

METHOD, SYSTEM, DEVICE, MEDIUM AND DEVICE FOR CDN INTER-NODE ENCRYPTION

The present application claims priority to Chinese Patent Application No. 201710069825.2 filed to China National Intellectual Property Administration on February 8, 2017 and entitled "METHOD, SYSTEM AND DEVICE FOR CDN INTER-NODE ENCRYPTION", 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 are not limited to the communication field, and in particular to a method, system, device, medium and apparatus for CDN inter-node encryption.

Background of the present invention

With the increasing proportion of security-oriented HTTP channels (Hyper Text Transfer Protocol over Secure Socket Layer, HTTPS) applied in network applications, more and more websites are migrated to HTTPS. For a Content Delivery Network (CDN) responsible for infrastructures in the Internet, how to efficiently provide full-link encryption becomes a difficult problem. CDN nodes mostly adopt a multi-level cache mechanism, and the CDN nodes include edge nodes and parent nodes classified according to geographical locations of large areas. The HTTPS for full link means that all links among clients, edge nodes, parent nodes and source stations employ HTTPS communication mode. Since both the links from the clients to the edge nodes and the links from the parent nodes to the origin server involve the communication with a third party, optimization means are limited. Particularly, it is also necessary to implement a complete HTTPS process between the edge node and the parent node. Consequently, the loads on nodes at both ends participating in operation are relatively high.

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, system, device, medium and apparatus for CDN inter-node encryption.

An embodiment of the present invention provides a method for CDN inter-node encryption, including:

generating a symmetric key set and a key index by a key center, and sending the symmetric key set and the key index to each Content Delivery Network (CDN) node; and

receiving, by the CDN node, the symmetric key set and the key index from the key center, determining a key from the symmetric key set according to the key index, and using the key to perform encryption and decryption processing when performing Hyper Text Transfer Protocol (HTTP) data transmission with other CDN nodes.

The method is further featured by:

the sending, by the key center, the symmetric key set and the key index to each CDN node includes: sending the symmetric key set and the key index to each CDN node through an encryption channel.

The method is further featured by:

the using, by the CDN node, the key to perform encryption and decryption processing when performing HTTP data transmission with other CDN nodes includes: when the CDN node is an edge node, using the key to encrypt an HTTP request, sending the encrypted HTTP request to a parent node, and using the key to decrypt an HTTP response after receiving the HTTP response from the parent node; and/or, when the CDN node is a parent node, after receiving an HTTP request from an edge node, using the key to decrypt the HTTP request, using the key to encrypt an HTTP response and sending the encrypted HTTP response to the edge node.

The method is further featured by:

the generating a symmetric key set and a key index by a key center, and sending the symmetric key set and the key index to each CDN node includes:

generating, by the key center, the key index at a first time interval randomly or according to a preset algorithm, and sending the generated key index to the CDN nodes;

and, generating, by the key center, the symmetric key set at a second time interval randomly or according to a preset algorithm, and sending the generated symmetric key set to the CDN nodes, wherein the second time interval is greater than the first time interval; or

generating, by the key center, the key index at a first time interval randomly or according to a preset algorithm, and sending the generated key index to the CDN nodes; and, generating, by the key center, the symmetric key set at a second time interval randomly or according to a preset algorithm and generating the key index at a second time interval randomly or according to a preset algorithm, and sending the generated symmetric key set and key index to the CDN nodes, wherein the second time interval is greater than the first time interval.

The method is further featured by:

the key index has a range of $[x,y]$, wherein both x and y are integers and the number of symmetric keys in the symmetric key set is obtained by adding one to a difference between y and x .

An embodiment of the present invention provides a device for CDN inter-node encryption, applied to a key center, including a generation module and a sending module;

the generation module is configured to generate a symmetric key set and a key index; and

the sending module is configured to send the key set generated by the generation module to each CDN node and further configured to send the key index generated by the generation module to each CDN node.

The device is further featured by:

the sending module is further configured to send the symmetric key set and the key index to each CDN node through an encryption channel.

The device is further featured by:

the generation module is further configured to generate the key index at a first time interval randomly or according to a preset algorithm, and generate the symmetric key set at a second time interval randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval; or, the generation module is further

configured to generate the key index at a first time interval randomly or according to a preset algorithm, and generate the symmetric key set at a second time interval randomly or according to a preset algorithm and generate the key index at a second time interval randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval.

An embodiment of the present invention provides a device for CDN inter-node encryption, applied to a CDN node, including a receiving module and an encryption processing method;

the receiving module is configured to receive a key set from a key center and further configured to receive a key index from the key center; and

the encryption processing module is configured to determine a key from the symmetric key set according to the key index and use the key to perform encryption and decryption processing when performing HTTP data transmission with other CDN nodes.

The device is further featured by:

the encryption processing module is further configured to: when the CDN node is an edge node, use the key to encrypt an HTTP request, send the encrypted HTTP request to a parent node, and use the key to decrypt an HTTP response after receiving the HTTP response from the parent node; and, the encryption processing module is further configured to: when the CDN node is a parent node, use the key to decrypt the HTTP request after receiving an HTTP request from an edge node, and, use the key to encrypt an HTTP response and send the encrypted HTTP response to the edge node.

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

An embodiment of the present invention further 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 in the method described above when executing the programs.

The embodiments of the present invention skip the HTTPS handshake process that consumes mostly and utilize the controllable characteristics of both end nodes to directly

use the symmetric key, realize a lightweight encryption process, achieve the same encryption effect as a standard HTTPS, reduce encryption overhead between CDN edge nodes and parent nodes and reduce loads on the servers at both ends. The present invention also employs a mechanism for randomly generating and periodically and dynamically updating symmetric keys, which are more secure than public keys and corresponding private keys in the certificates used by conventional HTTPS.

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 flowchart of a method for CDN inter-node encryption according to an embodiment;

Fig. 2 is a structural diagram of a device for CDN inter-node encryption, applied to a key center, according to an embodiment; and

Fig. 3 is a structural diagram of a device for CDN inter-node encryption, applied to a CDN node, according to an embodiment.

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.

Fig. 1 is a flowchart of a method for CDN inter-node encryption according to an embodiment. The method includes the following steps.

Step 101: A key center generates a symmetric key set and a key index and sends the key set and the key index to each CDN node.

Step 102: The CDN node receives the symmetric key set and the key index from the key center, determines a key from the symmetric key set according to the key index, and uses this key to perform encryption and decryption processing when performing HTTP

data transmission with other CDN nodes.

Wherein:

in the step 101, the symmetric key set is stored in a memory of the key center but not in a fixed storage medium, so that the security of keys can be improved.

In the step 101, the key center sending the symmetric key set and the key index to each CDN node includes: sending the symmetric key set and the key index to each CDN node through an encryption channel.

In the step 101, the key center generates a key index at a first time interval randomly or according to a preset algorithm and sends the generated key index to the CDN nodes, wherein a typical sending approach is synchronously sending the key index to each CDN node; and, the key center generates a symmetric key set at a second time interval randomly or according to a preset algorithm and sends the generated symmetric key set to the CDN nodes, wherein a typical sending approach is synchronously sending the symmetric key set to each CDN node, and the second time interval is greater than the first time interval. Or, the key center generates a key index at a first time interval randomly or according to a preset algorithm and sends the generated key index to the CDN nodes; and, the key center generates a symmetric key set at a second time interval randomly or according to a preset algorithm, generates a key index randomly or according to a preset algorithm and sends the generated symmetric key set and key index to the CDN nodes, wherein the second time interval is greater than the first time interval.

The applicant of the present invention considers that both sides of the communication between an edge node and a parent node are computing facilities that can be controlled by the CDN manufacturer, it is important to optimize the communication between the two types of nodes. In the step 102, the CDN node using this key to perform encryption and decryption processing when performing HTTP data transmission with other CDN nodes includes: when the CDN node is an edge node, using the key to encrypt an HTTP request, sending the encrypted HTTP request to a parent node, and using the key to decrypt an HTTP response after receiving the HTTP response from the parent node; and/or, when the CDN node is a parent node, after receiving an HTTP request from an edge node, using the key to decrypt the HTTP request, using the key to encrypt an HTTP response and sending

the encrypted HTTP response to the edge node.

In this method, the key index has a range of $[x,y]$, wherein both x and y are integers and the number of symmetric keys in the symmetric key set is obtained by adding one to a difference between y and x . For example, the key index has a range of $[0,(n-1)]$, wherein n is the number of symmetric keys in the symmetric key set. For another example, the key index has a range of $[1,n]$, wherein n is the number of symmetric keys in the symmetric key set.

In the embodiments of the present invention, a system for CDN inter-node encryption includes a key center and a CDN node.

The key center is configured to generate a symmetric key set and a key index and sends the key set and the key index to each CDN node.

The CDN node is configured to determine, from the symmetric key set, a key according to the index acquired from the key center and use this key to perform encryption and decryption processing when performing HTTP data transmission with other CDN nodes.

Fig. 2 is a structural diagram of a device for CDN inter-node encryption, which is applied to a key center. The device includes a generation module and a sending module.

The generation module is configured to generate a symmetric key set and a key index.

The sending module is configured to send the key set generated by the generation module to each CDN node and further configured to send the key index generated by the generation module to each CDN node.

Wherein:

the sending module is specifically configured to send the key set and the key index to each CDN node through an encryption channel.

The generation module is further configured to generate a key index at a first time interval randomly or according to a preset algorithm, and generate a symmetric key set at a second time interval randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval; or, the generation module is further configured to generate a key index at a first time interval randomly or according to a preset

algorithm, and generate a symmetric key set at a second time interval randomly or according to a preset algorithm and generate a key index randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval.

Fig. 3 is a structural diagram of a device for CDN inter-node encryption, which is applied to a CDN node. The device includes a receiving module and an encryption processing module.

The receiving module is configured to receive a key set from a key center and further configured to receive a key index from the key center.

The encryption processing module is configured to determine a key from the symmetric key set according to the key index and use the key to perform encryption and decryption processing when performing HTTP data transmission with other CDN nodes.

The encryption processing module is further configured to: when the CDN node is an edge node, use the key to encrypt an HTTP request, send the encrypted HTTP request to a parent node, and use the key to decrypt an HTTP response after receiving the HTTP response from the parent node; and, the encryption processing module is further configured to: when the CDN node is a parent node, use the key to decrypt the HTTP request after receiving an HTTP request from an edge node, and, use the key to encrypt an HTTP response and send the encrypted HTTP response to the edge node.

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

An embodiment of the present invention further 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 programs, the processor implements the steps in the method described above.

Specific embodiments

Step 1): A key center randomly generates a symmetric key set K, and this symmetric key set contains a plurality of symmetric keys.

Step 2): A symmetric key center synchronously sends the symmetric key set K to all edge nodes and parent nodes through an encryption channel.

Step 3): The symmetric key center randomly generates a symmetric key index I , and the index has a range of $[0, (n-1)]$, wherein n is the number of symmetric keys in the key set K .

Step 4): The symmetric key center synchronously sends the symmetric key index I to all edge nodes and parent nodes through an encryption channel.

Step 5): When an edge node sends an HTTP request to a parent node, $K[I]$ is used as a key to encrypt the HTTP request.

Step 6): When the parent node receives the encrypted HTTP request, $K[I]$ is also used as a key to decrypt data so as to obtain the original text of the HTTP request.

Step 7): When the parent node sends an HTTP response to the edge node, $K[I]$ is used as a key to encrypt the HTTP response.

Step 8): When the edge node receives the encrypted HTTP response, $K[I]$ is also used as a key to decrypt data so as to obtain the original text of the HTTP response.

Step 9): The symmetric key center re-executes the steps 3) and 4) at a time interval T_1 to generate a new key index I and synchronously sends the new key index I to all edge nodes and parent nodes.

Step 10): The symmetric key center re-executes the steps 1) and 2) at a time interval T_2 ($T_2 > T_1$) to generate a new key set K and synchronously sends the new key set K to all edge nodes and parent nodes. Or, the symmetric key center re-executes the steps 1), 2), 3) and 4) at a time interval T_2 ($T_2 > T_1$) to generate a new key set K and a new key index I and synchronously sends the new key set K and the new key index I to all edge nodes and parent nodes.

The embodiments of the present invention skip the HTTPS handshake process that consumes mostly and utilize the controllable characteristics of both end nodes to directly use the symmetric key, realize a lightweight encryption process, achieve the same encryption effect as a standard HTTPS, reduce encryption overhead between CDN edge nodes and parent nodes and reduce loads on the servers at both ends. The embodiments of the present invention also employ a mechanism for randomly generating and periodically and dynamically updating symmetric keys, which are more secure than public keys and corresponding private keys in the certificates used by conventional HTTPS.

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 or all of 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

The embodiments of the present invention skip the HTTPS handshake process that consumes mostly and utilize the controllable characteristics of both end nodes to directly use the symmetric key, realize a lightweight encryption process, achieve the same encryption effect as a standard HTTPS, reduce encryption overhead between CDN edge nodes and parent nodes and reduce loads on the servers at both ends.

CLAIMS

1. A method for CDN inter-node encryption, comprising:

generating a symmetric key set and a key index by a key center randomly or according to a preset algorithm, and sending the symmetric key set and the key index to each Content Delivery Network (CDN) node; and

receiving, by the CDN node, the symmetric key set and the key index from the key center, determining a key from the symmetric key set according to the key index, and using the key to perform encryption and decryption processing when performing Hyper Text Transfer Protocol (HTTP) data transmission with other CDN nodes;

wherein the generating a symmetric key set and a key index by a key center, and sending the symmetric key set and the key index to each CDN node comprises:

generating, by the key center, the key index at a first time interval randomly or according to a preset algorithm, and sending the generated key index to the CDN nodes; and, generating, by the key center, the symmetric key set at a second time interval randomly or according to a preset algorithm, and sending the generated symmetric key set to the CDN nodes, wherein the second time interval is greater than the first time interval;
or

generating, by the key center, the key index at a first time interval randomly or according to a preset algorithm, and sending the generated key index to the CDN nodes; and, generating, by the key center, the symmetric key set at a second time interval randomly or according to a preset algorithm and generating the key index at a second time interval randomly or according to a preset algorithm, and sending the generated symmetric key set and key index to the CDN nodes, wherein the second time interval is greater than the first time interval.

2. The method for CDN inter-node encryption according to claim 1, wherein:

the sending, by the key center, the symmetric key set and the key index to each CDN node comprises: sending the symmetric key set and the key index to each CDN node through an encryption channel.

3. The method for CDN inter-node encryption according to claim 1, wherein:

the using, by the CDN node, the key to perform encryption and decryption processing

when performing HTTP data transmission with other CDN nodes comprises: when the CDN node is an edge node, using the key to encrypt an HTTP request, sending the encrypted HTTP request to a parent node, and using the key to decrypt an HTTP response after receiving the HTTP response from the parent node; and/or, when the CDN node is a parent node, after receiving an HTTP request from an edge node, using the key to decrypt the HTTP request, using the key to encrypt an HTTP response and sending the encrypted HTTP response to the edge node.

~~4. The method for CDN inter-node encryption according to claim 1, wherein:~~

~~the generating a symmetric key set and a key index by a key center, and sending the symmetric key set and the key index to each CDN node comprises:~~

~~generating, by the key center, the key index at a first time interval randomly or according to a preset algorithm, and sending the generated key index to the CDN nodes; and, generating, by the key center, the symmetric key set at a second time interval randomly or according to a preset algorithm, and sending the generated symmetric key set to the CDN nodes, wherein the second time interval is greater than the first time interval; or~~

~~or, generating, by the key center, the key index at a first time interval randomly or according to a preset algorithm, and sending the generated key index to the CDN nodes; and, generating, by the key center, the symmetric key set at a second time interval randomly or according to a preset algorithm and generating the key index at a second time interval randomly or according to a preset algorithm, and sending the generated symmetric key set and key index to the CDN nodes, wherein the second time interval is greater than the first time interval.~~

~~54.~~ The method for CDN inter-node encryption according to claim 1, wherein:

the key index has a range of [x,y], wherein both x and y are integers and the number of symmetric keys in the symmetric key set is obtained by adding one to a difference between y and x.

~~65.~~ A device for CDN inter-node encryption, applied to a key center, comprising a generation module and a sending module;

the generation module is configured to generate a symmetric key set and a key index

randomly or according to a preset algorithm, wherein the generation module is further configured to generate the key index at a first time interval randomly or according to a preset algorithm, and generate the symmetric key set at a second time interval randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval; or, the generation module is further configured to generate the key index at a first time interval randomly or according to a preset algorithm, and generate the symmetric key set at a second time interval randomly or according to a preset algorithm and generate the key index at a second time interval randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval; and

the sending module is configured to send the key set generated by the generation module to each CDN node and further configured to send the key index generated by the generation module to each CDN node.

76. The device for CDN inter-node encryption according to claim 65, wherein:

the sending module is further configured to send the symmetric key set and the key index to each CDN node through an encryption channel.

~~8. The device for CDN inter-node encryption according to claim 6, wherein:~~

~~the generation module is further configured to generate the key index at a first time interval randomly or according to a preset algorithm, and generate the symmetric key set at a second time interval randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval; or, the generation module is further configured to generate the key index at a first time interval randomly or according to a preset algorithm, and generate the symmetric key set at a second time interval randomly or according to a preset algorithm and generate the key index at a second time interval randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval.~~

97. A device for CDN inter-node encryption, applied to a CDN node, comprising a receiving module and an encryption processing method;

the receiving module is configured to receive a symmetric key set from a key center and further configured to receive a key index from the key center, the key set and the key index being generated randomly or according to a preset algorithm, wherein the key index

is generated, by the key center, at a first time interval randomly or according to a preset algorithm, and the symmetric key set is generated, by the key center, at a second time interval randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval; or, the key index is generated, by the key center, at a first time interval randomly or according to a preset algorithm, and the symmetric key set is generated, by the key center, at a second time interval randomly or according to a preset algorithm and the key index is generated at a second time interval randomly or according to a preset algorithm, wherein the second time interval is greater than the first time interval;

and

the encryption processing module is configured to determine a key from the symmetric key set according to the key index and use the key to perform encryption and decryption processing when performing HTTP data transmission with other CDN nodes.

~~108~~. The device for CDN inter-node encryption according to claim ~~97~~, wherein:

the encryption processing module is further configured to: when the CDN node is an edge node, use the key to encrypt an HTTP request, send the encrypted HTTP request to a parent node, and use the key to decrypt an HTTP response after receiving the HTTP response from the parent node; and, the encryption processing module is further configured to: when the CDN node is a parent node, after receiving an HTTP request from an edge node, use the key to decrypt the HTTP request, use the key to encrypt an HTTP response and send the encrypted HTTP response to the edge node.

~~119~~. A computer-readable storage medium stored with computer programs that, when executed by a processor, implements the steps in the method according to any one of claims 1 to ~~54~~.

~~1210~~. 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 in the method according to any one of claims 1 to ~~5-4~~ when executing the programs.