

说明书

数据处理方法、装置、计算机设备、存储介质及产品

本申请要求于2023年06月13日提交中国专利局、申请号为2023107006506、申请名称为“数据处理方法、装置、计算机设备、存储介质及产品”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及计算机技术领域，尤其涉及一种数据处理方法、一种数据处理装置、一种计算机设备、一种计算机可读存储介质及一种计算机程序产品。

背景技术

在诸如：支付场景、门禁场景、游戏场景等各种业务场景中，往往涉及大量的业务需求（例如支付场景中涉及对资产支付的需求，又如门禁场景中涉及开门需求等），大量的业务需求伴随着大量的数据交互，因此，为避免用户恶意交易等异常的数据交互，需在业务场景中设置相应的风控策略。

目前，业务场景中的风控策略的调整一般需要人工申请，需要找到对应的申请方式方可发起关于风控策略的申请，不够灵活。

发明内容

本申请实施例提出了一种数据处理方法、装置、计算机设备、存储介质及产品，能够在业务场景中对用户的信用指标进行等级调整，从而灵活调整该用户在业务场景下的风控策略。

一方面，本申请实施例提供了一种数据处理方法，该方法包括：

获取在业务场景中针对预设对象采集到的生物识别数据；

基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果；

获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标；

其中，第二信用指标与第一信用指标不相同；在业务场景中，第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。

一方面，本申请实施例提供了一种数据处理装置，该装置包括：

获取单元，用于获取在业务场景中针对预设对象采集到的生物识别数据；

处理单元，用于基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果；

处理单元，还用于获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标；

其中，第二信用指标与第一信用指标不相同；在业务场景中，第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。

一方面，本申请实施例提供一种计算机设备，该计算机设备包括存储器和处理器，存储器存储有计算机程序，计算机程序被处理器执行时，使得处理器执行上述的数据处理方法。

一方面，本申请实施例提供一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，该计算机程序被计算机设备的处理器读取并执行时，使得计算机设备执行上述的数据处理方法。

一方面，本申请实施例提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行上述的数据处理方法。

本申请实施例中，获取在业务场景中针对预设对象采集到的生物识别数据，从而可以基于生物识别数据对预设对象进行身份识别处理，得到该预设对象的识别结果，由于身份识别需求往往与具体的业务场景

息息相关，因此本申请可以在特定的业务场景（例如支付场景、门禁场景、游戏场景等）下按照用户的生物识别数据对当前用户进行身份识别处理，可以提高身份识别的场景适配性；获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标；其中，第二信用指标与第一信用指标不相同，并且第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。由此可见，本申请可以通过在业务场景对用户进行身份识别处理，并按照识别结果来灵活调整该用户的信用指标，从而随着用户的信用指标的变更（即由第一信用指标变更为第二信用指标），针对该用户的风控策略也随之变更，因此，本申请可以在特定业务场景中基于指标调整方式来灵活调整相应的风控策略。

附图说明

- 图 1 是本申请实施例提供的一种数据处理系统的架构示意图；
- 图 2 是本申请实施例提供的一种数据处理场景的架构示意图；
- 图 3 是申请实施例提供的一种数据处理方法的流程示意图；
- 图 4 是申请实施例提供的另一种数据处理方法的流程示意图；
- 图 5a 是本申请实施例提供的一种等级调整处理的界面示意图；
- 图 5b 是本申请实施例提供的另一种等级调整处理的界面示意图；
- 图 6 是本申请实施例提供的一种数据处理场景的流程示意图；
- 图 7a 是本申请实施例提供的一种刷掌支付场景的流程示意图；
- 图 7b 是本申请实施例提供的另一种刷掌支付场景的流程示意图；
- 图 8 是本申请实施例提供的一种数据处理装置的结构示意图；
- 图 9 是本申请实施例提供的一种计算机设备的结构示意图。

具体实施方式

本申请提供了一种数据处理方案，适用于诸如：支付场景、门禁场景、游戏场景等业务场景中，能够在上述业务场景中对用户进行身份识别，并按照识别结果来灵活调整该用户的安全信用等级（即信用指标），以变更该用户在相应业务场景中的风控策略，从而可以满足业务场景下更多地业务需求。具体地，该数据处理方案的原理大致如下：

（1）在业务场景中检测到针对预设对象的身份识别需求时（例如支付场景中需要预设对象进行刷脸支付时、门禁场景中需要预设对象核验身份时），获取针对该预设对象所采集到的生物识别数据。其中，此处的业务场景可以为支付场景、核身场景（如门禁场景）、游戏场景中的任一个业务场景，预设对象即为需要被进行身份核验或身份识别的任一个对象（通常为对象）；此处的生物识别数据则是可用于反映预设对象的身份的数据，例如：手掌数据、手掌数据、指纹数据、人脸数据、瞳孔数据等。

（2）基于生物识别数据对预设对象进行身份识别处理，得到该预设对象的识别结果。其中，此处的识别结果用于反映对预设对象的身份识别是否成功，因此识别结果包括识别成功和识别失败，所谓识别成功则是指对预设对象的身份识别成功，识别失败则是指对预设对象的身份识别失败。

（3）获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标；其中，第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。应当理解，预设对象是指在业务场景中预先执行了身份注册的对象，因此当预设对象在业务场景中进行身份注册后可以为该预设对象分配相应的第一信用指标，然后可根据实时业务场景中对该预设对象进行身份识别后得到的识别结果来调整第一信用指标，以调整该预设对象的风控策略。

由此可见，本申请可以在业务场景中针对具备身份识别需求的用户（即预设对象）进行身份识别处理，从而可以按照身份识别处理得到的识别结果来灵活调整该用户的信用指标；由于在业务场景中不同的信用

指标可关联不同的风控策略,因此随着用户的信用指标的变更(即由第一信用指标变更为第二信用指标),针对该用户的风控策略也随之变更,也即本申请可以在特定业务场景中基于指标调整方式来灵活调整相应的风控策略,可以针对同一用户灵活调整该用户的风控策略,风控管理方式更加灵活。

下面对本申请实施例涉及的相关技术术语进行介绍:

一、业务场景、预设对象:

业务场景是指能够提供业务服务,并支持对预设对象进行生物识别(或身份识别)的场景;此处的预设对象是指:业务场景中的任一对象,或者,业务场景中的指定对象(如支付场景中需进行支付的对象)。例如业务服务为支付服务,则业务场景为支付场景,在该支付场景中,允许对支付对象进行身份识别;又如业务服务为核身服务,则业务场景为门禁场景,在该门禁场景中,允许对核身对象进行身份识别;还如业务服务为游戏服务,则业务场景可以为游戏场景,在该游戏场景中,允许对游戏对象进行身份识别。

二、生物识别数据:

生物识别数据是指用于对用户(即预设对象)进行身份识别或生物识别的数据,所谓身份识别至少包括:手掌识别、指纹识别、人脸识别、瞳孔识别。其中,该生物识别数据可以包括但不限于:手掌数据、指纹数据、人脸数据、瞳孔数据。具体地,手掌识别是一种基于手掌数据对用户进行身份识别的技术;指纹识别是一种基于指纹数据对用户进行身份识别的技术;人脸识别是一种基于人脸数据对用户进行身份识别的技术;瞳孔识别是一种基于瞳孔数据对用户进行身份识别的技术。

本申请中,主要涉及基于手掌识别技术对预设对象进行身份识别处理,以得到该预设对象的识别结果,识别结果可以包括识别成功和识别失败。具体地,该手掌识别技术可以应用于诸如:支付场景、门禁场景、游戏场景等各种业务场景中。例如,在支付场景中可以采集预设对象的手掌数据,并基于该手掌数据对该预设对象进行身份识别,若识别成功即可执行后续支付处理等操作;又如,在门禁场景中可以采集预设对象的手掌数据,并基于该手掌数据对该预设对象进行身份识别,若识别成功即可执行后续的开门等操作。

三、第一信用指标、及第二信用指标:

所谓信用指标可以是基于预设的管理规则为同一业务场景中的不同对象所分配的一种指标,例如通过管理规则对用户的身份信息、以及在业务场景中的操作数据等进行分析后,方可得到该用户对应的信用指标,可选的,信用指标是一种用于标识用户(即预设对象)在业务场景中的安全信用等级;所谓安全信用等级,故名思意,是指对象在业务场景中所具备的、用于表征该对象的安全信用的等级,安全信用等级数据形态可以为:中文、英文、字符串等。具体地,不同业务场景中所对应的信用指标所指示的安全信用等级数据形态可以相同,也可以不相同。另外需要说明的是,不同业务场景中所规定的安全信用等级类型及数量可以相同,也可以不相同,其具体数量和类型可以基于管理规则的不同而不同;例如在支付场景中具备4种类型的安全信用等级;又如,在门禁场景中具备3种类型的安全信用等级。例如,在支付场景中对应的信用指标所指示的安全信用等级可以表示为:初级、中级、高级、极高级;又如,在门禁场景中对应的信用指标所指示的安全信用等级可以表示为:80%、90%、100%;还如,在游戏场景中对应的信用指标所指示的安全信用等级可以表示为:等级1、等级2、等级3,等等。本申请中,第一信用指标与第二信用指标不相同,例如,第一信用指标所指示的安全信用等级(例如高级)可以高于第二信用指标所指示的安全信用等级(例如中级);又如,第一信用指标所指示的安全信用等级(例如高级)可以低于第二信用指标所指示的安全信用等级(例如极高级)。

四、风控策略:

风控策略的全称为风险控制策略,风险控制策略是一种用于采取各种措施和方法,消灭或减少风险事件发生的各种可能性的策略。具体地,不同业务场景中所对应的风控策略不相同,例如支付场景中的风控策略可以包括对:支付额度、支付频次等进行风险控制的策略;又如核身场景中的风控策略可以包括对:身份篡改、信息窃取等进行风险控制的策略。

本申请中，业务场景中的风控策略随着预设对象的信用指标的变化而动态调整，具体地，第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。例如在支付场景中，预设对象的信用指标为第一信用指标（例如该第一信用指标所指示的安全信用等级可以为中级），则该第一信用指标所关联的风控策略可以包括一笔订单的最高支付额度为 1000；当预设对象的信用指标调整为第二信用指标时（例如该第二信用指标所指示的安全信用等级可以为高级），则该第二信用指标所关联的风控策略可以包括一笔订单的最高支付额度为 2000。

五、云技术：

本申请中，上述提及的数据处理方案中主要包括：获取在业务场景中针对预设对象采集到的生物识别数据、基于生物识别数据对预设对象进行身份识别处理、根据识别结果对第一信用指标进行等级调整处理等处理过程，这些处理过程往往涉及大量的数据计算以及数据存储服务，需要花费大量的计算机运营成本。因此，本申请所涉及到的数据计算以及数据存储等服务均可以由云技术中的云存储技术进行实现。即，将区块链通过云存储技术存储在“云”上，当需要将业务系统中交易过程所产生的交易数据存储至区块链时，可以通过云存储技术将这些交易数据上传到“云”上的区块链中；并且，当需要读取这些交易数据时，可以随时从“云”上的区块链中读取数据，可以降低对计算机设备的存储要求，扩大区块链的应用范围。

其中，所谓云技术（Cloud technology）基于云计算商业模式应用的网络技术、信息技术、整合技术、管理平台技术、应用技术等的总称，可以组成资源池，按需所用，灵活便利。云计算技术将变成重要支撑。其中，云技术可以包括云存储技术，所谓云存储(cloud storage)是在云计算概念上延伸和发展出来的一个新的概念，分布式云存储系统(以下简称存储系统)是指通过集群应用、网格技术以及分布存储文件系统等功能，将网络中大量各种不同类型的存储设备通过应用软件或应用接口集合起来协同工作，共同对外提供数据存储和业务访问功能的一个存储系统。

六、人工智能：

人工智能(Artificial Intelligence, AI)是利用数字计算机或者数字计算机控制的机器模拟、延伸和扩展人的智能，感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统。人工智能技术是一门综合学科，涉及领域广泛，既有硬件层面的技术也有软件层面的技术。人工智能基础技术一般包括如传感器、专用人工智能芯片、云计算、分布式存储、大模型训练技术、操作/交互系统、机电一体化等技术。人工智能软件技术主要包括计算机视觉技术、语音处理技术、自然语言处理技术以及机器学习/深度学习等几大方向。

本申请实施例提供的数据处理方案主要涉及人工智能领域的机器学习技术相结合。例如，可基于机器学习技术训练特征提取模型，并采用训练后的特征提取模型（例如第一特征提取模型和第二特征提取模型）对预设对象的生物识别数据进行特征提取处理，得到预设对象生物特征。后续，可以基于预设对象的生物特征对该预设对象进行身份识别。其中，机器学习(Machine Learning, ML)是一门多领域交叉学科，涉及概率论、统计学、逼近论、凸分析、算法复杂度理论等多门学科。专门研究计算机怎样模拟或实现人类的学习行为，以获取新的知识或技能，重新组织已有的知识结构使之不断改善自身的性能。机器学习是人工智能的核心，是使计算机具有智能的根本途径，其应用遍及人工智能的各个领域。机器学习和深度学习通常包括人工神经网络、置信网络、强化学习、迁移学习、归纳学习、式教学习等技术。

七、区块链：

区块链是分布式数据存储、P2P(Peer to Peer, 点对点)传输、共识机制、加密算法等计算机技术的新型应用模式。区块链本质上是一个去中心化的数据库，是一串使用密码学方法相关联产生的数据块(也可称为区块)，每一个数据块中包含了一批次网络交易的信息，用于验证其信息的有效性(防伪)和生成下一个数据块。区块链以密码学方式保证数据不可篡改和不可伪造。

本申请中，数据处理过程中涉及诸多数据，例如：生物识别数据、识别结果、第一信用指标、第二信

用指标、风控策略等。可选的，本申请可将上述数据发送至区块链进行存储，基于区块链的不可篡改、可追溯等特性可避免数据被篡改或泄露，从而提高数据处理过程的安全性和可靠性。

需要特别说明的是，在本申请中，涉及到的数据处理过程中的相关数据，例如：生物识别数据、识别结果、第一信用指标、第二信用指标、风控策略等等。在本申请以上实施例运用到具体产品或技术中时，需获得用户许可或同意，且相关数据收集、使用和处理过程需遵守国家地区的相关法律法规和标准，符合合法、正当、必要的原则，不涉及获取法律法规禁止或限制的数据类型。在一些可选的实施例中，本申请实施例中所涉及的相关数据是经过对象单独授权后获取的，另外，在获取对象单独授权时，向对象表明所涉及的相关数据的用途。

下面结合图1和图2对本申请实施例提出的数据处理系统进行详细介绍。

请参见图1，图1是本申请实施例提供的一种数据处理系统的架构示意图。该数据处理系统的架构图包括：服务器104以及终端设备集群，其中，终端设备集群包括：终端设备101、终端设备102、终端设备103等多个终端设备。其中，终端设备集群中的任一终端设备与服务器104之间可以通过有线或无线通信方式进行直接或间接地连接。

终端设备集群中的各终端设备可以是手机、平板电脑、笔记本电脑、掌上电脑、移动互联网设备(MID, mobile internet device)、车载设备、飞行器、可穿戴设备(诸如智能手表、智能手环、计步器等智能设备)、虚拟现实设备(例如VR(Virtual Reality, 虚拟现实)设备、AR(Augmented Reality, 增强现实)设备)等等。可以理解的是，终端设备集群中的各终端设备的类型可以相同或不同，例如：终端设备101可以是手机，终端设备102也可以是手机。再如：终端设备101可以是平板电脑，终端设备103可以是车载设备。本申请并不对终端设备集群中的终端设备的数量及类型进行限定。

服务器104可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN(Content Delivery Network, 内容分发网络)、以及大数据和人工智能平台等基础云计算服务的云服务器。

接下来，以数据处理系统中的任一终端设备(例如终端设备101)为例，对终端设备101和服务器104之间的交互过程进行相应阐述：

①终端设备101响应于预设对象的身份识别请求，然后获取在业务场景中针对预设对象采集到的生物识别数据。具体地，在支付场景中，身份识别请求可以为预设对象提交的支付请求；在门禁场景中，身份识别请求可以为预设对象提交的核身请求。

②终端设备101将获取到的该生物识别数据发送至服务器104。服务器104在接收到预设对象的生物识别数据后，可以基于该生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果。

③服务器104可以获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标。

④服务器104可以将第二信用指标发送至终端设备101，其中，第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。后续，终端设备101在业务场景中即可基于第二信用指标所指示的风控策略对预设对象进行业务管理。

需要说明的是，上述数据处理的交互过程仅用于示例，并不对终端设备和服务器的具体执行过程进行限定。例如，获取预设对象在业务场景中对应的第一信用指标也可以由任一终端设备来执行；又如，对图结构进行分析处理的过程也可以由服务器来执行。可选的，本申请上述数据处理过程中所涉及的：生物识别数据的获取过程、基于生物识别数据对预设对象进行身份识别处理的过程、以及根据识别结果对第一信用指标进行等级调整处理等所有过程均可由任一终端设备或服务器单独执行。

在一种可能的实现方式中，可以将本申请实施例提供的数据处理系统部署在区块链系统中，例如可以

将服务器 104 和终端设备集群中包括的每个终端设备（例如终端设备 101、终端设备 102、以及终端设备 103 等）均当成区块链的节点设备，共同构成区块链网络。因此本申请实施例的数据处理过程中所涉及到的：生物识别数据的获取过程、基于生物识别数据对预设对象进行身份识别处理的过程、以及根据识别结果对第一信用指标进行等级调整处理等过程均可以在区块链上执行，这样既可以保证数据处理流程的公平公正化，同时可以使得数据处理流程具备可追溯性，同时保证数据处理过程中数据安全性，从而提升整个数据处理流程的安全性和可靠性。

本申请提供的数据处理系统可以适用于诸如：支付场景、核身场景、游戏场景等各种业务场景中。接下来，以业务场景是刷掌识别场景（例如支付场景和核身场景）为例，对刷掌识别场景中涉及的具体架构进行详细阐述。

请参见图 2，图 2 是本申请实施例提供的一种刷掌识别场景的架构示意图。如图 2 所示，该刷掌识别场景涉及：刷掌设备 A、刷掌设备 B、刷掌设备 C、以及后端服务器。可选的，刷掌设备 A 可以为图 1 所示的数据处理系统中的终端设备 101，该刷掌设备用于；刷掌设备 B 可以为图 1 所示的数据处理系统中的终端设备 102，刷掌设备 C 可以为图 1 所示的数据处理系统中的终端设备 103，后端服务器可以为图 1 所示的数据处理系统中的服务器 104。其中，刷掌设备 A、刷掌设备 B、刷掌设备 C 中分别运行有刷掌客户端（APP），不同的刷掌设备所适用的业务场景可以相同，也可以不相同，例如刷掌设备 A 适用于核身场景，又如刷掌设备 B 适用于小额支付场景（支付额度在 10000 以内），还如刷掌设备适用于大额支付场景（支付额度大于 10000）；后端服务器用于为上述各刷掌设备（刷掌设备 A、刷掌设备 B、刷掌设备 C）提供后端服务。接下来，分别对刷掌设备（例如刷掌设备 A）以及后端服务器进行详细介绍：

一、刷掌设备 A。

刷掌设备 A 配置有：采集设备、刷掌客户端/APP（Application，应用程序）。其中，采集设备例如可以为 3D 摄像头（在传统摄像头基础上添加了用于检测活体相关的软硬件，包括深度相机和红外相机，可保证信息安全）。其中，3D 摄像头主要包括：彩色传感器（RGB Sensor）、红外传感器（IR Sensor）；刷掌客户端配置有：手掌识别模块、场景配置模块以及支付应用模块。下面对刷掌设备中的各个模块进行说明。

①RGB Sensor 和 IR Sensor：统称为采集设备，可用于采集预设对象的生物流媒体数据。其中，RGB Sensor 用于拍摄彩色图像，IR Sensor 用于拍摄红外图像，可基于 RGB Sensor 拍摄的彩色图像和 IR Sensor 拍摄的红外图像生成预设对象的生物流媒体数据。

②手掌识别模块：用于接收采集设备（RGB Sensor 和 IR Sensor）采集到的生物流媒体数据，并对生物流媒体数据进行数据处理，得到生物识别数据。其中，数据处理可以包括：优选处理和活检处理，其中，优选处理是指对生物流媒体数据包括的多张生物图像按照预设选择条件（例如清晰度、图像对比度、图像亮度等条件）进行选择处理以得到较优的图像，活检处理是指辨别预设对象是否为活体。

③场景配置模块：用于获取刷掌设备的出厂信息，并基于该出厂信息生成刷掌设备 A 的场景配置信息，然后将刷掌设备 A 的场景配置信息发送至后端服务器进行记录并存储。其中，刷掌设备 A 的场景配置信息可以包括但不限于：设备标识（MCH_ID），SN（Serial Number，字符串序列号）、刷掌设备所处业务场景的安全验证等级 on_auto_type（用于指示是否无人自助，即无人监督场景）、以及 app_type（业务场景，如支付 pay、核身 identify）。

④支付应用模块：用于根据当前刷掌设备的场景配置信息确定当前刷掌设备所处的业务场景，并启动相应的业务服务，具体地，基于场景配置信息，不同的业务场景会启动不同的业务服务。例如业务场景为支付场景，则当用户刷掌识别通过后该支付应用模块所启动的业务服务为：返回付款码。又如业务场景为门禁场景，则当用户刷掌识别通过后该支付应用模块所启动的业务服务为：返回开门指示信息（OPENID）等。可选的，当用户被风控时，即当前用户未认证到满足当前业务场景的安全信用等级时，则会显示提示

信息,该提示信息用于提示当前用户不满足业务条件,引导用户通过手机扫码或者后续在其他可认证后提升等级的业务场景进行等级提升后再试。

二、后端服务器:

后端服务器用于为刷掌设备 A 提供后端服务,后端服务详细可以包括:刷掌识别服务、场景管控服务、信用等级管控服务、支付服务等。

①刷掌识别服务:接收来自刷掌设备中采集设备所采集到的生物识别数据(例如手掌数据),并对该手掌数据进行特征提取,以对预设对象进行身份识别处理。其中,此处的特征提取可以包括:掌纹特征提取和掌静脉特征提取,从而可以得到预设对象的掌纹特征和掌静脉特征,后续可基于掌纹特征和掌静脉特征对该预设对象进行身份识别处理。本申请采用的双因子特征(掌纹特征提取和掌静脉特征)相较于单因子特征更加丰富、准确,从而可以提高身份识别的准确性,保证数据处理过程的安全性和可靠性。

②场景管控服务:用于标识每个业务场景所需的安全信用等级以及记录每台刷掌设备所归属的业务场景。其中,业务场景可以包括:支付场景、核身场景(如门禁场景)、游戏场景。例如,刷掌设备 A 所归属的业务场景为核身场景,该核身场景所需的安全信用等级为等级 1;又如,刷掌设备 B 所归属的业务场景为小额支付场景,该小额支付场景所需的安全信用等级为等级 2;还如,刷掌设备 C 所归属的业务场景为大额支付场景,该大额支付场景所需的安全信用等级为等级 3。

③信用等级管控服务:用于记录当前用户的信用指标(或安全信用等级)以及分配唯一的风控策略,以及当用户当前信用指标所指示的安全信用等级不满足场景要求时的功能引导。其中,一个信用指标关联有一个风控策略,不同业务场景所对应的风控策略不相同。

④支付服务:在对预设对象进行身份识别处理并得到识别结果后,若识别结果为识别成功,则可以用该支付服务完成后续的资产转移处理(如将预设对象所拥有的资产转移至收款对象的账户中)。

本申请实施例中,可以在业务场景中针对具备身份识别需求的用户(即预设对象)进行身份识别处理,从而可以按照身份识别处理得到的识别结果来灵活调整该用户的信用指标;由于在业务场景中不同的信用指标可关联不同的风控策略,因此随着用户的信用指标的变更(即由第一信用指标变更为第二信用指标),针对该用户的风控策略也随之变更,也即本申请可以在特定业务场景中基于指标调整方式来灵活调整相应的风控策略,可以针对同一用户灵活调整该用户的风控策略,风控管理方式更加灵活。

可以理解的是,本申请实施例描述的系统架构示意图是为了更加清楚的说明本申请实施例的技术方案,并不构成对于本申请实施例提供的技术方案的限定,本领域普通技术人员可知,随着系统架构的演变和新业务场景的出现,本申请实施例提供的技术方案对于类似的技术问题,同样适用。

接下来对本申请实施例提出的数据处理方法进行详细描述。

请参见图 3,图 3 是本申请实施例所提供的一种数据处理方法的流程示意图。该数据处理方法可以由计算机设备执行,该计算机设备可以是图 1 所示的数据处理系统中终端设备或服务器。其中,该数据处理方法主要包括但不限于如下步骤 S301~S303:

S301: 获取在业务场景中针对预设对象采集到的生物识别数据。

在一种可能的实现方式中,生物识别数据可以是在业务场景中实时采集到的数据,具体来说:响应于预设对象在业务场景中提交的身份识别请求,该身份识别请求用于请求对预设对象进行身份识别;然后可以采用身份识别技术(例如手掌识别技术、指纹识别技术、人脸识别技术、或瞳孔识别技术等)对预设对象进行数据采集,得到预设对象的生物识别数据。具体地,采用不同类型的身份识别技术所采集到的生物识别数据的类型不相同,例如采用手掌识别技术获取到的生物识别数据为手掌数据;同理,采用指纹识别技术获取到的生物识别数据为指纹数据;采用人脸识别技术获取到的生物识别数据为人脸数据,等等。在此实施方式下,生物识别数据是在业务场景中实时采集到的数据,实时采集的数据有利于对预设对象进行更准确的身份识别处理。

在另一种可能的实现方式中，生物识别数据可以是在从数据库中获取的历史采集数据，具体来说：从数据库中获取预设对象的生物识别数据，该生物识别数据是在业务场景中预先采集到的数据。在此实施方式下，计算机设备可以从数据库中便捷地获取到针对预设对象所采集的历史数据，此处的历史数据是指历史时间已经完成采集的数据。历史时间以当前系统时间为参考基准，历史时间即是指当前系统时间之前已经到达的时间。

下面以实时采集数据为例，对生物识别数据的采集过程进行详细说明：

在一种可能的实现方式中，计算机设备获取在业务场景中针对预设对象采集到的生物识别数据，可以包括如下步骤：①调用采集设备采集预设对象的生物流媒体数据，生物流媒体数据包括对预设对象采集得到的多张生物图像，其中，生物流媒体数据可以包括但不限于：视频、图像、音频等数据。具体来说，预设对象的生物流媒体数据可以是在预设时间段内（例如半分钟、一分钟）调用采集设备采集到的多张生物图像，不同场景中对采集到的生物图像的类型不相同。例如手掌识别场景中，调用采集设备采集到的生物图像为手掌图像；又如指纹识别场景中，调用采集设备采集到的生物图像为指纹图像；还如人脸识别场景中，调用采集设备采集到的生物图像为人脸图像。

②按照预设选择条件对多张生物图像进行选择处理，得到预设对象的生物识别数据。此处，预设选择条件包括：图像尺寸（例如图像的长、宽等尺寸）、拍摄角度（例如 90 度、45 度）、图像对比度、图像亮度、清晰度中的任一种或多种。可选的，若按照预设选择条件所选择出来的生物图像包括多张，则可以从多张生物图像中进行再次选择处理，此处的再次选择处理可以包括：随机选择、按照采集时间选择等选择方式。例如，若按照预设选择条件选择得到三张生物图像：img1、img2、img3，且这三张生物图像的采集时间依次为：img1>img2>img3，则可以将 img1 作为最终优选出来的生物识别数据。可选的，在按照预设选择条件选择得到生物图像后，可以进一步对选择得到的生物图像进行图像处理（例如图像增强），并将图像处理后的生物图像作为预设对象的生物识别数据。

按照上述方式，对采集到的生物流媒体数据进行优选处理后得到用于进行身份识别的生物识别数据，可以使得该生物识别数据更加准确、可靠。

S302：基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果。

具体地，对预设对象进行身份识别处理的实质是识别预设对象的身份，通常来说，生物特征是能够唯一标识用户身份的特征。因此，本申请基于预设对象的生物识别数据对预设对象进行身份识别处理时，具体包括：可以获取生物识别数据的类型，并按照不同类型的生物识别数据采取相适应的身份识别技术进行身份识别（其中，一种类型的生物识别数据与一种身份识别技术相适应），从而可以对用户身份进行识别认证。例如，生物识别数据为手掌数据，则可以采用手掌识别技术对该手掌数据进行手掌识别处理；又如，生物识别数据为指纹数据，则可以采用指纹识别技术对该指纹数据进行指纹识别处理；还如，生物识别数据为人脸数据，则可以采用人脸识别技术对该人脸数据进行人脸识别处理。

下面如何对预设对象进行身份识别处理的具体过程进行详细说明。

在一种可能的实现方式中，计算机设备基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果，可以包括如下步骤：①对生物识别数据进行特征提取处理，得到预设对象的生物特征。例如，生物识别数据为手掌数据，则特征提取得到的生物特征可以为手掌特征；又如生物识别数据为指纹数据，则特征提取得到的生物特征可以为指纹特征；还如生物识别数据为人脸数据，则特征提取得到的生物特征可以为人脸特征。②获取预设对象的注册数据，注册数据是由预设对象在业务场景中进行身份注册成功后生成的，注册数据包括注册特征。需要说明的是，若预设对象是基于手掌注册方式进行身份注册的，则该预设对象的注册特征包括手掌特征；同理，若预设对象是基于人脸注册方式进行身份注册的，则该预设对象的注册特征包括人脸特征。③基于预设对象的生物特征、以及预设对象的注册特征，对预设对象进行身份识别处理，得到预设对象的识别结果，识别结果可以包括识别成功和识别失败。具体来说，可以对

生物特征和注册特征进行特征匹配，以对预设对象进行身份识别，具体地，可以计算预设对象的生物特征和注册特征之间的特征相似度，若特征相似度大于或等于相似度阈值，则可以确定对该预设对象身份识别通过，即确定识别结果为识别成功；若特征相似度小于该相似度阈值，则可以确定对该预设对象身份识别不通过，即确定识别结果为识别失败。

接下来，以生物识别数据为手掌数据为例，对手掌数据进行特征提取处理的具体过程进行详细说明。在一种可能的实现方式中，计算机设备对生物识别数据进行特征提取处理，得到预设对象的生物特征，可以包括如下步骤：

①对手掌数据进行掌静脉特征提取处理，得到预设对象的掌静脉特征；以及，对手掌数据进行掌纹特征提取处理，得到预设对象的掌纹特征。具体地，可以采用第一特征提取模型提取预设对象的掌纹特征，以及采用第二特征提取模型提取预设对象的掌静脉特征，第一特征提取模型与第二特征提取模型可以相同，也可以不相同。例如，第一特征提取模型或第二特征提取模型可以为神经网络模型，神经网络模型例如可以包括但不限于：CNN(Convoluntional neural networks, 卷积神经网络)模型、RNN(Recurrent neural networks, 循环神经网络)模型、LSTM(Long Short Term Memory, 长短期记忆)模型、GRU(Gated recurrent units, 门循环单元)模型等，本申请实施例并不对神经网络模型的模型结构进行具体限定。

②对掌纹特征和掌静脉特征进行特征融合处理，得到预设对象的生物特征；其中，特征融合处理至少包括以下任一种：特征加权处理、特征对齐处理、特征运算处理。例如，可以对掌纹特征和掌静脉特征进行加权运算，得到预设对象的生物特征；又如，可以对掌纹特征和掌静脉特征进行平均运算，得到预设对象的生物特征；还如，还可以对掌纹特征和掌静脉特征进行特征对齐处理（例如掌纹特征的特征维度为 $k1 \times k2$ ，掌静脉特征的特征维度为 $k2 \times k3$ ，则可以将掌静脉特征的特征维度与掌纹特征的特征维度进行对齐，由于特征对齐处理后二者的特征维度相同，可以便于后续的特征处理），得到预设对象的生物特征。

按照上述方式，当预设对象的生物识别数据为手掌数据时，可以提取该预设对象的掌纹掌静脉双因子特征（掌静脉特征和掌纹特征）进行身份识别，双因子特征相较于单因子特征（掌静脉特征或者掌纹特征）的优势在于在身份识别时具备更高的准确性和安全性。并且，掌静脉特征的识别难度较高，不易被伪造或模拟，因此进行双因子特征的提取方式可以提高对预设对象进行身份识别的准确性和可靠性。

S303：获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标；其中，在业务场景中，第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。

具体地，在业务场景中，针对同一用户的风控策略可以跟随信用指标的等级调整而动态调整，即针对预设对象而言，第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。例如，业务场景为支付场景，在该支付场景中，预设对象的第一信用指标所指示的安全信用等级（例如中级）所关联的风控策略可以为：该预设对象所支付的任一笔订单的最高支付额度超过 1000 时所采取的策略；预设对象的第一信用指标所指示的安全信用等级（例如高级）所关联的风控策略可以为：该预设对象所支付的任一笔订单的最高支付额度超过 2000 时所采取的策略。也就是说，在支付场景中，风控策略用于控制用户单笔订单所支付的最高额度。

在一种可能的实现方式中，计算机设备根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标，可以包括：若识别结果为识别成功，则按照第一调整方式对第一信用指标进行等级提升处理，得到第二信用指标。其中，第一调整方式用于指示对第一信用指标所指示安全信用等级进行等级提升处理，若安全信用等级为等级 1，则按照第一调整方式可以将该预设对象从等级 1 调整为等级 2，以得到预设对象的第二信用指标。

在另一种可能的实现方式中，计算机设备根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标，还可以包括：获取业务场景的场景配置信息，场景配置信息包括业务场景的安全验证等级；若

业务场景的安全验证等级满足等级调整条件、且识别结果为识别成功，则按照第一调整方式对第一信用指标进行等级提升处理，得到第二信用指标。其中，安全验证等级可用于指示业务场景是否存在对象进行监督的情况，若业务场景为存在对象监督的场景，则该业务场景的安全验证等级为第一等级；若业务场景为不存在对象监督的场景，则该业务场景的安全验证等级为第二等级。

下面对第一信用指标的等级调整处理的具体过程进行详细阐述。

一、按照识别结果对第一信用指标进行等级调整处理。

在一种可能的实现方式中，计算机设备根据识别结果对第一信用指标进行等级调整处理，可以包括以下几种方式：①若识别结果为识别成功，则按照第一调整方式对第一信用指标进行等级提升处理，得到第二信用指标，例如将预设对象从等级 2（第一信用指标）提升至等级 3（第二信用指标）；②若识别结果为识别失败，则按照第二调整方式对第一信用指标进行等级降低处理，得到第三信用指标，例如将预设对象从等级 2（第一信用指标）降低至等级 1（第三信用指标）；③若识别结果为识别失败，则对第一信用指标进行等级保持处理，即将预设对象的等级 2（第一信用指标）进行保持。其中，第一调整方式和第二调整方式不相同；此处的不相同可以包括：对第一信用指标的等级调整幅度不同（即第一调整方式所指示的等级调整幅度与第二调整方式所指示的等级调整幅度不同）、对第一信用指标的等级调整方式不同。

具体来说，若第一信用指标所指示的安全信用等级为中级，则第一调整方式所指示的调整幅度可以为提升一个等级，则可以将预设对象的信用指标从中级提升为高级；若第一信用指标所指示的安全信用等级为中级，则第二调整方式所指示的调整幅度可以为降低一个等级，则可以将预设对象的信用指标从中级降低为初级。需要说明的是，第一调整方式的调整幅度和第二调整方式的调整幅度可以相同，也可以不相同，例如等级调整处理可以包括：在等级提升时，可上调一个等级；在等级降低时，同样可下调一个等级；又如等级调整处理还可以包括：在等级提升时，可上调两个等级；在等级降低时，同样可下调一个等级。在此实现方式中，可按照识别结果来对信用指标进行调整处理，识别成功即可上调该预设对象的信用指标的安全信用等级，识别失败即可下调该预设对象的信用指标的安全信用等级。

二、按照业务场景和识别结果综合对第一信用指标进行等级调整处理。

在一种可能的实现方式中，计算机设备根据识别结果、以及业务场景的场景配置信息对第一信用指标进行等级调整处理，可以包括以下几种方式：

①若业务场景的安全验证等级满足等级调整条件、且识别结果为识别成功，则按照第一调整方式对第一信用指标进行等级提升处理，得到第二信用指标。例如，业务场景为存在对象监督的场景（即该业务场景的安全验证等级为第一等级）、且识别结果为识别成功，则可以将预设对象从等级 2（第一信用指标）提升至等级 3（第二信用指标）。

②若业务场景的安全验证等级不满足等级调整条件、或识别结果为识别失败，则按照第二调整方式对第一信用指标进行等级降低处理，得到第三信用指标。例如，业务场景为不存在对象监督的场景（即该业务场景的安全验证等级为第二等级）、或识别结果为识别失败，则可以将预设对象从等级 2（第一信用指标）降低至等级 1（第三信用指标）。

③若业务场景的安全验证等级满足等级调整条件、且识别结果为识别失败，则对第一信用指标进行等级保持处理。例如，业务场景为存在对象监督的场景（即该业务场景的安全验证等级为第一等级）、且识别结果为识别成功，则可以将将预设对象的等级 2（第一信用指标）进行保持。

④若业务场景的安全验证等级不满足等级调整条件、且识别结果为识别成功，则对第一信用指标进行等级保持处理。例如，业务场景为不存在对象监督的场景（即该业务场景的安全验证等级为第二等级）、且识别结果为识别成功，则可以将将预设对象的等级 2（第一信用指标）进行保持。

上述方式①-④中，等级调整条件可以包括存在对象进行监督的条件，例如业务场景的安全验证等级为第一等级，则该业务场景满足等级调整条件；又如业务场景的安全验证等级为第二等级，则该业务场景不

满足等级调整条件。也就是说，该等级调整条件用于指示需在有对象监督的场景中方可执行等级调整。

三、按照业务场景、历史业务数据、以及识别结果综合对第一信用指标进行等级调整处理。

在一种可能的实现方式中，若业务场景的安全验证等级不满足等级调整条件（即业务场景为不存在对象监督的场景），则可获取该预设对象的历史业务数据，并按照获取到的历史业务数据和识别结果对该预设对象的第一信用指标进行等级调整处理。其中，历史业务数据至少可以包括：历史时间段内该预设对象在业务场景中所产生的业务数据、历史时间段内该预设对象在其它业务场景（例如存在对象监督的场景）中所产生的数据。举例来说，在支付场景中，历史业务数据可以包括该预设对象在历史一个月内（即从当前时间点向前回溯一个月）所产生的历史支付数据，计算机设备可将获取到预设对象的历史支付数据作为样本数据，并基于该样本数据训练一个等级识别模型，该等级识别模型可用于在业务场景中识别预设对象的安全信用等级，此处，等级识别模型可以为任意网络结构的神经网络模型，本申请实施例对此不作限定。后续，可基于训练好的等级识别模型对预设对象进行等级识别处理，此处的等级识别处理是指识别该预设对象的安全信用等级，①例如，若识别得到的安全信用等级满足信用等级阈值（例如高级）且识别结果为识别成功，则可以对该预设对象进行等级提升处理，即将该预设对象从第一信用指标提升至第二信用指标；②又如，若识别得到的安全信用等级满足信用等级阈值（例如高级）、或者识别结果为识别失败，则可以对该预设对象进行等级保持处理；③还如，若识别得到的安全信用等级不满足信用等级阈值且识别结果为识别失败，则可以对该预设对象进行等级降级处理，即将该预设对象从第一信用指标降低至第三信用指标。

具体地，历史支付数据可以包括：支付时间、支付数量、支付金额等数据，计算机设备在基于历史支付数据训练等级识别模型的过程中，具体可以包括：首先，可对该预设对象的历史支付数据进行数据分析，以提取支付特征（例如是否按时支付、支付频次是否频繁、以及支付金额是否异常等特征）；然后，按照提取到的支付特征进行等级识别模型的训练。采用这种方式，可基于用户的历史支付数据训练等级识别模型，从而可采用训练好的等级识别模型对该用户的安全信用等级进行评估，以满足业务场景长期处于无人监管条件下，可按照个人历史业务数据进行等级调整的特殊业务需求，由于等级识别模型是基于用户的历史业务数据训练得到，那么次采用等级识别模型对用户识别得到的安全信用等级的可信度较高，从而可准确、可靠地对用户的信用指标进行等级调整。

本申请实施例中，可以在业务场景中针对具备身份识别需求的用户（即预设对象）进行身份识别处理，从而可以按照身份识别处理得到的识别结果来灵活调整该用户的信用指标；由于在业务场景中不同的信用指标可关联不同的风控策略，因此随着用户的信用指标的变更（即由第一信用指标变更为第二信用指标），针对该用户的风控策略也随之变更，也即本申请可以在特定业务场景中基于指标调整方式来灵活调整相应的风控策略，可以针对同一用户灵活调整该用户的风控策略，风控管理方式更加灵活。

请参见图4，图4是本申请实施例所提供的另一种数据处理方法的流程示意图。该数据处理方法可以由计算机设备执行，该计算机设备可以是图1所示的数据处理系统中终端设备或服务器。其中，该数据处理方法主要包括但不限于如下步骤S401~S404：

S401：获取在业务场景中针对预设对象采集到的生物识别数据。

在一种可能的实现方式中，计算机设备获取在业务场景中针对预设对象采集到的生物识别数据，可以包括如下步骤：①调用采集设备采集预设对象的生物流媒体数据，生物流媒体数据包括对预设对象采集得到的多张生物图像，其中，生物流媒体数据可以包括但不限于：视频、图像、音频等数据。具体来说，预设对象的生物流媒体数据可以是在预设时间段内（例如半分钟、一分钟）调用采集设备采集到的多张生物图像，不同场景中对采集到的生物图像的类型不相同。例如手掌识别场景中，调用采集设备采集到的生物图像为手掌图像；又如指纹识别场景中，调用采集设备采集到的生物图像为指纹图像；还如人脸识别场景中，调用采集设备采集到的生物图像为人脸图像。②按照预设选择条件对多张生物图像进行选择处理，

得到预设对象的生物识别数据。此处的预设选择条件包括：图像尺寸（例如图像的长、宽等尺寸）、拍摄角度（例如 90 度、45 度）、图像对比度、图像亮度、清晰度中的任一种或多种。可选的，若按照预设选择条件所选择出来的生物图像包括多张，则可以从多张生物图像中进行再次选择处理，此处的选择处理可以包括：随机选择、按照采集时间选择等方式，例如，若按照预设选择条件选择得到三张生物图像：img1、img2、img3，且这三张生物图像的采集时间依次为：img1>img2>img3，则可以将 img1 作为最终优选出来的生物识别数据。可选的，在按照预设选择条件选择得到生物图像后，可以进一步对选择得到的生物图像进行图像处理（例如图像增强），并将图像处理后的生物图像作为预设对象的生物识别数据。

按照上述方式，对采集到的生物流媒体数据进行优选处理后得到用于进行身份识别的生物识别数据，可以使得该生物识别数据更加准确、可靠。

S402：基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果。

具体地，对预设对象进行身份识别处理的实质是识别预设对象的身份，通常来说，生物特征是能够唯一标识用户身份的特征。因此，本申请可以基于预设对象的生物识别数据对预设对象进行身份识别处理，具体可以按照不同类型的生物识别数据采取相应的技术进行身份识别，从而可以对用户身份进行识别认证。例如，生物识别数据为手掌数据，则可以采用手掌识别技术对该手掌数据进行手掌识别处理；又如，生物识别数据为指纹数据，则可以采用指纹识别技术对该指纹数据进行指纹识别处理；还如，生物识别数据为人脸数据，则可以采用人脸识别技术对该人脸数据进行人脸识别处理。

需要说明的是，本申请实施例中步骤 S401-S402 所对应的执行操作详细可参见上述图 3 实施例中步骤 S301-S302 所对应的执行操作，本申请实施例在此不再赘述。

在一种可能的实现方式中，计算机设备基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果之后，还包括如下步骤：若识别结果为识别成功，则输出提示界面，提示界面包括提示区域和调整控件，提示区域用于提示预设对象是否授权对第一信用指标的等级调整处理，调整控件用于接收对第一信用指标的等级调整处理的确认操作；响应于预设对象在提示区域中触发的授权确认操作，触发执行获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理的步骤。具体来说，当识别结果为识别成功，响应于在提示区域中针对第一控件触发的授权确认操作，将第一信用指标进行等级调整至第二信用指标；当识别结果为识别失败，响应于在提示区域中针对所述第二控件触发的授权确认操作，将第一信用指标进行等级降低至第三信用指标；当识别结果为识别成功或识别失败，响应于在提示区域中针对第三控件触发的授权确认操作，将第一信用指标进行等级保持处理。

下面结合图 5a 和图 5b 对如何进行等级调整的界面流程进行相应说明。

请参见图 5a，图 5a 是本申请实施例提供的一种等级调整处理的界面示意图。如图 5a 所示，提示界面 S501 中设置有提示区域 5011，该提示区域 5011 中显示有提示信息，该提示信息用于提示预设对象是否授权对第一信用指标的等级调整处理，等级调整处理包括：等级降低处理、等级提升处理、等级保持处理中的任一种或多种；例如该提示信息 5012 可以为：当前等级可进行等级提升处理，请您确认是否进行等级提升。该提示界面 S501 中还设置有调整控件，调整控件用于接收对第一信用指标的等级调整处理的确认操作。其中，调整控件包括：第一控件 5013、第二控件 5014、第三控件 5015；以及，该提示界面 S501 中还设置有取消控件 5016，第一控件 5013 用于接收等级提升处理的确认操作；第二控件 5014 用于接收等级降低处理的确认操作；第三控件 5015 用于接收等级降低处理的确认操作；以及，取消控件 5016 用于接收等级调整处理的取消操作。举例来说，若提示信息显示为对第一信用指标进行等级提升处理，则用户可点击第一控件 5013，以将第一信用指标进行等级提升至第二信用指标；此时，由于等级调整处理为等级提升处理，则第二控件 5014、第三控件 5015 的状态均可被设置为不可点击状态，即第二控件 5014 和第三控件 5015 均无法响应于用户的点击操作（例如单击、双击、长按等任一种操作），在该情况下，允许用户点击第一控件 5013 和取消控件 5016，但不允许用户点击第二控件 5014 和第三控件 5015。同理，若提示

信息显示为对第一信用指标进行等级降低处理,则在该情况下,允许用户点击第二控件 5014 和取消控件 5016,但不允许用户点击第一控件 5013 和第三控件 5015。

请参见图 5b,图 5b 是本申请实施例提供的另一种等级调整处理的界面示意图。如图 5b 所示,该提示界面 S502 中设置有提示区域 5021,该提示区域 5021 中显示有提示信息,该提示信息用于提示预设对象是否授权对第一信用指标的等级调整处理,等级调整处理包括:等级降低处理、等级提升处理、等级保持处理中的任一种或多种;例如该提示信息 5022 可以为:请您确认是否进行等级调整。该提示界面 S502 中还设置有调整控件 5023 和取消控件 5024,若用户点击取消控件 5024,则表示该用户不同意进行等级调整;若用户点击调整控件 5023,则可以显示提示界面 S503。其中,在该提示界面 S503 中显示有提示信息 5031,例如提示信息 5031 可以为:当前等级可进行等级提升处理,请您确认是否进行等级提升。在该情况下,该提示界面 S503 中显示有第一控件 5032 和取消控件 5033,若用户点击该第一控件 5031,则表示该用户同意进行等级调整,可将第一信用指标进行等级提升至第二信用指标。

基于以上描述,在对用户(预设对象)进行身份识别处理后,可以输出提示界面,从而让用户自定义选择是否进行等级调整,这种方式可以满足用户不希望进行等级调整的特殊业务需求,从而可以在业务场景中提升用户体验。

S403: 获取预设对象在业务场景中对应的第一信用指标。

在一种可能的实现方式中,第一信用指标是指预设对象在业务场景中完成身份注册后,为预设对象分配的信用指标;若业务场景为支付场景;则计算机设备获取在业务场景中针对预设对象采集到的生物识别数据之前,还包括:响应于预设对象在支付场景中的身份注册请求,获取支付场景的场景配置信息,场景配置信息包括支付场景的安全验证等级;若支付场景的安全验证等级满足等级调整条件,则在支付场景中按照支付场景的安全验证等级为预设对象分配信用指标;若支付场景的安全验证等级不满足等级调整条件,则在支付场景中将参考信用指标确定为预设对象分配的信用指标。

具体来说,若支付场景为存在对象监督的场景(即该支付场景的安全验证等级为第一等级,例如第一等级为高级),则可以将该支付场景的安全验证等级(高级)作为该预设对象的第一信用指标(高级);若支付场景为不存在对象监督的场景(即该支付场景的安全验证等级为第二等级),则可以默认该用户的第一信用指标为初级(参考信用指标)。采用这种方式,可以按照身份注册时业务场景的安全验证等级(即是否存在对象监督)来为预设对象分配相应的信用指标,从而可以使得预设对象的信用指标更加贴合场景需求。

S404: 获取业务场景的场景配置信息,根据场景配置信息和识别结果对第一信用指标进行等级调整处理,得到第二信用指标。

在一种可能的实现方式中,计算机设备根据场景配置信息和识别结果对第一信用指标进行等级调整处理,得到第二信用指标,可以包括:若业务场景的安全验证等级满足等级调整条件、且识别结果为识别成功,则按照第一调整方式对第一信用指标进行等级提升处理,得到第二信用指标。其中,安全验证等级可用于指示业务场景是否存在对象进行监督的情况,若业务场景为存在对象监督的场景,则该业务场景的安全验证等级为第一等级;若业务场景为不存在对象监督的场景,则该业务场景的安全验证等级为第二等级。等级调整条件可以包括存在对象进行监督的条件,例如业务场景的安全验证等级为第一等级,则该业务场景满足等级调整条件;又如业务场景的安全验证等级为第二等级,则该业务场景不满足等级调整条件。举例来说,若业务场景为存在对象监督的场景(即该业务场景的安全验证等级为第一等级)、且识别结果为识别成功,则可以将预设对象从等级 2(第一信用指标)提升至等级 3(第二信用指标)。

应当理解,本申请实施例提供的数据处理方法适用于诸如:支付场景、门禁场景、游戏场景等业务场景中,能够在上述业务场景中对用户进行身份识别,并按照识别结果来灵活调整该用户的安全信用等级(即信用指标),以变更该用户在相应业务场景中的风控策略,从而可以满足业务场景下更多地业务需求。

下面结合图 6 对数据处理场景的完整流程进行详细介绍。

请参见图 6，图 6 是本申请实施例提供的一种数据处理场景的流程示意图。如图 6 所示，该数据处理场景的流程主要涉及：图 2 所示的数据处理系统中的刷掌设备 A、刷掌设备 B、刷掌设备 C、以及后端服务器。其中，该数据处理场景的流程主要包括但不限于如下步骤 S601~S611。具体地，该数据处理场景的流程主要涉及：场景配置流程、身份注册流程以及刷掌识别流程，下面依次对上述三个流程的具体步骤进行相应阐述。

一、场景配置流程（S601-S603）。

S601：刷掌设备 A 向后端服务器提交无人值守场景 A 的第一场景配置请求。

具体实现时，刷掌设备 A 所属的业务场景 A 为不存在对象监督的场景（即无人值守场景 A），该业务场景 A 为核身场景，刷掌设备 A 可以在业务场景 A 中生成针对预设对象的第一场景配置请求，并将该第一场景配置请求发送至后端服务器。其中，第一场景配置请求中包括业务场景 A 的场景配置信息，例如场景配置信息可以包括但不限于：业务场景 A 的安全验证等级（用于指示是否存在对象监督/是否有人值守）。

可选的，后端服务器可以响应于该第一场景配置请求，并基于业务场景 A 的场景配置信息对业务场景 B 进行场景配置，得到配置结果。其中，该配置结果可以包括：配置成功或配置失败。后续，后端服务器可以将该配置结果返回至刷掌设备 A（如步骤 S6011 所示）。

S602：刷掌设备 B 向后端服务器提交有人值守场景 B 的第二场景配置请求。

具体实现时，刷掌设备 B 所属的业务场景 B 为存在对象监督的场景（即有人值守场景 B），该业务场景 B 为小额支付的场景（即支付额度小于第一支付阈值），刷掌设备 B 可以在业务场景 B 中生成针对预设对象的第二场景配置请求，并将该第二场景配置请求发送至后端服务器。其中，第二场景配置请求中包括业务场景 B 的场景配置信息，例如场景配置信息可以包括但不限于：业务场景 B 的安全验证等级（用于指示是否存在对象监督/是否有人值守）。

可选的，后端服务器可以响应于该第二场景配置请求，并基于业务场景 B 的场景配置信息对业务场景 B 进行场景配置，得到配置结果。其中，该配置结果可以包括：配置成功或配置失败。后续，后端服务器可以将该配置结果返回至刷掌设备 B（如步骤 S6021 所示）。

S603：刷掌设备 C 向后端服务器提交有人值守场景 C 的第三场景配置请求。

具体实现时，刷掌设备 C 所属的业务场景 C 为存在对象监督的场景（即有人值守场景 C），该业务场景 C 为大额支付的场景（即支付额度大于或等于第二支付阈值，第二支付阈值大于第一支付阈值），刷掌设备 C 可以在业务场景 C 中生成针对预设对象的第三场景配置请求，并将该第三场景配置请求发送至后端服务器。其中，第三场景配置请求中包括业务场景 C 的场景配置信息，例如场景配置信息可以包括但不限于：业务场景 C 的安全验证等级（用于指示是否存在对象监督/是否有人值守）。

可选的，后端服务器可以响应于该第三场景配置请求，并基于业务场景 C 的场景配置信息对业务场景 C 进行场景配置，得到配置结果。其中，该配置结果可以包括：配置成功或配置失败。后续，后端服务器可以将该配置结果返回至刷掌设备 C（如步骤 S6031 所示）。

二、身份注册流程、以及刷掌识别流程（S604-S611）。

S604：刷掌设备 A 获取预设对象的刷掌核身的身份注册请求。

具体实现时，预设对象可在刷掌设备 A 所属的业务场景 A（即刷掌核身的门禁场景）中进行身份注册，生成身份注册请求，该身份注册请求可以包括预设对象的身份信息，例如，身份信息可以包括但不限于：身份标识、ID 等用于唯一标识用户身份的数据。本申请中，由于主要涉及刷掌识别，因此预设对象的身份信息可以包括预设对象的手掌数据。

S605：刷掌设备 A 基于身份注册请求向后端服务器进行身份注册。

具体实现时，后端服务器在接收到身份注册请求后，可以按照预设对象的身份信息对预设对象进行身份注册，并在身份注册完成后，为该预设对象在业务场景 A 中分配信用指标（例如第一信用指标），以生成注册结果。其中，该注册结果可以包括：注册成功或注册失败。

可选的，后端服务器可以将注册结果返回至刷掌设备 A（如步骤 S6051 所示）。以及，刷掌设备 A 可以将注册结果返回至预设对象（如步骤 S6052 所示）。

S606：刷掌设备 A 获取预设对象的刷掌核身请求。

具体实现时，预设对象需在业务场景 A（即刷掌核身的门禁场景）中请求开门，即可向刷掌设备 A 提交刷掌核身请求，该刷掌核身请求用于请求对预设对象进行身份识别（例如手掌识别）。

S607：刷掌设备 A 将刷掌核身请求发送至后端服务器。

具体实现时，刷掌设备 A 响应于该刷掌核身请求，并在业务场景 A 中调用采集设备采集预设对象的生物识别数据，并将采集到的生物识别数据发送至后端服务器。

可选的，后端服务器基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果（识别成功或识别失败），并将该识别结果返回至刷掌设备 A（如步骤 S6071 所示）。后续，刷掌设备可将该识别结果返回至预设对象（如步骤 S6072 所示）。

S608：刷掌设备 B 获取预设对象的刷掌支付请求（小额）。

具体实现时，该刷掌支付请求用于请求处理的资产为小额资产，所谓小额资产是指资产量小于第一支付阈值。

S609：刷掌设备 B 向后端服务器请求进行刷掌支付（小额）。

具体实现时，后端服务器响应于预设对象的小额刷掌支付请求，并对该预设对象进行刷掌识别处理，若对该预设对象进行刷掌识别通过，则可以调用支付服务执行资产转移处理（支付处理），以生成支付结果，该支付结果可以包括支付成功或支付失败。

可选的，后端服务可以将支付结果返回至刷掌设备 B（如步骤 S6091 所示）；刷掌设备 B 可以将支付结果返回至预设对象（如步骤 S6092 所示）。

S610：刷掌设备 C 获取预设对象的刷掌支付请求（大额）。

具体实现时，该刷掌支付请求用于请求处理的资产为大额资产，所谓大额资产是指资产量大于或等于第二支付阈值，第二支付阈值大于第一支付阈值。

S611：刷掌设备 C 向后端服务器请求进行刷掌支付（大额）。

具体实现时，后端服务器响应于预设对象的大额刷掌支付请求，并对该预设对象进行刷掌识别处理，若对该预设对象进行刷掌识别通过，则可以调用支付服务执行资产转移处理（支付处理），以生成支付结果，该支付结果可以包括支付成功或支付失败。

可选的，后端服务可以将支付结果返回至刷掌设备 C（如步骤 S6111 所示）；刷掌设备 C 可以将支付结果返回至预设对象（如步骤 S6112 所示）。

下面以支付场景为例，对刷掌识别的过程进行详细说明。

在一种可能的实现方式中，业务场景为支付场景，在支付场景中的风控策略用于指示：一个信用指标对应一个支付额度；计算机设备根据识别结果将预设对象从第一信用指标进行等级调整处理，得到第二信用指标之后，还包括如下步骤：检测在支付场景中请求处理的资产数额；若第二信用指标所对应的支付额度大于或等于请求处理的资产数额，则调用支付服务对资产数额所对应的资产执行转移处理；若第二信用指标所对应的支付额度小于请求处理的资产数额，则输出提示信息，提示信息用于触发对预设对象的第二信用指标进行等级调整处理，以使得等级调整处理后的第二信用指标所对应的支付额度大于或等于请求处理的资产数额。

请参见图 7a，图 7a 是本申请实施例提供的一种刷掌支付场景的流程示意图。如图 7a 所示，预设对象

可在支付场景中进行刷掌识别，并调用刷掌设备采集该预设对象的手掌数据，在刷掌识别界面中显示手掌数据，并对该手掌数据进行识别处理，若识别成功，且预设对象的第二信用指标所对应的支付额度大于或等于在当前支付场景中请求处理的资产数额，则显示支付处理界面，并调用支付服务对资产数额所对应的资产执行支付处理。请参见图 7b，图 7b 是本申请实施例提供的另一种刷掌支付场景的流程示意图。如图 7b 所示，预设对象可在支付场景中进行刷掌识别，若预设对象的第二信用指标所对应的支付额度小于在当前支付场景中请求处理的资产数额，则输出提示信息，例如提示信息包括：您的安全信用等级不满足当前支付条件，请稍后再试！后续，即可在其它可认证的业务场景中对第二信用指标进行等级提升后，再进行支付。通过这种方式，可以在支付场景中结合用户的信用指标所指示的安全信用等级的高低来灵活调整风控策略，从而保证相关业务处理过程的可靠性和安全性。

本申请实施例中，不同的刷掌设备需对不同的业务场景进行场景配置，以便于用户在已配置的相应业务场景（例如刷掌核身场景、支付场景等）中完成身份注册；后续，用户即可在业务场景中执行开门、支付等相关业务处理操作。本申请通过信任用户进行自行场景注册的同时，结合不断调整的精细化风控策略，对用户的刷掌进行逐步验证和信任升级，在保证安全性的同时，逐步提升用户在各种业务场景下的体验感。

上述详细阐述了本申请实施例的方法，为了便于更好地实施本申请实施例的上述方案，相应地，下面提供了本申请实施例的装置，接下来，结合上述本申请实施例提供的数据处理方案，对本申请实施例的相关装置进行相应介绍。

请参见图 8，图 8 是本申请实施例提供的一种数据处理装置的结构示意图。如图 8 所示，该数据处理装置 800 可应用于前述实施例中所提及的计算机设备（如终端设备或服务器）。具体来说，数据处理装置 800 可以是运行于计算机设备中的一个计算机程序（包括程序代码），例如该数据处理装置 800 为一个应用软件；该数据处理装置 800 可以用于执行本申请实施例提供的数据处理方法中的相应步骤。具体实现时，该数据处理装置 800 具体可以包括：

获取单元 801，用于获取在业务场景中针对预设对象采集到的生物识别数据；

处理单元 802，用于基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果；

处理单元 802，还用于获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标；

其中，第二信用指标与第一信用指标不相同；在业务场景中，第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。

在一种可能的实现方式中，处理单元 802 根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标，用于执行以下操作：

获取业务场景的场景配置信息，场景配置信息包括业务场景的安全验证等级；

若业务场景的安全验证等级满足等级调整条件、且识别结果为识别成功，则按照第一调整方式对第一信用指标进行等级提升处理，得到第二信用指标。

在一种可能的实现方式中，识别结果包括识别成功或识别失败；处理单元 802 还用于执行以下操作中的任一种：

若业务场景的安全验证等级不满足等级调整条件、或识别结果为识别失败，则按照第二调整方式对第一信用指标进行等级降低处理，得到第三信用指标；

若业务场景的安全验证等级满足等级调整条件、且识别结果为识别失败，则对第一信用指标进行等级保持处理；

若业务场景的安全验证等级不满足等级调整条件、且识别结果为识别成功，则对第一信用指标进行等级保持处理。

在一种可能的实现方式中，处理单元 802 根据识别结果对第一信用指标进行等级调整处理，得到第二

信用指标，用于执行以下操作：

若业务场景的安全验证等级不满足等级调整条件，则获取预设对象的历史业务数据，并采用历史业务数据训练等级识别模型；

调用训练好的等级识别模型对预设对象进行等级识别处理，得到预设对象的安全信用等级；

按照预设对象的安全信用等级和识别结果，对第一信用指标进行等级调整处理，得到第二信用指标。

在一种可能的实现方式中，处理单元 802 基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果之后，还用于执行以下操作：

若识别结果为识别成功，则输出提示界面，提示界面包括提示区域和调整控件，提示区域用于提示预设对象是否授权对第一信用指标的等级调整处理，调整控件用于接收对第一信用指标的等级调整处理的确认操作；

响应于在提示区域中触发的授权确认操作，触发执行获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标的步骤。

在一种可能的实现方式中，等级调整处理包括：等级降低处理、等级提升处理、等级保持处理中的任一种或多种；调整控件包括第一控件、第二控件、第三控件；其中，第一控件用于接收等级提升处理的确认操作；第二控件用于接收等级降低处理的确认操作；第三控件用于接收等级保持处理的确认操作；

处理单元 802 还用于执行以下任一种操作：

当识别结果为识别成功，响应于在提示区域中针对第一控件触发的授权确认操作，将第一信用指标进行等级调整至第二信用指标；

当识别结果为识别失败，响应于在提示区域中针对第二控件触发的授权确认操作，将第一信用指标进行等级降低至第三信用指标；

当识别结果为识别成功或识别失败，响应于在提示区域中针对第三控件触发的授权确认操作，将第一信用指标进行等级保持处理。

在一种可能的实现方式中，处理单元 802 基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果，用于执行以下操作：

对生物识别数据进行特征提取处理，得到预设对象的生物特征；

获取预设对象的注册数据，注册数据是由预设对象在业务场景中进行身份注册成功后生成的，注册数据包括注册特征；

基于预设对象的生物特征、以及预设对象的注册特征，对预设对象进行身份识别处理，得到预设对象的识别结果。

在一种可能的实现方式中，生物识别数据包括手掌数据；处理单元 802 对生物识别数据进行特征提取处理，得到预设对象的生物特征，用于执行以下操作：

对手掌数据进行掌静脉特征提取处理，得到预设对象的掌静脉特征；以及，

对手掌数据进行掌纹特征提取处理，得到预设对象的掌纹特征；

对掌纹特征和掌静脉特征进行特征融合处理，得到预设对象的生物特征；

其中，特征融合处理至少包括以下任一种：特征加权处理、特征对齐处理、特征运算处理。

在一种可能的实现方式中，获取单元 801 获取在业务场景中针对预设对象采集到的生物识别数据，用于执行以下操作：

调用采集设备采集预设对象的生物流媒体数据，生物流媒体数据包括对预设对象采集得到的多张生物图像；

按照预设选择条件对多张生物图像进行选择处理，得到预设对象的生物识别数据；

其中，预设选择条件包括：图像尺寸、拍摄角度、图像对比度、图像亮度、清晰度中的任一种或多种。

在一种可能的实现方式中，业务场景为支付场景，在支付场景中的风控策略用于指示：一个信用指标对应一个支付额度；

处理单元 802 根据识别结果将预设对象从第一信用指标进行等级调整处理，得到第二信用指标之后，还用于执行以下操作：

检测在支付场景中请求处理的资产数额；

若第二信用指标所对应的支付额度大于或等于请求处理的资产数额，则调用支付服务对资产数额所对应的资产执行转移处理；

若第二信用指标所对应的支付额度小于请求处理的资产数额，则输出提示信息，提示信息用于触发对预设对象的第二信用指标进行等级调整处理，以使得等级调整处理后的第二信用指标所对应的支付额度大于或等于请求处理的资产数额。

在一种可能的实现方式中，第一信用指标是指预设对象在业务场景中完成身份注册后，为预设对象分配的信用指标；业务场景为支付场景；处理单元 802 获取在业务场景中针对预设对象采集到的生物识别数据之前，还包括：

响应于预设对象在支付场景中的身份注册请求，获取支付场景的场景配置信息，场景配置信息包括支付场景的安全验证等级；

若支付场景的安全验证等级满足等级调整条件，则在支付场景中按照支付场景的安全验证等级为预设对象分配信用指标；

若支付场景的安全验证等级不满足等级调整条件，则在支付场景中将参考信用指标确定为为预设对象分配的信用指标。

本申请实施例中，数据处理装置的各个单元所执行操作的具体实现和对应能够产生的效果可参考前述各实施例的相关描述，在此不再赘述。

请参见图 9，图 9 是本申请实施例提供的一种计算机设备的结构示意图。该计算机设备 900 用于执行前述方法实施例中终端设备或服务器所执行的步骤，该计算机设备 900 包括：一个或多个处理器 901；一个或多个输入设备 902，一个或多个输出设备 903 和存储器 904。上述处理器 901、输入设备 902、输出设备 903 和存储器 904 通过总线 905 连接。具体地，存储器 904 用于存储计算机程序，所述计算机程序包括程序指令，处理器 901 用于调用存储器 904 存储的程序指令，执行以下操作：

获取在业务场景中针对预设对象采集到的生物识别数据；

基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果；

获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标；

其中，第二信用指标与第一信用指标不相同；在业务场景中，第二信用指标所关联的风控策略与第一信用指标所关联的风控策略不相同。

在一种可能的实现方式中，处理器 901 根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标，用于执行以下操作：

获取业务场景的场景配置信息，场景配置信息包括业务场景的安全验证等级；

若业务场景的安全验证等级满足等级调整条件、且识别结果为识别成功，则按照第一调整方式对第一信用指标进行等级提升处理，得到第二信用指标。

在一种可能的实现方式中，识别结果包括识别成功或识别失败；处理器 901 还用于执行以下操作中的任一种：

若业务场景的安全验证等级不满足等级调整条件、或识别结果为识别失败，则按照第二调整方式对第一信用指标进行等级降低处理，得到第三信用指标；

若业务场景的安全验证等级满足等级调整条件、且识别结果为识别失败，则对第一信用指标进行等级保持处理；

若业务场景的安全验证等级不满足等级调整条件、且识别结果为识别成功，则对第一信用指标进行等级保持处理。

在一种可能的实现方式中，处理器 901 根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标，用于执行以下操作：

若业务场景的安全验证等级不满足等级调整条件，则获取预设对象的历史业务数据，并采用历史业务数据训练等级识别模型；

调用训练好的等级识别模型对预设对象进行等级识别处理，得到预设对象的安全信用等级；

按照预设对象的安全信用等级和识别结果，对第一信用指标进行等级调整处理，得到第二信用指标。

在一种可能的实现方式中，处理器 901 基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果之后，还用于执行以下操作：

若识别结果为识别成功，则输出提示界面，提示界面包括提示区域和调整控件，提示区域用于提示预设对象是否授权对第一信用指标的等级调整处理，调整控件用于接收对第一信用指标的等级调整处理的确认操作；

响应于在提示区域中触发的授权确认操作，触发执行获取预设对象在业务场景中对应的第一信用指标，并根据识别结果对第一信用指标进行等级调整处理，得到第二信用指标的步骤。

在一种可能的实现方式中，等级调整处理包括：等级降低处理、等级提升处理、等级保持处理中的一种或多种；调整控件包括第一控件、第二控件、第三控件；其中，第一控件用于接收等级提升处理的确认操作；第二控件用于接收等级降低处理的确认操作；第三控件用于接收等级保持处理的确认操作；

处理器 901 还用于执行以下任一种操作：

当识别结果为识别成功，响应于在提示区域中针对第一控件触发的授权确认操作，将第一信用指标进行等级调整至第二信用指标；

当识别结果为识别失败，响应于在提示区域中针对第二控件触发的授权确认操作，将第一信用指标进行等级降低至第三信用指标；

当识别结果为识别成功或识别失败，响应于在提示区域中针对第三控件触发的授权确认操作，将第一信用指标进行等级保持处理。

在一种可能的实现方式中，处理器 901 基于生物识别数据对预设对象进行身份识别处理，得到预设对象的识别结果，用于执行以下操作：

对生物识别数据进行特征提取处理，得到预设对象的生物特征；

获取预设对象的注册数据，注册数据是由预设对象在业务场景中进行身份注册成功后生成的，注册数据包括注册特征；

基于预设对象的生物特征、以及预设对象的注册特征，对预设对象进行身份识别处理，得到预设对象的识别结果。

在一种可能的实现方式中，生物识别数据包括手掌数据；处理器 901 对生物识别数据进行特征提取处理，得到预设对象的生物特征，用于执行以下操作：

对手掌数据进行掌静脉特征提取处理，得到预设对象的掌静脉特征；以及，

对手掌数据进行掌纹特征提取处理，得到预设对象的掌纹特征；

对掌纹特征和掌静脉特征进行特征融合处理，得到预设对象的生物特征；

其中，特征融合处理至少包括以下任一种：特征加权处理、特征对齐处理、特征运算处理。

在一种可能的实现方式中，处理器 901 获取在业务场景中针对预设对象采集到的生物识别数据，用于

执行以下操作：

调用采集设备采集预设对象的生物流媒体数据，生物流媒体数据包括对预设对象采集得到的多张生物图像；

按照预设选择条件对多张生物图像进行选择处理，得到预设对象的生物识别数据；

其中，预设选择条件包括：图像尺寸、拍摄角度、图像对比度、图像亮度、清晰度中的任一种或多种。

在一种可能的实现方式中，业务场景为支付场景，在支付场景中的风控策略用于指示：一个信用指标对应一个支付额度；

处理器 901 根据识别结果将预设对象从第一信用指标进行等级调整处理，得到第二信用指标之后，还用于执行以下操作：

检测在支付场景中请求处理的资产数额；

若第二信用指标所对应的支付额度大于或等于请求处理的资产数额，则调用支付服务对资产数额所对应的资产执行转移处理；

若第二信用指标所对应的支付额度小于请求处理的资产数额，则输出提示信息，提示信息用于触发对预设对象的第二信用指标进行等级调整处理，以使得等级调整处理后的第二信用指标所对应的支付额度大于或等于请求处理的资产数额。

在一种可能的实现方式中，第一信用指标是指预设对象在业务场景中完成身份注册后，为预设对象分配的信用指标；业务场景为支付场景；处理器 901 获取在业务场景中针对预设对象采集到的生物识别数据之前，还包括：

响应于预设对象在支付场景中的身份注册请求，获取支付场景的场景配置信息，场景配置信息包括支付场景的安全验证等级；

若支付场景的安全验证等级满足等级调整条件，则在支付场景中按照支付场景的安全验证等级为预设对象分配信用指标；

若支付场景的安全验证等级不满足等级调整条件，则在支付场景中将参考信用指标确定为为预设对象分配的信用指标。

本申请实施例中，计算机设备的处理器所执行的各个操作的具体实现和对应能够产生的效果可参考前述各实施例的相关描述，在此不再赘述。

此外，这里需要指出的是：本申请实施例还提供了一种计算机存储介质，且计算机存储介质中存储有计算机程序，且该计算机程序包括程序指令，当处理器执行上述程序指令时，能够执行前文所对应实施例中的方法，因此，这里将不再进行赘述。对于本申请所涉及的计算机存储介质实施例中未披露的技术细节，请参照本申请方法实施例的描述。作为示例，程序指令可以被部署在一个计算机设备上，或者在位于一个地点的多个计算机设备上执行，又或者，在分布在多个地点且通过通信网络互连的多个计算机设备上执行。

根据本申请的一个方面，本申请实施例还提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备可以执行前文所对应实施例中的方法，因此，这里将不再进行赘述。

以上所揭露的仅为本申请较佳实施例而已，当然不能以此来限定本申请之权利范围，因此依本申请权利要求所作的等同变化，仍属本申请所涵盖的范围。

权利要求书

1、一种数据处理方法，其特征在于，包括：

获取在业务场景中针对预设对象采集到的生物识别数据；

基于所述生物识别数据对所述预设对象进行身份识别处理，得到所述预设对象的识别结果；

获取所述预设对象在所述业务场景中对应的第一信用指标，并根据所述识别结果对所述第一信用指标进行等级调整处理，得到第二信用指标；

其中，所述第二信用指标与所述第一信用指标不相同；在所述业务场景中，所述第二信用指标所关联的风控策略与所述第一信用指标所关联的风控策略不相同。

2、如权利要求1所述的方法，其特征在于，所述根据所述识别结果对所述第一信用指标进行等级调整处理，得到第二信用指标，包括：

获取所述业务场景的场景配置信息，所述场景配置信息包括所述业务场景的安全验证等级；

若所述业务场景的安全验证等级满足等级调整条件、且所述识别结果为识别成功，则按照第一调整方式对所述第一信用指标进行等级提升处理，得到第二信用指标。

3、如权利要求1或2所述的方法，其特征在于，所述识别结果包括识别成功或识别失败；所述方法还包括以下任一种：

若所述业务场景的安全验证等级不满足等级调整条件、或所述识别结果为识别失败，则按照第二调整方式对所述第一信用指标进行等级降低处理，得到第三信用指标；

若所述业务场景的安全验证等级满足等级调整条件、且所述识别结果为识别失败，则对所述第一信用指标进行等级保持处理；

若所述业务场景的安全验证等级不满足等级调整条件、且所述识别结果为识别成功，则对所述第一信用指标进行等级保持处理；

其中，所述第一调整方式与所述第二调整方式不相同。

4、如权利要求1-3任一项所述的方法，其特征在于，所述根据所述识别结果对所述第一信用指标进行等级调整处理，得到第二信用指标，包括：

若业务场景的安全验证等级不满足等级调整条件，则获取所述预设对象的历史业务数据，并采用所述历史业务数据训练等级识别模型；

调用训练好的等级识别模型对所述预设对象进行等级识别处理，得到所述预设对象的安全信用等级；

按照所述预设对象的安全信用等级和所述识别结果，对所述第一信用指标进行等级调整处理，得到第二信用指标。

5、如权利要求1-4任一项所述的方法，其特征在于，所述基于所述生物识别数据对所述预设对象进行身份识别处理，得到所述预设对象的识别结果之后，所述方法还包括：

若所述识别结果为识别成功，则输出提示界面，所述提示界面包括提示区域和调整控件，所述提示区域用于提示所述预设对象是否授权对所述第一信用指标的等级调整处理，所述调整控件用于接收对所述第一信用指标的等级调整处理的确认操作；

响应于在所述提示区域中触发的授权确认操作，触发执行获取所述预设对象在所述业务场景中对应的第一信用指标，并根据所述识别结果对所述第一信用指标进行等级调整处理，得到第二信用指标的步骤。

6、如权利要求1-5任一项所述的方法，所述等级调整处理包括：等级降低处理、等级提升处理、等级保持处理中的任一种或多种；所述调整控件包括第一控件、第二控件、第三控件；其中，所述第一控件用于接收等级提升处理的确认操作；所述第二控件用于接收等级降低处理的确认操作；所述第三控件用于接收等级保持处理的确认操作；

所述方法还包括以下任一种：

当所述识别结果为识别成功，响应于在所述提示区域中针对所述第一控件触发的授权确认操作，将所述第一信用指标进行等级调整至第二信用指标；

当所述识别结果为识别失败，响应于在所述提示区域中针对所述第二控件触发的授权确认操作，将所述第一信用指标进行等级降低至第三信用指标；

当所述识别结果为识别成功或识别失败，响应于在所述提示区域中针对所述第三控件触发的授权确认操作，将所述第一信用指标进行等级保持处理。

7、如权利要求 1-6 任一项所述的方法，其特征在于，所述基于所述生物识别数据对所述预设对象进行身份识别处理，得到所述预设对象的识别结果，包括：

对所述生物识别数据进行特征提取处理，得到所述预设对象的生物特征；

获取所述预设对象的注册数据，所述注册数据是由所述预设对象在所述业务场景中进行身份注册成功后生成的，所述注册数据包括注册特征；

基于所述预设对象的生物特征、以及所述预设对象的注册特征，对所述预设对象进行身份识别处理，得到所述预设对象的识别结果。

8、如权利要求 1-7 任一项所述的方法，其特征在于，所述生物识别数据包括手掌数据；所述对所述生物识别数据进行特征提取处理，得到所述预设对象的生物特征，包括：

对所述手掌数据进行掌静脉特征提取处理，得到所述预设对象的掌静脉特征；以及，

对所述手掌数据进行掌纹特征提取处理，得到所述预设对象的掌纹特征；

对所述掌纹特征和所述掌静脉特征进行特征融合处理，得到所述预设对象的生物特征；

其中，所述特征融合处理至少包括以下任一种：特征加权处理、特征对齐处理、特征运算处理。

9、如权利要求 1-8 任一项所述的方法，其特征在于，所述获取在业务场景中针对预设对象采集到的生物识别数据，包括：

调用采集设备采集所述预设对象的生物流媒体数据，所述生物流媒体数据包括对所述预设对象采集得到的多张生物图像；

按照预设选择条件对所述多张生物图像进行选择处理，得到所述预设对象的生物识别数据；

其中，所述预设选择条件包括：图像尺寸、拍摄角度、图像对比度、图像亮度、清晰度中的任一种或多种。

10、如权利要求 1-9 任一项所述的方法，其特征在于，所述业务场景为支付场景，在所述支付场景中的风控策略用于指示：一个信用指标对应一个支付额度；

所述根据所述识别结果将所述预设对象从第一信用指标进行等级调整处理，得到第二信用指标之后，还包括：

检测在所述支付场景中请求处理的资产数额；

若所述第二信用指标所对应的支付额度大于或等于所述请求处理的资产数额，则调用支付服务对所述资产数额所对应的资产执行转移处理；

若所述第二信用指标所对应的支付额度小于所述请求处理的资产数额，则输出提示信息，所述提示信息用于触发对所述预设对象的第二信用指标进行等级调整处理，以使得等级调整处理后的第二信用指标所对应的支付额度大于或等于所述请求处理的资产数额。

11、如权利要求 1-10 任一项所述的方法，其特征在于，所述第一信用指标是指所述预设对象在所述业务场景中完成身份注册后，为所述预设对象分配的信用指标；所述业务场景为支付场景；所述获取在业务场景中针对预设对象采集到的生物识别数据之前，还包括：

响应于预设对象在所述支付场景中的身份注册请求，获取所述支付场景的场景配置信息，所述场景配置信息包括所述支付场景的安全验证等级；

若所述支付场景的安全验证等级满足等级调整条件，则在所述支付场景中按照所述支付场景的安全验证等级为所述预设对象分配信用指标；

若所述支付场景的安全验证等级不满足等级调整条件，则在所述支付场景中将参考信用指标确定为所述预设对象分配的信用指标。

12、一种数据处理装置，其特征在于，包括：

获取单元，用于获取在业务场景中针对预设对象采集到的生物识别数据；

处理单元，用于基于所述生物识别数据对所述预设对象进行识别处理，得到所述预设对象的识别结果；

所述处理单元，还用于获取所述预设对象在所述业务场景中对应的第一信用指标，并根据所述识别结果对所述第一信用指标进行等级调整处理，得到第二信用指标；

其中，所述第二信用指标与所述第一信用指标不相同；在所述业务场景中，所述第二信用指标所关联的风控策略与所述第一信用指标所关联的风控策略不相同。

13、一种计算机设备，其特征在于，包括：存储装置和处理器；

存储器，所述存储器中存储一条或多条计算机程序；

处理器，用于加载所述一条或多条计算机程序实现如权利要求 1-11 中任一项所述的数据处理方法。

14、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机程序，所述计算机程序适于被处理器加载并执行如权利要求 1-11 中任一项所述的数据处理方法。

15、一种计算机程序产品，其特征在于，所述计算机程序产品包括计算机程序，所述计算机程序适于被处理器加载并执行如权利要求 1-11 中任一项所述的数据处理方法。