PRIVACY DATA ACCESS METHOD AND APPARATUS, AND SYSTEM

TECHNICAL FIELD

[0001] One or more embodiments of this specification relate to the field of computer technologies, and in particular, to a privacy data access method and apparatus, and a system.

BACKGROUND

[0002] Currently, user data is increasingly closely monitored, especially for data related to user privacy. A privacy-preserving computation (privacy-preserving computation) technology needs to be used to enable privacy data to be available but invisible, and to be computable but unrecognizable. A TEE-based privacy-preserving computation technology has better real-time performance and scalability, and can support millisecond-level real-time privacy-preserving computation. Therefore, a requirement for monitoring data involving user privacy can be met. Currently, a TEE-based privacy data access solution is required.

SUMMARY

[0003] One or more embodiments of this specification provide a privacy data access method and apparatus, and a system.

[0004] According to a first aspect, a privacy data access method is provided, and is applied to a TEE system. A plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK. The plurality of TEE applications include a first application that provides a management service and a second application that provides a business service. The method is executed by the SDK, and the method includes: obtaining a data access request from the second application, where the request includes an asset identifier corresponding to a target user; obtaining, based on the asset identifier, access configuration information corresponding to the target user from the first application, where the access configuration information includes a storage address of a digital asset corresponding to the target

user in an external storage device of the TEE system; and performing privacy-related data access to the external storage device of the TEE system based on the access configuration information, where the data access includes data reading or data writing.

[0005] According to a second aspect, a risk control privacy data analysis method is provided, and is applied to a TEE system. A plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications include a management application and a risk control analysis application. The method includes: receiving, by the risk control analysis application, indication information used to indicate privacy data analysis, where the indication information includes identification information corresponding to a target user and an analysis type; sending, by the risk control analysis application, a query request based on the indication information, where the query request includes the identification information; receiving, by the SDK, the query request, and obtaining, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and obtaining, by the SDK, to-be-analyzed data from the external storage device of the TEE system, and enabling, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

[0006] According to a third aspect, a TEE-based computer system is provided. A plurality of TEE applications are deployed in the system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications include a first application that provides a management service and a second application that provides a business service; and the system includes a memory, a processor, and a computer program that is stored in the memory and that can run on the processor. The SDK implements the following steps when executing the program by using the processor: obtaining a data access request from the second application, where the request includes an asset identifier corresponding to a target user; obtaining, based on the asset identifier, access configuration information corresponding to the target user from the first application, where the access configuration information includes a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and performing privacy-related data access to the external storage device of the TEE system based on the access configuration information, where the data access includes data reading or data writing.

[0007] According to a fourth aspect, a TEE-based computer system is provided. A plurality of

TEE applications are deployed in the system, and the plurality of TEE applications are jointly integrated with an SDK. The plurality of TEE applications include a management application and a risk control analysis application. The system includes a memory, a processor, and a computer program stored in the memory and running on the processor. When executing the program by using the processor, the risk control analysis application implements the following steps: receiving indication information used to indicate privacy data analysis, where the indication information includes identification information corresponding to a target user and an analysis type; and sending a query request based on the indication information, where the query request includes the identification information. When executing the program by using the processor, the SDK implements the following steps: receiving the query request, and obtaining, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and obtaining to-be-analyzed data from the external storage device of the TEE system, and enabling, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

[0008] According to a fifth aspect, a privacy data access apparatus is provided, and is applied to a TEE system. A plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK. The plurality of TEE applications include a first application that provides a management service and a second application that provides a business service. The apparatus is deployed in the SDK, and the apparatus includes: a first obtaining module, configured to obtain a data access request from the second application, where the request includes an asset identifier corresponding to a target user; a second obtaining module, configured to obtain, based on the asset identifier, access configuration information corresponding to the target user from the first application, where the access configuration information includes a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and an access module, configured to perform privacy-related data access to the external storage device of the TEE system based on the access configuration information, where the data access includes data reading or data writing.

[0009] According to a sixth aspect, a risk control privacy data analysis apparatus is provided, and is applied to a TEE system. A plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; and the plurality of TEE

applications include a management application and a risk control analysis application. The apparatus includes: a receiving module, configured to be used by the risk control analysis application to receive indication information used to indicate privacy data analysis, where the indication information includes identification information corresponding to a target user and an analysis type; a sending module, configured to be used by the risk control analysis application to send a query request based on the indication information, where the query request includes the identification information; an obtaining module, configured to be used by the SDK to receive the query request, and obtain, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and an analysis module, configured to be used by the SDK to obtain to-be-analyzed data from the external storage device of the TEE system, and enable, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

[0010] According to a seventh aspect, a computer-readable nonvolatile storage medium is provided. The storage medium stores a computer program, and the computer program is executed by a processor to implement the method according to any one of the first aspect or the second aspect.

[0011] The technical solutions provided in the embodiments of this specification may include the following beneficial effects:

[0012] According to the privacy data access method and apparatus, and a system provided in the embodiments of this specification, a plurality of TEE applications deployed in the TEE system are jointly integrated with an SDK, which is used as a privacy calculation plane of the TEE system. The integrated SDK accesses privacy data with relatively high reusability, so that plaintext privacy data leaving the TEE system is encrypted without incurring application layer system code, and ciphertext privacy data entering the TEE system is decrypted, which makes the solution easier to popularize.

[0013] It should be understood that the foregoing general description and the following detailed description are merely exemplary and explanatory, and are not intended to limit this application.

BRIEF DESCRIPTION OF DRAWINGS

[0014] To describe technical solutions in embodiments of this specification more clearly, the following briefly describes the accompanying drawings needed for describing the embodiments. Clearly, the accompanying drawings in the following description merely show some embodiments of this specification, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0015] FIG. 1 is an architectural diagram of a TEE system according to an example embodiment of this specification;

[0016] FIG. 2 is an interactive flowchart of a privacy data access method according to an example embodiment of this specification;

[0017] FIG. 3 is an interactive flowchart of another risk control privacy data analysis method according to an example embodiment of this specification;

[0018] FIG. 4 is a block diagram of a privacy data access apparatus according to an example embodiment of this specification;

[0019] FIG. 5 is a block diagram of a risk control privacy data analysis apparatus according to an example embodiment of this specification; and

[0020] FIG. 6 is a block diagram of a computer system according to an example embodiment of this specification.

DESCRIPTION OF EMBODIMENTS

[0021] To enable a person skilled in the art to better understand the technical solutions in this specification, the following clearly and completely describes the technical solutions in the embodiments of this specification with reference to the accompanying drawings in the embodiments of this specification. It is clear that the described embodiments are merely some rather than all of the embodiments of this specification. All other embodiments obtained by a person of ordinary skill in the art based on embodiments of this specification without creative efforts shall fall within the protection scope of this specification.

[0022] Currently, user data is increasingly closely monitored, especially for data related to user privacy. A privacy-preserving computation technology needs to be used to enable privacy data to be available but invisible, and to be computable but unrecognizable. A TEE-based privacy-

preserving computation technology has better real-time performance and scalability, and can support millisecond-level real-time privacy-preserving computation. Therefore, a requirement for monitoring data involving user privacy can be met. The full name of TEE is trusted execution environment, which is an area on the CPU of the device. This area provides a more secure space for data and code execution, and ensures confidentiality and integrity of the data and code. Generally, the privacy-related data is encrypted ciphertext data before entering the TEE environment. When entering the TEE environment, the ciphertext data needs to be decrypted, so as to ensure that the data is available plaintext data after entering the TEE environment. The privacy-related data is unencrypted plaintext data before leaving the TEE environment. When leaving the TEE environment, the plaintext data needs to be encrypted, so as to ensure that the data is invisible and unrecognizable ciphertext data after leaving the TEE environment.

[0023] In a related technology, an application program that is at an application layer of the TEE system and that involves system IO operations is generally modified, so as to implement controllable encryption and decryption at a field level of the IO operation in the TEE system, that is, to decrypt external data entering the TEE system or encrypt internal data leaving the TEE system, so as to ensure that privacy-related data is ciphertext that can protect privacy outside the TEE system, and is plaintext that can be used for calculation inside the TEE system. However, to modify the application program involving system IO operations, it is necessary to invade the application layer system code, which makes the modification cost high, requires much repetitive work, and is difficult to promote.

[0024] According to the privacy data access solution provided in the embodiments of this specification, a plurality of TEE applications deployed in the TEE system are jointly integrated with an SDK, which is used as a privacy calculation plane of the TEE system. The integrated SDK accesses privacy data with relatively high reusability, so that plaintext privacy data leaving the TEE system is encrypted without incurring application layer system code, and ciphertext privacy data entering the TEE system is decrypted, which makes the solution easier to popularize.

[0025] FIG. 1 is an architectural diagram of a TEE system according to an example embodiment.

[0026] Inside the TEE system, a plurality of TEE applications are deployed. As shown in FIG. 1, the plurality of TEE applications may include, for example, a management application program used to provide a management service and several service application programs (for example, a

service application program 1, ..., and a service application program n) used to provide business services. The plurality of TEE applications are jointly integrated with an SDK, and the SDK may communicate between a management application and a service application. Outside the TEE system, at least one storage device S is disposed. For example, HBase may be deployed in the storage device S. The storage device S may store data that needs to enter the TEE system, or store data generated by the TEE system. The TEE system may establish a connection to the storage device S through the SDK, and read data from the storage device S or write data into the storage device S.

[0027] Specifically, when any service application program in the service application program 1 to the service application program n needs to access data, the service application program may send a request for accessing data to the management application program, and the SDK may intercept the request sent by the service application program. The request may include an asset identifier corresponding to a user M. The SDK may obtain, based on the asset identifier, access configuration information corresponding to the user M. The access configuration information is used to access a database deployed in the storage device S, and the access configuration information may include a storage address of a digital asset corresponding to the user M in the storage device S. The SDK may perform, based on the access configuration information, privacy-related data access on the storage device S outside the TEE system. The data access may be data reading, or may be data writing.

[0028] For example, in an embodiment, if the service application program generates new data D1 related to the user M, the service application sends a data write request Q1. In addition to the asset identifier of the user M, the request Q1 may further include data D1 that needs to be written into the storage device S. The data D1 is plaintext data generated inside the TEE system. After receiving the request Q1, the SDK may send, based on the request Q1, a request Q2 for obtaining the access configuration information to the management application program. The management application program returns the access configuration information to the SDK in response to the request Q2. In addition to the storage address of the digital asset corresponding to the user M in the storage device S, the access configuration information may further include a privacy-related field in the data D1 and an encryption key Y1. The SDK may encrypt the privacy-related field in the data D1 by using the key Y1, and use the encrypted field and a non-privacy-related field as data D2. The data D2 is written into the digital asset corresponding to the user M in the storage

device S according to the storage address of the digital asset corresponding to the user M in the storage device S.

[0029] For another example, in another embodiment, if the service application program needs to analyze or query data D3 of the user M, a data read request Q3 may be sent, and the request Q3 may include the asset identifier of the user M. After receiving the request Q3, the SDK may send, based on the request Q3, a request Q4 for obtaining the access configuration information to the management application program. The management application program returns the access configuration information to the SDK in response to the request Q4. In addition to the storage address of the digital asset corresponding to the user M in the storage device S, the access configuration information may further include a privacy-related field in the data and a decryption key Y2. The SDK may obtain to-be-read data D4 from the storage device S according to the storage address of the digital asset corresponding to the user M, decrypt a privacy-related field in the data D4 by using the key Y2, and use the decrypted field and a non-privacy-related field as the data D3. The data D3 is returned to the service application program for analysis or query by the service application program.

[0030] The following describes the solutions provided in this specification in detail with reference to specific embodiments.

[0031] As shown in FIG. 2, FIG. 2 is an interactive flowchart of a privacy data access method according to an example embodiment. The method may be applied to a TEE system. A plurality of TEE applications are deployed in the TEE system. The TEE applications may include a data access application, an authorization authentication application, and a service application. These TEE applications are jointly integrated with an SDK, and an external storage device is disposed outside the TEE system. The data access application and the authorization authentication service may be applications used for management, and the service application may be an application that provides a service (for example, provides a risk control consulting service, or provides a risk control analysis service).

[0032] First, in step 201, a user may first perform asset registration and identity authentication. The user may be a variety of institutions or organizations. Specifically, for example, the user M may send an asset registration request to the data access application by using a terminal device held by the user M, and the asset registration request may include registration information of the user M. For example, the registration information of the user M may include but is not limited to

an asset identifier of the user M and a public key held by the user M. In response to the asset registration request, the data access application may record the registration information of the user M in association with the user identifier of the user M, and return a result of registration success to the user M. The user M may further send an authorization request that carries authorization information to the authorization authentication application. For example, the authorization information may include a public key of the TEE system. The authorization authentication application may perform authorization authentication on the user M based on the authorization information, and return a result of the authorization authentication to the user M. After the authorization authentication on the user M succeeds, the digital asset of the user M may be stored in the external storage device, and address information of the digital asset of the user M and a privacy-related field in the digital asset of the user M are recorded in the data access application. In addition, the service application may access digital asset information of the user M. For example, the service application may write the digital asset information of the user M to the external storage device, or may read the digital asset information of the user M from the external storage device.

[0033] In a case, for example, after detecting an exception event related to the user M, the service application that provides the risk control consulting service may write exception event data to the external storage device. Specifically, in step 202a, the service application may send a data write request, and the SDK may intercept the data write request by using, for example, AspectJ. The data write request may include but is not limited to data that needs to be written (for example, the exception event information related to the user M), the asset identifier of the user M, identification information of the user M, and authorization authentication information used for authentication. The SDK may first send, to the authorization authentication application based on the data write request, an authentication request that carries the identification information of the user M and the authorization authentication information. The authorization authentication application may perform identity authentication on the user M based on the authentication request.

[0034] Next, in step 203a, in a case in which the identity authentication succeeds, the SDK may send an access configuration information obtaining request to the data access application. The access configuration information obtaining request may include the asset identifier of the user M. The data access application obtains, in response to the access configuration information obtaining request, access configuration information associated with the asset identifier of the user M from pre-recorded data, and returns the access configuration information to the SDK. The access

configuration information may include but is not limited to a storage address A1 of the digital asset corresponding to the user M in the external storage device, a privacy-related field in the data, and an encryption key Y1 held by the TEE system.

[0035] Finally, in step 204a, the SDK may encrypt, by using the key Y1, the privacy-related field in the data that needs to be written, and write, according to the storage address A1, a non-privacy-related field and the encrypted data into the external storage device. Then, the write success result is returned to the service application.

[0036] In another case, for example, when the service application that provides a risk control consulting service needs to query historical data related to the user M, data needs to be read from the external storage device. Specifically, in step 202b, the service application may send a data read request, and the SDK may intercept the data read request by using, for example, AspectJ. The data read request may include but is not limited to a query condition of data that needs to be read, the asset identifier of the user M, the identification information of the user M, the authorization authentication information used for authentication, and the like. The SDK may first send, to the authorization authentication application based on the data read request, an authentication request that carries the identification information of the user M and the authorization authentication information. The authorization authentication application may perform identity authentication on the user M based on the authentication request.

[0037] Next, in step 203b, in a case in which the identity authentication succeeds, the SDK may send an access configuration information obtaining request to the data access application. The access configuration information obtaining request may include the asset identifier of the user M. The data access application may obtain, after receiving the access configuration information obtaining request, access configuration information associated with the asset identifier of the user M from pre-recorded data, and return the access configuration information to the SDK. The access configuration information may include but is not limited to a storage address A1 of the digital asset corresponding to the user M in the external storage device, a privacy-related field in the data, and a decryption key. It should be noted that if the to-be-read data is data directly uploaded by the user M to the external storage device, the decryption key may be a public key held by the user M. If the to-be-read data is data generated and uploaded by the TEE system, the decryption key may be a decryption key Y2 held by the TEE system. The encryption key Y1 is corresponding to the decryption key Y2.

[0038] Finally, in step 204b, the SDK may read the data from the external storage device according to the storage address A1, decrypt the privacy-related field in the read data by using the key Y2, and return a non-privacy-related field and the decrypted data to the service application.

[0039] According to the privacy data access method provided in the embodiments of this specification, a plurality of TEE applications deployed in the TEE system are jointly integrated with an SDK, which is used as a privacy calculation plane of the TEE system. The integrated SDK accesses privacy data with relatively high reusability, so that plaintext privacy data leaving the TEE system is encrypted without incurring application layer system code, and ciphertext privacy data entering the TEE system is decrypted, which makes the solution easier to popularize.

[0040] As shown in FIG. 3, FIG. 3 is an interactive flowchart of another risk control privacy data analysis method according to an example embodiment. The method may be applied to a TEE system. TEE applications such as a management application and a risk control analysis application are deployed in the TEE system. These TEE applications are jointly integrated with an SDK, and an external storage device is disposed outside the TEE system. The risk control analysis application is configured to provide a risk control analysis service.

[0041] Specifically, in step 301, the risk control analysis application receives indication information that is sent by a client and that is used to indicate privacy data analysis. For example, the indication information may include but is not limited to identification information of a user K, a query condition of to-be-analyzed data, and an analysis type. The analysis type may represent a data analysis manner or the like.

[0042] In step 302, the risk control analysis application sends a query request, where the query request may carry an asset identifier of the user K. The SDK intercepts the query request by using AspectJ, and sends a query information obtaining request to the management application based on the asset identifier of the user K. The management application may obtain the query information based on the asset identifier of the user K, and return the query information to the SDK. The query information may include but is not limited to a storage address A2 of the digital asset of the user K in the external storage device, a decryption key, a privacy-related field in the to-be-analyzed data, and the like.

[0043] In step 303, the SDK may obtain the to-be-analyzed data from the external storage device based on the storage address A2 of the digital asset of the user K in the external storage device and the query condition of the to-be-analyzed data. Then, a privacy-related field in the to-

be-analyzed data is decrypted by using the decryption key, and a non-privacy-related field and a decrypted result are returned to the risk control analysis application. The risk control analysis application can analyze the data according to the analysis type to obtain the analysis result.

[0044] In the risk control privacy data analysis method provided in the foregoing embodiment of this specification, after the risk control analysis application receives the indication information for privacy data analysis, the SDK integrated in the TEE system may obtain the storage address of the to-be-analyzed data in the external storage device of the TEE system from the management application, obtain the to-be-analyzed data from the external storage device of the TEE system based on the storage address, process the to-be-analyzed data, and return the to-be-analyzed data to the risk control analysis application, so that the risk control analysis application can analyze the processed to-be-analyzed data. There is no need to modify application layer code of the TEE system, so that the solution can be easily popularized.

[0045] It should be noted that although the operations of the methods of the embodiments of this specification are described in a particular order in the foregoing embodiments, it is not required or implied that these operations should be performed in the particular order or that all the operations shown should be performed to achieve the desired results. In contrast, the order for executing the steps depicted in the flowchart may be changed. Additionally or alternatively, some steps may be omitted, a plurality of steps may be combined into one step for execution, and/or one step may be broken down into a plurality of steps for execution.

[0046] Corresponding to the foregoing embodiment of the privacy data access method, this specification further provides an embodiment of a privacy data access apparatus.

[0047] As shown in FIG. 4, FIG. 4 is a block diagram of a privacy data access apparatus according to an example embodiment, and the apparatus is applied to a TEE system. A plurality of TEE applications are deployed in the TEE system. The plurality of TEE applications are jointly integrated with an SDK. The plurality of TEE applications include a first application that provides a management service and a second application that provides a business service. The apparatus is deployed in the SDK, and the apparatus may include: a first obtaining module 401, a second obtaining module 402, and an access module 403.

[0048] The first obtaining module 401 is configured to obtain a data access request from the second application, where the request includes an asset identifier corresponding to a target user.

[0049] The second obtaining module 402 is configured to obtain, based on the asset identifier,

access configuration information corresponding to the target user from the first application, where the access configuration information includes a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system.

[0050] The access module 403 is configured to perform privacy-related data access to the external storage device of the TEE system based on the access configuration information, where the data access includes data reading or data writing.

[0051] As shown in FIG. 5, FIG. 5 is a block diagram of a risk control privacy data analysis apparatus shown in an example embodiment of this specification. The apparatus is applied to a TEE system. A plurality of TEE applications are deployed in the TEE system. The plurality of TEE applications are jointly integrated with an SDK. The plurality of TEE applications include a management application and a risk control analysis application. The apparatus may include a receiving module 501, a sending module 502, an obtaining module 503, and an analysis module 504.

[0052] The receiving module 501 is configured to indicate the risk control analysis application to receive indication information used to indicate privacy data analysis, where the indication information includes identification information corresponding to a target user and an analysis type.

[0053] The sending module 502 is configured to indicate the risk control analysis application to send a query request based on the indication information, where the query request includes the identification information.

[0054] The obtaining module 503 is configured to indicate the SDK to receive the query request, and obtain, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system.

[0055] The analysis module 504 is configured to indicate the SDK to obtain to-be-analyzed data from the external storage device of the TEE system, and enable, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

[0056] For ease of description, the foregoing apparatus is described separately based on modules according to functions. Certainly, during implementation of this specification, functions of modules may be implemented in one or more software and/or hardware devices.

[0057] The specification also provides a computer-readable non-transitory storage medium, where the storage medium stores a computer program, which, when executed by a processor, can

be used to perform one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Herein, the computer-readable non-transitory storage medium or media may include one or more semiconductor-based or other integrated circuits (ICs) (such, as for example, field-programmable gate arrays (FPGAs) or application-specific ICs (ASICs)), hard disk drives (HDDs), hybrid hard drives (HHDs), optical discs, optical disc drives (ODDs), magneto-optical discs, magneto-optical drives, floppy diskettes, floppy disk drives (FDDs), magnetic tapes, solid-state drives (SSDs), RAM-drives, SECURE DIGITAL cards or drives, any other suitable computer-readable non-transitory storage media, or any suitable combination of two or more of these, where appropriate. A computer-readable non-transitory storage medium may be volatile, non-volatile, or a combination of volatile and non-volatile, where appropriate.

[0058] The specification also provides a computer system. FIG. 6 illustrates an example computer system 1000. In particular embodiments, one or more computer systems 1000 perform one or more steps of one or more methods described or illustrated herein. In particular embodiments, one or more computer systems 1000 provide functionality described or illustrated herein. In particular embodiments, software running on one or more computer systems 1000 performs one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Particular embodiments include one or more portions of one or more computer systems 1000. Herein, reference to a computer system may encompass a computing device, and vice versa, where appropriate. Moreover, reference to a computer system may encompass one or more computer systems, where appropriate.

[0059] This disclosure contemplates any suitable number of computer systems 1000. This disclosure contemplates computer system 1000 taking any suitable physical form. As example and not by way of limitation, computer system 1000 may be an embedded computer system, a system-on-chip (SOC), a single-board computer system (SBC) (such as, for example, a computer-on-module (COM) or system-on-module (SOM)), a desktop computer system, a laptop or notebook computer system, an interactive kiosk, a mainframe, a mesh of computer systems, a mobile telephone, a personal digital assistant (PDA), a server, a tablet computer system, or a combination of two or more of these. Where appropriate, computer system 1000 may include one or more computer systems 1000; be unitary or distributed; span multiple locations; span multiple machines; span multiple data centers; or reside in a cloud, which may include one or more cloud components

in one or more networks. Where appropriate, one or more computer systems 1000 may perform without substantial spatial or temporal limitation one or more steps of one or more methods described or illustrated herein. As an example and not by way of limitation, one or more computer systems 1000 may perform in real time or in batch mode one or more steps of one or more methods described or illustrated herein. One or more computer systems 1000 may perform at different times or at different locations one or more steps of one or more methods described or illustrated herein, where appropriate.

[0060] In particular embodiments, computer system 1000 includes a processor 1002, memory 1004, storage 1006, an input/output (I/O) interface 1008, a communication interface 1010, and a bus 1012. Although this disclosure describes and illustrates a particular computer system having a particular number of particular components in a particular arrangement, this disclosure contemplates any suitable computer system having any suitable number of any suitable components in any suitable arrangement.

[0061] In particular embodiments, processor 1002 includes hardware for executing instructions, such as those making up a computer program. As an example and not by way of limitation, to execute instructions, processor 1002 may retrieve (or fetch) the instructions from an internal register, an internal cache, memory 1004, or storage 1006; decode and execute them; and then write one or more results to an internal register, an internal cache, memory 1004, or storage 1006. In particular embodiments, processor 1002 may include one or more internal caches for data, instructions, or addresses. This disclosure contemplates processor 1002 including any suitable number of any suitable internal caches, where appropriate. As an example and not by way of limitation, processor 1002 may include one or more instruction caches, one or more data caches, and one or more translation lookaside buffers (TLB s). Instructions in the instruction caches may be copies of instructions in memory 1004 or storage 1006, and the instruction caches may speed up retrieval of those instructions by processor 1002. Data in the data caches may be copies of data of 80 in memory 1004 or storage 1006 for instructions executing at processor 1002 to operate on; the results of previous instructions executed at processor 1002 for access by subsequent instructions executing at processor 1002 or for writing to memory 1004 or storage 1006; or other suitable data. The data caches may speed up read or write operations by processor 1002. The TLBs may speed up virtual-address translation for processor 1002. In particular embodiments, processor 1002 may include one or more internal registers for data, instructions, or addresses. This disclosure

contemplates processor 1002 including any suitable number of any suitable internal registers, where appropriate. Where appropriate, processor 1002 may include one or more arithmetic logic units (ALUs); be a multi-core processor; or include one or more processors 1002. Although this disclosure describes and illustrates a particular processor, this disclosure contemplates any suitable processor.

[0062] In particular embodiments, memory 1004 includes main memory for storing instructions for processor 1002 to execute or data for processor 1002 to operate on. As an example and not by way of limitation, computer system 1000 may load instructions from storage 1006 or another source (such as, for example, another computer system 1000) to memory 1004. Processor 1002 may then load the instructions from memory 1004 to an internal register or internal cache. To execute the instructions, processor 1002 may retrieve the instructions from the internal register or internal cache and decode them. During or after execution of the instructions, processor 1002 may write one or more results (which may be intermediate or final results) to the internal register or internal cache. Processor 1002 may then write one or more of those results to memory 1004. In particular embodiments, processor 1002 executes only instructions in one or more internal registers or internal caches or in memory 1004 (as opposed to storage 1006 or elsewhere) and operates only on data in one or more internal registers or internal caches or in memory 1004 (as opposed to storage 1006 or elsewhere). One or more memory buses (which may each include an address bus and a data bus) may couple processor 1002 to memory 1004. Bus 1012 may include one or more memory buses, as described below. In particular embodiments, one or more memory management units (MMUs) reside between processor 1002 and memory 1004 and facilitate accesses to memory 1004 requested by processor 1002. In particular embodiments, memory 1004 includes random access memory (RAM). This RAM may be volatile memory, where appropriate. Where appropriate, this RAM may be dynamic RAM (DRAM) or static RAM (SRAM). Moreover, where appropriate, this RAM may be single-ported or multi-ported RAM. This disclosure contemplates any suitable RAM. Memory 1004 may include one or more memories 1004, where appropriate. Although this disclosure describes and illustrates particular memory, this disclosure contemplates any suitable memory.

[0063] In particular embodiments, storage 1006 includes mass storage for data or instructions. As an example and not by way of limitation, storage 1006 may include a hard disk drive (HDD), a floppy disk drive, flash memory, an optical disc, a magneto-optical disc, magnetic tape, or a

Universal Serial Bus (USB) drive or a combination of two or more of these. Storage 1006 may include removable or non-removable (or fixed) media, where appropriate. Storage 1006 may be internal or external to computer system 1000, where appropriate. In particular embodiments, storage 1006 is non-volatile, solid-state memory. In particular embodiments, storage 1006 includes read-only memory (ROM). Where appropriate, this ROM may be mask-programmed ROM, programmable ROM (PROM), erasable PROM (EPROM), electrically erasable PROM (EEPROM), electrically alterable ROM (EAROM), or flash memory or a combination of two or more of these. This disclosure contemplates mass storage 1006 taking any suitable physical form. Storage 1006 may include one or more storage control units facilitating communication between processor 1002 and storage 1006, where appropriate. Where appropriate, storage 1006 may include one or more storages 1006. Although this disclosure describes and illustrates particular storage, this disclosure contemplates any suitable storage.

[0064] In particular embodiments, I/O interface 1008 includes hardware, software, or both, providing one or more interfaces for communication between computer system 1000 and one or more I/O devices. Computer system 1000 may include one or more of these I/O devices, where appropriate. One or more of these I/O devices may enable communication between a person and computer system 1000. As an example and not by way of limitation, an I/O device may include a keyboard, keypad, microphone, monitor, mouse, printer, scanner, speaker, still camera, stylus, tablet, touch screen, trackball, video camera, another suitable I/O device or a combination of two or more of these. An I/O device may include one or more sensors. This disclosure contemplates any suitable I/O devices and any suitable I/O interfaces 1008 for them. Where appropriate, I/O interface 1008 may include one or more device or software drivers enabling processor 1002 to drive one or more of these I/O devices. I/O interface 1008 may include one or more I/O interfaces 1008, where appropriate. Although this disclosure describes and illustrates a particular I/O interface, this disclosure contemplates any suitable I/O interface.

[0065] In particular embodiments, communication interface 1010 includes hardware, software, or both providing one or more interfaces for communication (such as, for example, packet-based communication) between computer system 1000 and one or more other computer systems 1000 or one or more networks. As an example and not by way of limitation, communication interface 1010 may include a network interface controller (NIC) or network adapter for communicating with an Ethernet or other wire-based network or a wireless NIC (WNIC) or wireless adapter for

communicating with a wireless network, such as a WI-FI network. This disclosure contemplates any suitable network and any suitable communication interface 1010 for it. As an example and not by way of limitation, computer system 1000 may communicate with an ad hoc network, a personal area network (PAN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), or one or more portions of the Internet or a combination of two or more of these. One or more portions of one or more of these networks may be wired or wireless. As an example, computer system 1000 may communicate with a wireless PAN (WPAN) (such as, for example, a BLUETOOTH WPAN), a WI-FI network, a WI-MAX network, a cellular telephone network (such as, for example, a Global System for Mobile Communications (GSM) network), or other suitable wireless network or a combination of two or more of these. Computer system 1000 may include any suitable communication interface 1010 for any of these networks, where appropriate. Communication interface 1010 may include one or more communication interfaces 1010, where appropriate. Although this disclosure describes and illustrates a particular communication interface, this disclosure contemplates any suitable communication interface.

[0066] In particular embodiments, bus 1012 includes hardware, software, or both coupling components of computer system 1000 to each other. As an example and not by way of limitation, bus 1012 may include an Accelerated Graphics Port (AGP) or other graphics bus, an Enhanced Industry Standard Architecture (EISA) bus, a front-side bus (FSB), a HYPERTRANSPORT (HT) interconnect, an Industry Standard Architecture (ISA) bus, an INFINIBAND interconnect, a low-pin-count (LPC) bus, a memory bus, a Micro Channel Architecture (MCA) bus, a Peripheral Component Interconnect (PCI) bus, a PCI-Express (PCIe) bus, a serial advanced technology attachment (SATA) bus, a Video Electronics Standards Association local (VLB) bus, or another suitable bus or a combination of two or more of these. Bus 1012 may include one or more buses 1012, where appropriate. Although this disclosure describes and illustrates a particular bus, this disclosure contemplates any suitable bus or interconnect.

[0067] It should be further noted that the term "include", "comprise" or any other variant thereof is intended to cover non-exclusive inclusion, so that a process, method, commodity, or device that includes a series of elements includes not only those elements but also other elements that are not explicitly listed, or includes elements inherent in such a process, method, commodity, or device. In the absence of more restrictions, an element defined by the statement "includes a..." does not rule out a case that a process, method, commodity, or device including the element has

another same element.

[0068] The embodiments in the present specification are described in a progressive way. For same or similar parts of the embodiments, references can be made to the embodiments mutually. Each embodiment focuses on a difference from other embodiments. Particularly, the system embodiments are briefly described since they are basically similar to the method embodiments. For related parts, references can be made to related descriptions in the method embodiments.

[0069] The foregoing descriptions are merely embodiments of this specification, and are not intended to limit this specification. A person skilled in the art may make various modifications or changes in this specification. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of this specification shall fall within the protection scope of the claims of this specification.

CLAIMS

1. A privacy data access method, applied to a TEE system, wherein a plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a first application that provides a management service and a second application that provides a business service; and the method is executed by the SDK, and the method comprises:

obtaining a data access request from the second application, wherein the request comprises an asset identifier corresponding to a target user;

obtaining, based on the asset identifier, access configuration information corresponding to the target user from the first application, wherein the access configuration information comprises a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

performing privacy-related data access to the external storage device of the TEE system based on the access configuration information, wherein the data access comprises data reading or data writing.

2. The method according to claim 1, wherein the request further comprises identification information corresponding to the target user and authorization authentication information; and before the obtaining access configuration information from the first application, the method further comprises:

sending, to the first application, an authentication request that carries the identification information corresponding to the target user and the authorization authentication information, to perform identity authentication by using the first application; and

when the identity authentication succeeds, performing the operation of obtaining the access configuration information from the first application.

3. The method according to claim 1, wherein the data access comprises data writing; the request further comprises first data to be written; the first data is plaintext data generated inside the TEE system; and the access configuration information further comprises a privacy-related field in data and an encryption key held by the TEE system; and

the performing privacy-related data access to the external storage device of the TEE system based on the access configuration information comprises:

encrypting, by using the encryption key, a privacy-related field in the first data to obtain second data; and

writing, according to the storage address of the digital asset corresponding to the target user, the second data into the digital asset corresponding to the target user in the external storage device of the TEE system.

4. The method according to claim 1, wherein the data access comprises data reading; the access configuration information further comprises a privacy-related field in data and a decryption key; and the performing privacy-related data access to the external storage device of the TEE system based on the access configuration information comprises:

obtaining to-be-read third data from the external storage device of the TEE system according to the storage address of the digital asset corresponding to the target user;

decrypting, by using the decryption key, a privacy-related field in the third data to obtain fourth data for internal use in the TEE system; and

returning the fourth data to the second application.

5. The method according to claim 4, wherein if the third data is data that is generated by a target user outside the TEE system and encrypted with a private key of the target user, the decryption key comprises a public key of the target user; or if the to-be-read third data is data that is generated inside the TEE system and encrypted, the decryption key comprises a decryption key held by the TEE system.

6. The method according to claim 1, wherein the obtaining a data access request from the second application comprises: intercepting, by using AspectJ, the data access request sent by the second application.

7. The method according to claim 1, wherein the privacy data comprises risk control data, and the second application comprises a risk control service application; and the data reading comprises history data query, and the data writing comprises exception event data update.

8. A risk control privacy data analysis method, applied to a TEE system, wherein a plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a management application and a risk control analysis application; and the method comprises:

receiving, by the risk control analysis application, indication information used to indicate privacy data analysis, wherein the indication information comprises identification information

corresponding to a target user and an analysis type;

sending, by the risk control analysis application, a query request based on the indication information, wherein the query request comprises the identification information;

receiving, by the SDK, the query request, and obtaining, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

obtaining, by the SDK, to-be-analyzed data from the external storage device of the TEE system, and enabling, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

9. The method according to claim 8, wherein the enabling, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type comprises:

decrypting at least a part of fields of the to-be-analyzed data to obtain target data;

returning the target data to the risk control analysis application; and

performing, by the risk control analysis application, an analysis operation on the target data according to the analysis type, to obtain an analysis result.

10. A TEE-based computer system, where a plurality of TEE applications are deployed in the system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a first application that provides a management service and a second application that provides a business service; the system comprises a memory, a processor, and a computer program stored in the memory and running on the processor, and the SDK implements the following steps when executing the program by using the processor:

obtaining a data access request from the second application, wherein the request comprises an asset identifier corresponding to a target user;

obtaining, based on the asset identifier, access configuration information corresponding to the target user from the first application, wherein the access configuration information comprises a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

performing privacy-related data access to the external storage device of the TEE system based on the access configuration information, wherein the data access comprises data reading or data writing.

11. The system according to claim 10, wherein the request further comprises identification information corresponding to the target user and authorization authentication information; and before the obtaining access configuration information from the first application, the following steps are further executed:

sending, to the first application, an authentication request that carries the identification information corresponding to the target user and the authorization authentication information, to perform identity authentication by using the first application; and

when the identity authentication succeeds, performing the operation of obtaining the access configuration information from the first application.

12. The system according to claim 10, wherein the data access comprises data writing; the request further comprises first data to be written; the first data is plaintext data generated inside the TEE system; and the access configuration information further comprises a privacy-related field in data and an encryption key held by the TEE system; and

the performing privacy-related data access to the external storage device of the TEE system based on the access configuration information comprises:

encrypting, by using the encryption key, a privacy-related field in the first data to obtain second data; and

writing, according to the storage address of the digital asset corresponding to the target user, the second data into the digital asset corresponding to the target user in the external storage device of the TEE system.

13. The system according to claim 10, wherein the data access comprises data reading; the access configuration information further comprises a privacy-related field in data and a decryption key; and the performing privacy-related data access to the external storage device of the TEE system based on the access configuration information comprises:

obtaining to-be-read third data from the external storage device of the TEE system according to the storage address of the digital asset corresponding to the target user;

decrypting, by using the decryption key, a privacy-related field in the third data to obtain fourth data for internal use in the TEE system; and

returning the fourth data to the second application.

14. The system according to claim 13, wherein if the third data is data that is generated by a target user outside the TEE system and encrypted with a private key of the target user, the

decryption key comprises a public key of the target user; or if the to-be-read third data is data that is generated inside the TEE system and encrypted, the decryption key comprises a decryption key held by the TEE system.

15. The system according to claim 10, wherein the obtaining a data access request from the second application comprises: intercepting, by using AspectJ, the data access request sent by the second application.

16. The method according to claim 10, wherein the privacy data comprises risk control data, and the second application comprises a risk control service application; and the data reading comprises history data query, and the data writing comprises exception event data update.

17. A TEE-based computer system, wherein a plurality of TEE applications are deployed in the system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a management application and a risk control analysis application; and the system comprises a memory, a processor, and a computer program stored in the memory and running on the processor, wherein when executing the program by using the processor, the risk control analysis application implements the following steps: receiving indication information used to indicate privacy data analysis, wherein the indication information comprises identification information corresponding to a target user and an analysis type; and sending a query request based on the indication information, wherein the query request comprises the identification information;

wherein when executing the program by using the processor, the SDK implements the following steps: receiving the query request, and obtaining, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and obtaining to-be-analyzed data from the external storage device of the TEE system, and enabling, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

18. A privacy data access apparatus, applied to a TEE system, wherein a plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a first application that provides a management service and a second application that provides a business service; and the apparatus is deployed in the SDK, and the apparatus comprises:

a first obtaining module, configured to obtain a data access request from the second application, wherein the request comprises an asset identifier corresponding to a target user;

a second obtaining module, configured to obtain, based on the asset identifier, access configuration information corresponding to the target user from the first application, wherein the access configuration information comprises a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

an access module, configured to perform privacy-related data access to the external storage device of the TEE system based on the access configuration information, wherein the data access comprises data reading or data writing.

19. A risk control privacy data analysis apparatus, applied to a TEE system, wherein a plurality of TEE applications are deployed in the TEE system, and the plurality of TEE applications are jointly integrated with an SDK; the plurality of TEE applications comprise a management application and a risk control analysis application; and the apparatus comprises:

a receiving module, configured to indicate the risk control analysis application to receive indication information used to indicate privacy data analysis, wherein the indication information comprises identification information corresponding to a target user and an analysis type;

a sending module, configured to indicate the risk control analysis application to send a query request based on the indication information, wherein the query request comprises the identification information;

an obtaining module, configured to indicate the SDK to receive the query request, and obtain, from the management application based on the identification information, a storage address of a digital asset corresponding to the target user in an external storage device of the TEE system; and

an analysis module, configured to indicate the SDK to obtain to-be-analyzed data from the external storage device of the TEE system, and enable, based on the to-be-analyzed data, the risk control analysis application to obtain an analysis result based on the analysis type.

20. A computer-readable nonvolatile storage medium, wherein the storage medium stores a computer program, and when the computer program is performed by a processor, the method according to any one of claims 1 to 9 is implemented.