

DEVICE FINGERPRINT VERIFICATION METHOD, DEVICE FINGERPRINT GENERATION METHOD, AND ELECTRONIC DEVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present disclosure claims the priority to the Chinese patent application with the filling No. CN202410204010.0 filed on February 23, 2024, and entitled “DEVICE FINGERPRINT VERIFICATION METHOD, DEVICE FINGERPRINT GENERATION METHOD, AND ELECTRONIC DEVICE”, the contents of which are incorporated herein by reference in entirety.

TECHNICAL FIELD

[0002] The present disclosure belongs to the technical field of network security, and particularly relates to a device fingerprint verification method, a device fingerprint generation method, and an electronic device.

BACKGROUND ART

[0003] The device fingerprint is configured for uniquely identifying device features or unique device identifiers of the device. The device fingerprint can include some inherent, difficult-to-tamper, and unique device identifiers and feature collections of the device, for example: a mobile phone is provided with a unique International Mobile Equipment Identity (IMEI) number during the manufacturing process, which is used for uniquely identifying the device; and for another example: a network card of a computer is provided with a unique Media Access Control Address (MAC address) during the manufacturing process. However, during the use of the device fingerprint, replacement or tampering may occur, resulting in the security of the device fingerprint not being ensured.

SUMMARY

[0004] The present disclosure provides a device fingerprint verification method, a device fingerprint generation method, and an electronic device, for solving the technical problem in the prior art that the device fingerprint is replaced or tampered with, resulting in the security of the device fingerprint not being ensured.

[0005] In a first aspect, the embodiment of the present disclosure provides a device fingerprint verification method, including: acquiring request data sent by a client, wherein the request data includes target device fingerprint information corresponding to the client, the target device fingerprint information includes initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes a first generation time of generating the target device fingerprint information; restoring first verification information corresponding to the first generation time according to the target device fingerprint information; and verifying the target device fingerprint information according to the first verification information.

[0006] In the above solution, after acquiring the target device fingerprint information corresponding to the target device, since the target device fingerprint information includes the initial device fingerprint information and the time information spliced therewith, the first verification information corresponding to the first generation time in the time information can be restored, and the target device fingerprint information can be verified quickly based on the first verification information, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[0007] In an optional embodiment, after the step of verifying the target device fingerprint information according to the first verification information, the method further includes: restoring, when the verification of the first verification information is normal, second verification information corresponding to the initial device fingerprint information according to the target device fingerprint information; and verifying the target device fingerprint information according to the second verification information. In the above solution, if the verification of the first verification information is normal, the target device fingerprint information can be further verified, and more accurate verification of the target device fingerprint information is performed by restoring the second verification information corresponding to the initial device fingerprint information, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[0008] In optional embodiment, the step of verifying the target device fingerprint information according to the second verification information, includes: decrypting the second verification information; and determining whether the second verification information is successfully decrypted, wherein unsuccessful decryption of the second verification information indicates that the target device fingerprint information is abnormal. In the above solution, the decryption verification of the target device fingerprint information can be realized by decrypting the second verification information, so as to improve the accuracy of the verification and ensure the security of the device fingerprint.

[0009] In an optional embodiment, the initial device fingerprint information includes service information; after determining whether the second verification information is successfully decrypted, the method further includes: determining whether a service verification information is the same as the service information when the second verification information is successfully decrypted and corresponding third verification information is obtained, wherein the service verification information is verification information in the third verification information corresponding to the service information, and the service verification information being not the same as the service information indicates that the target device fingerprint information is abnormal. In the above solution, if the second verification information is verified to be normal, the target device fingerprint information can be further verified, and service verification of the target device fingerprint information is realized by determining whether the service verification information in the decrypted third verification information is the same as the service information, so as to improve the accuracy of the service verification and ensure the security of the device fingerprint.

[0010] In a second aspect, the embodiment of the present disclosure provides a device fingerprint generation method, including: acquiring initial device fingerprint information

corresponding to a client and a first generation time, wherein the first generation time is a time for generating target device fingerprint information; generating the target device fingerprint information according to the initial device fingerprint information and the first generation time, wherein the target device fingerprint information includes the initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes the first generation time.

[0011] In the above solution, after acquiring the initial device fingerprint information corresponding to the target device and the first generation time corresponding to the generation of the target device fingerprint information, the target device fingerprint information can be generated according to the initial device fingerprint information and the first generation time; based on the target device fingerprint information, the device fingerprint can be verified, so as to determine whether replacement or tampering occurs in the use process of the device fingerprint, and ensure the security of the device fingerprint.

[0012] In an optional embodiment, the step of generating the target device fingerprint information according to the initial device fingerprint information and the first generation time includes: splicing the initial device fingerprint information and the first generation time to obtain the target device fingerprint information. In the above solution, the initial device fingerprint information and the first generation time can be spliced together, so that the target device fingerprint information can be quickly verified based on the first generation time, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[0013] In an optional embodiment, the step of generating the target device fingerprint information according to the initial device fingerprint information and the first generation time includes: encoding the first generation time to obtain the time information; and splicing the initial device fingerprint information and the time information to obtain the target device fingerprint information. In the above solution, the first generation time can be encoded first, and then the initial fingerprint information can be spliced with the encoded time information, so that the data amount of the target device fingerprint information can be reduced on the basis of realizing quick verification.

[0014] In an optional embodiment, the step of acquiring initial device fingerprint information corresponding to a client includes: acquiring a device fingerprint ID and device feature information corresponding to the client, wherein the device feature information includes at least one of: a second generation time for generating the device fingerprint ID for the first time, verifiable information corresponding to the client, and service information corresponding to the client; and generating the initial device fingerprint information according to the device fingerprint ID and the device feature information. In the above solution, the initial device fingerprint information can include the device fingerprint ID and the device feature information, so that more usage scenarios can be adapted and different verifications can be performed on the target device fingerprint information based on different scenarios, thereby reducing the risk of the device fingerprint ID being replaced or tampered, and ensuring the security of the device fingerprint.

[0015] In optional embodiments, the step of generating the initial device fingerprint information according to the device fingerprint ID and the device feature information includes: splicing the device fingerprint ID and the device feature information to obtain first device

fingerprint information; encrypting the first device fingerprint information to obtain second device fingerprint information; and performing character transcoding on the second device fingerprint information to obtain the initial device fingerprint information. In the above solution, after splicing the device fingerprint ID and the device feature information, the spliced first device fingerprint information can be encrypted and character transcoding can be performed, so as to further reduce the risk of the device fingerprint being replaced or tampered, and ensure the security of the device fingerprint.

[0016] In optional embodiments, the step of performing character transcoding on the second device fingerprint information to obtain the initial device fingerprint information includes: performing character transcoding on the second device fingerprint information using a preset transcoding method to obtain the initial device fingerprint information, wherein the initial device fingerprint information does not include special characters. In the above solution, the second device fingerprint information can be performed with a character transcoding using a preset transcoding method to obtain the initial device fingerprint information that does not include special characters. Since the device fingerprint will serve as a parameter of the request, and special characters present potential risks during transmission, the above transcoding method can reduce the above risks, thereby ensuring the security of the device fingerprint.

[0017] In a third aspect, the embodiment of the present disclosure provides another device fingerprint verification method, including: acquiring initial device fingerprint information corresponding to a client and a first generation time, wherein the first generation time is a time for generating target device fingerprint information; generating the target device fingerprint information according to the initial device fingerprint information and the first generation time, wherein the target device fingerprint information includes the initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes the first generation time; acquiring request data sent by a client, wherein the request data includes target device fingerprint information corresponding to the client; restoring the first verification information corresponding to the first generation time according to the target device fingerprint information; and verifying the target device fingerprint information according to the first verification information.

[0018] In the above solution, after acquiring the initial device fingerprint information corresponding to the target device and the first generation time corresponding to the generation of the target device fingerprint information, the target device fingerprint information can be generated according to the initial device fingerprint information and the first generation time; based on the target device fingerprint information, the device fingerprint can be verified quickly, so as to determine whether replacement or tampering occurs in the use process of the device fingerprint, and ensure the security of the device fingerprint.

[0019] In a fourth aspect, the embodiment of the present disclosure provides a device fingerprint verification apparatus, including: a first acquisition module, configured for acquiring request data sent by a client, wherein the request data includes target device fingerprint information corresponding to the client, the target device fingerprint information includes initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes a first generation time of generating the target device fingerprint information; a first restoring module, configured for restoring the first verification information corresponding to the first generation time according

to the target device fingerprint information; and a first verification module, configured for verifying the target device fingerprint information according to the first verification information.

[0020] In the above solution, after acquiring the target device fingerprint information corresponding to the target device, since the target device fingerprint information includes the initial device fingerprint information and the time information spliced therewith, the first verification information corresponding to the first generation time in the time information can be restored, and the target device fingerprint information can be verified quickly based on the first verification information, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[0021] In an optional embodiment, the device fingerprint verification apparatus further includes: a second restoring module, configured for restoring, when the verification of the first verification information is normal, second verification information corresponding to the initial device fingerprint information according to the target device fingerprint information; and a second verification module, configured for verifying the target device fingerprint information according to the second verification information. In the above solution, if the verification of the first verification information is normal, the target device fingerprint information can be further verified, and more accurate verification of the target device fingerprint information is performed by restoring the second verification information corresponding to the initial device fingerprint information, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[0022] In optional embodiments, the second verification module is specifically configured for: decrypting the second verification information; and determining whether the second verification information is successfully decrypted, wherein unsuccessful decryption of the second verification information indicates that the target device fingerprint information is abnormal. In the above solution, the decryption verification of the target device fingerprint information can be realized by decrypting the second verification information, so as to improve the accuracy of the verification and ensure the security of the device fingerprint.

[0023] In an optional embodiment, the initial device fingerprint information includes service information, and the device fingerprint verification apparatus further includes: a judgment module, configured for determining whether a service verification information is the same as the service information when the second verification information is successfully decrypted and corresponding third verification information is obtained, wherein the service verification information is verification information in the third verification information corresponding to the service information, and the service verification information being not the same as the service information indicates that the target device fingerprint information is abnormal. In the above solution, if the second verification information is verified to be normal, the target device fingerprint information can be further verified, and service verification of the target device fingerprint information is realized by determining whether the service verification information in the decrypted third verification information is the same as the service information, so as to improve the accuracy of the service verification and ensure the security of the device fingerprint.

[0024] In a fifth aspect, the embodiment of the present disclosure provides a device fingerprint generation apparatus, including: a second acquisition module, configured for acquiring initial device fingerprint information corresponding to a client and a first generation time, wherein the first generation time is a time for generating target device fingerprint information; and a first generation module, configured for generating the target device fingerprint information according to the initial device fingerprint information and the first generation time, wherein the target device fingerprint information includes the initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes the first generation time.

[0025] In the above solution, after acquiring the initial device fingerprint information corresponding to the target device and the first generation time corresponding to the generation of the target device fingerprint information, the target device fingerprint information can be generated according to the initial device fingerprint information and the first generation time; based on the target device fingerprint information, the device fingerprint can be verified, so as to determine whether replacement or tampering occurs in the use process of the device fingerprint, and ensure the security of the device fingerprint.

[0026] In optional embodiments, the first generation module is specifically configured for: splicing the initial device fingerprint information and the first generation time to obtain the target device fingerprint information. In the above solution, the initial device fingerprint information and the first generation time can be spliced together, so that the target device fingerprint information can be quickly verified based on the first generation time, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[0027] In optional embodiments, the first generation module is specifically configured for: encoding the first generation time to obtain the time information; and splicing the initial device fingerprint information and the time information to obtain the target device fingerprint information. In the above solution, the first generation time can be encoded first, and then the initial fingerprint information can be spliced with the encoded time information, so that the data amount of the target device fingerprint information can be reduced on the basis of realizing quick verification.

[0028] In optional embodiments, the second acquisition module is specifically configured for: acquiring a device fingerprint ID and device feature information corresponding to the client, wherein the device feature information includes at least one of: a second generation time for generating the device fingerprint ID for the first time, verifiable information corresponding to the client, and service information corresponding to the client; and generating the initial device fingerprint information according to the device fingerprint ID and the device feature information. In the above solution, the initial device fingerprint information can include the device fingerprint ID and the device feature information, so that more usage scenarios can be adapted and different verifications can be performed on the target device fingerprint information based on different scenarios, thereby reducing the risk of the device fingerprint ID being replaced or tampered, and ensuring the security of the device fingerprint.

[0029] In optional embodiments, the second acquisition module is further configured for: splicing the device fingerprint ID and the device feature information to obtain first device fingerprint information; encrypting the first device fingerprint information to obtain second

device fingerprint information; and performing character transcoding on the second device fingerprint information to obtain the initial device fingerprint information. In the above solution, after splicing the device fingerprint ID and the device feature information, the spliced first device fingerprint information can be encrypted and character transcoding can be performed, so as to further reduce the risk of the device fingerprint being replaced or tampered, and ensure the security of the device fingerprint.

[0030] In optional embodiments, the second acquisition module is further configured for: performing character transcoding on the second device fingerprint information using a preset transcoding method to obtain the initial device fingerprint information, wherein the initial device fingerprint information does not include special characters. In the above solution, the second device fingerprint information can be performed with a character transcoding using a preset transcoding method to obtain the initial device fingerprint information that does not include special characters. Since the device fingerprint will serve as a parameter of the request, and special characters present potential risks during transmission, the above transcoding method can reduce the above risks, thereby ensuring the security of the device fingerprint.

[0031] In a sixth aspect, the embodiment of the present disclosure provides another device fingerprint verification apparatus, including: a third acquisition module, configured for acquiring initial device fingerprint information corresponding to a client and a first generation time, wherein the first generation time is a time for generating target device fingerprint information; a second generation module, configured for generating the target device fingerprint information according to the initial device fingerprint information and the first generation time, wherein the target device fingerprint information includes the initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes the first generation time; a fourth acquisition module, configured for acquiring request data sent by a client, wherein the request data includes target device fingerprint information corresponding to the client; a third restoring module, configured for restoring the first verification information corresponding to the first generation time according to the target device fingerprint information; and a third verification module, configured for verifying the target device fingerprint information according to the first verification information.

[0032] In the above solution, after acquiring the initial device fingerprint information corresponding to the target device and the first generation time corresponding to the generation of the target device fingerprint information, the target device fingerprint information can be generated according to the initial device fingerprint information and the first generation time; based on the target device fingerprint information, the device fingerprint can be verified quickly, so as to determine whether replacement or tampering occurs in the use process of the device fingerprint, and ensure the security of the device fingerprint.

[0033] In a seventh aspect, the embodiments of the present disclosure provide an electronic device, including: a processor, a memory, and a bus; the processor and the memory complete communication with each other through the bus; the memory stores computer program instructions executable by the processor, and the processor invokes the computer program instructions to execute the device fingerprint verification method as described in the first aspect or the third aspect, or the device fingerprint generation method as described in the second aspect.

[0034] In an eighth aspect, the embodiments of the present disclosure provide a computer-readable storage medium, wherein the computer-readable storage medium stores computer program instructions. The computer program instructions, when run by a computer, cause the computer to execute the device fingerprint verification method as described in the first aspect or the third aspect, or the device fingerprint generation method as described in the second aspect.

[0035] Other features and advantages of the present disclosure will be set forth in the subsequent specification and, in part, become apparent from the specification or are understood by implementing the embodiments of the present disclosure. The objectives and other advantages of the present disclosure can be achieved and obtained through the structures particularly pointed out in the specification, the claims, and the drawings.

BRIEF DESCRIPTION OF DRAWINGS

[0036] In order to more clearly illustrate the technical solutions of the embodiments of the present disclosure, the following will briefly introduce the drawings used in the embodiments of the present disclosure. It should be understood that the following drawings only show some embodiments of the present disclosure, and therefore it should not be regarded as a limitation on the scope. Those ordinary skilled in the art can also obtain other related drawings based on these drawings without inventive effort.

[0037] FIG. 1 is a flowchart of a device fingerprint verification method provided by the embodiment of the present disclosure;

[0038] FIG. 2 is a flowchart of a device fingerprint generation method provided by the embodiment of the present disclosure;

[0039] FIG. 3 is a flowchart of another device fingerprint verification method provided by the embodiment of the present disclosure;

[0040] FIG. 4 is a block diagram of a structure of a device fingerprint verification apparatus provided by the embodiment of the present disclosure;

[0041] FIG. 5 is a block diagram of a structure of a device fingerprint generation apparatus provided by the embodiment of the present disclosure;

[0042] FIG. 6 is a block diagram of a structure of another device fingerprint verification apparatus provided by the embodiment of the present disclosure; and

[0043] FIG. 7 is a block diagram of the structure of an electronic device provided by the embodiment of the present disclosure.

DETAILED DESCRIPTION OF EMBODIMENTS

[0044] The following description will combine the drawings in the embodiments of the present disclosure to provide a clear and comprehensive explanation of the technical solution in the embodiments of the present disclosure.

[0045] It should be noted that the term "multiple" in the embodiment of the present disclosure refers to two or more than two. In view of this, in the embodiment of the present disclosure, "multiple" can also be understood as "at least two". The term "and/or" describes the relationship between associated objects, indicating that there can be three possible relationships. For example, "A and/or B" can represent: the presence of A alone, the presence of both A and B, or the presence of B alone. Additionally, unless otherwise specified, the character "/" herein

generally represents an "or" relationship between the preceding and following associated objects.

[0046] Referring to FIG.1, FIG. 1 is a flowchart of a device fingerprint verification method provided by the embodiment of the present disclosure. The device fingerprint verification method can be applied to the server, wherein the device fingerprint verification method can include the following steps:

[0047] step S101, acquiring request data sent by a client;

[0048] step S102, restoring first verification information corresponding to the first generation time according to the target device fingerprint information; and

[0049] step S103, verifying the target device fingerprint information according to the first verification information.

[0050] Specifically, in the above step S101, when the client needs to perform a service, the client can send request data to the server, so that the server can perform verification on the target device fingerprint information of the client based on the above request data.

[0051] The above request data can include target device fingerprint information corresponding to the client. As an implementation, the above target device fingerprint information can include initial device fingerprint information and time information; the above target device fingerprint information can be generated by splicing the above initial device fingerprint information and the time information.

[0052] The initial device fingerprint information can be generated based on information related to the client. It should be noted that, firstly, the embodiment of the present disclosure does not specifically limit the specific implementation of the above information related to the client, and a person skilled in the art may make appropriate adjustments according to actual situations. For example, the information related to the client can include one or more items of information such as a device fingerprint identity (identity document, ID), a time when the above device fingerprint ID is generated for the first time, verifiable information corresponding to the client, service information corresponding to the client, and the like.

[0053] In the embodiment of the present disclosure, the device fingerprint ID refers to a device feature or unique device identifier used to uniquely identify the client, and the device fingerprint information refers to a device identifier generated based on the device fingerprint ID and used to identify the target device. The difference between the two lies in that, one client corresponds to only one device fingerprint ID, but can correspond to multiple pieces of device fingerprint information.

[0054] The time when the device fingerprint ID is generated for the first time can provide some time information during the verification, so as to facilitate historical query, and can also be used for legal time verification; the verifiable information corresponding to the client can include attribute information related to the target device, for example: Android ID, device model, and other information; the service information can be used to characterize the corresponding service on the client, for example, assuming there are two applications (Apps), and the same device installs the two Apps, the device fingerprint ID is the same, but in order to distinguish the two Apps, two different pieces of service information can be generated, so that the target device fingerprint information issued by the two Apps is different.

[0055] Secondly, the embodiment of the present disclosure also does not specifically limit the specific implementation for generating the above initial device fingerprint information, and a

person skilled in the art may make appropriate adjustments according to actual situations. For example, the information related to the client can be input into a pre-trained neural network model to output the above initial device fingerprint information; or, multiple pieces of information related to the client can be spliced to obtain the above initial device fingerprint information; or, the information related to the client can be encrypted to obtain the above initial device fingerprint information, and the like.

[0056] The time information can be obtained based on a first generation time of generating the target device fingerprint information. As one implementation, the time information can include the above first generation time; as another implementation, the above first generation time can be processed first to obtain the above time information. It can be understood that the embodiment of the present disclosure does not specifically limit the specific implementation of processing the above first generation time, and a person skilled in the art may make appropriate adjustments according to actual situations. For example, the first generation time can undergo one or more processing operations such as compression, encryption, and transcoding.

[0057] In the above step S102, since the target device fingerprint information includes the initial device fingerprint information and the time information spliced with the initial device fingerprint information, the first verification information corresponding to the first generation time can be quickly restored from the target device fingerprint information.

[0058] As one implementation, if the time information includes the above first generation time, then the information at the position in the target device fingerprint information corresponding to the first generation time can be directly extracted to obtain the first verification information; as another implementation, if the first generation time is processed first, then after extracting the information at the position in the target device fingerprint information corresponding to the first generation time, inverse processing can be performed on the extracted data to obtain the first verification information.

[0059] In the above step S103, the objective of verifying the target device fingerprint information can be achieved by performing verification on the above first verification information. As one implementation, whether the first verification information is the same as the first generation time can be determined to perform verification on the first verification information.

[0060] If the first verification information is not the same as the first generation time, it indicates that the first verification information is abnormally verified, at this time, it indicates that the target device fingerprint information is abnormal, and subsequent processing can be directly performed as abnormal. For example, assuming that the first generation time is 2023 and the first verification information is 3023, then it indicates that the target device fingerprint information has been tampered with.

[0061] If the first verification information is the same as the first generation time, then it indicates that the verification of the first verification information is normal. At this time, as one implementation, it is considered that the target device fingerprint information is not abnormal; as another implementation, other verification manners are also adopted to further verify the target device fingerprint information.

[0062] In the above solution, after acquiring the target device fingerprint information corresponding to the target device, since the target device fingerprint information includes the

initial device fingerprint information and the time information spliced therewith, the first verification information corresponding to the first generation time in the time information can be restored, and the target device fingerprint information can be verified quickly based on the first verification information, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[0063] Further, based on the above embodiment, after the above step S103, the device fingerprint verification method provided by the embodiment of the present disclosure further includes the following steps:

[0064] step 1), restoring, when the verification of the first verification information is normal, second verification information corresponding to the initial device fingerprint information according to the target device fingerprint information; and

[0065] step 2), verifying the target device fingerprint information according to the second verification information.

[0066] Specifically, in the above step 1), if the first verification information is verified to be normal, then other verification manners are adopted to further verify the target device fingerprint information. As one implementation, second verification information corresponding to the initial device fingerprint information can be restored according to the target device fingerprint information.

[0067] It should be noted that the embodiment of the present disclosure does not make specific limitations on the specific implementation of restoring the initial device fingerprint information, and those skilled in the art can conduct appropriate adjustments according to the specific implementation of generating the initial device fingerprint information. For example, the initial device fingerprint information is split; or, the initial device fingerprint information is decrypted; or, the initial device fingerprint information is decoded.

[0068] In the above step 2), the objective of verifying the target device fingerprint information can be achieved by performing verification on the above second verification information. It should be noted that the embodiment of the present disclosure does not make specific limitations on the specific implementation of verifying the second verification information, and those skilled in the art can conduct appropriate adjustments according to the specific implementation of the initial device fingerprint information. For example, if the initial device fingerprint information is obtained through encryption, then it is determined whether the second verification information can be decrypted normally; or, if the initial device fingerprint information includes the device fingerprint ID, then it is determined whether the second verification information is the same as the device fingerprint ID; or, if the initial device fingerprint information includes service information, then it is determined whether the second verification information is the same as the service information.

[0069] In the above solution, if the verification of the first verification information is normal, the target device fingerprint information can be further verified, and more accurate verification of the target device fingerprint information is performed by restoring the second verification information corresponding to the initial device fingerprint information, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[0070] Further, based on the above embodiment, the step of verifying the target device fingerprint information according to the second verification information can specifically include the following steps:

[0071] step 1), decrypting the second verification information; and

[0072] step 2), determining whether the second verification information is decrypted successfully.

[0073] Specifically, in the above step 1), if encryption processing has been performed in the process of generating the initial device fingerprint information, then the objective of verifying the target device fingerprint information is achieved by decrypting and verifying the second verification information. Therefore, the above second verification information can be decrypted.

[0074] In the above step 2), whether the second verification information is decrypted successfully is determined, thereby achieving the verification of the second verification information. If the second verification information is not decrypted successfully, then it indicates that the second verification information verification is abnormal; at this time, it indicates that the target device fingerprint information is abnormal and is directly processed as an exception. For example, if the second verification information cannot be decrypted successfully or an exception in parameter parsing occurs during the process of decrypting the second verification information, then it indicates that the target device fingerprint information has been tampered with.

[0075] If the second verification information is decrypted successfully, then it indicates that the second verification information verification is normal. At this time, as one implementation, it is considered that the target device fingerprint information is not abnormal; as another implementation, other verification manners are also adopted to further verify the target device fingerprint information.

[0076] In the above solution, the decryption verification of the target device fingerprint information can be realized by decrypting the second verification information, so as to improve the accuracy of the verification and ensure the security of the device fingerprint.

[0077] Further, based on the above embodiment, the initial device fingerprint information can also include service information; at this time, after the above step of verifying the target device fingerprint information according to the second verification information, the device fingerprint verification method provided by the embodiment of the present disclosure further includes the following step:

[0078] determining whether a service verification information is the same as the service information when the second verification information is successfully decrypted and corresponding third verification information is obtained.

[0079] Specifically, in the above step, if the second verification information is decrypted successfully, then other verification manners are adopted to further verify the target device fingerprint information. As one implementation, if the initial device fingerprint information includes service information, then the objective of verifying the target device fingerprint information is achieved by performing service verification on the third verification information. Therefore, the service verification information in the decrypted third verification information is extracted, and whether the service verification information is the same as the service information is determined.

[0080] The service verification information is the verification information in the third verification information corresponding to the service information, and the service information is used to characterize the corresponding service on the client. If the service verification information is not the same as the service information, it indicates that the third verification information is abnormally verified, at this time, it indicates that the target device fingerprint information is abnormal, and subsequent processing can be directly performed as abnormal. For example, if the service verification information is not the same as the service information, then it is possible that the target device fingerprint information has been replaced.

[0081] If the service verification information is the same as the service information, then it indicates that the third verification information verification is normal. At this time, as one implementation, it is considered that the target device fingerprint information is not abnormal; as another implementation, other verification manners are also adopted to further verify the target device fingerprint information.

[0082] In the above solution, if the second verification information is verified to be normal, the target device fingerprint information can be further verified, and service verification of the target device fingerprint information is realized by determining whether the service verification information in the decrypted third verification information is the same as the service information, so as to improve the accuracy of the service verification and ensure the security of the device fingerprint.

[0083] Referring to FIG.2, FIG. 2 is a flowchart of a device fingerprint generation method provided by the embodiment of the present disclosure. The device fingerprint generation method can be applied to the server, wherein the device fingerprint generation method can include the following steps:

[0084] step S201, acquiring initial device fingerprint information corresponding to a client and a first generation time; and

[0085] step S202, generating the target device fingerprint information according to the initial device fingerprint information and the first generation time.

[0086] Specifically, in the above step S201, the initial device fingerprint information can be generated based on information related to the client. The information related to the client can include one or more items of information such as a device fingerprint ID, a time when the above device fingerprint ID is generated for the first time, verifiable information corresponding to the client, service information corresponding to the client, and the like.

[0087] The first generation time is the time of generating the target device fingerprint information, that is, the above first generation time can be the time when executing step S201 to step S202 provided by the embodiment of the present disclosure. As one implementation, the above first generation time can be the current time; as another implementation, the first generation time can be a future expected time for generating the target device fingerprint information. For example, the above first generation time can include at least one of year, month, day, hour, minute, and second.

[0088] It should be noted that the embodiment of the present disclosure does not specifically limit the specific implementation of acquiring the initial device fingerprint information and the first generation time, and those skilled in the art can perform appropriate adjustments according to the actual situation. For example, the initial device fingerprint information and the first generation time sent by an external device can be received; or, the initial device fingerprint

information and the first generation time stored locally or on the cloud can be read; or, the initial device fingerprint information can be generated in real-time, and so on.

[0089] In the above step S202, according to the initial device fingerprint information and the first generation time, the target device fingerprint information can be generated, wherein the target device fingerprint information includes the initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes the first generation time. Therefore, the initial device fingerprint information and the time information can be spliced together, so that the target device fingerprint information can be obtained.

[0090] In the above solution, after acquiring the initial device fingerprint information corresponding to the target device and the first generation time corresponding to the generation of the target device fingerprint information, the target device fingerprint information can be generated according to the initial device fingerprint information and the first generation time; based on the target device fingerprint information, the device fingerprint can be verified, so as to determine whether replacement or tampering occurs in the use process of the device fingerprint, and ensure the security of the device fingerprint.

[0091] Further, based on the above embodiment, as one implementation, the above step S202 specifically can include the following step:

[0092] splicing the initial device fingerprint information and the first generation time to obtain the target device fingerprint information.

[0093] Specifically, the initial device fingerprint information and the first generation time can be directly spliced together, so that the target device fingerprint information can be obtained. The manner of splicing the initial device fingerprint information and the first generation time is: adding the first generation time into the initial device fingerprint information, for example: assuming that the initial device fingerprint information is abcd and the first generation time is 2001, then the obtained target device fingerprint information after splicing can be abcd2001.

[0094] It should be noted that the embodiment of the present disclosure does not specifically limit the specific position of adding the first generation time in the initial device fingerprint information, and those skilled in the art can perform appropriate adjustments according to the actual situation. For example, the first generation time can be added after the initial device fingerprint information (e.g., abcd2001); or, the first generation time can be added before the initial device fingerprint information (e.g., 2001abcd); or, the first generation time can be added into the middle of the initial device fingerprint information (e.g., ab2001cd), and so on.

[0095] In the above solution, the initial device fingerprint information and the first generation time can be spliced together, so that the target device fingerprint information can be quickly verified based on the first generation time, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[0096] Further, based on the above embodiment, as another implementation, the above step S202 specifically can include the following step:

[0097] step 1), encoding the first generation time to obtain the time information; and

[0098] step 2), splicing the initial device fingerprint information and the time information to obtain the target device fingerprint information.

[0099] Specifically, in the above step 1), after encoding the first generation time to obtain time information, the initial device fingerprint information and the time information can be spliced together, so that the target device fingerprint information can be obtained.

[00100] It should be noted that the embodiment of the present disclosure does not specifically limit the specific implementation of encoding the first generation time, and those skilled in the art can perform appropriate adjustments according to the actual situation, for example: base conversion compression can be performed on the first generation time, or Huffman encoding can be performed on the first generation time, and so on.

[00101] Taking base conversion compression for the first generation time as an example, assuming that the first generation time is 20231030, base 58 can be used to perform base conversion compression on the above first generation time, and compressed time information 2MFYS can be obtained.

[00102] In the above step 2), the time information obtained after compression can be spliced with the initial device fingerprint information; it can be understood that the specific implementation of splicing the time information and the initial device fingerprint information is similar to the specific implementation of splicing the first generation time and the initial device fingerprint information, and will not be described in detail herein.

[00103] In the above solution, the first generation time can be encoded first, and then the initial fingerprint information can be spliced with the encoded time information, so that the data amount of the target device fingerprint information can be reduced on the basis of realizing quick verification.

[00104] Further, based on the above embodiment, the above step S201 specifically can include the following step:

[00105] step 1), acquiring the device fingerprint ID corresponding to the client and device feature information; and

[00106] step 2), generating the initial device fingerprint information according to the device fingerprint ID and the device feature information.

[00107] Specifically, in the above step 1), the device fingerprint ID corresponding to the client can be generated only once and then stored locally or on the cloud; and the device feature information corresponding to the client can be acquired and synchronously stored when generating the device fingerprint ID, or the device information can also be queried in real-time. The device feature information can include at least one of: a second generation time for generating the device fingerprint ID for the first time, verifiable information corresponding to the client, and service information corresponding to the client.

[00108] It should be noted that, firstly, the embodiment of the present disclosure does not specifically limit the specific implementation of acquiring the device fingerprint ID corresponding to the client, and a person skilled in the art may make appropriate adjustments according to actual situations. For example, the device fingerprint ID sent by an external device can be received; or, the device fingerprint ID stored locally or on the cloud can be read; or, the device fingerprint ID can be generated for the first time according to the device parameters reported by the client, and so on.

[00109] Secondly, the embodiment of the present disclosure does not specifically limit the specific implementation of acquiring the device feature information corresponding to the client either, and those skilled in the art can perform appropriate adjustments according to the actual

situation. For example, the device feature information sent by an external device can be received; or, the device feature information stored locally or on the cloud can be read; or, the device feature information can be queried in real-time, and so on.

[00110] It can be understood that the manner of acquiring the device fingerprint ID corresponding to the client and the manner of acquiring the device feature information corresponding to the client can be the same, or can be different.

[00111] In the above step 2), the embodiment of the present disclosure does not specifically limit the specific implementation of generating the initial device fingerprint information according to the device fingerprint ID and the device feature information, and those skilled in the art can perform appropriate adjustments according to the actual situation. For example, the device fingerprint ID and the device feature information can be spliced together to obtain the initial device fingerprint information; or, the device fingerprint ID and the device feature information can be encrypted to obtain the initial device fingerprint information; or, the device fingerprint ID and the device feature information can be encoded to obtain the initial device fingerprint information, and so on.

[00112] In the above solution, the initial device fingerprint information can include the device fingerprint ID and the device feature information, so that more usage scenarios can be adapted and different verifications can be performed on the target device fingerprint information based on different scenarios, thereby reducing the risk of the device fingerprint ID being replaced or tampered, and ensuring the security of the device fingerprint.

[00113] Further, based on the above embodiment, the step of generating the initial device fingerprint information according to the device fingerprint ID and the device feature information can specifically include the following steps:

[00114] step 1), splicing the device fingerprint ID and the device feature information to obtain first device fingerprint information;

[00115] step 2), encrypting the first device fingerprint information to obtain second device fingerprint information; and

[00116] step 3), performing character transcoding on the second device fingerprint information to obtain the initial device fingerprint information.

[00117] Specifically, in the above step 1), the device fingerprint ID and the device feature information can be spliced together, so that first device fingerprint information can be obtained.

[00118] The manner of splicing the device fingerprint ID and the device feature information can be: adding the device feature information into the device fingerprint ID, for example: assuming that the device fingerprint ID is efg, and the device feature information can include A, B, and C, then the first device fingerprint information obtained after splicing can be efgABC.

[00119] It should be noted that the embodiment of the present disclosure does not specifically limit the specific position of adding the device feature information into the device fingerprint ID, and those skilled in the art can perform appropriate adjustments according to the actual situation. For example, the device feature information can be added after the device fingerprint ID (such as efgABC); or, the device feature information can be added before the device fingerprint ID (such as ABCefg); or, the device feature information can be added to the middle of the device fingerprint ID (such as eABfCg), and so on.

[00120] In the above step 2), the first device fingerprint information obtained by splicing in the above step 1) can be encrypted, so that the second device fingerprint information can be obtained.

[00121] It should be noted that the embodiment of the present disclosure does not specifically limit the specific implementation of encrypting the first device fingerprint information, and those skilled in the art can perform appropriate adjustments according to the actual situation. For example, one or more algorithms in symmetric encryption algorithms, asymmetric encryption algorithms, and hash algorithm can be used to encrypt the first device fingerprint information.

[00122] In the above step 3), the second device fingerprint information obtained by encryption in the above step 2) can be subjected to character transcoding, so that initial device fingerprint information can be obtained.

[00123] It should be noted that the embodiment of the present disclosure does not specifically limit the specific implementation of transcoding the second device fingerprint information, and those skilled in the art can perform appropriate adjustments according to the actual situation. For example, one or more transcoding manners among ASCII encoding, BASE64, and BASE62 character transcoding manners can be used to perform character transcoding on the second device fingerprint information.

[00124] In the above solution, after splicing the device fingerprint ID and the device feature information, the spliced first device fingerprint information can be encrypted and character transcoding can be performed, so as to further reduce the risk of the device fingerprint being replaced or tampered, and ensure the security of the device fingerprint.

[00125] Further, based on the above embodiment, the step of performing character transcoding on the second device fingerprint information to obtain the initial device fingerprint information specifically can include the following step:

[00126] performing character transcoding on the second device fingerprint information using a preset transcoding method to obtain the initial device fingerprint information, wherein the initial device fingerprint information does not include special characters.

[00127] Specifically, as one embodiment, the special characters described above can include one or more symbols among "+", "/", and "="; as another embodiment, in the preset transcoding method, BASE62 without special characters can be used to perform character transcoding on the second device fingerprint information, so that the initial device fingerprint information without special characters can be obtained.

[00128] In the above solution, the second device fingerprint information can be performed with a character transcoding using a preset transcoding method to obtain the initial device fingerprint information that does not include special characters. Since the device fingerprint will serve as a parameter of the request, and special characters present potential risks during transmission, the above transcoding method can reduce the above risks, thereby ensuring the security of the device fingerprint.

[00129] Referring to FIG.3, FIG. 3 is a flowchart of another device fingerprint verification method provided by the embodiment of the present disclosure. The device fingerprint verification method can be applied to the server, wherein the device fingerprint verification method can include the following steps:

[00130] step S301, acquiring initial device fingerprint information corresponding to a client and a first generation time;

[00131] step S302, generating the target device fingerprint information according to the initial device fingerprint information and the first generation time;

[00132] step S303, acquiring request data sent by a client;

[00133] step S304, restoring the first verification information corresponding to the first generation time according to the target device fingerprint information; and

[00134] step S305, verifying the target device fingerprint information according to the first verification information.

[00135] Specifically, in the above step S301, the initial device fingerprint information can be generated based on information related to the client. The information related to the client can include one or more items of information such as a device fingerprint ID, a time when the above device fingerprint ID is generated for the first time, verifiable information corresponding to the client, service information corresponding to the client, and the like.

[00136] The first generation time is the time of generating the target device fingerprint information, that is, the above first generation time can be the time when executing step S301 to step S302 provided by the embodiment of the present disclosure. As one implementation, the above first generation time can be the current time; as another implementation, the first generation time can be a future expected time for generating the target device fingerprint information. For example, the above first generation time can include at least one of year, month, day, hour, minute, and second.

[00137] In the above step S302, according to the initial device fingerprint information and the first generation time, the target device fingerprint information can be generated, wherein the target device fingerprint information includes the initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes the first generation time. Therefore, the initial device fingerprint information and the time information can be spliced together, so that the target device fingerprint information can be obtained.

[00138] In the above step S303, when the client needs to perform a service, the client can send request data to the server, so that the server can perform verification on the target device fingerprint information of the client based on the above request data. The above request data can include target device fingerprint information corresponding to the client.

[00139] In the above step S304, since the target device fingerprint information includes the initial device fingerprint information and the time information spliced with the initial device fingerprint information, the first verification information corresponding to the first generation time can be quickly restored from the target device fingerprint information.

[00140] As one implementation, if the time information includes the above first generation time, then the information at the position in the target device fingerprint information corresponding to the first generation time can be directly extracted to obtain the first verification information; as another implementation, if the first generation time is processed first, then after extracting the information at the position in the target device fingerprint information corresponding to the first generation time, inverse processing can be performed on the extracted data to obtain the first verification information.

[00141] In the above step S305, the objective of verifying the target device fingerprint information can be achieved by performing verification on the above first verification information. As one implementation, whether the first verification information is the same as the first generation time can be determined to perform verification on the first verification information.

[00142] If the first verification information is not the same as the first generation time, it indicates that the first verification information is abnormally verified, at this time, it indicates that the target device fingerprint information is abnormal, and subsequent processing can be directly performed as abnormal. For example, assuming that the first generation time is 2023 and the first verification information is 3023, then it indicates that the target device fingerprint information has been tampered with.

[00143] If the first verification information is the same as the first generation time, then it indicates that the verification of the first verification information is normal. At this time, as one implementation, it is considered that the target device fingerprint information is not abnormal; as another implementation, other verification manners are also adopted to further verify the target device fingerprint information.

[00144] In the above solution, after acquiring the initial device fingerprint information corresponding to the target device and the first generation time corresponding to the generation of the target device fingerprint information, the target device fingerprint information can be generated according to the initial device fingerprint information and the first generation time; based on the target device fingerprint information, the device fingerprint can be verified quickly, so as to determine whether replacement or tampering occurs in the use process of the device fingerprint, and ensure the security of the device fingerprint.

[00145] In summary, the above-mentioned device fingerprint verification method and device fingerprint generation method can be executed on the server. After the server generates the target device fingerprint information, the above target device fingerprint information can be issued to the client; after the client receives the above target device fingerprint information, the above target device fingerprint information can be stored; when the client needs to perform a data request, the above target device fingerprint information can be carried, and the corresponding server, after receiving the data request from the client, can verify the target device fingerprint information carried in the above data request.

[00146] Referring to FIG.4, FIG. 4 is a block diagram of a structure of a device fingerprint verification apparatus provided by the embodiment of the present disclosure. The device fingerprint verification apparatus 400 includes: a first acquisition module 401, configured for acquiring request data sent by a client, wherein the request data includes target device fingerprint information corresponding to the client, the target device fingerprint information includes initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes a first generation time of generating the target device fingerprint information; a first restoring module 402, configured for restoring the first verification information corresponding to the first generation time according to the target device fingerprint information; and a first verification module 403, configured for verifying the target device fingerprint information according to the first verification information.

[00147] In the above solution, after acquiring the target device fingerprint information corresponding to the target device, since the target device fingerprint information includes the initial device fingerprint information and the time information spliced therewith, the first verification information corresponding to the first generation time in the time information can be restored, and the target device fingerprint information can be verified quickly based on the first verification information, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[00148] In an optional embodiment, the device fingerprint verification apparatus 400 further includes: a second restoring module, configured for restoring, when the verification of the first verification information is normal, second verification information corresponding to the initial device fingerprint information according to the target device fingerprint information; and a second verification module, configured for verifying the target device fingerprint information according to the second verification information.

[00149] In the above solution, if the verification of the first verification information is normal, the target device fingerprint information can be further verified, and more accurate verification of the target device fingerprint information is performed by restoring the second verification information corresponding to the initial device fingerprint information, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[00150] In optional embodiments, the second verification module is specifically configured for: decrypting the second verification information; and determining whether the second verification information is successfully decrypted, wherein unsuccessful decryption of the second verification information indicates that the target device fingerprint information is abnormal.

[00151] In the above solution, the decryption verification of the target device fingerprint information can be realized by decrypting the second verification information, so as to improve the accuracy of the verification and ensure the security of the device fingerprint.

[00152] In an optional embodiment, the initial device fingerprint information includes service information, and the device fingerprint verification apparatus 400 further includes: a judgment module, configured for determining whether a service verification information is the same as the service information when the second verification information is successfully decrypted and corresponding third verification information is obtained, wherein the service verification information is verification information in the third verification information corresponding to the service information, and the service verification information being not the same as the service information indicates that the target device fingerprint information is abnormal.

[00153] In the above solution, if the second verification information is verified to be normal, the target device fingerprint information can be further verified, and service verification of the target device fingerprint information is realized by determining whether the service verification information in the decrypted third verification information is the same as the service information, so as to improve the accuracy of the service verification and ensure the security of the device fingerprint.

[00154] Referring to FIG.5, FIG. 5 is a block diagram of a structure of a device fingerprint generation apparatus provided by the embodiment of the present disclosure. The device

fingerprint generation apparatus 500 includes: a second acquisition module 501, configured for acquiring initial device fingerprint information corresponding to a client and a first generation time, wherein the first generation time is a time for generating target device fingerprint information; and a first generation module 502, configured for generating the target device fingerprint information according to the initial device fingerprint information and the first generation time, wherein the target device fingerprint information includes the initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes the first generation time.

[00155] In the above solution, after acquiring the initial device fingerprint information corresponding to the target device and the first generation time corresponding to the generation of the target device fingerprint information, the target device fingerprint information can be generated according to the initial device fingerprint information and the first generation time; based on the target device fingerprint information, the device fingerprint can be verified, so as to determine whether replacement or tampering occurs in the use process of the device fingerprint, and ensure the security of the device fingerprint.

[00156] In optional embodiments, the first generation module 502 is specifically configured for: splicing the initial device fingerprint information and the first generation time to obtain the target device fingerprint information.

[00157] In the above solution, the initial device fingerprint information and the first generation time can be spliced together, so that the target device fingerprint information can be quickly verified based on the first generation time, so as to determine whether replacement or tampering occurs in the use process of the target device fingerprint information, and ensure the security of the device fingerprint.

[00158] In optional embodiments, the first generation module 502 is specifically configured for: encoding the first generation time to obtain the time information; and splicing the initial device fingerprint information and the time information to obtain the target device fingerprint information.

[00159] In the above solution, the first generation time can be encoded first, and then the initial fingerprint information can be spliced with the encoded time information, so that the data amount of the target device fingerprint information can be reduced on the basis of realizing quick verification.

[00160] In optional embodiments, the second acquisition module 501 is specifically configured for: acquiring a device fingerprint ID and device feature information corresponding to the client, wherein the device feature information includes at least one of: a second generation time for generating the device fingerprint ID for the first time, verifiable information corresponding to the client, and service information corresponding to the client; and generating the initial device fingerprint information according to the device fingerprint ID and the device feature information.

[00161] In the above solution, the initial device fingerprint information can include the device fingerprint ID and the device feature information, so that more usage scenarios can be adapted and different verifications can be performed on the target device fingerprint information based on different scenarios, thereby reducing the risk of the device fingerprint ID being replaced or tampered, and ensuring the security of the device fingerprint.

[00162] In optional embodiments, the second acquisition module 501 is further configured for: splicing the device fingerprint ID and the device feature information to obtain first device fingerprint information; encrypting the first device fingerprint information to obtain second device fingerprint information; and performing character transcoding on the second device fingerprint information to obtain the initial device fingerprint information.

[00163] In the above solution, after splicing the device fingerprint ID and the device feature information, the spliced first device fingerprint information can be encrypted and character transcoding can be performed, so as to further reduce the risk of the device fingerprint being replaced or tampered, and ensure the security of the device fingerprint.

[00164] In optional embodiments, the second acquisition module 501 is further configured for: performing character transcoding on the second device fingerprint information using a preset transcoding method to obtain the initial device fingerprint information, wherein the initial device fingerprint information does not include special characters.

[00165] In the above solution, the second device fingerprint information can be performed with a character transcoding using a preset transcoding method to obtain the initial device fingerprint information that does not include special characters. Since the device fingerprint will serve as a parameter of the request, and special characters present potential risks during transmission, the above transcoding method can reduce the above risks, thereby ensuring the security of the device fingerprint.

[00166] Referring to FIG.6, FIG. 6 is a block diagram of a structure of another device fingerprint verification apparatus provided by the embodiment of the present disclosure. The device fingerprint verification apparatus 600 includes: a third acquisition module 601, configured for acquiring initial device fingerprint information corresponding to a client and a first generation time, wherein the first generation time is a time for generating target device fingerprint information; a second generation module 602, configured for generating the target device fingerprint information according to the initial device fingerprint information and the first generation time, wherein the target device fingerprint information includes the initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information includes the first generation time; a fourth acquisition module 603, configured for acquiring request data sent by a client, wherein the request data includes target device fingerprint information corresponding to the client; a third restoring module 604, configured for restoring the first verification information corresponding to the first generation time according to the target device fingerprint information; and a third verification module 605, configured for verifying the target device fingerprint information according to the first verification information.

[00167] In the above solution, after acquiring the initial device fingerprint information corresponding to the target device and the first generation time corresponding to the generation of the target device fingerprint information, the target device fingerprint information can be generated according to the initial device fingerprint information and the first generation time; based on the target device fingerprint information, the device fingerprint can be verified quickly, so as to determine whether replacement or tampering occurs in the use process of the device fingerprint, and ensure the security of the device fingerprint.

[00168] Referring to FIG. 7, FIG. 7 is a block diagram of a structure of an electronic device provided by the embodiment of the present disclosure. The electronic device 700 includes: at

least one processor 701, at least one communication interface 702, at least one memory 703, and at least one communication bus 704. The communication bus 704 is configured to implement direct connection communication among these components, the communication interface 702 is configured to perform signaling or data communication with other node devices, and the memory 703 stores machine-readable instructions executable by the processor 701. When the electronic device 700 operates, the processor 701 communicates with the memory 703 via the communication bus 704, and the machine-readable instructions are executed by the processor 701 when invoked, so as to implement the above-described device fingerprint verification method or device fingerprint generation method.

[00169] For example, the processor 701 of the embodiment of the present disclosure can implement the following method by reading a computer program from the memory 703 via the communication bus 704 and executing the computer program: step S101, acquiring request data sent by a client; step S102, restoring first verification information corresponding to the first generation time according to the target device fingerprint information; and step S103, verifying the target device fingerprint information according to the first verification information. Alternatively, the following method can be implemented: step S201, acquiring initial device fingerprint information corresponding to a client and a first generation time; and step S202, generating the target device fingerprint information according to the initial device fingerprint information and the first generation time.

[00170] One or more processors 701 are provided, which can be an integrated circuit chip having signal processing capability. The processor 701 can be a general-purpose processor, including a central processing unit (CPU), a micro controller unit (MCU), a network processor (NP), or other conventional processors; it can also be a dedicated processor, including a neural-network processing unit (NPU), a graphics processing unit (GPU), a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), or other programmable logic devices, discrete gate or transistor logic devices, and discrete hardware components. Moreover, when the processor 701 includes multiple processors, a part thereof can be a general-purpose processor, and another part can be a dedicated processor.

[00171] One or more memories 703 are provided, and can be, but is not limited to, a random access memory (RAM), a read-only memory (ROM), a programmable read-only memory (PROM), an erasable programmable read-only memory (EPROM), an electric erasable programmable read-only memory (EEPROM), etc.

[00172] It can be understood that the structure shown in FIG. 7 is merely schematic, and the electronic device 700 can also include more or fewer components than those shown in FIG. 7 or can have a configuration different from that shown in FIG. 7. The components shown in FIG. 7 can be implemented by hardware, software, or a combination thereof. In the embodiment of the present disclosure, the electronic device 700 can be, but is not limited to, a desktop computer, a laptop, a smartphone, a smart wearable device, an in-vehicle device, or other physical devices, and can also be a virtual device such as a virtual machine. Further, the electronic device 700 is not necessarily a single device, and can also be a combination of multiple devices, such as a server cluster, and so on.

[00173] The embodiments of the present disclosure further provide a computer-readable storage medium, wherein the computer-readable storage medium stores computer program instructions. The computer program instructions, when executed by a computer, cause the

computer to perform the device fingerprint verification method or the device fingerprint generation method described in the above method embodiments.

[00174] In the embodiments provided by the present disclosure, it should be understood that the disclosed apparatuses and methods can also be implemented in other manners. The above-described embodiments of the device are merely schematic, for example, the division of the units described, which is only a logical functional division, can be divided in another way when actually implemented; also, for example, multiple units or components can be combined or can be integrated into another system, or some features can be ignored, or not implemented. On another point, the mutual coupling or direct coupling or communication connection shown or discussed herein can be an indirect coupling or communication connection through communication interfaces, devices or units, which can be electrical, mechanical or other forms.

[00175] In addition, the units illustrated as separate components can/cannot be physically separated, and the components displayed as units can/cannot be physical units, i.e., they can be located in one place or distributed to a plurality of network units. Some or all of these units can be selected according to actual needs to achieve the objective of the embodiment solution.

[00176] Further, each functional module in each embodiment of the present disclosure can be integrated together to form a separate part, or each module may exist separately, or two or more modules may be integrated to form a separate part.

[00177] It should be noted that functionality can be stored in a computer-readable storage medium if implemented as a software function module and sold or used as a standalone product. Based on this understanding, the technical solution of the present disclosure can essentially be embodied in the form of a software product, which contributes to or includes parts in the prior art. The software product is stored in a storage medium and includes multiple instructions for causing a computer device (which can be a personal computer, server, network device, etc.) to execute all or some of the steps of the methods described in various embodiments of the present disclosure. The aforementioned storage media include various media that can store program code, such as USB drives, external hard drives, read-only memory (ROM), random access memory (RAM), disks, or optical discs.

[00178] In this context, relationship terms such as first and second are used only to distinguish one entity or operation from another, without necessarily requiring or implying any such actual relationship or order between those entities or operations.

[00179] The above is only an embodiment of the present disclosure, which is not intended to limit the scope of protection of the present disclosure, and the present disclosure can have various changes and variations for those skilled in the art. Any modification, equivalent substitution, improvement, etc. made within the spirit and principles of the present disclosure shall be included in the scope of protection of the present disclosure.

CLAIMS

1. A device fingerprint verification method, comprising:

acquiring request data sent by a client, wherein the request data comprises target device fingerprint information corresponding to the client, the target device fingerprint information comprises initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information comprises a first generation time of generating the target device fingerprint information;

restoring first verification information corresponding to the first generation time according to the target device fingerprint information; and

verifying the target device fingerprint information according to the first verification information.
2. The device fingerprint verification method according to claim 1, wherein after the step of verifying the target device fingerprint information according to the first verification information, the method further comprises:

restoring, when a verification of the first verification information is normal, second verification information corresponding to the initial device fingerprint information according to the target device fingerprint information; and

verifying the target device fingerprint information according to the second verification information.
3. The device fingerprint verification method according to claim 2, wherein the step of verifying the target device fingerprint information according to the second verification information comprises:

decrypting the second verification information; and

determining whether the second verification information is successfully decrypted, wherein unsuccessful decryption of the second verification information indicates that the target device fingerprint information is abnormal.
4. The device fingerprint verification method according to claim 3, wherein the initial device fingerprint information comprises service information; after determining whether the second verification information is successfully decrypted, the method further comprises:

determining whether a service verification information is the same as the service information when the second verification information is successfully decrypted and corresponding third verification information is obtained, wherein the service verification information is verification information in the third verification information corresponding to the service information, and the service verification information being not the same as the service information indicates that the target device fingerprint information is abnormal.

5. A device fingerprint generation method, comprising:

acquiring initial device fingerprint information corresponding to a client and a first generation time, wherein the first generation time is a time for generating target device fingerprint information; and

generating the target device fingerprint information according to the initial device fingerprint information and the first generation time, wherein the target device fingerprint information comprises the initial device fingerprint information and time information spliced with the initial device fingerprint information, and the time information comprises the first generation time.

6. The device fingerprint generation method according to claim 5, wherein the step of generating the target device fingerprint information according to the initial device fingerprint information and the first generation time comprises:

splicing the initial device fingerprint information and the first generation time to obtain the target device fingerprint information.

7. The device fingerprint generation method according to claim 5, wherein the step of generating the target device fingerprint information according to the initial device fingerprint information and the first generation time comprises:

encoding the first generation time to obtain the time information; and

splicing the initial device fingerprint information and the time information to obtain the target device fingerprint information.

8. The device fingerprint generation method according to any one of claims 5 to 7, wherein the step of acquiring initial device fingerprint information corresponding to a client comprises:

acquiring a device fingerprint ID and device feature information corresponding to the client, wherein the device feature information comprises at least one of: a second generation time for generating the device fingerprint ID for the first time, verifiable information corresponding to the client, and service information corresponding to the client; and

generating the initial device fingerprint information according to the device fingerprint ID and the device feature information.

9. The device fingerprint generation method according to claim 8, wherein the step of generating the initial device fingerprint information according to the device fingerprint ID and the device feature information comprises:

splicing the device fingerprint ID and the device feature information to obtain first device fingerprint information;

encrypting the first device fingerprint information to obtain second device fingerprint information; and

performing character transcoding on the second device fingerprint information to obtain the initial device fingerprint information.

10. The device fingerprint generation method according to claim 9, wherein the step of performing character transcoding on the second device fingerprint information to obtain the initial device fingerprint information comprises:

performing the character transcoding on the second device fingerprint information using a preset transcoding method to obtain the initial device fingerprint information, wherein the initial device fingerprint information does not comprise special characters.

11. An electronic device, comprising a processor, a memory, and a bus, wherein

the processor and the memory communicate with each other through the bus; and

the memory stores computer program instructions executable by the processor; and the processor, when invoking the computer program instructions, is capable of performing the device fingerprint verification method according to any one of claims 1 to 4 or the device fingerprint generation method according to any one of claims 5 to 10.

12. A computer-readable storage medium, wherein the computer-readable storage medium stores computer program instructions, and the computer program instructions, when executed by a computer, cause the computer to perform the device fingerprint verification method according to any one of claims 1 to 4 or the device fingerprint generation method according to any one of claims 5 to 10.