

一种设备指纹校验方法、设备指纹生成方法及电子设备

相关申请的交叉引用

本申请要求享有于 2024 年 02 月 23 日提交的名称为“一种设备指纹校验方法、设备指纹生成方法及电子设备”的中国专利申请 CN202410204010.0 的优先权，该申请的全部内容通过引用并入本文中。

技术领域

本申请属于网络安全技术领域，特别是涉及一种设备指纹校验方法、设备指纹生成方法及电子设备。

背景技术

设备指纹用于唯一标识出设备的设备特征或者独特的设备标识。其中，设备指纹可以包括一些固有的、较难篡改的、唯一的设备标识以及设备的特征集合等，例如：手机在生产过程中都会被赋予一个唯一的国际移动设备识别码（International Mobile Equipment Identity, IMEI）编号，用于唯一标识该台设备；再如：电脑的网卡，在生产过程中会被赋予唯一的媒体访问控制地址（Media Access Control Address, MAC 地址）。但是，设备指纹在使用过程中，可能发生被替换、篡改的情况，从而导致设备指纹的安全性得不到保证。

发明内容

本申请提供一种设备指纹校验方法、设备指纹生成方法及电子设备，用于解决现有技术中设备指纹被替换、被篡改从而导致设备指纹的安全性得不到保证的技术问题。

第一方面，本申请实施例提供了一种设备指纹校验方法，包括：获取客户端发送的请求数据；其中，所述请求数据包括所述客户端对应的目标设备指纹信息，所述目标设备指纹信息包括初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括生成所述目标设备指纹信息的第一生成时间；根据所述目标设备指纹信息还原与所述第一生成时间对应的第一校验信息；根据所述第一校验信息对所述目标设备指纹信息进行校验。

在上述方案中，在获取到目标设备对应的目标设备指纹信息后，由于上述目标设备指纹信息包括初始设备指纹信息以及与其拼接的时间信息，因此可以通过还原与时间信息中的第一生成时间对应的第一校验信息，快速的基于上述第一校验信息对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，在所述根据所述第一校验信息对所述目标设备指纹信息进行校验之后，所述方法还包括：若所述第一校验信息校验正常，则根据所述目标设备指纹信息还原与所述初始设备指纹信息对应的第二校验信息；根据所述第二校验信息对所述目标设备指纹信息进行校验。在

上述方案中，若第一校验信息校验正常，则可以对目标设备指纹信息进行进一步校验，通过还原与初始设备指纹信息对应的第二校验信息，更准确的对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述根据所述第二校验信息对所述目标设备指纹信息进行校验，包括：对所述第二校验信息进行解密；判断所述第二校验信息是否解密成功；其中，所述第二校验信息解密不成功表征所述目标设备指纹信息存在异常。在上述方案中，可以通过对第二校验信息进行解密，实现对目标设备指纹信息的解密校验，从而提高校验的准确性，保证设备指纹的安全性。

在可选的实施方式中，所述初始设备指纹信息包括业务信息；在所述判断所述第二校验信息是否解密成功之后，所述方法还包括：若所述第二校验信息解密成功并得到对应的第三校验信息，则判断业务校验信息与所述业务信息是否相同；其中，所述业务校验信息为所述第三校验信息中与所述业务信息对应的校验信息，所述业务校验信息与所述业务信息不相同表征所述目标设备指纹信息存在异常。在上述方案中，若第二校验信息校验正常，则可以对目标设备指纹信息进行进一步校验，通过判断解密得到的第三校验信息中的业务校验信息与业务信息是否相同，从而实现对目标设备指纹信息的业务校验，从而提高校验的准确性，保证设备指纹的安全性。

第二方面，本申请实施例提供了一种设备指纹生成方法，包括：获取客户端对应的初始设备指纹信息以及第一生成时间；其中，所述第一生成时间为生成目标设备指纹信息的时间；根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息；其中，所述目标设备指纹信息包括所述初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括所述第一生成时间。

在上述方案中，在获取到目标设备对应的初始设备指纹信息以及生成目标设备指纹信息对应的第一生成时间后，可以根据上述初始设备指纹信息与第一生成时间生成目标设备指纹信息；基于上述目标设备指纹信息可以对设备指纹进行校验，从而判断设备指纹在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息，包括：拼接所述初始设备指纹信息以及所述第一生成时间，得到所述目标设备指纹信息。在上述方案中，可以将初始设备指纹信息以及第一生成时间拼接起来，从而可以快速的基于第一生成时间对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息，包括：对所述第一生成时间进行编码，得到所述时间信息；拼接所述初始设备指纹信息以及所述时间信息，得到所述目标设备指纹信息。在上述方案中，可以先对第一生成时间进行

编码后，再将初始指纹信息与编码后的时间信息拼接起来，从而可以在实现快速校验的基础上，降低目标设备指纹信息的数据量。

在可选的实施方式中，所述获取客户端对应的初始设备指纹信息，包括：获取所述客户端对应的设备指纹 ID 以及设备特征信息；其中，所述设备特征信息包括首次生成所述设备指纹 ID 的第二生成时间、所述客户端对应的可校验信息以及所述客户端对应的业务信息中的至少一项；根据所述设备指纹 ID 以及所述设备特征信息生成所述初始设备指纹信息。在上述方案中，初始设备指纹信息可以包括设备指纹 ID 以及设备特征信息，从而可以适配更多的使用场景并基于不同的场景对目标设备指纹信息进行不同的校验，从而降低设备指纹 ID 被替换、篡改的风险，保证设备指纹的安全性。

在可选的实施方式中，所述根据所述设备指纹 ID 以及所述设备特征信息生成所述初始设备指纹信息，包括：拼接所述设备指纹 ID 以及所述设备特征信息，得到第一设备指纹信息；对所述第一设备指纹信息进行加密，得到第二设备指纹信息；对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息。在上述方案中，可以在拼接设备指纹 ID 以及设备特征信息后，对拼接得到的第一设备指纹信息进行加密以及字符转码，从而进一步降低设备指纹被替换、篡改的风险，保证设备指纹的安全性。

在可选的实施方式中，所述对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息，包括：利用预设的转码方法对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息；其中，所述初始设备指纹信息中不包括特殊字符。在上述方案中，可以使用预设的转码方法对第二设备指纹信息进行字符转码，从而得到不包括特殊字符的初始设备指纹信息；由于设备指纹会作为请求的参数，特殊字符在传输过程中存在风险隐患，因此采用上述转码方式可以降低上述风险，从而保证设备指纹的安全性。

第三方面，本申请实施例提供另一种设备指纹校验方法，包括：获取客户端对应的初始设备指纹信息以及第一生成时间；其中，所述第一生成时间为生成目标设备指纹信息的时间；根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息；其中，所述目标设备指纹信息包括所述初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括所述第一生成时间；获取客户端发送的请求数据；其中，所述请求数据包括所述客户端对应的目标设备指纹信息；根据所述目标设备指纹信息还原与所述第一生成时间对应的第一校验信息；根据所述第一校验信息对所述目标设备指纹信息进行校验。

在上述方案中，在获取到目标设备对应的初始设备指纹信息以及生成目标设备指纹信息对应的第一生成时间后，可以根据上述初始设备指纹信息与第一生成时间生成目标设备指纹信息；基于上述目标设备指纹信息可以快速对设备指纹进行校验，从而判断设备指纹在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

第四方面，本申请实施例提供了一种设备指纹校验装置，包括：第一获取模块，用于获取客户端发送的请求数据；其中，所述请求数据包括所

述客户端对应的目标设备指纹信息，所述目标设备指纹信息包括初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括生成所述目标设备指纹信息的第一生成时间；第一还原模块，用于根据所述目标设备指纹信息还原与所述第一生成时间对应的第一校验信息；第一校验模块，用于根据所述第一校验信息对所述目标设备指纹信息进行校验。

在上述方案中，在获取到目标设备对应的目标设备指纹信息后，由于上述目标设备指纹信息包括初始设备指纹信息以及与其拼接的时间信息，因此可以通过还原与时间信息中的第一生成时间对应的第一校验信息，快速的基于上述第一校验信息对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述设备指纹校验装置还包括：第二还原模块，用于若所述第一校验信息校验正常，则根据所述目标设备指纹信息还原与所述初始设备指纹信息对应的第二校验信息；第二校验模块，用于根据所述第二校验信息对所述目标设备指纹信息进行校验。在上述方案中，若第一校验信息校验正常，则可以对目标设备指纹信息进行进一步校验，通过还原与初始设备指纹信息对应的第二校验信息，更准确的对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述第二校验模块具体用于：对所述第二校验信息进行解密；判断所述第二校验信息是否解密成功；其中，所述第二校验信息解密不成功表征所述目标设备指纹信息存在异常。在上述方案中，可以通过对第二校验信息进行解密，实现对目标设备指纹信息的解密校验，从而提高校验的准确性，保证设备指纹的安全性。

在可选的实施方式中，所述初始设备指纹信息包括业务信息；所述设备指纹校验装置还包括：判断模块，用于若所述第二校验信息解密成功并得到对应的第三校验信息，则判断业务校验信息与所述业务信息是否相同；其中，所述业务校验信息为所述第三校验信息中与所述业务信息对应的校验信息，所述业务校验信息与所述业务信息不相同表征所述目标设备指纹信息存在异常。在上述方案中，若第二校验信息校验正常，则可以对目标设备指纹信息进行进一步校验，通过判断解密得到的第三校验信息中的业务校验信息与业务信息是否相同，从而实现对目标设备指纹信息的业务校验，从而提高校验的准确性，保证设备指纹的安全性。

第五方面，本申请实施例提供一种设备指纹生成装置，包括：第二获取模块，用于获取客户端对应的初始设备指纹信息以及第一生成时间；其中，所述第一生成时间为生成目标设备指纹信息的时间；第一生成模块，用于根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息；其中，所述目标设备指纹信息包括所述初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括所述第一生成时间。

在上述方案中，在获取到目标设备对应的初始设备指纹信息以及生成目标设备指纹信息对应的第一生成时间后，可以根据上述初始设备指纹信息与第一生成时间生成目标设备指纹信息；基于上述目标设备指纹信息可以对设备指纹进行校验，从而判断设备指纹在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述第一生成模块具体用于：拼接所述初始设备指纹信息以及所述第一生成时间，得到所述目标设备指纹信息。在上述方案中，可以将初始设备指纹信息以及第一生成时间拼接起来，从而可以快速的基于第一生成时间对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述第一生成模块具体用于：对所述第一生成时间进行编码，得到所述时间信息；拼接所述初始设备指纹信息以及所述时间信息，得到所述目标设备指纹信息。在上述方案中，可以先对第一生成时间进行编码后，再将初始指纹信息与编码后的时间信息拼接起来，从而可以在实现快速校验的基础上，降低目标设备指纹信息的数据量。

在可选的实施方式中，所述第二获取模块具体用于：获取所述客户端对应的设备指纹 ID 以及设备特征信息；其中，所述设备特征信息包括首次生成所述设备指纹 ID 的第二生成时间、所述客户端对应的可校验信息以及所述客户端对应的业务信息中的至少一项；根据所述设备指纹 ID 以及所述设备特征信息生成所述初始设备指纹信息。在上述方案中，初始设备指纹信息可以包括设备指纹 ID 以及设备特征信息，从而可以适配更多的使用场景并基于不同的场景对目标设备指纹信息进行不同的校验，从而降低设备指纹 ID 被替换、篡改的风险，保证设备指纹的安全性。

在可选的实施方式中，所述第二获取模块还用于：拼接所述设备指纹 ID 以及所述设备特征信息，得到第一设备指纹信息；对所述第一设备指纹信息进行加密，得到第二设备指纹信息；对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息。在上述方案中，可以在拼接设备指纹 ID 以及设备特征信息后，对拼接得到的第一设备指纹信息进行加密以及字符转码，从而进一步降低设备指纹被替换、篡改的风险，保证设备指纹的安全性。

在可选的实施方式中，所述第二获取模块还用于：利用预设的转码方法对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息；其中，所述初始设备指纹信息中不包括特殊字符。在上述方案中，可以使用预设的转码方法对第二设备指纹信息进行字符转码，从而得到不包括特殊字符的初始设备指纹信息；由于设备指纹会作为请求的参数，特殊字符在传输过程中存在风险隐患，因此采用上述转码方式可以降低上述风险，从而保证设备指纹的安全性。

第六方面，本申请实施例提供了另一种设备指纹校验装置，包括：第三获取模块，用于获取客户端对应的初始设备指纹信息以及第一生成时间；其中，所述第一生成时间为生成目标设备指纹信息的时间；第二生成模块，

用于根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息；其中，所述目标设备指纹信息包括所述初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括所述第一生成时间；第四获取模块，用于获取客户端发送的请求数据；其中，所述请求数据包括所述客户端对应的目标设备指纹信息；第三还原模块，用于根据所述目标设备指纹信息还原与所述第一生成时间对应的第一校验信息；第三校验模块，用于根据所述第一校验信息对所述目标设备指纹信息进行校验。

在上述方案中，在获取到目标设备对应的初始设备指纹信息以及生成目标设备指纹信息对应的第一生成时间后，可以根据上述初始设备指纹信息与第一生成时间生成目标设备指纹信息；基于上述目标设备指纹信息可以快速对设备指纹进行校验，从而判断设备指纹在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

第七方面，本申请实施例提供了一种电子设备，包括：处理器、存储器和总线；所述处理器和所述存储器通过所述总线完成相互间的通信；所述存储器存储有可被所述处理器执行的计算机程序指令，所述处理器调用所述计算机程序指令能够执行如第一方面、第三方面所述的设备指纹校验方法或者如第二方面所述的设备指纹生成方法。

第八方面，本申请实施例提供一种计算机可读存储介质，所述计算机可读存储介质存储计算机程序指令，所述计算机程序指令被计算机运行时，使所述计算机执行如第一方面、第三方面所述的设备指纹校验方法或者如第二方面所述的设备指纹生成方法。

本申请的其他特征和优点将在随后的说明书阐述，并且，部分地从说明书中变得显而易见，或者通过实施本申请实施例了解。本申请的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他相关的附图。

图1为本申请实施例提供了一种设备指纹校验方法的流程图；

图2为本申请实施例提供了一种设备指纹生成方法的流程图；

图3为本申请实施例提供的另一种设备指纹校验方法的流程图；

图4为本申请实施例提供了一种设备指纹校验装置的结构框图；

图5为本申请实施例提供了一种设备指纹生成装置的结构框图；

图6为本申请实施例提供的另一种设备指纹校验装置的结构框图；

图7为本申请实施例提供了一种电子设备的结构框图。

具体实施方式

下面将结合本申请实施例中附图，对本申请实施例中的技术方案进行清楚、完整地描述。

需要说明的是，本发明实施例中的术语“多个”是指两个或两个以上，鉴于此，本发明实施例中也可以将“多个”理解为“至少两个”。“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，字符“/”，如无特殊说明，一般表示前后关联对象是一种“或”的关系。

请参照图 1，图 1 为本申请实施例提供的一种设备指纹校验方法的流程图，该设备指纹校验方法可以应用于服务端，其中，设备指纹校验方法可以包括如下步骤：

步骤 S101：获取客户端发送的请求数据。

步骤 S102：根据目标设备指纹信息还原与第一生成时间对应的第一校验信息。

步骤 S103：根据第一校验信息对目标设备指纹信息进行校验。

具体的，在上述步骤 S101 中，在客户端需要执行业务时，客户端可以向服务端发送请求数据，以使服务端可以基于上述请求数据对客户端的目标设备指纹信息进行校验。

其中，上述请求数据可以包括客户端对应的目标设备指纹信息。作为一种实施方式，上述目标设备指纹信息可以包括初始设备指纹信息以及时间信息；通过拼接上述初始设备指纹信息以及时间信息可以生成上述目标设备指纹信息。

初始设备指纹信息可以是基于与客户端相关的信息生成的。需要说明的是，首先，本申请实施例对上述与客户端相关的信息的具体实施方式不作具体的限定，本领域技术人员可以根据实际情况进行合适的调整。举例来说，与客户端相关的信息可以包括设备指纹身份标识 (Identity Document, ID)、首次生成上述设备指纹 ID 的时间、客户端对应的可校验信息、客户端对应的业务信息等信息中的一项或者多项信息。

其中，在本申请实施例中，设备指纹 ID 是指用于唯一标识出客户端的设备特征或者独特的设备标识，设备指纹信息是指根据设备指纹 ID 生成的用于标识出目标设备的设备标识。其中，两者的不同点在于，一个客户端仅对应一个设备指纹 ID，但可以对应多个设备指纹信息。

首次创建设备指纹 ID 的时间可以在校验时提供一些时间信息，以方便查询历史，同时也可以用来进行合法时间校验；客户端对应的可校验信息可以包括目标设备相关的属性信息，例如：安卓 ID、设备机型等信息；业务信息可以用于表征客户端上相应的业务，举例来说，假设有两个应用程序 (Application, App)，同一个设备安装这两个 App，其设备指纹 ID 相同，但是为了区分这两个 App，可以生成两个不同的业务信息，从而使得两个 APP 下发的目标设备指纹信息是不同的。

其次，本申请实施例对生成上述初始设备指纹信息的具体实施方式同样不作具体的限定，本领域技术人员可以根据实际情况进行合适的调整。

举例来说，可以将与客户端相关的信息输入预先训练好的神经网络模型中，输出上述初始设备指纹信息；或者，可以拼接多个与客户端相关的信息，得到上述初始设备指纹信息；或者，可以对与客户端相关的信息进行加密后，得到上述初始设备指纹信息等。

时间信息可以基于生成目标设备指纹信息的第一生成时间得到。作为一种实施方式，时间信息可以包括上述第一生成时间；作为另一种实施方式，可以先对上述第一生成时间进行处理后，再得到上述时间信息。可以理解的是，本申请实施例对上述处理第一生成时间的具体实施方式不作具体的限定，本领域技术人员可以根据实际情况进行合适的调整；举例来说，可以对第一生成时间进行压缩、加密、转码等一种或者多种处理。

在上述步骤 S102 中，由于目标设备指纹信息中包括初始设备指纹信息以及与初始设备指纹信息拼接的时间信息，因此，可以快速的将目标设备指纹信息中与第一生成时间对应的第一校验信息还原出来。

作为一种实施方式，若时间信息包括上述第一生成时间，则可以直接将目标设备指纹信息中与第一生成时间对应位置处的信息提取出来，即可得到第一校验信息；作为另一种实施方式，若先对第一生成时间进行了处理，则可以在将目标设备指纹信息中与第一生成时间对应位置处的信息提取出来后，对提取出来的数据进行相反的处理，即可得到第一校验信息。

在上述步骤 S103 中，可以通过对上述第一校验信息进行校验，实现对目标设备指纹信息进行校验的目的。作为一种实施方式，可以通过判断第一校验信息与第一生成时间是否相同，从而实现对第一校验信息进行校验。

其中，若第一校验信息与第一生成时间不相同，则表征第一校验信息校验异常，此时，说明目标设备指纹信息存在异常，可以直接按照异常进行后续处理。举例来说，假设第一生成时间为 2023，第一校验信息为 3023，则说明目标设备指纹信息被篡改了。

若第一校验时间与第一生成时间相同，则表征第一校验信息校验正常。此时，作为一种实施方式，可以认为目标设备指纹信息不存在异常；作为另一种实施方式，也可以采取其他校验方式对目标设备指纹信息进行进一步校验。

在上述方案中，在获取到目标设备对应的目标设备指纹信息后，由于上述目标设备指纹信息包括初始设备指纹信息以及与其拼接的时间信息，因此可以通过还原与时间信息中的第一生成时间对应的第一校验信息，快速的基于上述第一校验信息对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

进一步的，在上述实施例的基础上，在上述步骤 S103 之后，本申请实施例提供的设备指纹校验方法还可以包括如下步骤：

步骤 1)，若第一校验信息校验正常，则根据目标设备指纹信息还原与初始设备指纹信息对应的第二校验信息。

步骤 2)，根据第二校验信息对目标设备指纹信息进行校验。

具体的，在上述步骤 1) 中，若第一校验信息校验正常，则可以采取其

他校验方式对目标设备指纹信息进行进一步校验。作为一种实施方式，可以根据目标设备指纹信息还原与初始设备指纹信息对应的第二校验信息。

需要说明的是，本申请实施例对还原上述初始设备指纹信息的具体实施方式不作具体的限定，本领域技术人员可以根据生成上述初始设备指纹信息的具体实施方式进行合适的调整。举例来说，可以对初始设备指纹信息进行拆分；或者，可以对初始指纹信息进行解密；或者，可以对初始设备指纹信息解码等。

在上述步骤 2) 中，可以通过对上述第二校验信息进行校验，实现对目标设备指纹信息进行校验的目的。需要说明的是，本申请实施例对校验上述第二校验信息的具体实施方式不作具体的限定，本领域技术人员可以根据初始设备指纹信息的具体实施方式进行合适的调整。举例来说，若初始设备指纹信息是通过加密得到的，则可以判断第二校验信息是否能够正常解密；或者，若初始设备指纹信息中包括设备指纹 ID，则可以判断第二校验信息与设备指纹 ID 是否相同；或者，若初始设备指纹信息中包括业务信息，则可以判断第二校验信息与业务信息是否相同等。

在上述方案中，若第一校验信息校验正常，则可以对目标设备指纹信息进行进一步校验，通过还原与初始设备指纹信息对应的第二校验信息，更准确的对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

进一步的，在上述实施例的基础上，上述根据第二校验信息对目标设备指纹信息进行校验的步骤，具体可以包括如下步骤：

步骤 1)，对第二校验信息进行解密。

步骤 2)，判断第二校验信息是否解密成功。

具体的，在上述步骤 1) 中，若在生成初始设备指纹信息的过程中进行了加密处理，则可以通过对第二校验信息进行解密验证，实现对目标设备指纹信息进行校验的目的。因此，可以对上述第二校验信息进行解密。

在上述步骤 2) 中，可以通过判断第二校验信息是否解密成功，从而实现对第二校验信息进行校验。其中，若第二校验信息解密不成功，则表征第二校验信息校验异常，此时，说明目标设备指纹信息存在异常，可以直接按照异常进行后续处理。举例来说，无法成功解密第二校验信息或者解密第二校验信息的过程中出现参数解析异常的问题，则说明目标设备指纹信息被篡改了。

若第二校验信息解密成功，则表征第二校验信息校验正常。此时，作为一种实施方式，可以认为目标设备指纹信息不存在异常；作为另一种实施方式，也可以采取其他校验方式对目标设备指纹信息进行进一步校验。

在上述方案中，可以通过对第二校验信息进行解密，实现对目标设备指纹信息的解密校验，从而提高校验的准确性，保证设备指纹的安全性。

进一步的，在上述实施例的基础上，初始设备指纹信息还可以包括业务信息，此时，在上述根据第二校验信息对目标设备指纹信息进行校验的步骤之后，本申请实施例提供的设备指纹校验方法还可以包括如下步骤：

若第二校验信息解密成功并得到对应的第三校验信息，则判断业务校

验信息与业务信息是否相同。

具体的，在上述步骤中，若第二校验信息解密成功，则可以采取其他校验方式对目标设备指纹信息进行进一步校验。作为一种实施方式，若初始设备指纹信息中包括业务信息，则可以通过对第三校验信息进行业务验证，实现对目标设备指纹信息进行校验的目的。因此，可以提取解密得到的第三校验信息中的业务校验信息，并判断上述业务校验信息与业务信息是否相同。

业务校验信息为第三校验信息中与业务信息对应的校验信息，而业务信息可以用于表征客户端上相应的业务。其中，若业务校验信息与业务信息不相同，则表征第三校验信息校验异常，此时，说明目标设备指纹信息存在异常，可以直接按照异常进行后续处理。举例来说，业务校验信息与业务信息不相同，则可能出现目标设备指纹信息被替换的情况。

若业务校验信息与业务信息相同，则表征第三校验信息校验正常。此时，作为一种实施方式，可以认为目标设备指纹信息不存在异常；作为另一种实施方式，也可以采取其他校验方式对目标设备指纹信息进行进一步校验。

在上述方案中，若第二校验信息校验正常，则可以对目标设备指纹信息进行进一步校验，通过判断解密得到的第三校验信息中的业务校验信息与业务信息是否相同，从而实现对目标设备指纹信息的业务校验，从而提高校验的准确性，保证设备指纹的安全性。

请参照图 2，图 2 为本申请实施例提供的一种设备指纹生成方法的流程图，该设备指纹生成方法可以应用于服务端，其中，设备指纹生成方法可以包括如下步骤：

步骤 S201：获取客户端对应的初始设备指纹信息以及第一生成时间。

步骤 S202：根据初始设备指纹信息以及第一生成时间生成目标设备指纹信息。

具体的，在上述步骤 S201 中，初始设备指纹信息可以是基于与客户端相关的信息生成的，与客户端相关的信息可以包括设备指纹 ID、首次生成上述设备指纹 ID 的时间、客户端对应的可校验信息、客户端对应的业务信息等信息中的一项或者多项信息。

第一生成时间为生成目标设备指纹信息的时间，也就是说，上述第一生成时间可以是指执行本申请实施例提供的步骤 S201-步骤 S202 时的时间。作为一种实施方式，上述第一生成时间可以为当前时间；作为另一种实施方式，第一生成时间可以为未来预计生成目标设备指纹信息的时间。举例来说，上述第一生成时间可以包括年、月、日、时、分、秒中的至少一项。

需要说明的是，本申请实施例对获取初始设备指纹信息以及第一生成时间的具体实施方式不作具体的限定，本领域技术人员可以根据实际情况进行合适的调整。举例来说，可以接收外部设备发送的初始设备指纹信息以及第一生成时间；或者，可以读取本地或者云端存储的初始设备指纹信息以及第一生成时间；或者，可以实时生成初始设备指纹信息等。

在上述步骤 S202 中，根据上述初始设备指纹信息以及第一生成时间，

可以生成目标设备指纹信息。其中，目标设备指纹信息包括初始设备指纹信息以及与初始设备指纹信息拼接的时间信息，时间信息包括第一生成时间。因此，可以将初始设备指纹信息以及时间信息拼接起来，从而可以得到目标设备指纹信息。

在上述方案中，在获取到目标设备对应的初始设备指纹信息以及生成目标设备指纹信息对应的第一生成时间后，可以根据上述初始设备指纹信息与第一生成时间生成目标设备指纹信息；基于上述目标设备指纹信息可以对设备指纹进行校验，从而判断设备指纹在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

进一步的，在上述实施例的基础上，作为一种实施方式，上述步骤 S202 具体可以包括如下步骤：

拼接初始设备指纹信息以及第一生成时间，得到目标设备指纹信息。

具体的，可以直接将初始设备指纹信息以及第一生成时间拼接起来，从而可以得到目标设备指纹信息。其中，拼接初始设备指纹信息以及第一生成时间的方式为：将第一生成时间添加在初始设备指纹信息中，例如：假设初始设备指纹信息为 abcd，第一生成时间为 2001，则拼接后得到的目标设备指纹信息可以为 abcd2001。

需要说明的是，本申请实施例对将第一生成时间添加在初始设备指纹信息中的具体位置不作具体的限定，本领域技术人员可以根据实际情况进行合适的调整。举例来说，可以将第一生成时间添加在初始设备指纹信息后（如：abcd2001）；或者，可以将第一生成时间添加在初始设备指纹信息前（如：2001abcd）；或者，可以将第一生成时间添加在初始设备指纹信息中（如：ab2001cd）等。

在上述方案中，可以将初始设备指纹信息以及第一生成时间拼接起来，从而可以快速的基于第一生成时间对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

进一步的，在上述实施例的基础上，作为另一种实施方式，上述步骤 S202 具体可以包括如下步骤：

步骤 1)，对第一生成时间进行编码，得到时间信息。

步骤 2)，拼接初始设备指纹信息以及时间信息，得到目标设备指纹信息。

具体的，在上述步骤 1) 中，可以先对第一生成时间编码得到时间信息后，再将初始设备指纹信息以及时间信息拼接起来，从而可以得到目标设备指纹信息。

需要说明的是，本申请实施例对上述对第一生成时间进行编码的具体实施方式不作具体的限定，本领域技术人员可以根据实际情况进行合适的调整，例如：可以对第一生成时间进行进制压缩、或者对第一生成时间进行哈夫曼编码等。

以对第一生成时间进行进制压缩为例，假设第一生成时间为 20231030，可以采用 58 进制对上述第一生成时间进行进制压缩，得到压缩后的时间信

息 2MFYS。

在上述步骤 2) 中, 可以将压缩后得到的时间信息与初始设备指纹信息进行拼接; 可以理解的是, 拼接时间信息和初始设备指纹信息的具体实施方式, 与拼接第一生成时间和初始设备指纹信息的具体实施方式类似, 此处不再赘述。

在上述方案中, 可以先对第一生成时间进行编码后, 再将初始指纹信息与编码后的时间信息拼接起来, 从而可以在实现快速校验的基础上, 降低目标设备指纹信息的数据量。

进一步的, 在上述实施例的基础上, 上述步骤 S201 具体可以包括如下步骤:

步骤 1), 获取客户端对应的设备指纹 ID 以及设备特征信息。

步骤 2), 根据设备指纹 ID 以及设备特征信息生成初始设备指纹信息。

具体的, 在上述步骤 1) 中, 客户端对应的设备指纹 ID 可以仅生成一次后存储在本地或者云端; 而客户端对应的设备特征信息设备信息可以在生成设备指纹 ID 的同时获取并同步存储, 或者, 也可以实时查询设备信息。其中, 设备特征信息可以包括首次生成设备指纹 ID 的第二生成时间、客户端对应的可校验信息以及客户端对应的业务信息中的至少一项。

需要说明的是, 首先, 本申请实施例对获取客户端对应的设备指纹 ID 的具体实施方式不作具体的限定, 本领域技术人员可以根据实际情况进行合适的调整。举例来说, 可以接收外部设备发送的设备指纹 ID; 或者, 可以读取本地或者云端存储的设备指纹 ID; 或者, 可以根据客户端上报的设备参数首次生成设备指纹 ID 等。

其次, 本申请实施例对获取客户端对应的设备特征信息的具体实施方式也不作具体的限定, 本领域技术人员可以根据实际情况进行合适的调整。举例来说, 可以接收外部设备发送的设备特征信息; 或者, 可以读取本地或者云端存储的设备特征信息; 或者, 可以实时查询设备特征信息等。

可以理解的是, 获取客户端对应的设备指纹 ID 与获取客户端对应的设备特征信息的方式可以是相同的, 也可以是不同的。

在上述步骤 2) 中, 本申请实施例对根据设备指纹 ID 以及设备特征信息生成初始设备指纹信息的具体实施方式不作具体的限定, 本领域技术人员可以根据实际情况进行合适的调整。举例来说, 可以将设备指纹 ID 以及设备特征信息拼接起来得到初始设备指纹信息; 或者, 可以对设备指纹 ID 以及设备特征信息进行加密得到初始设备指纹信息; 或者, 可以对设备指纹 ID 以及设备特征信息进行编码得到初始设备指纹信息等。

在上述方案中, 初始设备指纹信息可以包括设备指纹 ID 以及设备特征信息, 从而可以适配更多的使用场景并基于不同的场景对目标设备指纹信息进行不同的校验, 从而降低设备指纹 ID 被替换、篡改的风险, 保证设备指纹的安全性。

进一步的, 在上述实施例的基础上, 上述根据设备指纹 ID 以及设备特征信息生成初始设备指纹信息的步骤, 具体可以包括如下步骤:

步骤 1), 拼接设备指纹 ID 以及设备特征信息, 得到第一设备指纹信

息。

步骤 2)，对第一设备指纹信息进行加密，得到第二设备指纹信息。

步骤 3)，对第二设备指纹信息进行字符转码，得到初始设备指纹信息。

具体的，在上述步骤 1) 中，可以将设备指纹 ID 以及设备特征信息拼接起来，从而可以得到第一设备指纹信息。

其中，拼接设备指纹 ID 以及设备特征信息的方式可以为：将设备特征信息添加在设备指纹 ID 中，例如：假设设备指纹 ID 为 efg，设备特征信息可以包括 A、B、C，则拼接后得到的第一设备指纹信息可以为 efgABC。

需要说明的是，本申请实施例对将设备特征信息添加在设备指纹 ID 中的具体位置不作具体的限定，本领域技术人员可以根据实际情况进行合适的调整。举例来说，可以将设备特征信息添加在设备指纹 ID 后（如：efgABC）；或者，可以将设备特征信息添加在设备指纹 ID 前（如：ABCefg）；或者，可以将设备特征信息添加在设备指纹 ID 中（如：eABfCg）等。

在上述步骤 2) 中，可以对上述步骤 1) 中拼接得到的第一设备指纹信息进行加密，从而可以得到第二设备指纹信息。

需要说明的是，本申请实施例对加密第一设备指纹信息的具体实施方式不作具体的限定，本领域技术人员可以根据实际情况进行合适的调整。举例来说，可以采用对称加密算法、非对称加密算法和哈希算法等加密算法中的一项或者多项算法对第一设备指纹信息进行加密。

在上述步骤 3) 中，可以对上述步骤 2) 中加密得到的第二设备指纹信息进行字符转码，从而可以得到初始设备指纹信息。

需要说明的是，本申请实施例对转码第二设备指纹信息的具体实施方式不作具体的限定，本领域技术人员可以根据实际情况进行合适的调整。举例来说，可以采用 ASCII 编码、BASE64、BASE62 等字符转码方式中的一项或者多项转码方式对第二设备指纹信息进行字符转码。

在上述方案中，可以在拼接设备指纹 ID 以及设备特征信息后，对拼接得到的第一设备指纹信息进行加密以及字符转码，从而进一步降低设备指纹被替换、篡改的风险，保证设备指纹的安全性。

进一步的，在上述实施例的基础上，上述对第二设备指纹信息进行字符转码，得到初始设备指纹信息的步骤，具体可以包括如下步骤：

利用预设的转码方法对第二设备指纹信息进行字符转码，得到初始设备指纹信息；其中，初始设备指纹信息中不包括特殊字符。

具体的，作为一种实施方式，上述特殊字符可以包括“+”“/”“=”等符号中的一项或者多项；作为另一种实施方式，在上述预设的转码方法中，可以利用去除特殊字符的 BASE62 对第二设备指纹信息进行字符转码，从而得到不包括特殊字符的初始设备指纹信息。

在上述方案中，可以使用预设的转码方法对第二设备指纹信息进行字符转码，从而得到不包括特殊字符的初始设备指纹信息；由于设备指纹会作为请求的参数，特殊字符在传输过程中存在风险隐患，因此采用上述转码方式可以降低上述风险，从而保证设备指纹的安全性。

请参照图 3，图 3 为本申请实施例提供的另一种设备指纹校验方法的流

程图，该设备指纹校验方法可以应用于服务端，其中，设备指纹校验方法可以包括如下步骤：

步骤 S301：获取客户端对应的初始设备指纹信息以及第一生成时间。

步骤 S302：根据初始设备指纹信息以及第一生成时间生成目标设备指纹信息。

步骤 S303：获取客户端发送的请求数据。

步骤 S304：根据目标设备指纹信息还原与第一生成时间对应的第一校验信息。

步骤 S305：根据第一校验信息对目标设备指纹信息进行校验。

具体的，在上述步骤 S301 中，初始设备指纹信息可以是基于与客户端相关的信息生成的，与客户端相关的信息可以包括设备指纹 ID、首次生成上述设备指纹 ID 的时间、客户端对应的可校验信息、客户端对应的业务信息等信息中的一项或者多项信息。

第一生成时间为生成目标设备指纹信息的时间，也就是说，上述第一生成时间可以是指执行本申请实施例提供的步骤 S301-步骤 S302 时的时间。作为一种实施方式，上述第一生成时间可以为当前时间；作为另一种实施方式，第一生成时间可以为未来预计生成目标设备指纹信息的时间。举例来说，上述第一生成时间可以包括年、月、日、时、分、秒中的至少一项。

在上述步骤 S302 中，根据上述初始设备指纹信息以及第一生成时间，可以生成目标设备指纹信息。其中，目标设备指纹信息包括初始设备指纹信息以及与初始设备指纹信息拼接的时间信息，时间信息包括第一生成时间。因此，可以将初始设备指纹信息以及时间信息拼接起来，从而可以得到目标设备指纹信息。

在上述步骤 S303 中，在客户端需要执行业务时，客户端可以向服务端发送请求数据，以使服务端可以基于上述请求数据对客户端的目标设备指纹信息进行校验。其中，上述请求数据可以包括客户端对应的目标设备指纹信息。

在上述步骤 S304 中，由于目标设备指纹信息中包括初始设备指纹信息以及与初始设备指纹信息拼接的时间信息，因此，可以快速的将目标设备指纹信息中与第一生成时间对应的第一校验信息还原出来。

作为一种实施方式，若时间信息包括上述第一生成时间，则可以直接将目标设备指纹信息中与第一生成时间对应位置处的信息提取出来，即可得到第一校验信息；作为另一种实施方式，若先对第一生成时间进行了处理，则可以在将目标设备指纹信息中与第一生成时间对应位置处的信息提取出来后，对提取出来的数据进行相反的处理，即可得到第一校验信息。

在上述步骤 S305 中，可以通过对上述第一校验信息进行校验，实现对目标设备指纹信息进行校验的目的。作为一种实施方式，可以通过判断第一校验信息与第一生成时间是否相同，从而实现对第一校验信息进行校验。

其中，若第一校验信息与第一生成时间不相同，则表征第一校验信息校验异常，此时，说明目标设备指纹信息存在异常，可以直接按照异常进行后续处理。举例来说，假设第一生成时间为 2023，第一校验信息为 3023，

则说明目标设备指纹信息被篡改了。

若第一校验时间与第一生成时间相同，则表征第一校验信息校验正常。此时，作为一种实施方式，可以认为目标设备指纹信息不存在异常；作为另一种实施方式，也可以采取其他校验方式对目标设备指纹信息进行进一步校验。

在上述方案中，在获取到目标设备对应的初始设备指纹信息以及生成目标设备指纹信息对应的第一生成时间后，可以根据上述初始设备指纹信息与第一生成时间生成目标设备指纹信息；基于上述目标设备指纹信息可以快速对设备指纹进行校验，从而判断设备指纹在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

综上，上述设备指纹校验方法以及设备指纹生成方法均可以在服务端中执行。服务端在生成目标设备指纹信息后，可以将上述目标设备指纹信息下发至客户端；客户端在接收到上述目标设备指纹信息后，可以存储上述目标设备指纹信息；当客户端需要进行数据请求时，可以携带上述目标设备指纹信息，相应的服务端在接收到客户端的数据请求后，可以对上述数据请求中携带的目标设备指纹信息进行校验。

请参照图 4，图 4 为本申请实施例提供的一种设备指纹校验装置的结构框图，该设备指纹校验装置 400 包括：第一获取模块 401，用于获取客户端发送的请求数据；其中，所述请求数据包括所述客户端对应的目标设备指纹信息，所述目标设备指纹信息包括初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括生成所述目标设备指纹信息的第一生成时间；第一还原模块 402，用于根据所述目标设备指纹信息还原与所述第一生成时间对应的第一校验信息；第一校验模块 403，用于根据所述第一校验信息对所述目标设备指纹信息进行校验。

在上述方案中，在获取到目标设备对应的目标设备指纹信息后，由于上述目标设备指纹信息包括初始设备指纹信息以及与其拼接的时间信息，因此可以通过还原与时间信息中的第一生成时间对应的第一校验信息，快速的基于上述第一校验信息对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述设备指纹校验装置 400 还包括：第二还原模块，用于若所述第一校验信息校验正常，则根据所述目标设备指纹信息还原与所述初始设备指纹信息对应的第二校验信息；第二校验模块，用于根据所述第二校验信息对所述目标设备指纹信息进行校验。

在上述方案中，若第一校验信息校验正常，则可以对目标设备指纹信息进行进一步校验，通过还原与初始设备指纹信息对应的第二校验信息，更准确的对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述第二校验模块具体用于：对所述第二校验信息进行解密；判断所述第二校验信息是否解密成功；其中，所述第二校验信息解密不成功表征所述目标设备指纹信息存在异常。

在上述方案中，可以通过对第二校验信息进行解密，实现对目标设备指纹信息的解密校验，从而提高校验的准确性，保证设备指纹的安全性。

在可选的实施方式中，所述初始设备指纹信息包括业务信息；所述设备指纹校验装置 400 还包括：判断模块，用于若所述第二校验信息解密成功并得到对应的第三校验信息，则判断业务校验信息与所述业务信息是否相同；其中，所述业务校验信息为所述第三校验信息中与所述业务信息对应的校验信息，所述业务校验信息与所述业务信息不相同表征所述目标设备指纹信息存在异常。

在上述方案中，若第二校验信息校验正常，则可以对目标设备指纹信息进行进一步校验，通过判断解密得到的第三校验信息中的业务校验信息与业务信息是否相同，从而实现对目标设备指纹信息的业务校验，从而提高校验的准确性，保证设备指纹的安全性。

请参照图 5，图 5 为本申请实施例提供的一种设备指纹生成装置的结构框图，该设备指纹生成装置 500 包括：第二获取模块 501，用于获取客户端对应的初始设备指纹信息以及第一生成时间；其中，所述第一生成时间为生成目标设备指纹信息的时间；第一生成模块 502，用于根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息；其中，所述目标设备指纹信息包括所述初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括所述第一生成时间。

在上述方案中，在获取到目标设备对应的初始设备指纹信息以及生成目标设备指纹信息对应的第一生成时间后，可以根据上述初始设备指纹信息与第一生成时间生成目标设备指纹信息；基于上述目标设备指纹信息可以对设备指纹进行校验，从而判断设备指纹在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述第一生成模块 502 具体用于：拼接所述初始设备指纹信息以及所述第一生成时间，得到所述目标设备指纹信息。

在上述方案中，可以将初始设备指纹信息以及第一生成时间拼接起来，从而可以快速的基于第一生成时间对目标设备指纹信息进行校验，从而判断目标设备指纹信息在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

在可选的实施方式中，所述第一生成模块 502 具体用于：对所述第一生成时间进行编码，得到所述时间信息；拼接所述初始设备指纹信息以及所述时间信息，得到所述目标设备指纹信息。

在上述方案中，可以先对第一生成时间进行编码后，再将初始指纹信息与编码后的时间信息拼接起来，从而可以在实现快速校验的基础上，降低目标设备指纹信息的数据量。

在可选的实施方式中，所述第二获取模块 501 具体用于：获取所述客户端对应的设备指纹 ID 及设备特征信息；其中，所述设备特征信息包括首次生成所述设备指纹 ID 的第二生成时间、所述客户端对应的可校验信息以及所述客户端对应的业务信息中的至少一项；根据所述设备指纹 ID 以及所述设备特征信息生成所述初始设备指纹信息。

在上述方案中，初始设备指纹信息可以包括设备指纹 ID 以及设备特征信息，从而可以适配更多的使用场景并基于不同的场景对目标设备指纹信息进行不同的校验，从而降低设备指纹 ID 被替换、篡改的风险，保证设备指纹的安全性。

在可选的实施方式中，所述第二获取模块 501 还用于：拼接所述设备指纹 ID 以及所述设备特征信息，得到第一设备指纹信息；对所述第一设备指纹信息进行加密，得到第二设备指纹信息；对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息。

在上述方案中，可以在拼接设备指纹 ID 以及设备特征信息后，对拼接得到的第一设备指纹信息进行加密以及字符转码，从而进一步降低设备指纹被替换、篡改的风险，保证设备指纹的安全性。

在可选的实施方式中，所述第二获取模块 501 还用于：利用预设的转码方法对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息；其中，所述初始设备指纹信息中不包括特殊字符。

在上述方案中，可以使用预设的转码方法对第二设备指纹信息进行字符转码，从而得到不包括特殊字符的初始设备指纹信息；由于设备指纹会作为请求的参数，特殊字符在传输过程中存在风险隐患，因此采用上述转码方式可以降低上述风险，从而保证设备指纹的安全性。

请参照图 6，图 6 为本申请实施例提供的另一种设备指纹校验装置的结构框图，该设备指纹校验装置 600 包括：第三获取模块 601，用于获取客户端对应的初始设备指纹信息以及第一生成时间；其中，所述第一生成时间为生成目标设备指纹信息的时间；第二生成模块 602，用于根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息；其中，所述目标设备指纹信息包括所述初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括所述第一生成时间；第四获取模块 603，用于获取客户端发送的请求数据；其中，所述请求数据包括所述客户端对应的目标设备指纹信息；第三还原模块 604，用于根据所述目标设备指纹信息还原与所述第一生成时间对应的第一校验信息；第三校验模块 605，用于根据所述第一校验信息对所述目标设备指纹信息进行校验。

在上述方案中，在获取到目标设备对应的初始设备指纹信息以及生成目标设备指纹信息对应的第一生成时间后，可以根据上述初始设备指纹信息与第一生成时间生成目标设备指纹信息；基于上述目标设备指纹信息可以快速对设备指纹进行校验，从而判断设备指纹在使用过程中是否存在被替换、篡改的情况，保证设备指纹的安全性。

请参照图 7，图 7 为本申请实施例提供的一种电子设备的结构框图，该电子设备 700 包括：至少一个处理器 701，至少一个通信接口 702，至少一个存储器 703 和至少一个通信总线 704。其中，通信总线 704 用于实现这些组件直接的连接通信，通信接口 702 用于与其他节点设备进行信令或数据的通信，存储器 703 存储有处理器 701 可执行的机器可读指令。当电子设备 700 运行时，处理器 701 与存储器 703 之间通过通信总线 704 通信，机器可读指令被处理器 701 调用时执行上述设备指纹校验方法或者设备指纹

生成方法。

例如，本申请实施例的处理器 701 通过通信总线 704 从存储器 703 读取计算机程序并执行该计算机程序可以实现如下方法：步骤 S101：获取客户端发送的请求数据。步骤 S102：根据目标设备指纹信息还原与第一生成时间对应的第一校验信息。步骤 S103：根据第一校验信息对目标设备指纹信息进行校验。或者可以实现如下方法：步骤 S201：获取客户端对应的初始设备指纹信息以及第一生成时间。步骤 S202：根据初始设备指纹信息以及第一生成时间生成目标设备指纹信息。

其中，处理器 701 包括一个或多个，其可以是一种集成电路芯片，具有信号的处理能力。上述的处理器 701 可以是通用处理器，包括中央处理器(Central Processing Unit, 简称 CPU)、微控制单元(Micro Controller Unit, 简称 MCU)、网络处理器(Network Processor, 简称 NP)或者其他常规处理器；还可以是专用处理器，包括神经网络处理器(Neural-network Processing Unit, 简称 NPU)、图形处理器(Graphics Processing Unit, 简称 GPU)、数字信号处理器(Digital Signal Processor, 简称 DSP)、专用集成电路(Application Specific Integrated Circuits, 简称 ASIC)、现场可编程门阵列(Field Programmable Gate Array, 简称 FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。并且，在处理器 701 为多个时，其中的一部分可以是通用处理器，另一部分可以是专用处理器。

存储器 703 包括一个或多个，其可以是，但不限于，随机存取存储器(Random Access Memory, 简称 RAM)、只读存储器(Read Only Memory, 简称 ROM)、可编程只读存储器(Programmable Read-Only Memory, 简称 PROM)、可擦除可编程只读存储器(Erasable Programmable Read-Only Memory, 简称 EPROM)、电可擦除可编程只读存储器(Electric Erasable Programmable Read-Only Memory, 简称 EEPROM)等。

可以理解，图 7 所示的结构仅为示意，电子设备 700 还可包括比图 7 中所示更多或者更少的组件，或者具有与图 7 所示不同的配置。图 7 中所示的各组件可以采用硬件、软件或其组合实现。于本申请实施例中，电子设备 700 可以是，但不限于台式机、笔记本电脑、智能手机、智能穿戴设备、车载设备等实体设备，还可以是虚拟机等虚拟设备。另外，电子设备 700 也不一定是单台设备，还可以是多台设备的组合，例如服务器集群，等等。

本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质存储计算机程序指令，所述计算机程序指令被计算机运行时，使所述计算机执行前述方法实施例所述的设备指纹校验方法或者设备指纹生成方法。

在本申请所提供的实施例中，应该理解到，所揭露装置和方法，可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，又例如，多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦

合或直接耦合或通信连接可以是通过一些通信接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

另外，作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

再者，在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分，也可以是各个模块单独存在，也可以两个或两个以上模块集成形成一个独立的部分。

需要说明的是，功能如果以软件功能模块的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory, ROM）随机存取存储器（Random Access Memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。

以上所述仅为本申请的实施例而已，并不用于限制本申请的保护范围，对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权利要求书

1. 一种设备指纹校验方法，其特征在于，包括：
获取客户端发送的请求数据；其中，所述请求数据包括所述客户端对应的目标设备指纹信息，所述目标设备指纹信息包括初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括生成所述目标设备指纹信息的第一生成时间；
根据所述目标设备指纹信息还原与所述第一生成时间对应的第一校验信息；
根据所述第一校验信息对所述目标设备指纹信息进行校验。
2. 根据权利要求 1 所述的设备指纹校验方法，其特征在于，在所述根据所述第一校验信息对所述目标设备指纹信息进行校验之后，所述方法还包括：
若所述第一校验信息校验正常，则根据所述目标设备指纹信息还原与所述初始设备指纹信息对应的第二校验信息；
根据所述第二校验信息对所述目标设备指纹信息进行校验。
3. 根据权利要求 2 所述的设备指纹校验方法，其特征在于，所述根据所述第二校验信息对所述目标设备指纹信息进行校验，包括：
对所述第二校验信息进行解密；
判断所述第二校验信息是否解密成功；其中，所述第二校验信息解密不成功表征所述目标设备指纹信息存在异常。
4. 根据权利要求 3 所述的设备指纹校验方法，其特征在于，所述初始设备指纹信息包括业务信息；在所述判断所述第二校验信息是否解密成功之后，所述方法还包括：
若所述第二校验信息解密成功并得到对应的第三校验信息，则判断业务校验信息与所述业务信息是否相同；其中，所述业务校验信息为所述第三校验信息中与所述业务信息对应的校验信息，所述业务校验信息与所述业务信息不相同表征所述目标设备指纹信息存在异常。
5. 一种设备指纹生成方法，其特征在于，包括：
获取客户端对应的初始设备指纹信息以及第一生成时间；其中，所述第一生成时间为生成目标设备指纹信息的时间；
根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息；其中，所述目标设备指纹信息包括所述初始设备指纹信息以及与所述初始设备指纹信息拼接的时间信息，所述时间信息包括所述第一生成时间。
6. 根据权利要求 5 所述的设备指纹生成方法，其特征在于，所述根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息，包括：
拼接所述初始设备指纹信息以及所述第一生成时间，得到所述目标设

- 备指纹信息。
7. 根据权利要求 5 所述的设备指纹生成方法，其特征在于，所述根据所述初始设备指纹信息以及所述第一生成时间生成所述目标设备指纹信息，包括：
- 5 对所述第一生成时间进行编码，得到所述时间信息；
 拼接所述初始设备指纹信息以及所述时间信息，得到所述目标设备指纹信息。
8. 根据权利要求 5-7 任一项所述的设备指纹生成方法，其特征在于，所述获取客户端对应的初始设备指纹信息，包括：
- 10 获取所述客户端对应的设备指纹 ID 及设备特征信息；其中，所述设备特征信息包括首次生成所述设备指纹 ID 的第二生成时间、所述客户端对应的可校验信息以及所述客户端对应的业务信息中的至少一项；
 根据所述设备指纹 ID 以及所述设备特征信息生成所述初始设备指纹信息。
- 15 9. 根据权利要求 8 所述的设备指纹生成方法，其特征在于，所述根据所述设备指纹 ID 以及所述设备特征信息生成所述初始设备指纹信息，包括：
- 拼接所述设备指纹 ID 以及所述设备特征信息，得到第一设备指纹信息；
- 20 对所述第一设备指纹信息进行加密，得到第二设备指纹信息；
 对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息。
10. 根据权利要求 9 所述的设备指纹生成方法，其特征在于，所述对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息，包括：
- 25 利用预设的转码方法对所述第二设备指纹信息进行字符转码，得到所述初始设备指纹信息；其中，所述初始设备指纹信息中不包括特殊字符。
11. 一种电子设备，其特征在于，包括：处理器、存储器和总线；
 所述处理器和所述存储器通过所述总线完成相互间的通信；
 所述存储器存储有可被所述处理器执行的计算机程序指令，所述处理器调用所述计算机程序指令能够执行如权利要求 1-4 任一项所述的设备指纹校验方法或者如权利要求 5-10 任一项所述的设备指纹生成方法。
- 30 12. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储计算机程序指令，所述计算机程序指令被计算机运行时，使所述计算机执行如权利要求 1-4 任一项所述的设备指纹校验方法或者如权利要求 5-10 任一项所述的设备指纹生成方法。
- 35