(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 5 月 19 日 (19.05.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/099683 A1

(51) 国际专利分类号:
H04L 1/18 (2006.01)

(21) 国际申请号: PCT/CN2020/129003

(22) 国际申请日: 2020 年 11 月 16 日 (16.11.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 华为云计算技术有限公司 (**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国贵州省贵安新区黔中大道交兴功路华为云数据中心, Guizhou 550025 (CN)。

(72) 发明人: 单卫华 (**SHAN, Weihua**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 张春丽 (**ZHANG, Chunli**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所 (普通合伙) (**SHENPAT INTELLECTUAL PROPERTY AGENCY**); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦B座18C2、18D、18E、18E2, Guangdong 518001 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) **Title:** DATA TRANSMISSION METHOD AND APPARATUS, DEVICE, SYSTEM, AND STORAGE MEDIUM

(54) 发明名称: 一种数据传输方法、装置、设备、系统及存储介质

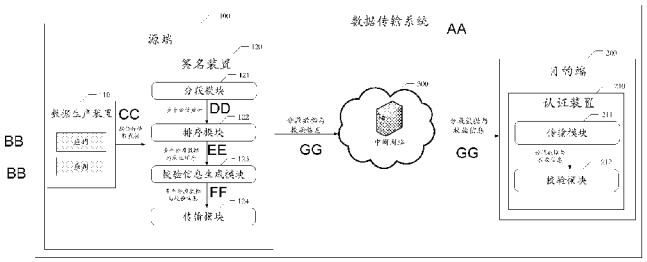

图 2

100 Source end
110 Data production apparatus
120 Signing apparatus
121 Segmenting module
122 Ordering module
123 Check information generation module
124, 211 Transmission module
200 Destination end
210 Authentication module
212 Check module
300 Intermediate network
AA Data transmission system
BB Application
CC Provide data to be transmitted
DD Multiple pieces of segmented data
EE Multiple pieces of segmented data and sending order
FF Multiple pieces of segmented data and check information
GG Segmented data and check information

(57) **Abstract:** A data transmission method, comprising: a source end acquiring data to be transmitted, segmenting said data into multiple pieces of segmented data, and determining a sending order of each piece of segmented data, so that check information of each piece of segmented data can be generated according to the segmented data and the sending order of each piece of segmented data; and then sending the multiple pieces of segmented data and corresponding check information to a destination end. In this way, the destination end can check the received segmented data on the basis of the receiving order and the check information of each piece of segmented data, so as to determine whether the segmented data has a transmission abnormality during the transmission process. Thus, when it is found after checking that there is segmented data having a transmission abnormality, the destination end can determine that the data to be transmitted has a transmission abnormality, rather than make a determination only after the transmission of the entire data to be transmitted is completed, thereby effectively increasing the efficiency of check of data to be transmitted. Also provided are a data transmission apparatus, a device, a system, and a storage medium.

WO 2022/099683 A1

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：一种数据传输方法，源端获取待传输数据，并将待传输数据切分为多个分段数据，并确定每个分段数据的发送顺序，从而可以根据该分段数据以及每个分段数据的发送顺序，生成每个分段数据的校验信息，然后将多个分段数据以及对应的校验信息发送给目的端。这样，目的端可以基于每个分段数据的接收顺序、校验信息对接收到的分段数据进行校验，从而确定分段数据在传输过程中是否存在传输异常。如此，当校验出存在分段数据出现传输异常时，目的端即可确定该待传输数据存在传输异常，无需等到整个待传输数据传输完毕才能确定，从而有效提高了待传输数据的校验效率。还提供了用于数据传输的装置、设备、系统及存储介质。

一种数据传输方法、装置、设备、系统及存储介质

技术领域

本申请涉及数据安全技术领域，尤其涉及一种数据传输方法、装置、设备、系统及存储介质。

背景技术

在数据通信场景中，源端与目的端在通信时相互传输的数据，可能会因为在传输过程中遭受攻击而被篡改，为此，源端与目的端之间通常是采用数字签名或者基于哈希的消息认证码（Hash-based Message Authentication Code，HMAC）技术对待传输的数据进行签名校验，以提高源端与目的端之间通信的数据的可靠性。

但是，目的端需要在接收完整的待传输数据后，才能根据源端为该待传输数据生成的数字签名，校验其接收到的待传输数据是否与源端发送的待传输数据一致，这使得当待传输数据较大时，目的端对待传输数据的校验效率较低。

发明内容

本申请提供了一种数据传输方法，用于提高对待传输数据的校验效率。此外，本申请还提供了一种数据传输装置、设备、系统、计算机可读存储介质以及计算机程序产品。

第一方面，本申请提供了一种数据传输方法，应用于源端，源端可以获取待传输数据，例如可以是源端上的一个或者多个应用所产生的数据等，并将待传输数据切分为多个分段数据，并确定每个分段数据的发送顺序，从而可以根据该分段数据以及每个分段数据的发送顺序，生成每个分段数据的校验信息，然后，签名装置可以将多个分段数据以及多个分段数据分别对应的校验信息发送给目的端。这样，目的端可以基于每个分段数据的接收顺序对接收到的分段数据以及校验信息进行校验，从而可以确定每个分段数据在传输过程中是否存在传输异常。

如此，在对待传输数据的多个分段数据进行传输的过程中，当通过校验信息校验出存在分段数据出现传输异常时，目的端即可确定该待传输数据存在传输异常，无需等到整个待传输数据传输完毕才能确定，从而有效提高了待传输数据的校验效率。而且，由于校验信息是根据分段数据的发送顺序生成，并且该发送顺序也无需传输给目的端（目的端可以基于与发送顺序对应的接收顺序生成校验信息并对分段数据校验），因此，目的端可以根据分段数据的接收顺序，校验出待传输数据中的多个分段数据在传输过程中是否被篡改、替换以及重组。如此，在提高数据校验的效率的同时，也进一步提高了数据传输的安全性。

其中，源端是一次会话过程中数据的发送方，而目的端是一次会话过程中数据的接收方。源端与目的端可以是由硬件或者软件实现，并且，源端与目的端可以是相同类型的硬件或者软件实现，也可以是不同类型的硬件或者软件实现，本实施例对此并不进行限定。

在一种可能的实施方式中，当校验信息具体为 HMAC 时，源端生成每个分段数据的校

验信息的过程，具体可以是将每个分段数据以及每个分段数据的发送顺序与密钥相组合，从而进行 HMAC 运算，获得每个分段数据对应的校验信息。

在一种示例中，针对于每个分段数据，源端可以将分段数据与该分段数据的发送顺序进行字符拼接，并对拼接得到的数据进行哈希运算，生成相应的摘要，然后，源端可以利用预先保存的密钥对生成的摘要进行加密，并将加密密文作为该分段数据对应的校验信息。相应的，目的端在对分段数据进行校验时，可以将接收到的分段数据与该分段数据的接收顺序进行字符拼接，并对拼接得到的数据进行同等的哈希运算，生成相应的摘要；同时，目的端可以利用预先保存的密钥对接收到的校验信息进行解密。然后，目的端可以通过比较生成的摘要与解密得到的摘要是否一致确定该分段数据在传输过程中是否存在传输异常。

在另一种示例中，针对于每个分段数据，源端可以采用相应的哈希算法对分段数据进行哈希运算，生成该分段数据对应的摘要，然后，源端可以将预先保存的加密密钥与该分段数据的发送顺序进行字符拼接，并基于拼接所得到的新密钥对生成的摘要进行加密，从而可以将得到的加密密文作为该分段数据对应的校验信息。相应的，目的端在对分段数据进行校验时，可以将该分段数据的接收顺序与预先保存的解密密钥进行字符拼接，并基于拼接得到的新密钥对接收到的校验信息进行解密，得到摘要；同时，目的端可以基于接收到的分段数据生成摘要，并通过比较生成的摘要与解密得到的摘要是否一致确定该分段数据在传输过程中是否存在传输异常。

在又一种示例中，针对于每个分段数据，源端可以采用相应的哈希算法对分段数据进行哈希云端，生成该分段数据对应的摘要，然后，源端可以将生成的摘要与该分段数据对应的发送顺序进行字符拼接，得到新的摘要，并利用预先保存的密钥对拼接得到的新摘要进行加密，从而可以将得到的加密密文作为该分段数据对应的校验信息。相应的，目的端在对分段数据进行校验时，可以利用预先保存的解密密钥对接收到的校验信息进行解密，并从解密得到的摘要中去除发送顺序，得到新的摘要；同时，目的端可以对接收到的分段数据进行哈希运算，生成相应的摘要。这样，目的端可以比较这两个摘要是否一致，以便于确定该分段数据在传输过程中是否存在传输异常。

在一种可能的实施方式中，源端与目的端之间可以通过会话传输待传输数据，则，源端在向目的端传输数据之前，可以先向目的端发送当前的会话标识，然后，源端在生成每个分段数据对应的校验信息时，可以是根据每个分段数据、每个分段数据的发送顺序以及该会话标识，生成每个分段数据的校验信息。这样，目的端在对每个分段数据进行校验时，可以结合该分段数据对应的会话标识进行校验，从而分段数据在传输过程中，存在两个不同会话中具有相同发送顺序的分段数据发生互换，目的端也可以校验出该当前所接收到的分段数据不是源端发送的分段数据，进而可以进一步提高数据通信的可靠性。

在一种可能的实施方式中，源端可以是在向目的端发送第一个分段数据以及该第一个分段数据的校验信息之前向目的端发送会话标识，并具体可以是向目的端发送携带有该会话的标识的请求头。

进一步的，源端向目的端发送的携带有该会话标识的请求中，还可以包括该请求头对

应的校验信息，从而目的端可以对利用该校验信息对接收到的请求头进行校验，从而确定接收到的请求头中所携带的内容是否在传输过程中被篡改。

在一种可能的实施方式中，源端在向目的端发送多个分段数据以及多个分段数据对应的校验信息时，具体可以是向目的端发送最后一个分段数据、最后一个分段数据的校验信息以及结束标识，其中，该结束标识指示多个分段数据传输完毕。如此，目的端可以通过该结束标识确定当前所接收到的多个分段数据，是否为源端所要传输给目的端的所有分段数据，从而目的端可以及时识别出分段数据在传输过程中是否被攻击者截断。

在一种可能的实施方式中，源端在获取待传输数据之前，可以先启动多个传输线程，并对获取的待传输资源进行切分，得到多个待传输数据，然后，源端可以通过每个传输线程，向目的端发送至少一个待传输数据的分段数据以及该分段数据对应的校验信息。如此，可以实现源端向目的端并行传输待传输数据，从而可以提高待传输资源在源端与目的端之间的传输效率。

在一种可能的实施方式中，源端在通过每个传输线程向目的端发送至少一个待传输数据的分段数据以及对应的校验信息之前，可以先发送携带有描述数据的请求头至目的端，从而目的端可以基于待传输数据的描述数据，确定接收到的多个待传输数据属于同一待传输资源，以便于目的端对接收到的多个待传输数据进行整合。其中，描述数据可以包括以下至少一种：待传输资源的标识以及待传输数据的切片范围。其中，待传输资源的标识例如可以是待传输资源的文件名等，待传输数据的切片范围例如可以是该数据的切片标识、切片大小等。

在一种可能的实施方式中，源端还可以基于时间信息和/或位置信息生成每个分段数据对应的校验信息，从而可以增加对于分段数据的校验维度，进一步提高数据校验的可靠性。

第二方面，本申请实施例还提供了一种数据传输方法，该方法应用于目的端。目的端可以接收来自源端的多个分段数据以及每个分段数据对应的校验信息，其中，所接收到的多个分段数据是由源端对待传输数据进行切分得到；然后，目的端可以确定每个分段数据的接收顺序，并根据每个分段数据、每个分段数据的接收顺序以及每个分段数据的校验信息，校验待传输数据中的每个分段数据是否传输异常。

如此，在对待传输数据的多个分段数据进行传输的过程中，当通过校验信息校验出存在分段数据出现传输异常时，目的端即可确定该待传输数据存在传输异常，无需等到整个待传输数据传输完毕才能确定，从而有效提高了待传输数据的校验效率。而且，由于校验信息是根据分段数据的发送顺序生成，并且该发送顺序也无需传输给目的端（目的端可以基于与发送顺序对应的接收顺序生成校验信息并对分段数据校验），因此，目的端可以根据分段数据的接收顺序，校验出待传输数据中的多个分段数据在传输过程中是否被篡改、替换以及重组。如此，在提高数据校验的效率的同时，也进一步提高了数据传输的安全性。

在一种可能的实施方式中，校验信息具体为HMAC，则目的端在校验待传输数据中的每个分段数据是否传输异常时，具体可以是根据每个分段数据、每个分段数据的接收顺序、密钥以及接收到的校验信息，确定待传输数据中的每个分段数据是否传输异常。

针对于每个分段数据、每个分段数据的接收顺序以及密钥的组合，在一种示例中，针

对于每个分段数据，源端可以将分段数据与该分段数据的发送顺序进行字符拼接，并对拼接得到的数据进行哈希运算，生成相应的摘要，然后，源端可以利用预先保存的密钥对生成的摘要进行加密，并将加密密文作为该分段数据对应的校验信息。相应的，目的端在对分段数据进行校验时，可以将接收到的分段数据与该分段数据的接收顺序进行字符拼接，并对拼接得到的数据进行同等的哈希运算，生成相应的摘要；同时，目的端可以利用预先保存的密钥对接收到的校验信息进行解密。然后，目的端可以通过比较生成的摘要与解密得到的摘要是否一致确定该分段数据在传输过程中是否存在传输异常。

在另一种示例中，针对于每个分段数据，源端可以采用相应的哈希算法对分段数据进行哈希运算，生成该分段数据对应的摘要，然后，源端可以将预先保存的加密密钥与该分段数据的发送顺序进行字符拼接，并基于拼接所得到的新密钥对生成的摘要进行加密，从而可以将得到的加密密文作为该分段数据对应的校验信息。相应的，目的端在对分段数据进行校验时，可以将该分段数据的接收顺序与预先保存的解密密钥进行字符拼接，并基于拼接得到的新密钥对接收到的校验信息进行解密，得到摘要；同时，目的端可以基于接收到的分段数据生成摘要，并通过比较生成的摘要与解密得到的摘要是否一致确定该分段数据在传输过程中是否存在传输异常。

在又一种示例中，针对于每个分段数据，源端可以采用相应的哈希算法对分段数据进行哈希云端，生成该分段数据对应的摘要，然后，源端可以将生成的摘要与该分段数据对应的发送顺序进行字符拼接，得到新的摘要，并利用预先保存的密钥对拼接得到的新摘要进行加密，从而可以将得到的加密密文作为该分段数据对应的校验信息。相应的，目的端在对分段数据进行校验时，可以利用预先保存的解密密钥对接收到的校验信息进行解密，并从解密得到的摘要中去除发送顺序，得到新的摘要；同时，目的端可以对接收到的分段数据进行哈希运算，生成相应的摘要。这样，目的端可以比较这两个摘要是否一致，以便于确定该分段数据在传输过程中是否存在传输异常。

在一种可能的实施方式中，目的端可以通过会话接收到源端发送的待传输数据，则目的端还可以接收来自源端的会话的标识；则目的端在校验分段数据是否存在传输异常时，具体可以是根据每个分段数据、每个分段数据的接收顺序、每个分段数据的校验信息以及当前会话的标识，校验待传输数据中的每个分段数据是否传输异常。这样，即使分段数据在传输过程中，存在两个不同会话中具有相同发送顺序的分段数据发生互换，目的端也可以校验出该当前所接收到的分段数据不是源端发送的分段数据，进而可以进一步提高数据通信的可靠性。

在一种可能的实施方式中，目的端可以接收来自源端的请求头，该请求头中携带有当前源端与目的端之间的会话的标识，从而目的端可以从该请求头中解析出会话标识。

在一种可能的实施方式中，目的端可以接收源端发送的请求头对应的校验信息，从而基于该请求头对应的校验信息确定该请求头中所携带的内容在传输过程中是否被篡改。

在一种可能的实施方式中，目的端在接收来自源端的多个分段数据以及每个分段数据对应的校验信息的过程中，可以是接收来自源端的最后一个分段数据、最后一个分段数据的校验信息以及结束标识，其中，该结束标识指示多个分段数据传输完毕。如此，目的端

可以通过该结束标识确定当前所接收到的多个分段数据，是否为源端所要传输给目的端的所有分段数据，从而目的端可以及时识别出分段数据在传输过程中是否被攻击者截断。

在一种可能的实施方式中，目的端在接收来自源端的多个分段数据以及每个分段数据对应的校验信息时，具体可以是接收源端通过每个传输线程发送的至少一个待传输数据的分段数据以及对应的校验信息，其中，不同传输线程用于传输对待传输资源切分得到的不同待传输数据，从而源端向目的端并行传输待传输数据，进而可以提高待传输资源在源端与目的端之间的传输效率。

在一种可能的实施方式中，目的端在接收源端通过每个传输线程发送的至少一个待传输数据的分段数据以及对应的校验信息之前，可以接收来自源端的携带有描述信息的请求头，其中，待传输资源的标识例如可以是待传输资源的文件名等，待传输数据的切片范围例如可以是该数据的切片标识、切片大小等。

在一种可能的实施方式中，源端还可以基于时间信息和/或位置信息生成每个分段数据对应的校验信息，从而可以增加对于分段数据的校验维度，进一步提高数据校验的可靠性。

第三方面，本申请提供一种源端，该源端用于实现第一方面或第一方面任一种可能实现方式中源端执行的数据传输方法的各个模块。

第四方面，本申请提供一种目的端，该源端用于实现第二方面或第二方面任一种可能实现方式中目的端执行的数据传输方法的各个模块。

第五方面，本申请提供一种数据传输系统，包括源端和目的端，其中，源端用于执行上述第一方面或第一方面任一种可能的实施方式中的数据传输方法，目的端用于执行上述第二方面以及第二方面任一种可能的实施方式中的数据传输方法。

第六方面，本申请提供一种计算设备，所述计算设备包括处理器和存储器；所述处理器用于执行所述存储器中存储的指令，执行上述第一方面或第一方面任一种可能的实施方式中源端执行的数据传输方法。

第七方面，本申请提供一种计算设备，所述计算设备包括处理器和存储器；所述处理器用于执行所述存储器中存储的指令，执行上述第二方面或第二方面任一种可能的实施方式中目的端执行的数据传输方法。

第八方面，本申请提供一种计算机可读存储介质，所述计算机可读存储介质中存储有指令，当其在计算机设备上运行时，使得该计算机设备执行上述第一方面或第一方面的任一种实现方式所述的方法。

第九方面，本申请提供一种计算机可读存储介质，所述计算机可读存储介质中存储有指令，当其在计算机设备上运行时，使得该计算机设备执行上述第二方面或第二方面的任一种实现方式所述的方法。

第十方面，本申请提供了一种包含指令的计算机程序产品，当其在计算机设备上运行时，使得计算机设备执行上述第一方面或第一方面的任一种实现方式所述的方法。

第十一方面，本申请提供了一种包含指令的计算机程序产品，当其在多个计算机设备上运行时，使得计算机设备执行上述第二方面或第二方面的任一种实现方式所述的方法。

本申请在上述各方面提供的实现方式的基础上，还可以进行进一步组合以提供更多实

现方式。

附图说明

为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，还可以根据这些附图获得其它的附图。

图 1 为一种应用场景的架构示意图；

图 2 为本申请实施例中一种数据传输系统的架构示意图；

图 3 为本申请实施例中对待传输数据进行切分以及生成校验信息的示意图；

图 4 为本申请实施例中并行传输多个待传输数据的示意图；

图 5 为本申请实施例中源端 100 向目的端 200 传输请求头示意图；

图 6 为本申请实施例中一示例性请求头示意图；

图 7 为本申请实施例中源端 100 与目的端 200 之间传输数据的流程示意图；

图 8 为本申请实施例中一种计算机设备的硬件结构示意图；

图 9 为本申请实施例中又一种计算机设备的硬件结构示意图。

具体实施方式

实际应用中，数据在源端与目的端之间进行传输时，可能会遭受中间人攻击，导致目的端所接收到的数据（如文件、数据流等）与源端发送的数据并不相同。如图 1 所示，源端在通过网络（internet）将文件发送给目的端的过程中，中间人（通过代理服务器）对该文件的攻击手段主要为“篡改”，即将合法的文件段内容（也即源端发送的文件）进行修改，如将部分内容修改成其他内容等，使得目的端最终所接收到的完整文件与源端发送的原始完整文件的内容存在差异，从而影响了源端与目的端之间通信的可靠性。

基于此，源端在发送文件之前，可以基于数字签名或者 HMAC 为整个文件进行签名，并将签名以及整个文件发送给目的端，然后，由目的端通过校验签名来检测接收到的文件是否在传输过程中被篡改，以提高源端与目的端之间通信的可靠性。

其中，数字签名，也可以被称为公钥数字签名，具体是只有信息的发送者才能产生的别人无法伪造的一段数字串，该数字串同时也是对信息的发送者发送信息真实性的一个有效证明。一套数字签名通常定义两种互补的运算，一种用于签名，另一种用于验证。

HMAC，是一种基于 Hash 函数和密钥进行消息认证的方法，它要求通信双方共享密钥、约定算法、对传输数据进行 Hash 运算，形成固定尺寸的认证码。通信双方通过认证码的校验来确定传输数据的合法性。

但是，上述对于文件的校验方式，目的端需要在接收完整的文件后才能校验该文件是否出现传输异常，并且在确定文件存在传输异常后，通知源端重新发送整个文件。因此，该文件中未出现传输异常的部分仍旧需要重新从源端传输至目的端，这使得文件的校验以及传输效率较低。特别的，当源端与服务器之间传输的文件较大时，目的端可能长时间无法接收到正常的完整文件。攻击者也可能基于此不断发送大的错误文件消耗目的端算力。

基于此，本申请实施例提供了一种数据传输方法，用于提高对需要传输的文件等数据的校验效率。具体实现时，源端可以对待传输数据进行分段，源端确定该待传输数据包括的多个分段数据的发送顺序，并基于该发送顺序生成每个分段数据对应的校验信息。然后，源端可以将该校验信息与该分段数据发送给目的端。这样，目的端针对于每个接收到的分段数据，均可以根据目的端接收该分段数据的接收顺序以及该分段数据对应的校验信息对该分段数据进行校验，以确定该分段数据在传输过程中是否出现传输异常，也即确定待传输数据在传输过程中是否出现传输异常。

如此，在数据传输过程中，目的端可以及时确定出存在传输异常的分段数据，无需等待整个待传输数据传输完成后才能进行校验，从而提高了数据校验效率。并且，由于校验信息是根据分段数据的发送顺序生成，并且该发送顺序也无需传输给目的端（目的端可以基于与发送顺序对应的接收顺序生成校验信息并对分段数据校验），因此，目的端可以根据分段数据的接收顺序，校验出待传输数据中的多个分段数据在传输过程中是否被篡改、替换以及重组。如此，在提高数据校验的效率的同时，也进一步提高了数据传输的安全性。

进一步的，对于目的端所确定出存在传输异常的分段数据，源端可以仅重传该分段数据至目的端，而无需重传整个待传输数据，因此，待传输数据中未出现传输异常的分段数据可以无需再传输至目的端，从而可以提高数据的传输效率。

下面结合附图，对本申请的实施例进行描述。

本申请的说明书及附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的术语在适当情况下可以互换，这仅仅是描述本申请的实施例中对相同属性的对象在描述时所采用的区分方式。

参见图 2 所示的数据传输系统的结构示意图，该数据传输系统包括源端 100 以及目的端 200，源端 100 与目的端 200 之间通过中间网络 300 进行通信。其中，源端 100 是指一次会话过程中数据的发送方，而目的端 200 是指该会话过程中数据的接收方。源端 100 与目的端 200 可以是具有通信能力的任何设备，或者是设备上的软件模块等。具体的，当源端 100 与目的端 200 基于硬件实现时，源端 100 可以是提供数据的终端，目的端 200 可以是接收数据的服务器等；或者，源端 100，也可以是提供数据的服务器，而目的端 200 可以是接收数据的终端等。其中，源端 100 与目的端 200 可以是同一类型的设备，也可以是不同类型的设备。如源端 100 与目的端 200 均可以是终端，即两个终端之间可以通过中间网络 300 相互收发数据，或者，源端 100 与目的端 200 均可以是服务器，即在两个服务器之间进行数据通信。

当源端 100 与目的端 200 具体为设备上的软件模块时，源端 100 可以是运行在设备上的客户端，而目的端 200 可以是云平台所提供的云服务模块。当然，也可以是由云服务模块向客户端发送数据，即源端 100 为云服务模块，而目的端 200 为客户端，或者源端 100 与目的端 200 均为客户端或者均为云服务模块。作为一种示例，源端 100 中可以包括数据生产装置 110 以及签名装置 120。其中，数据生产装置 110 用于产生需要传输至目的端 200 的待传输数据。而签名装置 120 用于对待传输数据进行分段、签名等处理。

其中，该数据生产装置 110 可以包括一个或多个应用，而签名装置 120 可以作为软件开发工具包（software development kit，SDK）内嵌入该应用中。或者，数据生产装置 110 可以包含多个应用，而签名装置 120 可以作为源端 100 中独立的应用软件，能够同时为多个应用所产生的待传输数据进行处理。

签名装置 120 中包括分段模块 121、排序模块 122、校验信息生成模块 123 以及传输模块 124。其中，源端 100 在传输数据之前，可以通过分段模块 121 对待传输数据进行切分，得到该待传输数据对应的多个分段数据。如图 3 所示，分段模块 121 可以将待传输数据切分成（N+1）个分段数据，分别为分段数据 0（segment 0）至分段数据 N（segment N）。示例性的，分段模块 121 可以按照预设尺寸（size）对待传输数据进行切分，切分得到的多个分段数据的尺寸相同，当然，最后一个分段数据的尺寸可以小于或等于该预设尺寸。该预设尺寸可以预先由技术人员进行预先设定，也可以是由源端自定设定，例如 1M Byte（MB），64K Byte（KB）等。比如，对于一份尺寸为 1024KB 的待传输数据，假设分段模块 121 按照 64KB 的预设尺寸切分待传输数据时，可以得到 16 个分段数据。分段模块 121 也可以采用其它方式对待传输数据进行分段，例如不采用固定的预设尺寸进行数据分段，每个分段数据的尺寸可以不同。

在分段模块 121 切分待传输数据得到多个分段数据后，排序模块 122 可以确定该多个分段数据向目的端 200 发送的顺序。示例性的，排序模块 122 可以将各个分段数据在待传输数据中的排布顺序，作为该分段数据发送给目的端 200 的顺序。例如，排序模块 122 将待传输数据的第一个分段数据（头 64KB）排序为 1，后续第一个分段数据基于该排序被第一个发送给目的端 200，将待传输数据的第二个分段数据（第 64KB 至 128KB 的数据）排序为 2，后续第二个分段数据基于该排序被第二个发送给目的端 200，依次类推。

在其它可能的示例中，排序模块 122 可以是对多个分段数据进行随机排序，如，源端 100 可以基于预设的随机算法确定出每个分段数据的发送顺序。则，通常情况下，源端 100 发送各个分段数据的顺序与各个分段数据在待传输数据中的排布顺序不同。这样，即使源端 100 在传输各个分段数据时遭受攻击，也难以根据各个分段数据的发送顺序/传输顺序确定各个分段数据在待传输数据中的排布顺序，从而难以基于各个分段数据重构得到待传输数据，进一步提高了待传输数据的传输安全性。

在排序模块 122 为每个分段数据确定发送顺序后，签名装置 120 可以通过校验信息生成模块 123 为每个分段数据生成相应的校验信息，如图 3 所示，针对于分段模块 121 切分得到的分段数据 0 至分段数据 N，校验信息生成模块 123 可以基于各个分段数据生成相应的校验信息 0 至校验信息 N。具体实现时，针对于多个分段数据中的任意一个分段数据（以下称之为目标分段数据），校验信息生成模块 123 可以结合目标分段数据的发送顺序、分段数据以及密钥，为该目标分段数据生成相应的校验信息，该校验信息用于后续目标分段数据在传输至目的端 200 时的一致性校验。

实际应用中，该校验信息，可以是该目标分段数据对应的数字签名。示例性的，本实施例提供了以下几种生成校验信息的方式。

方式一：校验信息生成模块 123 可以将目标分段数据与发送顺序进行数据拼接（或者

其他方式的组合），并为拼接后的数据内容生成摘要，再利用源端100保存的公钥对该摘要进行加密，即可得到该目标分段数据对应的数字签名。

方式二：校验信息生成模块123为目标分段数据生成摘要后，将该摘要与目标分段数据的发送顺序进行数据拼接（或者其他方式的组合），并利用源端100保存的公钥对拼接得到的摘要进行加密，从而得到该目标分段数据对应的数字签名。

在其他可能的实施方式中，该校验信息，也可以是结合发送顺序而生成的该目标分段数据对应的HMAC，或者可以是其它结合发送顺序而生成的并且能够用于对目标分段数据进行一致性校验的数据等。

例如，方式三：当校验信息具体为HMAC时，针对于每个分段数据（即目标分段数据），校验信息生成模块123可以将源端100保存的加密密钥与目标分段数据对应的发送顺序进行数据拼接（或者采用其它方式组合），得到拼接后的密钥，再利用拼接后的密钥对基于目标分段数据生成的摘要进行加密，得到该目标分段数据对应的HMAC，并作为该目标分段数据对应的校验信息。

方式四：校验信息生成模块123可以将目标分段数据与加密密钥进行数据拼接，得到拼接后的数据，再利用源端100保存的加密密钥对基于拼接后的数据所生成的摘要进行加密，得到该目标分段数据对应的HMAC。

方式五：校验信息生成模块123在基于目标分段数据生成摘要后，将该摘要与该目标分段数据对应的发送顺序进行数据拼接（或者其它方式组合），并利用源端100保存的加密密钥对拼接得到的摘要进行加密，得到该目标分段数据对应的HMAC。当然，上述对于生成校验信息的具体实现方式仅作为一些示例性说明，并不用于限定其在实际应用中的具体实现。

在得到目标分段数据以及该目标分段数据对应的校验信息后，签名装置120通过传输模块124将目标分段数据以及该校验信息发送给目的端200。

作为一种示例，源端100可以与目的端200之间通过超文本传输协议（HyperText Transfer Protocol，HTTP）或者超文本传输安全协议（HyperText Transfer Protocol Secure，HTTPS）建立通信连接，并在该连接下将待传输数据通过中间网络300传输至目的端200。其中，中间网络300针对于传输模块124发送的每个分段数据以及该分段数据对应的校验信息，可以将其拆分成多个分段子数据，并针对于每个分段分段子数据采用网际互联（Internet Protocol，IP）协议将其封装成IP协议报文，如基于传输控制协议（Transmission Control Protocol，TCP）或用户数据报协议（User Datagram Protocol，UDP）对各个分段子数据进行报文封装等。然后，中间网络300可以将分段数据对应的各个IP协议报文发送给目的端200。其中，每个IP协议报文中可以携带有部分分段数据和/或该分段数据对应的（部分或全部）校验信息。

在一种可选的方案中，为提高目的端200对于接收到的目标分段数据的验证可靠性，签名装置120不将该目标分段数据的发送顺序发送给目的端200，从而避免该发送顺序在由源端100至目的端200的传输过程中被窃取，从而避免影响目的端200对于接收到的目标分段数据的校验，如攻击者可能在篡改传输的目标分段数据时，还基于窃取的发送顺序

对目标分段数据的数字签名也进行篡改等。

目的端200中可以包括传输模块211以及校验模块212。其中，传输模块211可以用于接收源端100发送的目标分段数据以及该目标分段数据对应的校验信息，并可以进一步确定该目标分段数据以及该目标分段数据对应的校验信息的接收顺序，该接收顺序例如可以是目的端200接收的第几个分段数据，然后将目标分段数据、校验信息以及接收顺序交由校验模块212进行数据校验。校验模块212可以根据该校验信息、目标分段数据以及接收顺序，对目标分段数据进行校验，以确定该目标分段数据是否存在传输异常，即校验目的端200所接收到的目标分段数据与源端100发送的目标分段数据是否一致。

作为一种示例，当校验信息具体为数字签名时。若签名装置120基于上述方式一中的实现方式生成数据签名，则校验模块212在进行校验时，可以利用目的端200保存的私钥对接收到的数字签名进行解密，得到摘要A，并按照相同规则将目标分段数据与接收顺序进行数据拼接，并根据拼接后的数据内容生成摘要B。然后，校验模块212将摘要A与摘要B进行比较，确定两个摘要是否一致，若是，则校验模块212可以确定目标分段数据不存在传输异常，即目的端200所接收到的目标分段数据与源端100发送的目标分段数据一致；而若两个摘要不一致，则校验模块212可以确定目标分段数据存在传输异常，即目的端200所接收到的目标分段数据与源端100发送的目标分段数据不一致，比如，目标分段数据可能存在内容篡改，或者在传输过程中被替换等。

在其它示例中，若签名装置120基于上述方式二生成数字签名，则校验模块212在进行校验时，可以利用目的端200保存的私钥对接收到的数字签名进行解密，得到摘要A，并根据源端100生成数字签名的规则，从该摘要A中推导出目标分段数据对应的摘要B，如从摘要A中去除发送顺序的部分获得摘要B。并且，校验模块212可以根据接收到的目标分段数据生成摘要C。然后，校验模块212可以比较该摘要B与摘要C是否一致，若是，则校验模块212可以确定目标分段数据不存在传输异常，而若不是，则校验模块212可以确定目标分段数据存在传输异常。上述两个示例，仅作为在校验信息具体为数字签名时校验模块212对目标分段数据进行校验过程的示例性说明，实际应用中，也可以采用其它实现方式。

此外，校验信息，也可以是结合发送顺序而生成的该目标分段数据对应的HMAC，或者可以是其它结合发送顺序而生成的并且能够用于对目标分段数据进行一致性校验的数据等。

示例性的，当校验信息具体为HMAC时，若签名装置120基于上述方式三生成HMAC，针对于每个分段数据（即目标分段数据），校验模块212将目的端200保存的解密密钥与该目标分段数据对应的接收顺序进行数据拼接（或者采用其它方式组合），得到拼接后的密钥，再利用拼接后的密钥对接收到的校验信息（即HMAC）进行解密，得到摘要A；然后校验模块212基于接收到的目标分段数据生成的摘要B，并比对摘要A与摘要B是否一致。若两个摘要一致，则校验模块212可以确定目标分段数据不存在传输异常，而若不是，则校验模块212可以确定目标分段数据存在传输异常。

当校验信息具体为HMAC时，若签名装置120基于上述方式四生成HMAC，校验模

块 212 可以将接收到的目标分段数据与该目标分段数据对应的接收顺序进行数据拼接（或者采用其它方式组合），并基于拼接得到的数据内容生成相应的摘要 A，然后，校验模块 212 可以利用目的端 200 保存的解密密钥对接收到的校验信息进行解密，得到摘要 B，并将摘要 A 与摘要 B 进行比对，确定两个摘要是否一致。若一致，则校验模块 212 可以确定目标分段数据不存在传输异常，否则，确定目标分段数据存在传输异常。

当校验信息具体为 HMAC 时，若签名装置 120 基于上述方式五生成 HMAC，校验模块 212 可以利用解密密钥对接收到的校验信息进行解密，得到摘要 A，并从摘要 A 中去除目标分段数据对应的接收顺序，得到摘要 B；然后，校验模块 212 可以基于接收到的目标分段数据生成摘要 C，并比较摘要 B 与摘要 C 是否一致。若一致，则校验模块 212 可以确定目标分段数据不存在传输异常，否则，确定目标分段数据存在传输异常。

本实施例中，校验模块 212 可以根据目标分段数据的接收顺序以及接收到的校验信息，对接收到的目标分段数据进行校验的具体实现过程可以采用任意可适用的实现方式，本实施例对此并不进行限定和赘述。

基于上述过程，源端 100 与目的端 200 在传输待传输数据中的每个分段数据时，均可以按照上述过程对传输的分段数据进行校验，并且在当前传输的分段数据通过校验时，源端 100 继续向目的端 200 传输下一个分段数据。而若当前传输的分段数据未通过校验，则目的端 200 可以通知源端 100 重新传输该分段数据，并对重新传输的分段数据继续进行校验，直至目的端 200 所接收到的分段数据与源端 100 发送的分段数据一致时才传输下一个分段数据。由于每个分段数据的数据量小于待传输数据的数据量，因此，通过对传输的每个分段数据进行校验，可以有效提高校验效率。而且，即使任意分段数据在传输过程中发生替换（即利用其它分段数据来替换当前正在传输的分段数据）、重放（即重复发送相同分段数据）以及顺序重组（即多个分段数据在传输过程中的顺序被重新组合）等传输异常时，目的端 200 均可以通过上述校验过程进行及时确定传输异常的发生。

进一步的，源端 100 还可以通知目的端 200 待传输数据被传输完毕，以使得目的端 200 能够确定当前所接收到的多个分段数据包含待传输数据的所有分段数据。同时，目的端 200 也能依据是否收到源端 100 发送的待传输数据传输完毕的通知而确定待传输数据中的部分分段数据是否在传输过程中被攻击者截断。

在一种示例性的实现方式中，源端 210 在向目的端 200 成功传输待传输数据的所有分段数据后，可以继续向目的端 200 传输一个特殊的分段数据，以下称之为结束分段数据。其中，结束分段数据中可以携带有结束标识，该结束标识能够用于指示该待传输数据的多个分段数据均已经成功传输至目的端 200。源端 100 中的分段模块 121 在对待传输数据进行切分并得到多个分段数据的同时，还可以构造出一个尺寸为 0 的结束分段数据，并由排序模块 122 确定该结束分段数据的发送顺序为最后发送。同时，校验信息生成模块 123 可以根据该结束分段数据所对应的发送顺序，为该结束分段数据生成数字签名，然后，交由传输模块 124 向目的端 200 发送该结束分段数据以及相应的数字签名。这样，当目的端 200 接收到该结束分段数据并完成对该结束分段数据的校验后，可以确定待传输数据的多个分段数据传输完成。如此，实现了整个待传输数据由源端 100 至目的端 200 的成功传输。

而在其它可能的实施方式中，源端 100 在向目的端 200 发送分段数据的同时，还发送待传输数据是否结束的结束标识，比如可以是在发送最后一个分段数据以及该最后一个分段数据对应的校验信息时，发送结束标识。这样，中间网络 300 在传输每个分段数据时，可以基于该分段数据生成多个报文（每个报文携带分段数据中的部分数据），并在报文头（或者报文中的其它位置）中新定义结束指示字段，该结束指示字段用于指示当前传输的分段数据为最后一个分段数据，并根据该结束标识的取值在报文头中定义结束指示字段的值。例如，当该结束指示字段的值为 0 时，表征待传输数据未传输完毕，而当结束指示字段的值为 1 时，表征待传输数据传输完毕。实际应用中，若分段模块 121 将待传输数据切分成（N+1）个分段数据，则源端 100 向目的端 200 发送的第 1 个至第 N 个分段数据对应的报文中，结束指示字段的数值可以为 0；而源端 100 向目的端 200 发送的第（N+1）个分段数据对应的报文中，结束指示字段的数值可以为 1，用于告知目的端 200 待传输数据的最后一个分段数据已经完成传输。

当然，上述示例，仅用于对源端 100 通知目的端 200 待传输数据传输完成的实现过程的示例性说明，在其它实施例中，源端 100 也可以是基于其它方式通知目的端 200 待传输数据的传输过程结束，比如，源端 100 单独向目的端 200 发送传输结束的指示消息，该指示消息中携带有结束标识等，本实施例对此并不进行限定。

上述实施例中，签名装置 120 可以通过单个线程实现上述对于待传输数据的分段、确定发送顺序、生成校验信息以及发送分段数据的过程，而在实际应用中，签名装置 120 也可以是通过多个线程，向目的端 200 并发传输数据，以提高源端 100 向目的端 200 的数据传输效率。

作为一种示例性的实施方式，数据生产装置 110 可以将待传输资源切分成多个待传输数据，比如切分成第一待传输数据以及第二待传输数据，并将这两个待传输数据传输给签名装置 120。而签名装置 120 可以具有多个线程，以具有线程 1 以及线程 2 为例。在对待传输数据进行签名时，签名装置 120 可以基于上述实施例用每个线程处理一个待传输数据。具体的，如图 4 所示，签名装置 120 利用线程 1，对第一待传输数据进行切分，得到第一待传输数据的多个分段数据，并进一步为该第一待传输数据的每个分段数据确定发送顺序以及相应的第一校验信息，再利用该线程 1 将第一待传输数据的多个分段数据以及每个分段数据对应的第一校验信息发送给目的端 200。其中，第一校验信息，即根据第一待传输数据的分段数据进行生成。类似的，对于第二待传输数据，签名装置 120 可以利用线程 2 对该第二待传输数据进行分段、确定发送顺序、生成校验信息以及向目的端 200 发送第二待传输数据的各个分段数据以及相应校验信息的过程。其中，第二校验信息，即根据第二待传输数据的分段数据进行生成。本实施例中，对于签名装置 120 利用线程 1 向目的端 200 传输第一待传输数据的具体实现过程，以及利用线程 2 向目的端 200 传输第二待传输数据的具体实现过程，可以参见上述相关之处描述，本实施例对此不再进行赘述。

其中，源端 100 可以先启动多个传输线程，再将获取到的待传输资源切分成多个待传输数据，也可以是在切分得到多个待传输数据后，启动多个传输线程，或者二者同时执行等，本实施例中，对这两个过程的具体执行顺序并不进行限定。

相应的，目的端 200 上至少可以具有两个线程，为便于区分，以下称之为线程 3 以及线程 4。认证装置 210 可以利用线程 3 接收源端 100 利用线程 1 发送的第一待传输数据对应的各个分段数据以及校验信息，并对接收到的该分段数据进行相应的校验；同时，认证装置 210 可以利用线程 4 接收源端 220 利用线程 2 发送的第二待传输数据对应的各个分段数据以及校验信息，并对接收到的该分段数据进行相应的校验。其中，线程 3 以及线程 4 对分段数据进行校验的具体实现过程可以参见上述相关之处描述，在此不做赘述。

为便于目的端 200 确定第一待传输数据以及第二待传输数据为同一待传输资源下的两个不同待传输数据，在一些可能的实施方式中，源端 100 在向目的端 200 发送第一待传输数据以及第二待传输数据的各个分段数据的同时，还向目的端 200 发送第一待传输数据以及第二待传输数据分别对应的描述数据，具体是通过线程 1 向目的端 200 发送第一待传输数据的描述数据，通过线程 2 向目的端 200 发送第二待传输数据的描述数据。这样，目的端 200 在接收到第一待传输数据的分段数据以及第二待传输数据的分段数据时，可以根据第一待传输数据以及第二待传输数据的描述数据，确定该第一待传输数据的分段数据以及第二待传输数据的分段数据属于同一待传输资源，并基于第一待传输数据的各个分段数据以及第二待传输数据的各个分段数据，整合得到完整的待传输资源。

作为一种示例，第一待传输数据的描述数据，例如可以包括第一待传输数据所属的待传输资源的标识（resource ID），如文件名、统一资源定位符（uniform resource locator，URL）或者经过哈希运算的 URL 等。进一步的，描述数据，还可以包括该第一待传输数据的切片范围（range）。其中，第一待传输数据的切片范围，例如可以是第一待传输数据的切片大小、切片标识等。第二待传输数据的描述数据，与第一待传输数据的描述数据类似，在此不做赘述。

进一步的，签名装置 120 在利用线程 1 为第一待传输数据的每个分段数据生成第一校验信息时，也可以根据该分段数据的发送顺序以及该第一待传输数据的描述数据进行生成。例如，当第一校验信息具体为数字签名时，签名装置 120 可以利用线程 1 为该分段数据生成摘要，并将该摘要与该分段数据对应的发送顺序、第一待传输数据的描述数据进行数据拼接，并对拼接后所得到的数据内容进行加密，得到该分段数据所对应的数字签名等。相应的，认证装置 210 在利用线程 3 为对该分段数据进行校验时，可以利用公钥对接收到的该分段数据对应的校验信息进行解密，并从解密得到的数据内容中反算出该分段数据对应的摘要，从而通过比对该摘要与根据接收到的分段数据所生成的摘要是否一致，来确定认证装置 210 接收到的分段数据与签名装置 120 发送的分段数据是否一致。类似的，针对于第二待传输数据中的各个分段数据，签名装置 120 也可以是利用线程 2，根据第二待传输数据的描述数据以及该分段数据对应的发送顺序，生成该分段数据对应的第二校验信息，其具体实现方式可参见生成第一校验信息之处的相关描述，在此不做赘述。

实际应用中，签名装置 120 也可以是利用多个线程，同时对数据生产装置 110 提供的多个不同的待传输数据分别进行签名，并在完成签名后，将多个不同的待传输数据以及校验信息并行传输至目的端，其具体实现过程与上述签名装置 120 为两个待传输数据分别签名并传输的具体实现类似，可参见前述相关之处描述，在此不做赘述。

实际应用的一些场景中，在待传输数据的多个分段数据由源端 100 传输至目的端 200 的过程中，存在部分分段数据被攻击者利用其它数据的具有相同发送顺序的分段数据进行替换的可能性。比如，假设同时存在源端 A_1 向目的端 A_2 发送待传输数据 a，以及源端 B_1 向目的端 B_2 发送待传输数据 b，则攻击者可以在源端 A_1 以及源端 A_2 传输分段数据的过程中，将具有相同发送顺序的部分分段数据进行互换。比如，假设源端 A_1 依次发送待传输数据 a 中的分段数据 a_1、a_2、a_3、a_4、a_5，源端 A_2 依次发送待传输数据 b 中的分段数据 b_1、b_2、b_3、b_4、b_5，则攻击者可以将待传输数据 a 中的分段数据 a_3 与待传输数据 b 中的分段数据 b_3 进行互换，从而目的端 A_2 所接收到的分段数据依次为 a_1、a_2、b_3、a_4、a_5，而目的端 B_2 所接收到的分段数据依次为 b_1、b_2、a_3、b_4、b_5，如此，造成目的端 A_1 与 A_2 所接收到的数据存在异常。

基于此，在将待传输数据的各个分段数据传输至目的端 200 的过程中，传输模块 124 可以先向目的端 200 发送目标分段数据（即待传输数据的多个分段数据中的任意一个分段数据）对应的会话标识，该会话标识用于标识传输该目标分段数据所对应的会话。这样，目的端 200 的认证装置 210 可以基于该会话标识，校验所接收到的不同分段数据是否属于同一会话，从而使得目的端 200 所接收到的不同分段数据属于该会话所对应的同一待传输资源。

其中，该会话标识，例如可以是数据传输的任务标识（SessionID）、请求标识（RequestID）、通用唯一识别码（Universally Unique Identifier，UUID）、为该会话生成的随机数（RandomNumber）、头哈希值（HeaderHash）、头签名值（HeaderSignature）中的任意一种或多种，或者可以是将上述任意一种或多种信息进行特征组合，并将组合得到的信息作为待传输数据的会话标识等。本实施例中，对于会话标识的具体实现方式并不进行限定。

在一种防止替换攻击的示例性实施方式中，传输模块 124 可以构造请求头，如基于 HTTP 协议的请求头等，该请求头中携带有待传输数据对应的会话标识。作为一种示例，传输模块 124 可以构造出入图 6 所示的请求头，其中，该请求头中的部分字段（头部）可以用于记录该请求头的属性信息，如请求类型、版本号等信息；该请求头中的另一部分字段可以用于记录待传输数据对应的会话标识，实际应用中，该部分字段可以是通过对已有的字段或者保留字段进行重定义，以实现利用该部分字段记录会话标识。然后，传输模块 124 可以将该请求头发送给目的端 200，如图 5 所示。这样，目的端 200 可以从接收到的请求头中解析出该会话标识，并确定后续接收到的多个分段数据为均通过该会话标识所对应的会话完成传输。

相应的，校验信息生成模块 123 在为待传输数据中的每个分段数据生成校验信息时，可以根据该分段数据的发送顺序以及该分段数据对应的会话标识（也即该分段数据所属的待传输数据对应的会话标识）生成校验信息。比如，当校验信息具体为数字签名时，校验信息生成模块 123 可以将该发送顺序以及会话标识与根据分段数据生成的摘要进行数据拼接，并对拼接得到的数据内容进行加密处理，则，得到的加密密文即可以是该分段数据对应的数字签名。相应的，对于目的端 200 接收到的各个分段数据，校验模块 212 可以根据从请求头中解析出的会话标识以及该分段数据对应的接收顺序，对该分段数据进行校验，

以确定目的端200所接收到的分段数据与源端100发送的分段数据是否一致。

这样，当攻击者将通过不同会话传输的不同待传输数据的分段数据进行互换时，目的端200中的认证装置210（具体可以是校验模块212）可以通过该分段数据对应的会话标识确定目的端200所接收到的分段数据与源端100发送的分段数据不一致，从而确定该分段数据在传输过程中出现异常。

在进一步可能的实施方式中，请求头在源端100与目的端200之间进行传输时，目的端200还可以对该请求头进行校验，具体校验源端100发送的请求头与目的端200接收到的请求头是否一致，以确定该请求头在传输过程中是否遭受篡改等攻击。示例性的，源端100中校验信息生成模块123还可以为构造的请求头生成校验信息，并将该请求头的校验信息添加至请求头中的校验部分字段中，如图6所示。这样，目的端200中在接收到该请求头后，校验模块212可以从该请求头中的校验部分字段中解析出该请求头对应的校验信息，并利用该校验信息对请求头中的内容进行校验。其中，该校验部分可以是与头部合并，也可以是区别于头部的字段，比如，该校验部分可以是请求头中的尾部字段，本实施例对请求头中携带会话标识以及校验信息的具体实现方式并不进行限定。当校验模块212确定目的端200接收到的请求头与源端100发送的请求头一致时，源端100可以开始向目的端200发送待传输数据中的各个分段数据；而当校验模块212确定目的端200接收到的请求头出现传输异常时，则目的端200可以终止与源端100之间的连接，或者要求源端100重新传输请求头等，并且直至目的端200接收到的请求头与源端100发送的请求头一致时才允许源端100进一步传输分段数据。

实际应用中，源端100中的传输模块124在构造请求头时，还可以在该请求头中添加更多的其它信息来加强对于目的端200所接收到的待传输数据的校验。示例性的，传输模块124还可以在请求头中添加时间信息和/或位置信息。其中，时间信息，例如可以是源端100发送分段数据与目的端200接收到分段数据之间的最大允许时间差等，当然，也可以是其它可适用的在时间维度对分段数据进行校验的信息等；位置信息，例如可以是接收到分段数据的目的端200所允许的网络位置/地理位置，或者，可以是其它可适用的在位置维度对分段数据进行校验的信息等。

值得注意的是，上述示例仅用于对源端100与目的端200协同校验分段数据的具体实现方式进行示例性说明，并不用于限定其具体实现局限于上述实现方式。应当理解，实际应用中，上述各实现方式之间可以相互组合。比如，在其它可能的实施方式中，源端100所生成的请求头中，不仅可以包括会话标识、请求头对应的数字签名，还可以包括上述时间信息和/或位置信息等。进一步的，当源端100基于多个线程向目的端200传输待传输数据时，每个线程可以生成相应的请求头，并且每个线程所生成的请求头中还可以包括该线程所传输的子数据的描述数据等。

根据上述实施例所描述的数据传输过程，本申请实施例还提供了数据传输方法，接下来从各装置交互的角度对该数据传输方法进行介绍。

参见图7所示的数据传输方法的流程图，该方法应用于上述数据传输系统，该数据传

输系统包括源端100以及目的端200，该方法具体包括如下步骤：

S701：源端100获取待传输数据。

实际应用中，源端100中可以存在运行有一个或者多个应用，并且该应用可以产生需要传输至目的端200的数据。比如，当目的端200为云平台提供的对象存储服务（Object Storage Service，OBS）时，用户可以在源端100上通过客户端将数据上传至OBS服务的桶中，或者由该客户端定时将用户数据上传至桶中。则，客户端所要上传的数据即为本实施例中的待传输数据。

S702：源端100构建携带有会话标识的请求头，并将向目的端200发送该请求头。

实际应用中，攻击者可能在数据传输过程中，将不同会话中的数据进行相互替换，从而使得目的端200所接收到的数据并非是源端100实际发送的数据，为此，本实施例中，可以先将当前的会话标识传输给目的端200，以便于目的端后续结合该会话标识对接收到的数据进行校验。

在进一步可能的实施方式中，源端100还可以向目的端发送该请求头对应的校验信息，以便于目的端200利用该校验信息对接收到的请求头进行信息校验，从而确定该请求头中所携带的信息在传输过程中是否被篡改。

S703：源端100将待传输数据切分为多个分段数据。

具体实现时，源端100可以将该待传输数据按照固定尺寸进行等长分段，则每个分段数据的尺寸可以相同，其中，最后一个分段数据的尺寸可以与其它分段数据的尺寸相同或者不同。而在其它示例中，源端100也可以是所切分得到的多个分段数据也可以是具有不同的尺寸，本实施例中，对于源端100如何切分待传输数据的具体实现并不进行限定。

S704：源端100确定每个分段数据的发送顺序。

作为一种示例，源端100可以将分段数据在待传输数据中的排序作为该分段数据的发送顺序，比如，对于源端100切分得到的第一个分段数据，其可以被第一个发送给目的端，而对于源端100切分得到的第二个分段数据，其可以被第二个发送给目的端，以此类推。当然，在其它示例中，每个分段数据的发送顺序也可以是与分段数据在待传输数据中的排序存在差异，本实施例对此并不限定。

S705：源端100根据每个分段数据以及每个分段数据的发送顺序，生成每个分段数据的校验信息。

其中，校验信息可以是该分段数据对应的数字签名，或者可以是HMAC。源端100可以根据每个分段数据、每个分段数据的发送顺序以及源端100预先保存的加密密钥的组合，生成该分段数据对应的校验信息，其具体实现可参见前述实施例中相关之处描述，在此不做赘述。

S706：源端100向目的端发送多个分段数据以及该多个分段数据对应的校验信息至目的端。

对于一份待传输数据，源端100可以启动一个传输线程，并利用该传输系统将该待传输数据发送给目的端200。实际应用中，源端100可以同时启动多个传输线程，并利用该多个传输线程分别向目的端200传输不同的待传输数据。其中，源端100利用每个传输线

程向目的端200传输一份待传输数据的具体实现过程可以相近。

特别的，当源端100需要向目的端200传输一份待传输资源时，源端100可以将该待传输资源切分成多份不同的待传输数据，并利用不同传输线程分别传输不同的待传输数据，如此，可以实现待传输资源在源端100与目的端200之间的并行传输，从而可以有效提高资源传输效率。

值得注意的是，为降低攻击者能够获知分段数据的发送顺序的可能性，源端100不将该分段数据的发送顺序传输至目的端200，这样，攻击者因为无法获知到该分段数据的发送顺序，从而难以攻击该分段数据的校验信息。

进一步的，为便于目的端200对于多份待传输数据的整合，源端100可以向目的端发送每份待传输数据对应的描述数据，该描述数据例如可以是待传输数据所属资源的标识和/或切片范围，从而目的端200可以根据该描述数据整合接收到的多份不同的待传输数据，从而整合得到整个待传输资源。示例性的，该描述数据可以被携带于上述请求头中，当然，也可以是单独发送，本实施例对此并不进行限定。

S707：目的端200确定每个分段数据的接收顺序。

S708：目的端200根据每个分段数据、每个分段数据的接收顺序以及每个分段数据的校验信息，校验待传输数据中的每个分段数据是否传输异常。

目的端200在接收到分段数据以及该分段数据对应的校验信息时，可以记录该分段数据的接收顺序，并利用该分段数据的接收顺序，结合分段数据以及该分段数据的校验信息对接收到的分段数据进行校验，以确定该分段数据在传输过程中是否存在传输异常。

值得注意的是，源端100与目的端200在传输多个分段数据的过程中，分段数据在源端100的发送顺序与该分段数据在目的端200的接收顺序保持一致。

具体实现时，目的端200可以通过对接收到的分段数据、该分段数据的接收顺序、密钥以及接收到的校验信息进行相应的运算，校验接收到的分段数据是否存在传输异常，其具体校验过程，可参见前述实施例中的相关之处描述，在此不做赘述。

实际应用中，源端100可以向目的端200逐个传输分段数据，并在目的端200完成对当前接收到的分段数据的校验后，通知源端100向目的端200传输下一个分段数据。这样，当其中任意一个分段数据在传输过程中存在传输异常，目的端200可以通过对该分段数据的校验过程及时发现，从而可以提高校验效率。进一步的，目的端200可以在确定分段数据异常时，断开与源端100之间的连接，或者通知源端100重新传输该分段数据。

在一些可能的实施方式中，为便于告知目的端200当前传输的多个分段数据为所有分段数据，源端100可以向目的端200发送结束标识，该结束标识用于标识源端100向目的端200传输的最后一个分段数据。这样，目的端200可以通过该结束标识确定当前所接收到的多个分段数据为源端100发送的所有分段数据。并且，当该多个分段数据在传输过程中存在攻击者截断时，目的端200可以通过未接收到源端100发送的结束标识或者源端100发送的结束标识的取值，来确定目的端200是否接收到了源端100发送的所有分段数据，从而当存在攻击者截断部分分段数据时，目的端200可以及时发现。

图 8 至图 9 分别提供了一种计算机设备。图 8 所示的计算机设备 800 具体可以用于实现上述图 2 所示实施例源端 100 中签名装置 120 的功能，图 9 所示的计算机设备 900 具体可以用于实现上述图 2 所示实施例中目的端 200 中认证装置 210 的功能。

计算机设备 800 包括总线 801、处理器 802、通信接口 803 和存储器 804。处理器 802、存储器 804 和通信接口 803 之间通过总线 801 通信。计算机设备 800 在实现图 2 以及图 7 所示实施例的情况下，且图 2 以及图 7 实施例中所描述的源端 100 中的签名装置 120 为通过软件实现的情况下，执行签名装置 120 中分段模块 121、排序模块 122 以及校验信息生成模块 123 功能所需的软件或程序代码存储在存储器 804 中。传输模块 124 功能可以通过通信接口 803 实现，处理器 802 用于执行存储器 804 中的指令，实现签名装置 120 所执行的方法。

计算机设备 900 包括总线 901、处理器 902、通信接口 903 和存储器 904。处理器 902、存储器 904 和通信接口 903 之间通过总线 901 通信。计算机设备 900 在实现图 2 以及图 7 所示实施例的情况下，且图 2 以及图 7 实施例中所描述的目的端 200 中的认证装置 210 为通过软件实现的情况下，执行认证装置 210 中校验模块 212 功能所需的软件或程序代码存储在存储器 904 中。传输模块 211 功能可以通过通信接口 903 实现，处理器 902 用于执行存储器 904 中的指令，实现认证装置 210 所执行的方法。

此外，本申请实施例还提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机设备上运行时，使得计算机设备执行上述实施例中所述源端 100 所执行的方法。

本申请实施例还提供了另一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机设备上运行时，使得计算机设备执行上述实施例中所述目的端 200 所执行的方法。

本申请实施例还提供了一种计算机程序产品，所述计算机程序产品被计算机执行时，所述计算机执行前述数据传输方法的任一方法。该计算机程序产品可以为一个软件安装包，在需要使用前述数据提供方法的任一方法的情况下，可以下载该计算机程序产品并在计算机上执行该计算机程序产品。

另外需说明的是，以上所描述的装置实施例仅仅是示意性的，其中所述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模块来实现本实施例方案的目的。另外，本申请提供的装置实施例附图中，模块之间的连接关系表示它们之间具有通信连接，具体可以实现为一条或多条通信总线或信号线。

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件的方式来实现，当然也可以通过专用硬件包括专用集成电路、专用 CPU、专用存储器、专用元器件等来实现。一般情况下，凡由计算机程序完成的功能都可以很容易地用相应的硬件来实现，而且，用来实现同一功能的具体硬件结构也可以是多种多样的，例如模拟电路、数字电路或专用电路等。但是，对本申请而言更多情况下软件程

序实现是更佳的实施方式。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可读取的存储介质中，如计算机的软盘、U盘、移动硬盘、ROM、RAM、磁碟或者光盘等，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，训练设备，或者网络设备等）执行本申请各个实施例所述的方法。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。

所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、训练设备或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、训练设备或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存储的任何可用介质或者是包含一个或多个可用介质集成的训练设备、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘（Solid State Disk，SSD））等。

权 利 要 求

1、一种数据传输方法，其特征在于，所述方法应用于源端，所述方法包括：

获取待传输数据；

将所述待传输数据切分为多个分段数据；

确定所述多个分段数据的发送顺序；

根据每个分段数据以及每个分段数据的发送顺序，生成每个分段数据的校验信息；

发送所述多个分段数据以及所述多个分段数据对应的校验信息至目的端。

2、如权利要求 1 所述的方法，其特征在于，所述根据每个分段数据以及每个分段数据的发送顺序，生成每个分段数据的校验信息，包括：

将每个分段数据和每个分段数据的发送顺序与密钥的组合，进行基于哈希的消息认证码 HMAC 运算，获得每个分段数据的校验信息。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述待传输数据通过会话传输；所述根据每个分段数据以及每个分段数据的发送顺序，生成每个分段数据的校验信息，包括：

根据每个分段数据、每个分段数据的发送顺序以及所述会话的标识，生成每个分段数据的校验信息；

所述方法还包括：

发送所述会话的标识至所述目的端。

4、如权利要求 3 所述的方法，其特征在于，所述发送所述会话的标识至所述目的端，包括：

向所述目的端发送第一个分段数据以及所述第一个分段数据的校验信息之前，发送携带有所述会话的标识的请求头至所述目的端。

5、如权利要求 1 至 4 任一所述的方法，其特征在于，所述发送所述多个分段数据以及所述多个分段数据对应的校验信息至目的端，包括：

发送最后一个分段数据、所述最后一个分段数据的校验信息以及结束标识至目的端，所述结束标识指示所述多个分段数据传输完毕。

6、如权利要求 1 至 5 任一所述的方法，其特征在于，在所述获取待传输数据前，所述方法还包括：

启动多个传输线程；

获取待传输资源，将所述待传输资源切分为多个待传输数据；

所述发送所述多个分段数据以及所述多个分段数据对应的校验信息至目的端，包括：

通过每个传输线程，发送至少一个待传输数据的分段数据以及对应的校验信息至所述目的端。

7、如权利要求 6 所述的方法，其特征在于，通过每个传输线程，发送至少一个待传输数据的分段数据以及对应的校验信息至所述目的端，包括：

每个传输线程，向所述目的端发送所述至少一个待传输数据的第一个分段数据以及对应的校验信息之前，发送携带有描述数据的请求头至所述目的端；其中，所述描述数据包括以下至少一种：

所述待传输资源的标识以及所述待传输数据的切片范围。

8、一种数据传输方法，其特征在于，所述方法应用于目的端，所述方法包括：

接收来自源端的多个分段数据以及每个分段数据对应的校验信息，所述多个分段数据基于对待传输数据进行切分得到；

确定每个分段数据的接收顺序；

根据每个分段数据、每个分段数据的接收顺序以及每个分段数据的校验信息，校验所述待传输数据中的每个分段数据是否传输异常。

9、如权利要求 8 所述的方法，其特征在于，所述校验信息包括基于哈希的消息认证码 HMAC，所述根据每个分段数据、每个分段数据的接收顺序以及每个分段数据的校验信息，校验所述待传输数据中的每个分段数据是否传输异常，包括：

根据每个分段数据、每个分段数据的接收顺序、密钥以及接收到的校验信息，确定所述待传输数据中的每个分段数据是否传输异常。

10、如权利要求 8 或 9 所述的方法，其特征在于，所述待传输数据通过会话传输，所述方法还包括：

接收来自所述源端的所述会话的标识；

所述根据每个分段数据、每个分段数据的接收顺序以及每个分段数据的校验信息，校验所述待传输数据中的每个分段数据是否传输异常，包括：

根据每个分段数据、每个分段数据的接收顺序、每个分段数据的校验信息以及所述会话的标识，校验所述待传输数据中的每个分段数据是否传输异常。

11、如权利要求 10 所述的方法，其特征在于，所述接收来自所述源端的所述会话的标识，包括：

接收来自所述源端的携带有所述会话的标识的请求头。

12、如权利要求 8 至 11 任一项所述的方法，其特征在于，所述接收来自源端的多个分段数据以及每个分段数据对应的校验信息，包括：

接收来自源端的最后一个分段数据、所述最后一个分段数据的校验信息以及结束标识，所述结束标识指示所述多个分段数据传输完毕。

13、如权利要求 8 至 12 任一项所述的方法，其特征在于，所述接收来自源端的多个分段数据以及每个分段数据对应的校验信息，包括：

接收所述源端通过每个传输线程发送的至少一个待传输数据的分段数据以及对应的校验信息，不同传输线程用于传输对待传输资源切分得到的不同待传输数据。

14、如权利要求 13 所述的方法，其特征在于，所述接收所述源端通过每个传输线程发送的至少一个待传输数据的分段数据以及对应的校验信息，包括：

在接收所述源端通过每个传输线程发送的至少一个待传输数据的分段数据以及对应的校验信息之前，接收来自所述源端的携带有描述信息的请求头，所述描述数据包括以下至少一种：

所述待传输资源的标识以及所述待传输数据的切片范围。

15、一种数据传输系统，其特征在于，所述系统包括如权利要求 1 至 7 任一项所述的

源端，以及如权利要求 8 至 14 任一项所述的目的端。

16、一种计算设备，其特征在于，所述计算设备包括处理器和存储器；

所述处理器用于执行所述存储器中存储的指令，执行如权利要求 1 至 7 任一项所述的方法。

17、一种计算设备，其特征在于，所述计算设备包括处理器和存储器；

所述处理器用于执行所述存储器中存储的指令，执行如权利要求 8 至 14 任一项所述的方法。

18、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中存储有指令，当其在计算设备上运行时，使得所述计算设备执行如权利要求 1 至 7 任一项所述的方法。

19、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中存储有指令，当其在计算设备上运行时，使得所述计算设备执行如权利要求 8 至 14 任一项所述的方法。

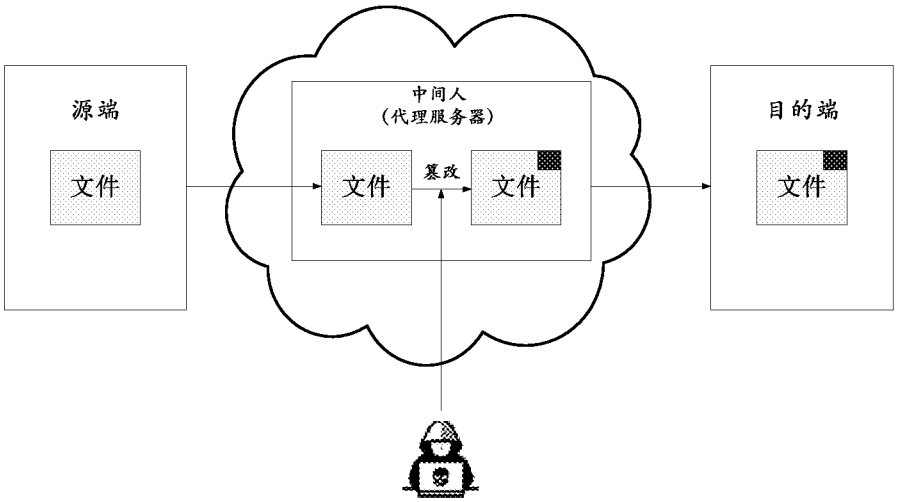

图 1

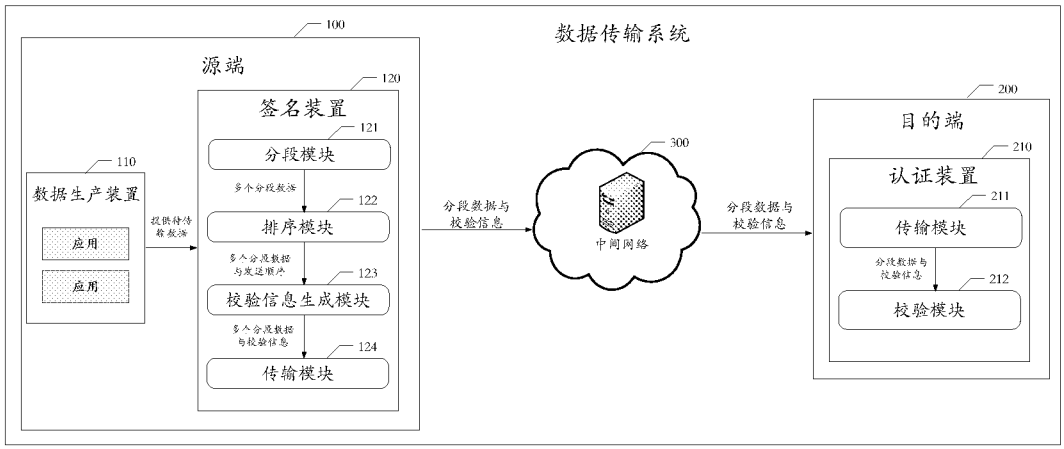
数据传输系统
100
源端
120
签名装置
121
分段模块
多个分段数据
122
排序模块
多个分段数据与发送顺序
123
校验信息生成模块
多个分段数据与校验信息
124
传输模块
110
数据生产装置
应用
应用
提供待传数据流
分段数据与校验信息
300
中间网络
分段数据与校验信息
200
目的端
210
认证装置
211
传输模块
分段数据与校验信息
212
校验模块

图 2

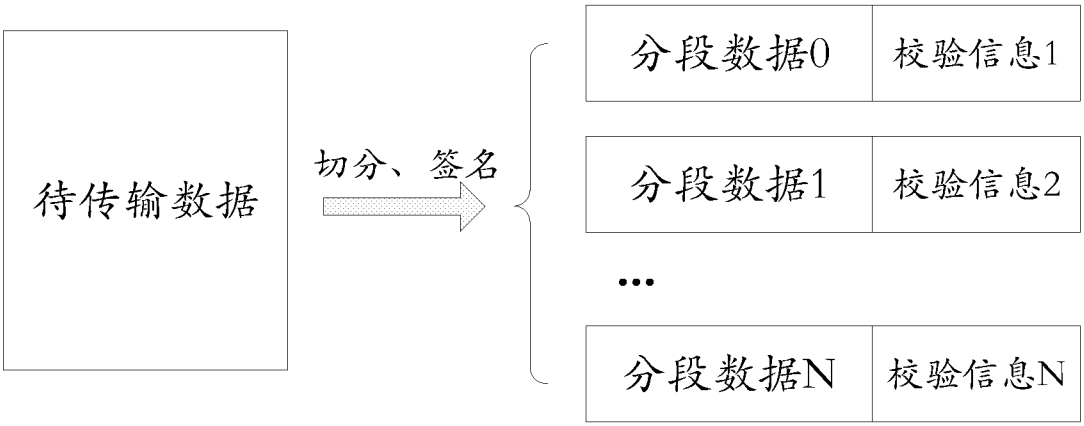
待传输数据
切分、签名
分段数据0
校验信息1
分段数据1
校验信息2
...
分段数据N
校验信息N

图 3

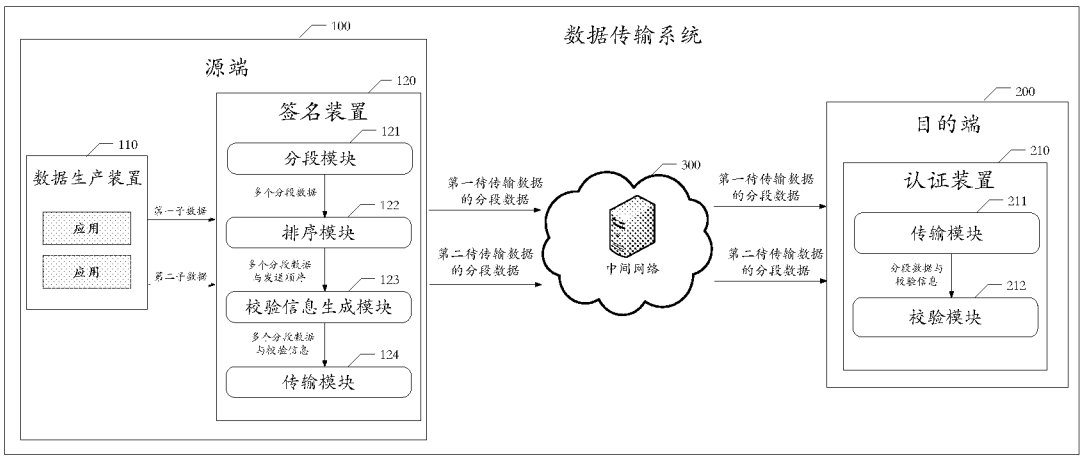
数据传输系统
100
源端
120
签名装置
121
分段模块
多个分段数据
122
排序模块
多个分段数据与发送顺序
123
校验信息生成模块
多个分段数据与校验信息
124
传输模块
110
数据生产装置
应用
应用
第一子数据
第二子数据
第一待传输数据的分段数据
第二待传输数据的分段数据
300
中间网络
第一待传输数据的分段数据
第二待传输数据的分段数据
200
目的端
210
认证装置
211
传输模块
分段数据与校验信息
212
校验模块

图 4

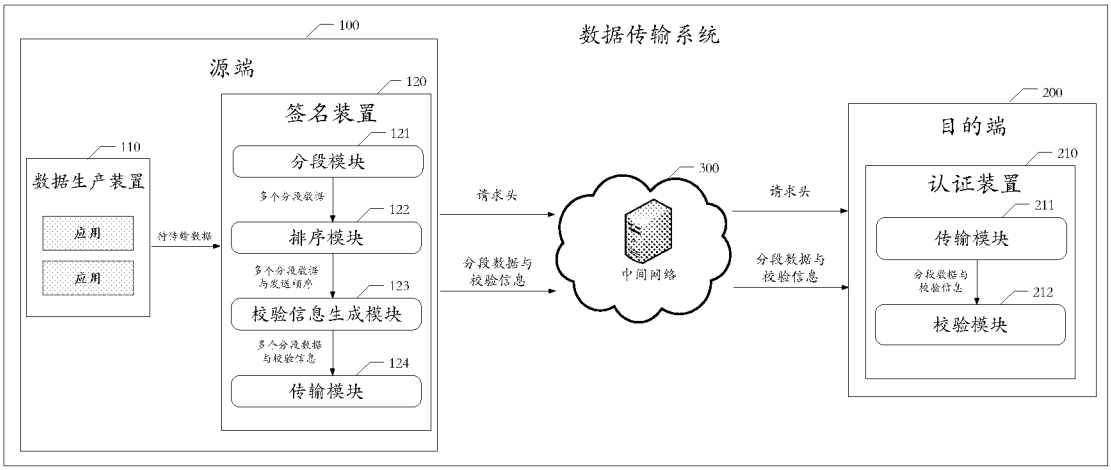
数据传输系统
100
源端
120
签名装置
121
分段模块
多个分段数据
122
排序模块
多个分段数据与发送顺序
123
校验信息生成模块
多个分段数据与校验信息
124
传输模块
110
数据生产装置
应用
应用
待传输数据
请求头
分段数据与校验信息
300
中间网络
请求头
分段数据与校验信息
200
目的端
210
认证装置
211
传输模块
分段数据与校验信息
212
校验模块

图 5

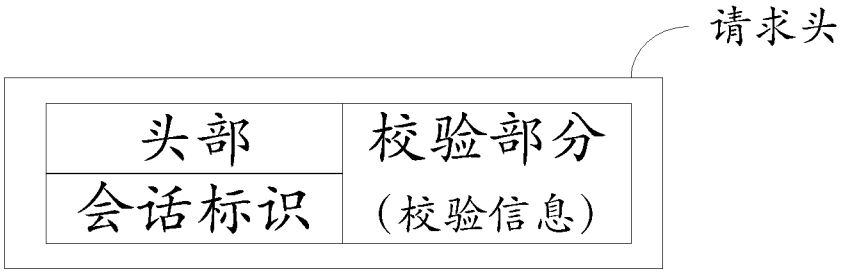
请求头
头部
会话标识
校验部分
(校验信息)

图 6

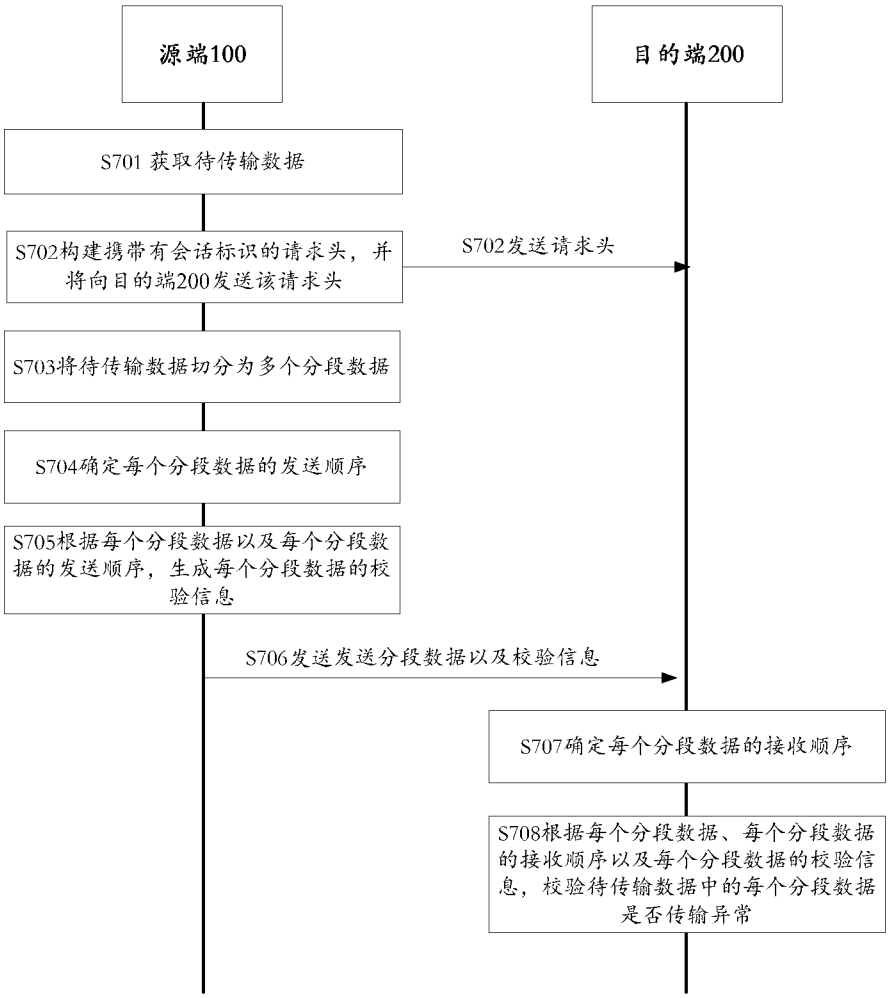
源端100
目的端200
S701 获取待传输数据
S702构建携带有会话标识的请求头，并将向目的端200发送该请求头
S702发送请求头
S703将待传输数据切分为多个分段数据
S704确定每个分段数据的发送顺序
S705根据每个分段数据以及每个分段数据的发送顺序，生成每个分段数据的校验信息
S706发送发送分段数据以及校验信息
S707确定每个分段数据的接收顺序
S708根据每个分段数据、每个分段数据的接收顺序以及每个分段数据的校验信息，校验待传输数据中的每个分段数据是否传输异常

图 7

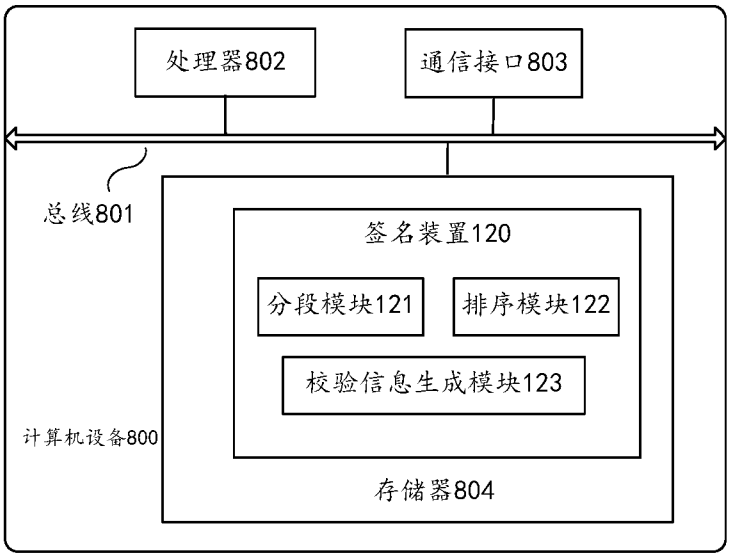
处理器802
通信接口803
总线801
签名装置120
分段模块121
排序模块122
校验信息生成模块123
计算机设备800
存储器804

图 8

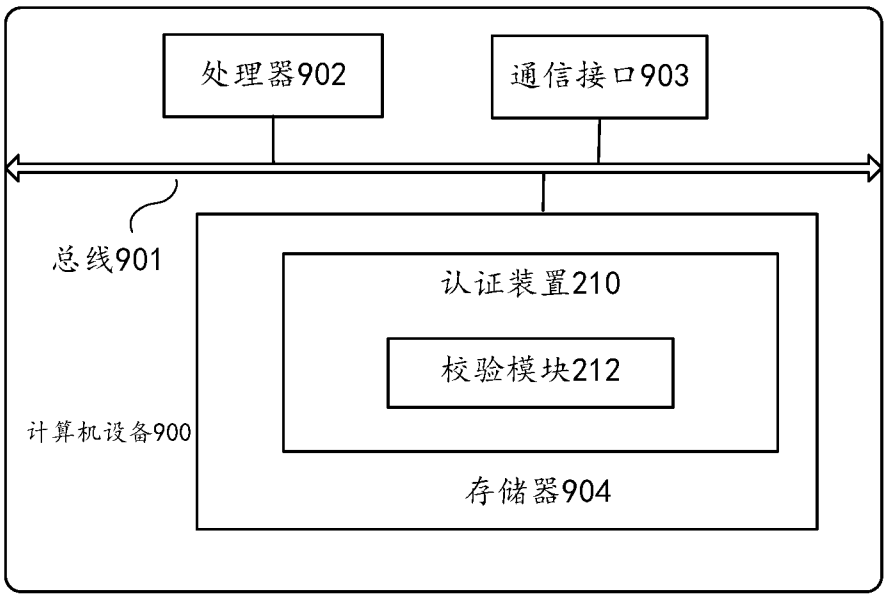
处理器902
通信接口903
总线901
认证装置210
校验模块212
计算机设备900
存储器904

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/129003

A. CLASSIFICATION OF SUBJECT MATTER

H04L 1/18(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, IEEE: 数据, 文件, 分割, 分块, 分段, 切分, 接收, 顺序, 次序, 发送, data, file, partition, block, segment, split, receive, order, send

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102938791 A (SITV SHANGHAI INTERACTIVE TELEVISION LIMITED) 20 February 2013 (2013-02-20) description, paragraphs [0020]-[0031]	1-19
Y	CN 110299970 A (TENDYRON CORPORATION) 01 October 2019 (2019-10-01) description, paragraphs [0041]-[0115]	1-19
Y	CN 102805887 A (ZHENG, Pan) 05 December 2012 (2012-12-05) description, paragraphs [0027]-[0039]	1-19
A	CN 107294878 A (CHINA MOBILE COMMUNICATION LTD., RESEARCH INSTITUTE et al.) 24 October 2017 (2017-10-24) entire document	1-19
A	CN 109194593 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 11 January 2019 (2019-01-11) entire document	1-19
A	US 2019394832 A1 (BEIJING XIAOMI MOBILE SOFTWARE CO., LTD.) 26 December 2019 (2019-12-26) entire document	1-19

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 July 2021	**12 August 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/129003

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 102938791 A	20 February 2013	None	
CN 110299970 A	01 October 2019	None	
CN 102805887 A	05 December 2012	None	
CN 107294878 A	24 October 2017	None	
CN 109194593 A	11 January 2019	None	
US 2019394832 A1	26 December 2019	WO 2018166042 A1	20 September 2018
		CN 107113658 A	29 August 2017

国际检索报告

国际申请号
PCT/CN2020/129003

A. 主题的分类

H04L 1/18(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, CNKI, WPI, EPODOC, IEEE：数据，文件，分割，分块，分段，切分，接收，顺序，次序，发送，data, file, partition, block, segment, split, receive, order, send

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 102938791 A (上海文广互动电视有限公司) 2013年 2月 20日 (2013-02-20) 说明书第[0020]-[0031]段	1-19
Y	CN 110299970 A (天地融科技股份有限公司) 2019年 10月 1日 (2019-10-01) 说明书第[0041]-[0115]段	1-19
Y	CN 102805887 A (郑攀) 2012年 12月 5日 (2012-12-05) 说明书第[0027]-[0039]段	1-19
A	CN 107294878 A (中国移动通信有限公司研究院 等) 2017年 10月 24日 (2017-10-24) 全文	1-19
A	CN 109194593 A (百度在线网络技术北京有限公司) 2019年 1月 11日 (2019-01-11) 全文	1-19
A	US 2019394832 A1 (BEIJING XIAOMI MOBILE SOFTWARE CO., LTD.) 2019年 12月 26日 (2019-12-26) 全文	1-19

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 7月 19日	2021年 8月 12日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国 北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 张千 电话号码 86-(10)-53961316

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/129003

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 102938791 A	2013年 2月 20日	无	
CN 110299970 A	2019年 10月 1日	无	
CN 102805887 A	2012年 12月 5日	无	
CN 107294878 A	2017年 10月 24日	无	
CN 109194593 A	2019年 1月 11日	无	
US 2019394832 A1	2019年 12月 26日	WO 2018166042 A1	2018年 9月 20日
		CN 107113658 A	2017年 8月 29日