METHOD AND APPARATUS FOR VERIFYING RISK IDENTIFICATION VULNERABILITY IN TRANSACTION SYSTEM, AND COMPUTER SYSTEM

说明书

检验交易系统的风险识别漏洞的方法、装置及计算机系统

技术领域

本说明书涉及计算机技术领域，尤其涉及一种检验交易系统的风险识别漏洞的方法、装置及计算机系统。

背景技术

金融行业中的交易系统，每天产生的交易数量巨大，涉及大量的资金流转，面临着复杂而多样的资金风险，需要大量人力和资源以保证资金安全。目前，主要依赖于依据专家经验在交易系统内部构建大量交易核对规则，用于进行风险识别。但是，交易系统的风险识别的有效性，也需要被检验。高效、及时的发现交易系统的风险识别中存在的漏洞，可以降低因漏洞导致交易风险未被发现而造成的交易事故的发生概率。

发明内容

本说明书实施例提供一种检验风险识别漏洞的测试数据的生成方法、装置、存储介质及计算机系统，以部分解决上述现有技术存在的问题。

本说明书提供了一种检验交易系统的风险识别漏洞的方法，包括：获取目标交易系统中实时交易对应的原始交易信息，根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取所述目标字段的一到多个历史字段值；根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语；所述提示语中指示所述变异字段值的语义符合目标字段的值的语义，且所述变异字段值不同于所述历史字段值、以及所述原始交易信息中

目标字段的原始字段值；将所述提示语输入目标大模型，得到所述变异字段值，根据所述变异字段值，检验目标交易系统是否存在风险识别漏洞。

本说明书提供了一种计算机系统，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如下步骤：获取目标交易系统中实时交易对应的原始交易信息，根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取所述目标字段的一到多个历史字段值；根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语；所述提示语中指示所述变异字段值的语义符合目标字段的值的语义，且所述变异字段值不同于所述历史字段值、以及所述原始交易信息中目标字段的原始字段值；将所述提示语输入目标大模型，得到所述变异字段值，根据所述变异字段值，检验目标交易系统是否存在风险识别漏洞。

本说明书提供了一种检验交易系统的风险识别漏洞的装置，所述装置包括：获取模块，用于获取目标交易系统中实时交易对应的原始交易信息，根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取所述目标字段的一到多个历史字段值；生成模块，用于根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语；所述提示语中指示所述变异字段值的语义符合目标字段的值的语义，且所述变异字段值不同于所述历史字段值、以及所述原始交易信息中目标字段的原始字段值；检验模块，用于将所述提示语输入目标大模型，得到所述变异字段值，根据所述变异字段值，检验目标交易系统是否存在风险识别漏洞。

本说明书提供了一种计算机可读非易失性存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述的检验风险识别漏洞的测试数据的生成方法。

本说明书实施例采用的上述至少一个技术方案能够达到以下有益效果中的至少一项：能够基于大模型和实时交易数据获取变异交易数据，并通过变异

交易数据检验交易系统的风险识别漏洞，使得可以高效、及时的发现交易系统风险识别中的漏洞，降低因漏洞导致的交易事故或资金损失的发生概率。

附图说明

此处所说明的附图用来提供对本说明书的进一步理解，构成本说明书的一部分，本说明书的示意性实施例及其说明用于解释本说明书，并不构成对本说明书的不当限定。在附图中：

图1为本说明书中一种检验交易系统的风险识别漏洞的方法的流程示意图；

图2为本说明书中一种检验交易系统的风险识别漏洞的方法的示意图；

图3为本说明书中交易知识库的示意图；

图4为本说明书中输入目标大模型的提示语的示意图；

图5为本说明书中获取变异交易信息的示意图；

图6为本说明书中通过变异交易信息检验风险识别漏洞的示意图；

图7为本说明书中一种检验交易系统的风险识别漏洞的装置的结构示意图；

图8为本说明书实施例提供的计算机系统的结构示意图。

具体实施方式

为使本说明书的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本说明书保护的范围。

如前所述，金融行业中的交易系统，每天产生的交易数量巨大，涉及大量的资金流转，面临着复杂而多样的资金风险，需要大量人力和资源以保证资金安全。目前，主要依赖于依据专家经验在交易系统内部构建大量交易核对规则，用于进行风险识别。但是，交易系统中交易核对规则的有效性，或者说，交易

系统的风险识别的有效性，通常也需要检验。高效、及时的发现交易系统风险识别中存在的漏洞，可以降低因漏洞导致的交易事故或资金损失的发生概率。目前，交易系统的风险识别的有效性，主要也依赖于向交易系统输入，通过人工构建的、用于检验交易系统的风险识别的测试数据而进行。但是，人工构建测试数据通常建立在人工分析交易核对规则的基础上。由于交易系统内部的交易核对规则通常数量巨大，单纯依赖人力使得难以得到足够数据且质量优良的测试数据，也使得快速的发现交易系统风险识别中的漏洞的难度很大。

为了解决上述问题，在本申请中，可以获取交易系统中实时交易的原始交易信息，解析出其中的目标字段，根据目标字段的字段信息，获取目标字段的多个历史字段值。然后，根据原始交易信息和历史字段值，构建生成目标字段的变异字段值的提示语。提示语中指示变异字段值的语义符合目标字段的值的语义、且不同于历史字段值和所述原始字段值。接着，将提示语输入目标大模型，得到目标字段的变异字段值。此后，可以根据原始交易信息和变异字段值，得到变异交易信息，通过变异交易信息，测试目标交易系统是否可以识别交易风险。

本申请中提供的检验交易系统的风险识别漏洞的方法，通过大模型和实时交易数据获取大量的变异交易数据，变异交易数据中包含的实时交易数据的目标字段的变异值。该变异值不同于实时交易数据中目标字段的实时值和历史值，但是其语义符合实时值和历史值的语义，使得该变异交易数据具有更强的迷惑交易系统的作用。通过将该变异交易数据输入交易系统，可以更好的检验出交易系统潜在的风险识别漏洞。因此，通过该方法能够可以高效、及时的发现交易系统风险识别中的漏洞，降低因漏洞导致的交易事故或资金损失的发生概率。此外，通过该方法还可以在无需人力分析交易系统中具体的风险识别规则的情况下，自动获取大量变异交易数据，并用于检验交易系统的风险识别漏洞，进一步降低了检验交易系统中风险识别漏洞的复杂度和消耗的人力工作量。

以下结合附图，详细说明本说明书各实施例提供的技术方案。

图 1 为本说明书中一种检验交易系统的风险识别漏洞的方法的流程示意图，具体可包括以下步骤：

S100：获取目标交易系统中实时交易对应的原始交易信息，原始交易信息包括目标字段的字段信息。原始交易信息，是目标交易系统中实时交易的交易信息。在不同的实施例中，目标交易系统可以是用于不同具体业务、或用于进行不同具体交易的交易系统，本说明书对此不做限制。在不同的实施例中，原始交易信息所具有的数据格式可以不同。在一个实施例中，例如可以是 Json（JavaScript Object Notation）格式。从而，可以通过解析特定数据格式的原始交易信息，得到原始交易信息中包括的目标字段的字段信息。在不同的实施例中，目标字段可以是不同的具体字段。例如，在一个实施例中，目标字段例如可以为交易金额字段、交易账户字段、交易币种字段、交易状态字段中的一种。在不同的实施例中，目标字段的字段信息也可以不同。例如，在一个实施例中，可以包括字段名称、字段类型、字段所属的表名称、字段对应的应用名称中的一种或多种。

在获取目标字段的字段信息后，可以根据目标字段的字段信息，从预先设立的交易知识库中获取目标字段的一到多个历史字段值。在不同的实施例中，预先设立的交易知识库的构建方式可以不同。进而，从预先设立的交易知识库中获取目标字段的历史字段值的具体方式也可以不同。在一个实施例中，交易知识库中可以预先保存有多个键值对，所述键值对中的键用于保存预先获取的所述目标交易系统的历史交易中的数据字段的字段信息的向量化特征，所述键值对中的值用于保存所述历史交易的交易信息。

图 3 为本说明书中交易知识库的示意图。如图 3 所示的例子中，交易知识库中可以预先保存有多个键值对，每个键值对中的健用于保存数据字段的字段信息（例如字段名称）的向量化特征，该键对应的值则用于保存历史交易的交易信息。进而，可以对所述目标字段的字段信息进行向量化处理，得到第一向量化特征，根据所述第一向量化特征，从交易知识库中获取与所述目标字段相

关的一到多条历史交易，从所述一到多条历史交易中提取目标字段的一到多个历史字段值。图 3 所示的例子中，例如可以对目标字段的字段名称，进行向量化处理，得到对应的向量化特征 v1，然后在交易知识库中查找到与向量化特征 v1 差异度例如低于预定阈值的键，例如字段信息特征 1 和字段信息特征 2。进而，可以从字段信息特征 1 和字段信息特征 2 分别对应的值（例如历史交易 1 的交易信息和历史交易 2 的交易信息）中，提取目标字段在历史交易 1 和历史交易 2 中的历史字段值。

S102：根据原始交易信息和历史字段值，构建生成目标字段的变异字段值的提示语。提示语中指示所述变异字段值的语义符合目标字段的值的语义，且所述变异字段值不同于所述历史字段值、以及原始交易信息中目标字段的原始字段值。

提示语是针对大模型的提示语句，用于指导大模型生成目标字段的变异字段值。在不同的实施例中，构建提示语的具体方式可以不同。在一个实施例中，可以将原始交易信息中目标字段的原始字段值，替换为所述历史字段值和所述原始字段值的合集，得到扩充交易信息；根据所述扩充交易信息，构建所述提示语。

图 4 为本说明书中输入目标大模型的提示语的示意图。如图 4 所示的例子中，例如原始交易信息为{"app_name": "app2", "table_name": "amount1", "field_name": "amount_type", "val_info": "[A_FEE]"。其中包括目标字段的字段名称（"field_name"）、字段所属的表名称（"table_name"）、字段对应的应用名称（"app_name"），以及目标字段的原始字段值（"val_info"）。该原始字段值例如为“A_FEE”。在步骤 S100 中例如通过字段名称获取了目标字段的多个历史值，例如为“B_FEE, C_FEE, D_PAY,E_FEE, F_COUPON”。则可以将原始交易信息中的原始字段值替换为历史字段值和所述原始字段值的合集，即将“A_FEE”替换为“A_FEE,B_FEE, C_FEE, D_PAY,E_FEE, F_COUPON”,得到扩充交易信息。进而，可以根据扩充交易信息构建提示语。在一个例子中，例如

图 4 所示，提示语中扩充交易信息的数据格式可以与原始交易信息的数据格式相同。

在另一个实施例中，还可以根据预先获取的试例交易信息、以及期望所述目标大模型针对所述试例交易信息的输出信息，构建试例提示信息；根据所述原始交易信息、所述历史字段值和所述试例提示信息，构建所述提示语。如图 4 所示的例子中，试例提示信息例如包括试例交易信息、以及期望目标大模型针对试例交易信息的输出信息，试例交易信息例如为<input> {"app_name": "app1", "table_name": "table1", "field_name": "index1", "val_info": "[0,1,2,3,4]"}，期望目标大模型针对试例交易信息的输出信息例如为<output> {"injValue": "5"}。通过在提示语中添加试例提示信息，可以更好的指导目标大模型根据扩充交易信息，生成目标字段的变异值。

S104：将提示语输入目标大模型，得到变异字段值，根据变异字段值，检验目标交易系统是否存在风险识别漏洞。大模型，是一种基于深度学习技术的大型神经网络模型。大模型通常可以包括数据巨大的神经网络参数，并通过海量的训练数据进行预训练。目标大模型，是可以根据输入的提示语，生成目标字段的变异字段值的大模型。在不同的实施例中，目标大模型可以是不同的具体类型或具有不同的神经网络结构的大模型，本说明书对此不做限制。在一个例子中，在将如图 4 所示的提示语输入目标大模型，目标大模型例如输出目标字段的变异字段值为“G_FEE”，它不同于扩充交易信息中包含的历史字段值和原始字段值、而它的语义符合史字段值和原始字段值的语义。

在通过目标大模型获取变异字段值之后，可以根据变异字段值，检验目标交易系统是否存在风险识别漏洞。在一个实施例中，可以将原始交易信息中目标字段的原始字段值替换为所述变异字段值，得到变异交易信息；将变异交易信息输入目标交易系统，若所述目标交易系统未识别交易风险，则确定目标交易系统存在风险识别漏洞。

图 5 为本说明书中获取变异交易信息的示意图。如图 5 所示，可以将原始

交易信息中目标字段的原始字段值，替换为通过大模型获取的目标字段的变异字段值，得到变异交易信息。图 6 为本说明书中通过变异交易信息检验风险识别漏洞的示意图。如图 6 所示，可以将变异交易信息输入目标交易系统，若目标交易系统在变异交易信息输入之后，未识别出交易风险，在确定目标交易系统存在风险识别漏洞。在一个例子中，还可以在确定目标交易系统存在风险识别漏洞之后，触发风险识别漏洞警报。在另一个例子中，若目标交易系统在变异交易信息输入之后，识别出交易风险，则不触发风险识别漏洞警报。

为了使得此后通过提示语（包含通过交易知识库检索的数据字段的历史交易值），对于目标大模型生成与以往的变异字段值不同的新的变异字段值的启示作用更强，在一个实施例中，在确定目标交易系统存在风险识别漏洞之后，还可以将所述变异交易信息和所述目标字段的字段信息，关联保存到所述交易知识库中。

以上为本说明书实施例提供的检验交易系统的风险识别漏洞的方法，基于同样的思路，本说明书还提供了相应的检验交易系统的风险识别漏洞的装置。如图 7 所示，该检验交易系统的风险识别漏洞的装置包括：获取模块 702，用于获取目标交易系统中实时交易对应的原始交易信息，根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取所述目标字段的一到多个历史字段值；生成模块 704，用于根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语；所述提示语中指示所述变异字段值的语义符合目标字段的值的语义，且所述变异字段值不同于所述历史字段值、以及所述原始交易信息中目标字段的原始字段值；检验模块 706，用于将所述提示语输入目标大模型，得到所述变异字段值，根据所述变异字段值，检验目标交易系统是否存在风险识别漏洞。

为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本说明书时可以把各模块的功能在同一个或多个软件和/或硬件中实现。

The specification also provides a computer-readable non-transitory storage medium, wherein

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.

The specification also provides a computer system. FIG. 8 illustrates an example computer system 800. In particular embodiments, one or more computer systems 800 perform one or more steps of one or more methods described or illustrated herein. In particular embodiments, one or more computer systems 800 provide functionality described or illustrated herein. In particular embodiments, software running on one or more computer systems 800 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 800. 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.

This disclosure contemplates any suitable number of computer systems 800. This disclosure contemplates computer system 800 taking any suitable physical form. As example and not by way of limitation, computer system 800 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 800 may include one or more computer systems 800; 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 800 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 800 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 800 may perform at different times or at different locations one or more steps of one or more methods described or illustrated herein, where appropriate.

In particular embodiments, computer system 800 includes a processor 802, memory 804, storage 806, an input/output (I/O) interface 808, a communication interface 810, and a bus 812. 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.

In particular embodiments, processor 802 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 802 may retrieve (or fetch) the instructions from an internal register, an internal cache, memory 804, or storage 806; decode and execute them; and then write one or more results to an internal register, an internal cache, memory 804, or storage 806. In particular embodiments, processor 802 may include one or more internal caches for data, instructions, or addresses. This disclosure contemplates processor 802 including any suitable number of any suitable internal caches, where appropriate. As an example and not by way of limitation, processor 802 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 804 or storage 806, and the instruction caches may speed up retrieval of those instructions by processor 802. Data in the data caches may be copies of data of 80 in memory 804 or storage 806 for instructions executing at processor 802 to operate on; the results

of previous instructions executed at processor 802 for access by subsequent instructions executing at processor 802 or for writing to memory 804 or storage 806; or other suitable data. The data caches may speed up read or write operations by processor 802. The TLBs may speed up virtual-address translation for processor 802. In particular embodiments, processor 802 may include one or more internal registers for data, instructions, or addresses. This disclosure contemplates processor 802 including any suitable number of any suitable internal registers, where appropriate. Where appropriate, processor 802 may include one or more arithmetic logic units (ALUs); be a multi-core processor; or include one or more processors 802. Although this disclosure describes and illustrates a particular processor, this disclosure contemplates any suitable processor.

In particular embodiments, memory 804 includes main memory for storing instructions for processor 802 to execute or data for processor 802 to operate on. As an example and not by way of limitation, computer system 800 may load instructions from storage 806 or another source (such as, for example, another computer system 800) to memory 804. Processor 802 may then load the instructions from memory 804 to an internal register or internal cache. To execute the instructions, processor 802 may retrieve the instructions from the internal register or internal cache and decode them. During or after execution of the instructions, processor 802 may write one or more results (which may be intermediate or final results) to the internal register or internal cache. Processor 802 may then write one or more of those results to memory 804. In particular embodiments, processor 802 executes only instructions in one or more internal registers or internal caches or in memory 804 (as opposed to storage 806 or elsewhere) and operates only on data in one or more internal registers or internal caches or in memory 804 (as opposed to storage 806 or elsewhere). One or more memory buses (which may each include an address bus and a data bus) may couple processor 802 to memory 804. Bus 812 may include one or more memory buses, as described below. In particular embodiments, one or more memory management units (MMUs) reside between processor 802 and memory 804 and facilitate accesses to memory 804 requested by processor 802. In particular embodiments, memory 804 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 804 may include one or more memories 804, where appropriate. Although this disclosure describes and illustrates particular memory, this disclosure contemplates any suitable memory.

In particular embodiments, storage 806 includes mass storage for data or instructions. As an example and not by way of limitation, storage 806 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 806 may include removable or non-removable (or fixed) media, where appropriate. Storage 806 may be internal or external to computer system 800, where appropriate. In particular embodiments, storage 806 is non-volatile, solid-state memory. In particular embodiments, storage 806 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 806 taking any suitable physical form. Storage 806 may include one or more storage control units facilitating communication between processor 802 and storage 806, where appropriate. Where appropriate, storage 806 may include one or more storages 806. Although this disclosure describes and illustrates particular storage, this disclosure contemplates any suitable storage.

In particular embodiments, I/O interface 808 includes hardware, software, or both, providing one or more interfaces for communication between computer system 800 and one or more I/O devices. Computer system 800 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 800. 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 808 for them. Where appropriate, I/O interface 808 may include one or more device or software drivers enabling processor 802 to drive one or more of these I/O devices. I/O interface 808 may include one or more I/O interfaces 808, where

appropriate. Although this disclosure describes and illustrates a particular I/O interface, this disclosure contemplates any suitable I/O interface.

In particular embodiments, communication interface 810 includes hardware, software, or both providing one or more interfaces for communication (such as, for example, packet-based communication) between computer system 800 and one or more other computer systems 800 or one or more networks. As an example and not by way of limitation, communication interface 810 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 810 for it. As an example and not by way of limitation, computer system 800 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 800 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 800 may include any suitable communication interface 810 for any of these networks, where appropriate. Communication interface 810 may include one or more communication interfaces 810, where appropriate. Although this disclosure describes and illustrates a particular communication interface, this disclosure contemplates any suitable communication interface.

In particular embodiments, bus 812 includes hardware, software, or both coupling components of computer system 800 to each other. As an example and not by way of limitation, bus 812 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 812 may include one or more buses 812, where appropriate. Although this disclosure describes and illustrates a particular bus, this disclosure contemplates any suitable bus or interconnect.

还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

权利要求书

1、一种检验交易系统的风险识别漏洞的方法，包括：

获取目标交易系统中实时交易对应的原始交易信息，根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取所述目标字段的一到多个历史字段值；

根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语；所述提示语中指示所述变异字段值的语义符合目标字段的值的语义，且所述变异字段值不同于所述历史字段值、以及所述原始交易信息中目标字段的原始字段值；

将所述提示语输入目标大模型，得到所述变异字段值，根据所述变异字段值，检验目标交易系统是否存在风险识别漏洞。

2、根据权利要求 1 所述的方法，其中，根据所述变异字段值，检验目标交易系统是否存在风险识别漏洞，包括：

将原始交易信息中目标字段的原始字段值替换为所述变异字段值，得到变异交易信息；

将变异交易信息输入目标交易系统，若所述目标交易系统未识别交易风险，则确定目标交易系统存在风险识别漏洞。

3、根据权利要求 2 所述的方法，还包括：

在确定目标交易系统存在风险识别漏洞之后，触发风险识别漏洞警报；

若所述目标交易系统识别出交易风险，则不触发风险识别漏洞警报。

4、根据权利要求 2 所示的方法，还包括，在确定目标交易系统存在风险识别漏洞之后，将所述变异交易信息和所述目标字段的字段信息，关联保存到所述交易知识库中。

5、根据权利要求 1 所述的方法，其中，所述交易知识库中预先保存有多个键值对，所述键值对中的键用于保存预先获取的所述目标交易系统的历史交易中数据字段的字段信息的向量化特征，所述键值对中的值用于保存所述历史

交易的交易信息；

根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取与所述目标字段相关的一到多个历史字段值，包括：

对所述目标字段的字段信息进行向量化处理，得到第一向量化特征，根据所述第一向量化特征，从交易知识库中获取与所述目标字段相关的一到多条历史交易，从所述一到多条历史交易中提取一到多个历史字段值。

6、根据权利要求 1 所述的方法，其中，根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语，包括：

将原始交易信息中目标字段的原始字段值，替换为所述历史字段值和所述原始字段值的合集，得到扩充交易信息；

根据所述扩充交易信息，构建所述提示语。

7、根据权利要求 1 所述的方法，其中，根据所述原始交易信息和所述历史字段值，构建生成变异字段值的提示语，包括：

根据预先获取的试例交易信息、以及期望所述目标大模型针对所述试例交易信息的输出信息，构建试例提示信息；

根据所述原始交易信息、所述历史字段值和所述试例提示信息，构建所述提示语。

8、根据权利要求 1 所述的方法，其中，字段信息包括字段名称、字段类型、字段所属的表名称、字段对应的应用名称中的一种或多种。

9、根据权利要求 1 所述的方法，其中，所述目标字段为交易金额字段、交易账户字段、交易币种字段、交易状态字段中的一种。

10、一种计算机系统，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如下步骤：

获取目标交易系统中实时交易对应的原始交易信息，根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取所述目标字段的一

到多个历史字段值；

根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语；所述提示语中指示所述变异字段值的语义符合目标字段的值的语义，且所述变异字段值不同于所述历史字段值、以及所述原始交易信息中目标字段的原始字段值；

将所述提示语输入目标大模型，得到所述变异字段值，根据所述变异字段值，检验目标交易系统是否存在风险识别漏洞。

11、如权利要求 10 所述的计算机系统，其中，根据所述变异字段值，检验目标交易系统是否存在风险识别漏洞，包括：

将原始交易信息中目标字段的原始字段值替换为所述变异字段值，得到变异交易信息；

将变异交易信息输入目标交易系统，若所述目标交易系统未识别交易风险，则确定目标交易系统存在风险识别漏洞。

12、如权利要求 11 所述的计算机系统，所述步骤还包括：

在确定目标交易系统存在风险识别漏洞之后，触发风险识别漏洞警报；

若所述目标交易系统识别出交易风险，则不触发风险识别漏洞警报。

13、如权利要求 11 所述的计算机系统，所述步骤还包括：

在确定目标交易系统存在风险识别漏洞之后，将所述变异交易信息和所述目标字段的字段信息，关联保存到所述交易知识库中。

14、如权利要求 10 所述的计算机系统，其中，所述交易知识库中预先保存有多个键值对，所述键值对中的键用于保存预先获取的所述目标交易系统的历史交易中数据字段的字段信息的向量化特征，所述键值对中的值用于保存所述历史交易的交易信息；

根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取与所述目标字段相关的一到多个历史字段值，包括：

对所述目标字段的字段信息进行向量化处理，得到第一向量化特征，根据

所述第一向量化特征，从交易知识库中获取与所述目标字段相关的一到多条历史交易，从所述一到多条历史交易中提取一到多个历史字段值。

15、根据权利要求 10 所述的计算机系统，其中，根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语，包括：

将原始交易信息中目标字段的原始字段值，替换为所述历史字段值和所述原始字段值的合集，得到扩充交易信息；

根据所述扩充交易信息，构建所述提示语。

16、如权利要求 10 所述的计算机系统，其中，根据所述原始交易信息和所述历史字段值，构建生成变异字段值的提示语，包括：

根据预先构建的试例交易信息、以及预先构建的所述目标大模型针对所述试例交易信息的输出信息，构建试例提示信息；

根据所述原始交易信息、所述历史字段值和所述试例提示信息，构建所述提示语。

17、如权利要求 10 所述的计算机系统，其中，字段信息包括字段名称、字段类型、字段所属的表名称、调用字段的应用名称中的一种或多种。

18、如权利要求 10 所述的方法，其中，所述目标字段为交易金额字段、交易账户字段、交易币种字段、交易状态字段中的一种。

19、一种检验交易系统的风险识别漏洞的装置，所述装置包括：

获取模块，用于获取目标交易系统中实时交易对应的原始交易信息，根据所述原始交易信息中目标字段的字段信息，从预先设立的交易知识库中获取所述目标字段的一到多个历史字段值；

生成模块，用于根据所述原始交易信息和所述历史字段值，构建生成目标字段的变异字段值的提示语；所述提示语中指示所述变异字段值的语义符合目标字段的值的语义，且所述变异字段值不同于所述历史字段值、以及所述原始交易信息中目标字段的原始字段值；

检验模块，用于将所述提示语输入目标大模型，得到所述变异字段值，根

据所述变异字段值，检验目标交易系统是否存在风险识别漏洞。

20、一种计算机可读非易失性存储介质，其特征在于，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述权利要求 1-9 任一项所述的方法。