# PRM交易欺诈监控系统拓展

以及互联网新技术应用调研报告

# 引言

随着中国银行业全面开放，行业竞争呈不断加剧之势。银行在以加快业务发展的方式来争夺客户市场的同时，也必须面临与此相伴且不断增长的各种风险的威胁。与国外先进银行相比，国内大多数商业银行目前仍处于欺诈风险管理的起步阶段，在管理技术、系统、人才等方面都略显不足，这与当前严峻的欺诈风险形势形成较大反差，使国内银行在欺诈风险管理的战略管理、业务操作、系统平台以及反欺诈技术等方面都面临着严峻的挑战。

# 1交易欺诈概况

交易欺诈的日益猖獗导致金融服务机构承受了巨大经济损失，为扭转这种局面，金融类机构应考虑主动投资反欺诈的技术手段、防控工具和策略，以减少欺诈带来的风险和资本损失。

# 欺诈交易的主要类型

从业务角度，欺诈类型分为发卡端欺诈和收单端欺诈。发卡端欺诈分为：虚假申请、伪卡欺诈、非面对面欺诈、未达卡、非法冒用（账户接管）等；收单端欺诈分为：商户欺诈套现、POS违规移机、商户侧录、伪冒交易合谋、卡号测试、恶意倒闭、洗单等。

# 发卡欺诈

1) 虚假申请

虚假申请是指使用虚假身份或冒用他人身份获取银行卡进行交易获取商品或服务的欺骗性行为。

2) 伪卡欺诈

伪卡欺诈是指按照银行卡磁条信息格式写磁、凸（平）印伪造真实、有效的银行卡进行交易的欺诈行为。

3) 非面对面欺诈

非面对面欺诈是指窃取真实持卡人卡片信息，以无需卡片出现的交易形式，利用他人信用卡的卡号、有效期、CVV2等卡片信息完成欺诈交易。

4) 未达卡

未达卡是指真实客户未收到信用卡，卡片在邮寄中被盗取，不法分子利用盗取的信用卡进行欺诈交易。

5) 非法冒用（账户接管）

非法冒用是指欺诈分子获取了真实持卡人信息全部或主要部分，并假冒真实持卡人对卡账户的信息进行变更，以达到欺诈消费目的。

# （二）收单欺诈

1) 商户欺诈套现

商户欺诈套现是指商户与不良持卡人或其他第三方勾结，或商户自身进行虚假交易套取现金的行为。

2) POS违规移机

POS违规移机是指商户未经收单机构许可，擅自将POS机具从收单机构登记的原始装机地址转移至另一地址的行为。

3) 商户侧录

商户侧录是指商户或收银员趁持卡人不备或使用欺骗手段，在恶意控制卡片期间，侧录盗取持卡人信用卡磁道信息。

4) 伪冒交易

伪冒交易指商户与不法分子合谋（或非合谋），在商户（或ATM机具）集中使用伪卡或失窃、被盗卡，或购买易变现商品，或享受相关服务。

5) 卡号测试

卡号测试是指为测试遗失卡、盗窃卡、伪造卡、通过卡号生成软件生成的卡号或其他非法获取的卡号的有效性，不法分子使用该类卡在商户进行小额授权申请，如果交易通过，就用来进行其他金额更大的欺诈交易。

6) 恶意倒闭

恶意倒闭是指不法商户在收单机构开设了看似合法经营的商户账户，受理银行卡。当收到大笔清算款项后商户立即关门，故意破产，负责人也马上销声匿迹，使收单机构承担此后的退单损失。

7) 洗单

洗单是指与收单机构签署了有效商户协议的商户，将未签约商户的交易在本商户的POS机或压印机上刷卡或压卡，假冒本店交易与收单机构清算。通过这种方式，可能将欺诈或非法交易合法化，并顺利收到交易款项。

# 1.2 欺诈交易的特征

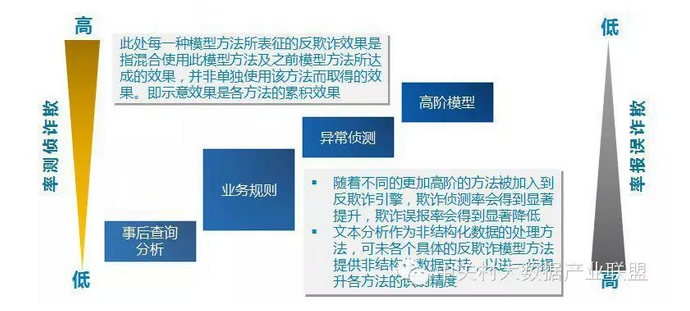
欺诈所涉及的交易行为一般具有非正常或非公平交易的属性，由于缺乏公平公正的交易动机和与实体经济活动相一致的资金运动规律，或有异于一般客户和账户的运用行为，从监测实践来看，欺诈交易行为经常表现为以下几类特征：交易金额、交易频率异常；交易流向或交易来源异常；交易用途或交易性质异常。以上是从交易行为的角度对欺诈交易特征进行剖析，从交易记录的角度分析，交易金额的异常通常体现在单笔或相关交易记录中，交易频率的异常通常体现在基于时间序列的交易记录中，而交易用途或交易性质的异常则通常体现在交易主体间的交易往来中。

# 1.3 金融机构对反欺诈的考虑

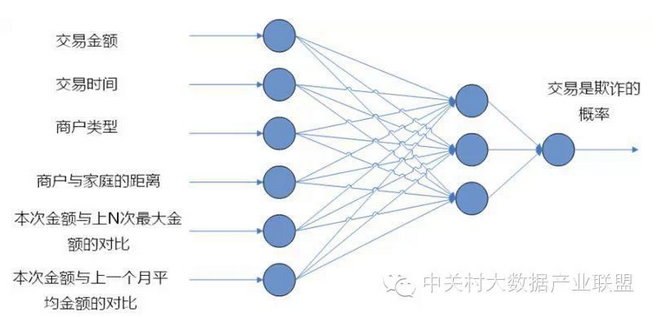
金融业是产生海量数据的行业，欺诈交易藏匿于成千上万的海量交易数据中，侦测的难度很大。如果能建立一套模型，快速从海量交易数据中有效发掘和识别出异常信息并分析评判，将帮助金融机构及时发现问题并做出决策，从而避免各种损失。

# 2 交易欺诈与大数据

交易级别的交易发欺诈手段很多，主要有事后查询分析、业务规则、异常侦测、高阶模型等：



国内外实践经验表明，用神经网络建立的交易反欺诈高阶模型比规则集、线性模型侦测率更高，误报率更小。高阶模型主要是神经网络模型。经典的是BP算法



上图是一个典型的神经网络模型的示意图。网络一般包含三或更多层，其至少包含的有输入层、隐含层及输出层。

**1 模型部分**

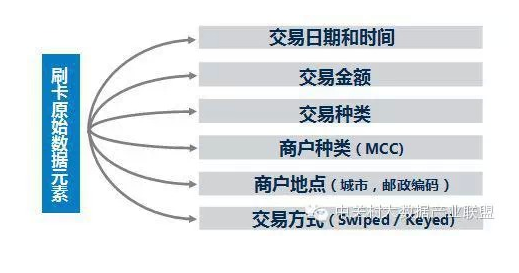
**2.1.1 建模的流程**

交易欺诈的建模流程与建模流程基本一致。但具体到每个环节的时候，是有区别的。具体区别见下面各个章节。

**2.1.2 数据获取**

数据应该包括以下类型数据：

1. 授权文件。授权文件一般包括，账号，交易金额，交易币种，交易日期，交易时间，交易商户地邮政编码、交易商户类别，…等等。该文件是最基本的文件，持卡人的消费模式都包含在里面。



b) 欺诈文件。欺诈文件是模型建制必需的标识文件。

c) 发卡文件。这是该信用卡的主文件。

d) 其他文件。包括还款信息，人口信息，征信局信息等等。此类数据与交易欺诈没有很直接的关系，但也有其一定的预测力。人口信息比如地址更改等和欺诈也有一定的内在联系。

**2.1.3 目标定义**

定义目标变量有如下过程:

1、将欺诈数据与交易数据相匹配，欺诈账户在欺诈窗口（第一次欺诈日到被发现之日）之间的所有交易即为欺诈性交易。

2、对非欺诈账户，其所有交易即为非欺诈性交易。

欺诈账户在第一次欺诈日之前的正常交易只为欺诈账户建立档案，但这些正常交易本身并不作为非欺诈性交易进入建模样本。

**2.1.4 变量与档案（profile）的设计**

这步和下步变量挑选是建造交易反欺诈模型的重点。

a) 原始变量的设计

一般只用当前交易的信息，如交易金额，商户种类，交易发生地与家庭住址的距离，交易发生的时间等等。同时可以对这些基本交易信息建立二维的交叉变量。对产生的非连续性变量进行相应的WOE（weight of evidence）处理。对所有变量进行缺失值和极端值的处理。

b) 档案型（profile）变量的设计

通过对信用卡账户交易历史的跟踪，可以提炼和发现信用卡账户的行为模式，这就是每个账户的档案。如果当前的交易与该账户的历史行为模式差别较大，则欺诈的可能性也较大。通俗的说，档案是该帐号的消费行为的标准答案。要判断当前的这笔是否交易欺诈，则需要将当前的交易信息与这个档案（标准答案）进行对比，相差越大则欺诈的概率越大。

**以时间为基础的档案型变量**

i 过去10分钟，30分钟，1小时，2小时…半天，1天，2天…1周…1月等时间段交易的次数或平均金额。

ii 当前交易金额与过去若干时间段的交易金额的均值和标准差的对比等等。

**以事件为基础的档案型变量**

i 过去2次，3次…10次…N次交易的平均金额

ii 过去2次，3次…10次…N次交易的最大金额

iii 当前交易金额与过去若干次的交易金额的均值，标准差和最大值的对比等等。



上图是信用卡的部分交易明细，经过提取，可以形成档案



不仅对交易金额可以提炼产生上述变量，对商户种类，交易地点与家庭地址的距离，交易时间，交易种类，交易方式，交易货币等信息均可以用同样的方法产生类似的变量。商户类型等这些分类型变量，需要用对应的 WOE代替，时间也是如此，要将时间划分为 7天×24 小时，然后用对应的WOE代替。需要注意的是，时间要使用当地时间，而不是系统时间。 判断该笔消费在当地是白天还是黑夜，当然，系统时间也是要的，用于对交易进行排序，判断交易的顺序。通过这些复杂的变量，可以捕捉到每个账户的历史行为模式，当前交易行为与历史行为模式的差距，交易发生的速率和动态等等。产生上述变量需要一定时间的交易历史（6—12月），涉及的交易量庞大，每笔交易的数据量也不小，如何有效地保存，清理，加工这些数据并在此基础上快速计算所需变量是一个技术关键。一般这步之后，有几千上万个变量。

那接下的工作就是从这上万个变量里寻找一组预测能力强，但变量之间相关弱的变量

**2.1.5 变量选择**

由于建模需要构建出大量的变量，有些变量预测能力强，有些变量预测能力弱，不筛选会影响效率。此外，变量的子集很可能高度相关，造成过拟和，模型的准确性和可靠性将受到损害。神经网络BP算法训练过程中，不能自动筛选变量。为了找到一组预测能力强、变量之间的相关性弱的变量，不影响模型准确性，增加模型稳定性。变量筛选的方法主要如下：

* 单变量预测能力筛选：
* 灵敏度分析
* 变量相关性检查：

经过变量筛选，剩下一二百个变量。一般交易反欺诈模型的变量远远多于信用模型、申请反欺诈模型，接下来就要用这些挑选好的数据进行模型训练了，

**2.1.6 模型训练。**

按以下步骤训练神经网络模型，直至模型效果最佳。

**1、**对所有设计产生的自变量先进行初步筛选，排除明显无预测能力的变量，剩余变量在神经网络模型训练过程中再进行精选。

**2、**根据输入变量的数目，设计合理的网络结构和隐节点数。一般交易欺诈模型有上百个变量，一层隐含层，十几个隐含节点。

**3、**根据设计好的网络结构，选取合适的训练参数和收敛条件，在上述第一步数据进一步划分后的纯训练数据上训练模型，在测试数据上测试模型效果。

**4、**在有了初步训练好的神经网络模型后，可用灵敏度分析等手段进一步筛选变量。

**5、**对每个分段（segment），步骤3到步骤5都要重复多次，调整输入变量，调整隐节点数，调整训练参数，最后选出一个在测试数据上表现最好的模型作为该分段的最终模型。

相对逻辑回归来说，神经网络的训练更加于经验，如何设计网络结构、各个参数大小等，

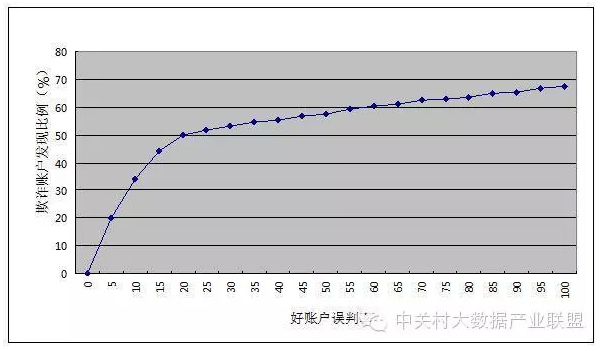
**2.1.7 模型验证**

验证模型主要有以下几种方法：

1、建模验证数据验证：对模型数据划分产生的验证数据上进行验证。

2、跨时间验证：在条件允许的情况下，可对模型在新数据上进行验证。

模型训练结束后，将训练好的模型运用到这部分验证数据上给交易逐个打分，以检验模型的效果。检验交易反欺诈模型的指标通常是欺诈账户发现比例与好账户误判率的比较。下图是一个交易反欺诈模型预测效果评估的示意图：



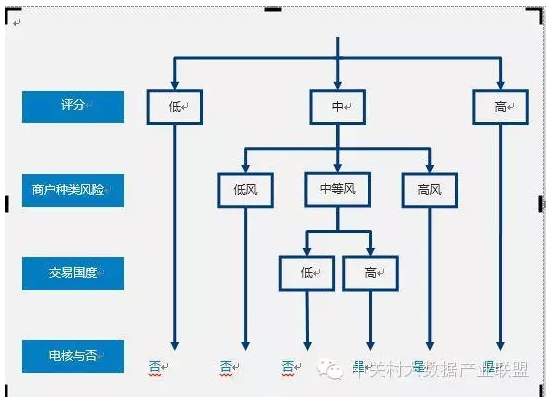
上图中如果操作点是20:1的误判率（AFPR），则欺诈账户发现比例(ADR)是50%。在某一个固定的误判率下，对应的欺诈账户发现比例越高，则模型的效果越好。

我们申请反欺诈、信用模型一般用ks评价模型的好坏。而交易反欺诈一般不是，一般用AFPR ------ADR 。

模型建完之后，需要有对应策略。

**2.1.8 构建基于模型的交易反欺诈策略。**

反欺诈策略的目标是最大限额地降低欺诈损失额，而预期欺诈损失额等于欺诈概率乘以交易额。由于反欺诈模型的评分反映了欺诈的概率，所以欺诈评分和交易额是反欺诈策略的主要依据，辅之以商户种类、交易国度、刷卡方式等。下图是简化了的反欺诈策略。



在制定以交易反欺诈模型为基础的交易反欺诈策略时，需要考虑下列因素之间的平衡：

●欺诈的损失  
●拒绝的交易量

●电话核对的交易量

●系统资源和人力资源的配置和容量

●客户的反应

●反欺诈的成本

●卡组织的限制

一个好的交易反欺诈策略应该达到以下3大目标：

●电话核对和拒绝的交易量适度，不会超过系统和资源负荷

●最大限度地发现和阻止欺诈性交易

●最小限度地影响真实交易

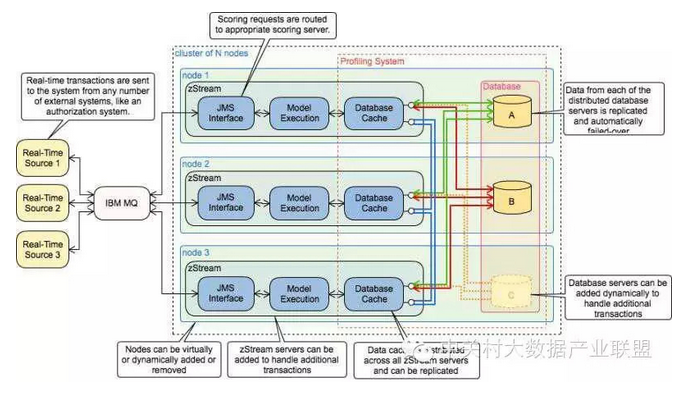
对欺诈风险较高的交易利用事后短信、电话联系、信件联系或电子邮件联系的方式，与卡用户在交易外进行沟通，核对可疑交易，如果证实某信用卡账号正在经历欺诈性交易（如卡用户证实某可疑交易非其所为），则立刻拒绝该卡的所有后续交易并给卡用户换发新的信用卡。这些反欺诈措施可以作为对实时反欺诈授权决策的有效补充。

有了模型，我们就需要系统上线。接下来我们将系统了。

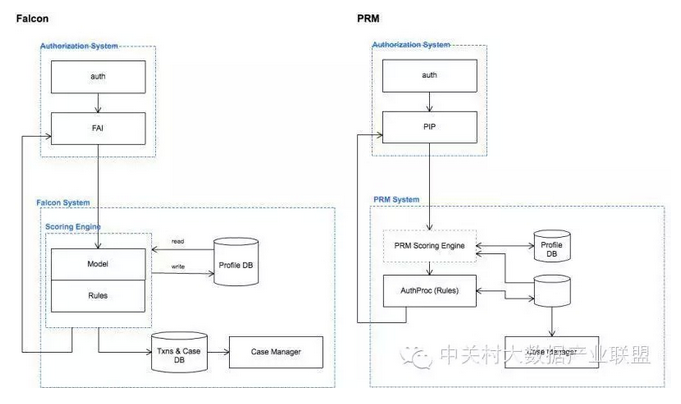
**2、系统部分**

交易级实时评分引擎（Real Time TransactionLevel Scoring Engine）能够以三种方式针对与交易反欺诈相关的多维档案系统进行更新：在内存中做实时的检索和更新；准实时检索和定期更新，例如重点关注名单等；与关系型数据库做离线检索和更新。档案系统支持多维档案处理，例如基于账户的档案、基于客户的档案、基于商户的档案。档案系统也具有中文字符处理能力。

账户档案可以载入计算机内存中，并且可以利用特别设计的算法分布在计算机集群上，使得每一笔交易都可以实时地针对档案进行检索和更新。同时，针对数值和中文字符开发的特殊压缩技术可以最小化整个系统对计算机内存的需求。我公司的交易反欺诈系统也同时支持非档案型的交易欺诈模型部署，在业界是当前唯一能够实现此类模型部署的系统。如下图所示：

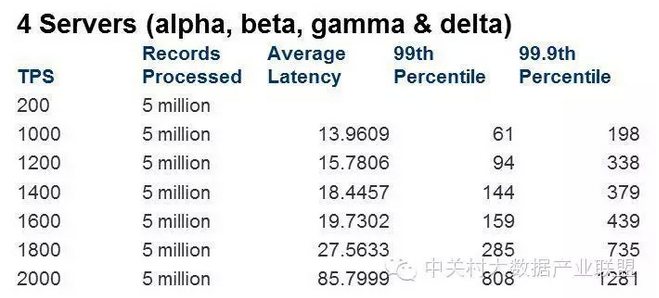


这个图的信息量较大。同时，我公司的交易反欺诈系统与市场上的其他系统相兼容。如下图所示：



下面是有关性能的测试。

· 60 million accounts,· Profile size: 32G ，



这是6个交易历史的数据，100个输入变量，25个隐含节点的效果。BP模型。

# 一、现状

**A、磁条卡易复制的现状**

由于磁条卡磁道信息容易被复制，从而仿制出伪卡，因而对磁条交易的监控应当更为严格一点。经讨论与研究，可以从以下几个方面加强风险防控：

1. 交易频次。交易频次过高可以考虑从发卡端直接进行阻断。同时目前PRM系统有针对24小时内交易频次大于等于6次便会出现告警的规则。
2. 交易金额。央行的管理通知是要求单笔交易金额超过2万，要有一种通信渠道附加通信验证，这其实也是在授权前在发卡端发短信验证码给客户，需要客户回复验证码方可通过交易。目前PRM无论是针对单笔还是日累计交易金额均有这方面的规则监控，根据不同银行业务情况不同，金额大小设定也不同。
3. 采用安全锁增强防控精细度。在这里我们可以对交易渠道、是否跨境、是否为实体卡交易进行不同的区分度控制。

**B、交易欺诈监控系统急需增加新的功能点**

PRM从2014年到现在恰好上线了三年，前两年问题较多，现在处于运行比较平稳的状态，也恰好是我们应当思考PRM何去何从，如何增加新的功能点，如何与现有快速发展的互联网技术相结合，收入增长的瓶颈都是需要我们思考的。

# 二、可借鉴的做法

在此基础上创新部如果要推出配套的外包解决方案，如果从PRM端进行考虑的话，只能是推出针对磁条卡监控的规则，只能是从规则上进改进，要么就是发卡前的单笔交易判断；我觉得我们更应该应该是从消费发生前的安全设定去进行考虑，提前对卡片做出某些设置。下面先贴出一些银行推出的持卡人可以对自己卡片做出某些安全上的设定的案例，我们可以借鉴一下。

1. **中信银行在APP里自己调额**



在中信银行的APP里持卡人可以根据个人安全需要将永久额度调低，或者根据消费需求调高临时额度。

1. **中信网付卡设置以及汇丰的第三方支付设置**



从上可以看出持卡人可以对交易金额、交易笔数、交易渠道等进行设定。

兴业银行一键锁卡“过程其实特别简单，现在已经完全不用再经过电话挂失，只需立即点击兴业银行手机银行,进入信用卡设置页面，打开‘锁定信用卡’，系统便会自动对绑定的信用卡进行管控。上行短信功能。真正做到“停”、“涨”、“限”切换自如，用卡随心。

1. **民生银行的信用卡安全锁**



民生的安全锁功能最大的特色是分渠道、分时间段可以设置锁定卡片。而我本人暂时不会有跨境交易，也基本上不会有去ATM上取款可能，所以这两项功能我都是全天二十四小时设定为关闭。

以上的设想都是基于一个基础——**PRM系统能否对接微信平台进行互动**。如果可以的话，可以将发卡系统里的一些参数设置权限下放到微信里，我们对持卡人的风险提醒可以以微信的形式发送，同时持卡人可以根据提醒的内容对卡片做出一些设置。

1. **欺诈侦测模型**

支付宝的芝麻信用分对于我们至少有两方面的提示。一是我们的欺诈审查不仅仅是依赖于当前交易的审查，应该来自于多维度数据，比如说我们是否可以基于交易地址、交易商户建立一个简单的个人行为模型。甚至于说信用评分本身是用于信审的，其实作为欺诈审查参考也是一个很重要的考量。第二个启示就是我们能否对交易也做一个评分。其实我们是可以根据已有的告警数据，不断地循环迭代生成一个用户黑名单、商户黑名单，也即是高风险卡片、高风险商户，再结合审查员的动作记录、触发的当前告警。

根据上述设想,可以利用的数理统计技术,如神经网络模型,进行深度的数据挖掘,发展交易欺诈风险评分模型,来预测信用卡或交易为欺诈的概率大小,为制定智能反欺诈策略提供科学的依据.

1. 制定以申请欺诈风险评分模型为基础的反欺诈策略(可以对接信审)
2. 制定以交易欺诈风险评分模型为基础的反欺诈策略

交易欺诈风险评分模型是以持卡人的交易行为模式为分析基础的,以对比当前交易与历史交易模式的差别为分析焦点,以精密的数理统计模型(典型的使用机器学习和神经网络模型)为分析手段,以预测当前交易为欺诈的概率为分析目标的模型.

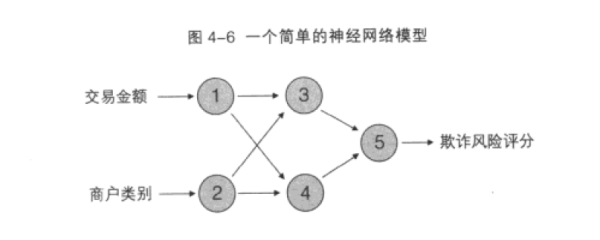
一个优秀的评分模型一定是基于统计分析技术的(典型的使用机器学习和神经网络模型)，可以准确和实时的进行风险评估，通过内部的模型更新增强对新的诈模式的适应能力，并通过分析各类人群的行为特征模式，利用先进的数理统计技术，进行深度的数据挖掘，不断修正风险决策模型，对各个流程进行科学有效的管理，将风险控制在合理范围内。

据我所知，目前银行业对于信贷风险的常见评级方法之一是通过打分法来进行的。即基于业内长期经验，从众多风险的指标中选择若干指标，并对各个指标给予适当的权重水平，设定各个指标具体数值。进而将授信对象的具体数据代入评级体系中，分析各个指标的打分情况。

这里有要介绍另一种基于机器学习和算法的反欺诈评分模型，既神经网络模型。基于神经网络的评分模型在当前的数据挖掘过程中具有特殊的地位，它能够使模型在不断的学习中逐步成长。本文会大致介绍将神经网络的数据挖掘方法应用于小额信贷数据的过程，探索适用于互金的信用风险评判的模型。

神经网络是一种通过模仿人脑信息，类似于大脑神经突触联接的结构加工过程的智能化信息处理技术及进行信息处理的数学模型，与博弈论中的动态博弈很相似，具有自适应性、自组织性以及较强劲的稳健性，在应用过程中具有很强的鲁棒性和容错性，能够并行处理方法，具有自学习性。拥有自组织、自适应性和很强的信息综合能力等良好性能，能同时处理定量和定性的信息，能很好的协调多种输入信息关系，适用于处理复杂非线性和不确定对象，能成功的应用于多种不同的信息处理。

如下图 :



1. **新技术**

5.1.NOSQL数据库应用(REDIS缓存)

Redis是一个使用ANSIC编写的开源、支持网络、基于内存、可选持久性的键值对存储数据库。

数据模型 :

Redis的外围由一个键、值映射的字典构成。与其他非关系型数据库主要不同在于：Redis中值的类型不仅限于字符串，还支持如下抽象数据类型：

字符串列表

无序不重复的字符串集合

有序不重复的字符串集合

键、值都为字符串的哈希表

值的类型决定了值本身支持的操作。Redis支持不同无序、有序的列表，无序、有序的集合间的交集、并集等高级服务器端原子操作。

持久化:

Redis通常将全部的数据存储在内存中。2.4版本后可配置为使用虚拟内存，[7]一部分数据集存储在硬盘上，但这个特性废弃了。

目前通过两种方式实现持久化：

使用快照，一种半持久耐用模式。不时的将数据集以异步方式从内存以RDB格式写入硬盘。

将数据集修改操作记录起来。Redis能够在后台对只可追加的记录作修改来避免无限增长的日志。

同步:

Redis支持主从同步。数据可以从主服务器向任意数量的从服务器上同步，从服务器可以是关联其他从服务器的主服务器。这使得Redis可执行单层树复制。从盘可以有意无意的对数据进行写操作。由于完全实现了发布/订阅机制，使得从数据库在任何地方同步树时，可订阅一个频道并接收主服务器完整的消息发布记录。同步对读取操作的可扩展性和数据冗余很有帮助

应用 :

(一)在业务上,加上REDIS缓存,提升响应速度

(二)部署REDIS的数据备份,实现快速主备切换

5.2大数据处理技术

系统应建立在基于大数据处理理念和能力的技术平台上，该平台应具有极强的数据处理能力，需能够处理银行当前和未来10年发展的数据处理能力需求，需能够提供较强的扩展能力. 该平台在达到上述需求时的软硬件成本应在合理范围内。

5.2.1 Apache Hadoop

Apache Hadoop是一款支持数据密集型分布式应用程序并以Apache 2.0许可协议发布的开源软件框架。它支持在商品硬件构建的大型集群上运行的应用程序。Hadoop是根据谷歌公司发表的MapReduce和Google文件系统的论文自行实现而成。所有的Hadoop模块都有一个基本假设，即硬件故障是常见情况，应该由框架自动处理。

Hadoop框架透明地为应用提供可靠性和数据移动。它实现了名为MapReduce的编程范式：应用程序被分区成许多小部分，而每个部分都能在集群中的任意节点上运行或重新运行。此外，Hadoop还提供了分布式文件系统，用以存储所有计算节点的数据，这为整个集群带来了非常高的带宽。MapReduce和分布式文件系统的设计，使得整个框架能够自动处理节点故障。它使应用程序与成千上万的独立计算的电脑和PB级的数据。现在普遍认为整个Apache Hadoop“平台”包括Hadoop内核、MapReduce、Hadoop分布式文件系统（HDFS）以及一些相关项目，有Apache Hive和Apache HBase等等

5.2.2 Apache Spark

Apache Spark是一个开源集群运算框架，最初是由加州大学柏克莱分校AMPLab所开发。相对于Hadoop的MapReduce会在运行完工作后将中介数据存放到磁盘中，Spark使用了内存内运算技术，能在数据尚未写入硬盘时即在内存内分析运算。Spark在内存内运行程序的运算速度能做到比Hadoop MapReduce的运算速度快上100倍，即便是运行程序于硬盘时，Spark也能快上10倍速度。Spark允许用户将数据加载至集群内存，并多次对其进行查询，非常适合用于机器学习算法。

使用Spark需要搭配集群管理员和分布式存储系统。Spark支持独立模式（本地Spark集群）、Hadoop YARN或Apache Mesos的集群管理。在分布式存储方面，Spark可以和HDFS、 Cassandra、OpenStack Swift和Amazon S3等接口搭载。Spark也支持伪分布式（pseudo-distributed）本地模式，不过通常只用于开发或测试时以本机文件系统取代分布式存储系统。在这样的情况下，Spark仅在一台机器上使用每个CPU核心运行程序。

应用:

(一)提取用户特征

(二)异常侦测

# 三、银联数据配套方案

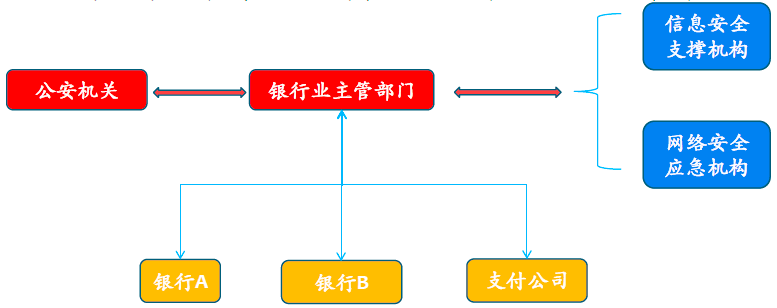
综合以上监管要求的现状以及各个银行做的比较好的人性化的功能，我觉得我们可以在我们的微信银行或者APP上增加一个安全锁功能，当然应当比民生现有的安全锁功能更加丰富。现在很多对卡片的设置，都是行内人士在发卡系统上对卡片的各种参数进行设置，可以考虑把一部分的设置权限下放到APP里由持卡人自己进行设定。

也就是说我们可以在民生银行安全锁功能基础上再增加上交易次数、交易金额、额度调整、交易渠道、卡片类型等功能的设定。

四、关于交易反欺诈的思考——建立体系（反欺诈联盟）

建立金融业整体交易欺诈监控防范体系，实现对金融业电子服务渠道中的欺诈事件实时监控、应急处理、信息共享的统一管理。

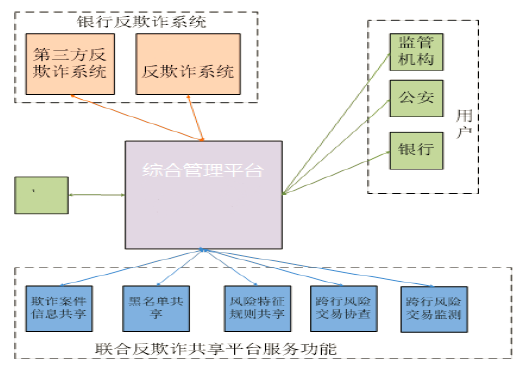
**关于体系建设的设想**：建立起由公安机关、银行业主管部门、信息安全支撑机构、网络安全应急机构和金融机构组成的总体架构。



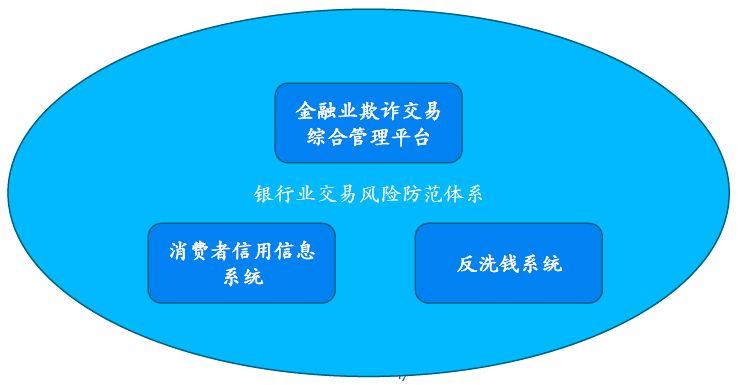
公安机关：黑名单数管理、发起跨行嫌疑交易风险信息协查活动、确认钓鱼网站；

银行业主管部门：欺诈案件信息共享、黑名单管理、灰名单管理、风险特征发布、跨行风险协查、跨行风险预警、金融业务系统漏洞库发布、钓鱼网站监测及钓鱼网站数据库发布、信用违约交易监测发布、反洗钱黑名单数据发布功能。

金融机构：上报案件、黑名单上报分享、灰名单上报及分享、风险特征规则分享、配合跨行风险交易协查、跨行风险交易预警及处理、金融业务系统漏洞分享、钓鱼网站报告、信用违约交易信息接收、洗钱黑名单分享功能。



银行业交易欺诈综合管理平台



金融机构、第三方支付公司应做好准备工作: 建立电子银行交易监控和反欺诈系统；制定交易欺诈风险管理规则。

五、数据挖掘在交易欺诈侦测中的应用

2 数据挖掘介绍

2.1 什么是数据挖掘

从技术上定义，数据挖掘（Data Mining）就是从大量的、不完全的、有噪声的、模糊的、随机的实际应用数据中，提取隐含在其中的、人们事先不知道但又有潜在用途的信息和知识的过程。这个定义包括以下几层含义：数据源必须是真实的、大量的、可能含噪声的；发现的是用户感兴趣的知识，并具有可接受、可理解、可运用的特点；发现的问题是具体的、特定的。

从商业角度看，数据挖掘是一种新的商业信息处理技术，其主要特点是对大量业务数据进行抽取、转换、分析和其他模型化处理，并从中提取辅助商业决策的关键数据。

简而言之，数据挖掘可以描述为：按企业既定业务目标，对大量的企业数据进行探索和分析，揭示隐藏的、未知的或验证已知的规律性，并进一步将其模型化的方法。

2.2 数据挖掘技术

最常见的数据挖掘技术包括分类预测、聚类分析、关联分析、演变分析以及异常诊断。

1) 分类预测

主要使用历史数据建立分类预测模型，并用所建立的模型对未来数据进行分类预测，可用于解决离散型数据和连续型数据的分类预测问题。主要包括树型结构的分类、基于规则的分类、最近邻居法、递归法、人工神经网络法、绘图法，以及向量机等。

2) 聚类分析

主要是指通过无指导学习将一个数据集的所有数据点划分成多个簇，相似数据处于同一簇中，不同簇的数据差异性较大。聚类分析方法包括K-均值聚类、自组映射、高斯混合模型、分层聚类、子空间聚类、图形算法以及基于密度的算法等。

3) 关联分析

主要是从海量数据中高效、准确地发现强相关性事件，对于发现隐藏在数据中的事物的内在联系有很大的帮助。方法包括关联规则分析、链接分析和统计相关计算等。

4) 演变分析

用于描述随时间变化的对象的变化规律或趋势。演变分析方法包括时间序列分析、序列或周期模式匹配，以及基于相似性的数据分析等。

5) 异常诊断（又称为偏差检测）

主要用于搜寻并发现数据中的异常点或异常时间。一种常见的异常监测方式是构建一个数据的正常行为档案，并用它来计算其他观测对象的异常指数，可以挖掘识别规则范围外的行为或其他异常行为。包括基于统计原理、距离和聚类分析的异常诊断技术等。

2.3 数据挖掘与传统分析方法的区别

数据挖掘与传统数据分析（如查询、报表、联机应用分析）的本质区别是：数据挖掘是在没有明确假设的前提下去挖掘信息、发现知识，数据挖掘得到的信息应具有先前未知、有效和实用三个特征。先前未知的信息是指该信息是预先未曾预料到的，即数据挖掘是要发现那些不能靠直觉发现、甚至违背直觉的信息或知识，挖掘出的信息越是出乎意料，就可能越有价值。在商业应用中最典型的例子就是一家连锁店通过数据挖掘发现了小孩尿布和啤酒之间有着惊人的联系。

3 数据挖掘在交易欺诈侦测中的应用

业务的发展和欺诈风险的变化，以及欺诈威胁的全球化和集团犯罪趋势，加大了欺诈犯罪的隐蔽性，增加了欺诈风险识别的难度。过去使用基于规则引擎的交易欺诈侦测，当一条交易提交给规则引擎时，规则引擎将其与加载在引擎中的业务规则进行匹配，看是否属于欺诈交易，然后根据判断结果激活那些符合当前数据状态下的业务规则，最后根据业务规则中声明的执行逻辑，触发应用程序中对应的操作。

但是欺诈交易识别是一种相对复杂的过程，能否有效识别已发生的欺诈交易，并对未来可能发生的欺诈模式做出预测，在很大程度上取决于所采用的识别方法、技术和手段的有效性。由于交易方式的多样性、交易主体行为的不确定性和交易记录的时变性，在交易欺诈识别领域，单一规则引擎方法往往存在适用性、效率和条件约束等问题，难以对交易的整体可疑度进行判断。要达到理想的识别效果，必须在深入分析交易信息的基础上，结合领域知识，选择科学合理的算法和信息汇总判定方式，综合各种检测方法发现的可疑线索，对交易记录的可疑度做出快速准确的整体判定。

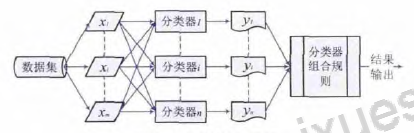
交易欺诈侦测是根据银行卡交易行为特征，将交易划分为正常交易或欺诈交易，其实质是一个分类问题，因此基于银行卡历史交易数据，利用数据挖掘中的分类学习算法，建立侦测模型。

决策树是数据挖掘中常用的分类工具，它是一个预测模型，代表的是对象属性与对象值之间的一种映射关系。树中每个节点表示某个对象，每个分叉路径则代表某个可能的属性值，而每个叶节点则对应从根节点到该叶节点所经历的路径所表示的对象的值。决策树作为一种归

纳分类算法，可以生成可理解的规则，可以清晰地显示哪些字段较为重要。然而目前大多数的决策树研究都只集中在单变量决策树，即决策树的每一个分类节点上都只检验一个分类属性，例如著名的ID3，C4.5等。这种单变量决策树的节点个数非常多、一棵子树在整棵决策树中重复出现，或者有的属性在某一条路径上多次被检验，这些都造成整棵树的规模很大，生成的规则随之变得复杂。同时对于那些各类别样本数量不一致的数据，在决策树当中信息增益的结果偏向于那些具有更多数值的特征。从交易历史样本统计特征显示，欺诈交易样本远远少于正常交易样本，即样本数据存在类别分布非均衡问题。为了解决单一分类器的不足，考虑利用组合的思想构造分类器，力图提高整体分类的效果和精度。

3.1 随机森林介绍

分类器组合的目的就是充分利用每个分类器的优点，挖掘分类器之间的互补性。图1显示了一个分类器组合的简单示意图，x为数据集中的元素，每个分类器对于一个样例都有一个分类结果y，通过分类器的组合规则，则可以决策出最终的类别。



分类器组合示意

通过组合分类器可以显著提高对样本数据的精度，

克服单个分类器分类的片面性。但是组合分类器通常也

需要更多的模型训练时间，分类结果也很大程度上取决

于基分类器的选择。

随机森林[3]（Random Forests）是一种组合分类器方法，它是一个包含多个决策树的分类器，并且其输出的类别是由个别树输出的类别的众数而定。为了得到随机森林，经常引入随机向量来控制每棵决策树的生长，通常为第k棵决策树生成随机向量θk，且θk独立同分布于

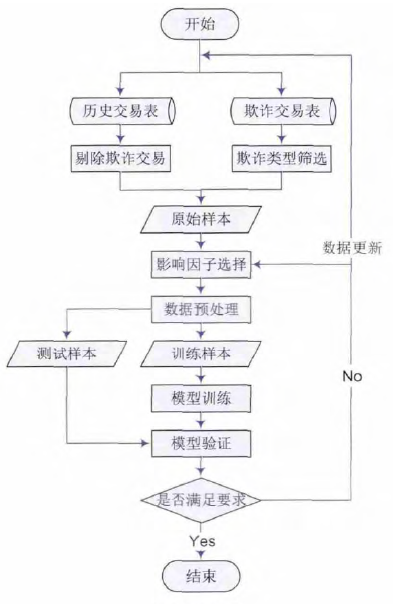
前面的随机向量。用训练集和随机向量θk生成一棵决策树，得到分类模型，其中X为输入变量（自变量）。通过上述方法构造不同训练集增加分类模型间的差异，可提高组合分类模型的外推预测能力。k轮训练后，可以得到一个分类模型序列，再用它们构成一个多分类模型系统，该系统的最终分类结果采用简单多数投票法。

随机森林引入两个随机性：①训练每棵树时，从全部训练样本中随机选取一个子集进行训练，用剩余的数据进行评测，评估其误差；②在每个内部节点，随机选取所有属性的一个子集作分裂属性集，以这个属性子集上最好的分裂方式对结点进行分裂，使得随机森林同单棵树分类器相比，对噪声、离群点以及过拟合更加鲁棒。

大量的理论和实践研究都证明了随机森林具有很高的预测准确率，对异常值和噪声具有很好的容忍度，且不容易出现过拟合，能够有效地处理大数据集，可以处理没有删减的成千上万的输入变量，能够在分类过程中给出变量重要性的估计，在不平衡数据集的类别总体中可以平衡误差，且运行速度非常快，是目前数据挖掘算法最热门的前沿研究领域之一，因此考虑基于随机森林构建交易欺诈侦测模型。

3.2 基于随机森林的交易欺诈侦测

基于随机森林的交易欺诈侦测建模需要进行影响因子选择、数据准备、数据预处理、模型训练以及模型验证等步骤。



建模流程

1) 影响因子选择

模型的影响因子特征变量分为原始变量和衍生变量。其中原始变量是直接从交易数据中获取的，为原始数据的某个字段，不需要再进行加工运算的，如收单机构标识码、发卡机构标识码、交易代码、交易渠道、交易金额、交易时间、商户类型等。而衍生变量是对原始字段进行加工、组合、统计而获得的变量。考虑到欺诈交易之间具有一定的相关性以及卡片的历史交易统计情况，衍生变量包括上笔型、历史特征型和历史统计型。其中上笔型变量从字面上就可以理解，即记录当前交易的卡片的上一笔最近的交易信息。历史特征型变量包括卡片首次交易时间、历史最大成功消费交易金额、卡片近期在高风险国家地区发生的交易笔数等。历史统计型变量即针对卡片和商户分别统计一段时期内的平均交易金额、成功交易笔数、失败交易笔数等信息。

2) 数据准备

在正常环境下，欺诈交易发生的概率很小，欺诈交易数量仅占很少一部分（<1%），因此，交易数据具有很大的不平衡性，不能按正常交易与欺诈交易1：1的比例生成训练样本，否则无法真实还原到生产数据；也不能将此比例设的过低，否则真实交易会完全掩盖欺诈交易的特征。从近两年的欺诈交易表和历史交易表中抽取欺诈交易数据和正常交易数据，分别生成训练样本及测试样本。

3) 数据预处理

数据预处理主要通过数据清洗、数据集成、数据归约、数据变换等方法对样本数据进行空值处理、异常值处理、连续值离散化、字符值数字化以及数据归一化处理，从而使样本数据满足模型训练要求，提高模型的训练学习效果。

现实世界的数据常常是有噪声、不完全的和不一致的。数据清洗过程就是填补遗漏数据、消除异常数据、平滑噪声数据，以及纠正不一致的数据。

数据集成操作，即将来自多个数据源的数据结合在一起并形成一个统一数据集合，需要解决模式集成、冗余和数据值冲突检测与消除等问题。

数据归约技术可以用来得到数据集的规约表示。比原始数据集小的多，但仍接近于保持原始数据的完整性。也就是说。在归约后的数据集上挖掘将更有效，仍然产生相同（或几乎相同）的分析结果，数据归约的策略包括维归约、数量归约和数据压缩。

在数据预处理阶段，数据被变换或统一，使得挖掘过程更有效，挖掘的模式更容易理解。数据变换包含平滑处理、合计处理、属性构造、规范化、离散化等。

4) 模型训练

主要采用两种方式进行模型的训练，一是采用开源软件Weka训练模型；二是采用开源的分布式框架Mahout进行模型训练，Mahout基于Hadoop分布式系统可以进行海量数据的模型训练。

5) 模型验证

使用混淆矩阵、召回率、精度等指标对模型效果进行评价，其中欺诈交易的召回率、精度是欺诈交易侦测重点关注的指标。

混淆矩阵是模式识别领域中一种常用的表达形式，它描绘样本数据的真实属性与识别结果类型之间的关系，是评价分类器性能的一种常用方法。

总体来说，召回率和精度越高，则模型质量越好。需要指出的是，这两个指标是一组对立的关系，需要针对实际的业务，找到一个平衡点。对于应用于实时拦截的模型，要求精度非常高，而对于应用于事后调查的模型，要求召回率比较高。

该实现方案在云计算平台上实现大数据的处理和分析，其优点是企业无需进行基础设施建设，硬件设施对最终用户是抽象的、透明的，系统能力可按需扩大或缩小，使用Hadoop分布式计算平台云服务完成大数据的处理和分析，极大地简化了大数据系统的线上部署和监控管理流程。

4 结束语

随着大数据时代的到来，技术不断向前推进发展以及应用需求不断快速变化，这些变革都推动了大数据价值的重新定义。正因为大数据的应用产生了巨大的甚至是难以估量的价值，未来越来越多的企业将加入大数据应用的浪潮，去发掘和利用大数据隐藏的价值来服务于企业自身的发展。本文讨论了大数据应用总体架构的设计原则和参考模型，同时结合一个企业级大数据应用的案例说明了在如何实际中应用这些原则和参考模型。本文可作为建设企业级大数据应用的架构参考。