved.

Brief Description of the Drawings

The drawings described herein are used for providing further understanding of the embodiments of the present invention and constitute a part of the present application. Illustrative embodiments of the present invention and descriptions thereof are used for explaining the embodiments of the present invention, rather than constituting any inappropriate limitations to the embodiments of the present invention. In the drawings: Fig. 1 is a flowchart of a method for performing smart hybrid acceleration on resources having different security levels in Embodiment 1;

Fig. 2 is a flowchart of a method for performing smart hybrid acceleration on resources having different security levels in Embodiment 2;

Fig. 3 is a structural diagram of a device for performing smart hybrid acceleration on resources having different security levels in Embodiment 3; and

Fig. 4 is a structure diagram of a device for performing smart hybrid acceleration on resources having different security levels in Embodiment 4.

Detailed Description of the present invention

Now, the embodiments of the present invention will be further described by specific implementations with reference to the drawings.

In the embodiments of the present invention, when a server can be controlled by a client terminal, the client terminal is able to set a self-defined resource extension field in a handshake request; however, when a server is uncontrollable for a client terminal, the client terminal is unable to set a self-defined resource extension field in a handshake request.

Embodiment 1

Fig. 1 is a flowchart of a method for performing smart hybrid acceleration on resources having different security levels in Embodiment 1. The method comprises steps of: receiving a handshake request from a client terminal; determining whether the handshake request contains a self-defined resource extension field; if the handshake request does not contain any self-defined resource extension field, acquiring a target domain name to be connected by the client terminal in the handshake request, and determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; and, if the handshake request contains a self-defined resource extension field, determining, according to content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal, and determining, according to the resource level, whether the acceleration processing is performed by a hardware acceleration method or a software acceleration method.

Wherein:

the step of determining whether the handshake request contains a self-defined resource extension field comprises: determining whether a client hello message of the handshake request contains the self-defined resource extension field.

The step of determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises: performing acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and performing acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level.

The step of determining, according to content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises: in a case where the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when the resource level is a high security level, and performing acceleration processing by a software acceleration method when the resource level is a low security level; or, in a case where the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when it is determined according to the resource type that the corresponding resource level is a high security level, and performing acceleration processing by a software acceleration method when it is determined according to the resource type that the corresponding resource level is a low security level. The resource type includes a static resource type or a dynamic resource type, or further includes information such as application involved and resource address. The static resource type corresponds to a low security level, and the dynamic resource type corresponds to a high security level.

In this embodiment of the present invention, the software acceleration method includes, but not limited to: a multi-prime RSA acceleration method.

Embodiment 2

Fig. 2 is a flowchart of a method for performing smart hybrid acceleration on resource having different security levels in Embodiment 2. The method comprises steps of: receiving a handshake request from a client terminal, acquiring, from the handshake request, a target domain name to be connected by the client terminal in the handshake request, and determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; or, receiving a handshake request from a client terminal, acquiring, from the handshake request, content in a self-defined resource extension field, determining, according to the content, a resource level of a resource accessed by the client terminal, and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method.

Wherein:

the step of determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises: performing acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and performing acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level.

The step of determining, according to the content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises: in a case where the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when the resource level is a high security level, and performing acceleration processing by a software acceleration method when the

resource level is a low security level; or, in a case where the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when it is determined according to the resource type that the corresponding resource level is a high security level, and performing acceleration processing by a software acceleration method when it is determined according to the resource type that the corresponding resource level is a low security level.

Embodiment 3

Corresponding to the method in Embodiment 1, as shown in Fig. 3, a device for performing smart hybrid acceleration on resources having different security levels comprises:

- a receiving module, configured to receive a handshake request from a client terminal;
- a determination module, configured to determine whether the handshake request contains a self-defined resource extension field;
- a first processing module, configured to: when the determination module determines that the handshake request does not contain any self-defined resource extension field, acquire a target domain name to be connected by the client terminal in the handshake request and determine, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; and
- a second processing method, configured to: when the determination module determines that the handshake request contains a self-defined resource extension field, determine, according to content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal and determine, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method.

The receiving module and the determination module are positioned in a front-end apparatus, and the first processing module and the second processing module are position in a Content Delivery Network (CDN) server or a non-CDN server; or, the

receiving module, the determination module, the first processing module and the second processing module are all positioned in a CDN server or a non-CDN server.

The determination module is further configured to determine, according to the determination whether a client hello message of the handshake request contains a self-defined resource extension field, whether the handshake request contains a self-defined resource extension field.

The first processing module is further configured to perform acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and perform acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level.

The first processing module is further configured to: when the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined that the resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined that the resource level is a low security level; and, when the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined according to the resource type that the corresponding resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined according to the resource type that the corresponding resource level is a low security level.

Embodiment 4

Corresponding the method in Embodiment 2, as shown in Fig. 4, a device for performing smart hybrid acceleration on resources having different security levels comprises:

a receiving module, configured to receive a handshake request from a client terminal;
and

a processing module, configured to: acquire, from the handshake request, a target

domain name to be connected by the client terminal in the handshake request, and determine, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; or, acquire, from the handshake request, content in a self-defined resource extension field, determine, according to the content, a resource level of a resource accessed by the client terminal, and determine, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method.

The processing module is configured to: perform acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and perform acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level; the processing module is further configured to: when the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined that the resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined that the resource level is a low security level; and, the processing module is further configured to: when the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined according to the resource type that the corresponding resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined according to the resource type that the corresponding resource level is a low security level.

An embodiment of the present invention provides a computer-readable storage medium stored with computer programs that, when executed by a processor, implement the steps of the method described above.

An embodiment of the present invention provides a computer apparatus, including a memory, a processor and computer programs that are stored on the memory and can be run on the processor. When executing the computer programs, the processor

implements the steps of the method described above.

In the embodiments of the present invention, different acceleration methods are used for resources having different security levels, and the saved computation capacity of an acceleration card is applied to resources having higher security requirements, so that the cost performance and the utilization efficiency of edge nodes of a CDN are improved.

It should be understood by a person of ordinary skill in the art that, modifications or equivalent replacements may be made to the technical solutions in the embodiments of the present invention without departing from the spirit and scope of the technical solutions in the embodiments of the present invention, and these modifications or equivalent replacements shall fall into the scope of the appended claims.

It should be understood by a person of ordinary skill in the art that, all or some of steps in the methods disclosed herein and the functional modules/units in the systems and devices disclosed herein may be implemented as software, firmware, hardware and proper combinations thereof. In the hardware implementations, the division of the functional modules/units mentioned in the foregoing descriptions does not necessarily correspond to the division of the physical components. For example, one physical component may have a plurality of functions, or one function or step may be cooperatively executed by a plurality of physical components. Some components or all components may be implemented as software executed by a processor such as a digital signal processor or a microprocessor, or hardware, or integrated circuits such as application-specific integrated circuits. The software may be distributed on a computer-readable medium. The computer-readable medium may include a computer storage medium (or a non-temporary medium) and a communication medium (or a temporary medium). As known to a person of ordinary skill in the art, the computer storage medium includes volatile and nonvolatile, removable and non-removable mediums implemented in any method or technology for storing information (such as computer-readable instructions, data structures, program modules or other data). The computer storage medium includes, but not limited to: RAM, ROM, EEPROM, a flash memory or other memory technologies, CN-ROM, a Digital Versatile Disc (DVD) or other optical disc storages, a magnetic cassette, a magnetic tape, a magnetic disc memory or

other magnetic storage devices, or any other medium that may be used for storing desirable information and may be accessed by a computer. In addition, as known to a person of ordinary skill in the art, the communication medium typically includes computer-readable instructions, data structures, program modules or other data such as carriers or modulation data signals in other transmission mechanisms, and may include any information delivery medium.

INDUSTRIAL APPLICABILITY

In this disclosure, different acceleration methods are used for resources having different security levels, and the saved computation capacity of an acceleration card is applied to resources having higher security requirements, so that the cost performance and the utilization efficiency of edge nodes of a CDN are improved.

CLAIMS

1. A method for performing smart hybrid acceleration on resources having different security levels, comprising steps of:

receiving a handshake request from a client terminal; determining whether the handshake request contains a self-defined resource extension field; if the handshake request does not contain any self-defined resource extension field, acquiring a target domain name to be connected by the client terminal in the handshake request, and determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; and, if the handshake request contains a self-defined resource extension field, determining, according to content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal, and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method.

2. The method for performing smart hybrid acceleration on resources having different security levels according to claim 1, wherein:

the step of determining whether the handshake request contains a self-defined resource extension field comprises: determining whether a client hello message of the handshake request contains the self-defined resource extension field.

3. The method for performing smart hybrid acceleration on resources having different security levels according to claim 1, wherein:

the step of determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises: performing acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and performing acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level; and

the step of determining, according to content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal and determining,

according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises:

in a case where the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when the resource level is a high security level, and performing acceleration processing by a software acceleration method when the resource level is a low security level;

or, in a case where the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when it is determined according to the resource type that the corresponding resource level is a high security level, and performing acceleration processing by a software acceleration method when it is determined according to the resource type that the corresponding resource level is a low security level, wherein the resource type comprises a static resource type or a dynamic resource type.

4. A method for performing smart hybrid acceleration on resources having different security levels, comprising steps of:

receiving a handshake request from a client terminal, acquiring, from the handshake request, a target domain name to be connected by the client terminal in the handshake request, and determining, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method;

or, receiving a handshake request from a client terminal, acquiring, from the handshake request, content in a self-defined resource extension field, determining, according to the content, a resource level of a resource accessed by the client terminal, and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method.

5. The method for performing smart hybrid acceleration on resources having different security levels according to claim 1, wherein:

The step of determining, according to a level of the target domain name, whether

acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises:

performing acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and performing acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level; and

the step of determining, according to the content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal and determining, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method comprises:

in a case where the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when the resource level is a high security level, and performing acceleration processing by a software acceleration method when the resource level is a low security level;

or, in a case where the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, performing acceleration processing by a hardware acceleration method when it is determined according to the resource type that the corresponding resource level is a high security level, and performing acceleration processing by a software acceleration method when it is determined according to the resource type that the corresponding resource level is a low security level.

6. A device for performing smart hybrid acceleration on resources having different security levels, comprising:

a receiving module, configured to receive a handshake request from a client terminal;

a determination module, configured to determine whether the handshake request contains a self-defined resource extension field;

a first processing module, configured to: when the determination module determines

that the handshake request does not contain any self-defined resource extension field, acquire a target domain name to be connected by the client terminal in the handshake request and determine, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; and

a second processing method, configured to: when the determination module determines that the handshake request contains a self-defined resource extension field, determine, according to content in the self-defined resource extension field, a resource level of a resource accessed by the client terminal and determine, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method;

wherein the receiving module and the determination module are positioned in a front-end apparatus, and the first processing module and the second processing module are positioned in a Content Delivery Network server or a non-CDN server; or, the receiving module, the determination module, the first processing module and the second processing module are all positioned in a CDN server or a non-CDN server.

7. The device for performing smart hybrid acceleration on resources having different security levels according to claim 6, wherein:

the determination module is further configured to determine, according to the determination whether a client hello message of the handshake request contains a self-defined resource extension field, whether the handshake request contains a self-defined resource extension field.

8. The device for performing smart hybrid acceleration on resources having different security levels according to claim 6, wherein:

the first processing module is further configured to perform acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and perform acceleration processing by a software acceleration method when it is determined that the level of the target domain name is a low security level; and

the second processing module is further configured to: when the content in the

self-defined resource extension field is a resource level of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined that the resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined that the resource level is a low security level; and, when the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined according to the resource type that the corresponding resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined according to the resource type that the corresponding resource level is a low security level.

9. A device for performing smart hybrid acceleration on resources having different security levels, applied to a Content Delivery Network server or a non-CDN server, comprising:

a receiving module, configured to receive a handshake request from a client terminal; and

a processing module, configured to: acquire, from the handshake request, a target domain name to be connected by the client terminal in the handshake request, and determine, according to a level of the target domain name, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method; or, acquire, from the handshake request, content in a self-defined resource extension field, determine, according to the content, a resource level of a resource accessed by the client terminal, and determine, according to the resource level, whether acceleration processing is performed by a hardware acceleration method or a software acceleration method.

10. The device for performing smart hybrid acceleration on resources having different security levels according to claim 1, wherein:

the processing module is configured to: perform acceleration processing by a hardware acceleration method when it is determined that the level of the target domain name is a high security level, and perform acceleration processing by a software

acceleration method when it is determined that the level of the target domain name is a low security level; the processing module is further configured to: when the content in the self-defined resource extension field is a resource level of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined that the resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined that the resource level is a low security level; and, the processing module is further configured to: when the content in the self-defined resource extension field is a resource type of a resource accessed by the client terminal, perform acceleration processing by a hardware acceleration method after it is determined according to the resource type that the corresponding resource level is a high security level, and perform acceleration processing by a software acceleration method after it is determined according to the resource type that the corresponding resource level is a low security level.

11. A computer-readable storage medium stored with computer programs that, when executed by a processor, implement the steps of the method according to any one of claims 1 to 3 and/or any one of claims 4 to 5.

12. A computer apparatus, comprising a memory, a processor and computer programs that are stored on the memory and can be run on the processor, the processor implementing the steps of the method according to any one of claims 1 to 3 and/or any one of claims 4 to 5 when executing the computer programs.