美团点评技术团队

美团点评业务风控系统构建经验

义哲 ·2017-01-13 18:20

本文根据“第八届中国系统架构师大会”演讲内容整理而成。

背景

美团最初以团购的形式出现，到现在有了很大的业务形态转变。尤其是经过与大众点评的业务融合，从单一业务发展成了覆盖到店餐饮、到店综合、猫眼、外卖、酒店、旅游等多个垂直领域的综合性电商，并且在各个领域都处于行业领先的地位。在这背后，美团点评不仅面临激烈的行业竞争，还有黑色产业（以下简称“黑产”）带来的各种风险，因为我们的业务有这样一些特点：

- **品类多、覆盖面广**：包括几乎所有吃喝玩乐服务，其中不乏容易被销赃的品类。
- **用户多、商户多**：美团点评拥有6亿以上用户，400万以上合作商家，覆盖了很大部分国内网民和商户。
- **交易高频**：每日订单峰值突破千万。

美团点评对黑产有着巨大的吸引力，归纳起来在这些方面尤其突出：

- **用户作弊**：大家常说的“薅羊毛”，用户为了骗取促销优惠的作弊行为。
- **商家刷单**：常见的有刷排名、刷销量、刷好评等违反商家平台协议的行为。
- **账户和支付安全**：公民信息盗用形势已经十分严峻，黑产从业者会在电商平台上盗取用户的余额，或使用他人支付信息来消费。

这些行为严重侵害平台用户和商户的利益、扰乱正常交易秩序，处理结果的好坏将决定整个业务的成败。所以美团点评需要一套灵活高效的风险控制系统和工作机制来防控这些风险。

归纳一下，风控系统面临的挑战有：

- **业务多、风险点多**：上面提到的风险涉及到各个业务的购买流程、用户操作、商家操作等多个场景。
- **变化快**：黑产的攻击手段升级，自身业务在变化，互联网环境也会不断变化。
- **我在明、敌在暗**：平台在明处，但攻击者是谁、会在什么时候出现、用什么方式进攻却无法预知。

接下来就以风控面临的这几个挑战为出发点，介绍我们在系统构建中所取得的经验。

系统构建经验

挑战一：业务多，风险点多

回到风控工作的起点，在了解业务所面临的风险类别后，首先要面对的问题就是：怎样才能知道有风险，并且能够控制风险？我们很容易想到，为了做到这些必须与业务系统对接，这部分系统我们称之为“对接系统”，它的目标抽象来说就是：**感知风险**和**控制风险**。

“**感知风险**”是指要收集尽可能完整的数据。风控需要关注：**谁、在什么时候、通过什么方式、对什么对象、做了什么**？这句话抽象概括了要感知的内容，绝大多数信息都可以套用到这句话。

第二个目标是“**控制风险**”。如果仅仅站在防守方的角度看，并不容易知道应该控制哪里；我们应该站在攻击者的角度思考：攻击者关注什么？答案是利益。以美团点评为例，可带来的利益有：

- **促销优惠**：相关的风险场景有下单、支付、购买、验券等。
- **商家销量和排名等**：涉及购买、搜索、销量展示等页面。
- **用户余额**：即需要控制登录、查看余额等动作。

以这样的角度排查，就不容易漏掉风险点。排查清风险点后，实际对接工作也有很大挑战：美团点评的细分业务有100多个，很多业务都有多种用户终端（iPhone, Android，H5，PC等）、多个业务后台（促销工具，商家后台等），需要对接的场景数量很多。所以感知风险、控制风险背后最大的挑战是如何与业务方紧密配合顺利对接。

在配合中，业务团队常顾虑因风控需求拖慢业务开发速度，而风控也常感到业务团队配合不足。在配合的问题上，应该先充分认识两个团队合作的目的，就好像生产汽车和生产安全气囊，安全气囊在大多数国家已经是汽车生产销售的必须要求；同理，在现今互联网服务中，安全配备也已经成为了用户体验、业务需求的一部分，一个忽略安全的产品，终究会被市场淘汰。另一方面对风控而言，业务发展是风控存在的前提，如果风控的安全需求影响到业务发展也是不合理的，因此风控要提高服务质量，让对接带来的负担降到最低——这就是对接系统设计的核心目标。

总结一下，**风控工作经验一：安全是业务的必要属性，没有安全保障的产品，终究会被市场淘汰； 风险控制要服务于业务，减少业务对接负担。**具体而言，业务接入风控的成本主要有**接入成本**和**运行成本**两方面。下面分别来看我们在风控系统构建中的做法。

接入成本

风控系统最早只是业务系统中的一个函数，逐步演化成了独立的服务。而这个独立服务与业务后台的交互最初时也沿用了旧的思路，即业务后台在关键动作前调用风控服务判断“有没有风险”。但这样每次新增加一个业务或新出现一个风险场景时，风控和业务都要重新对接联调。这样频繁地调整给上下游团队都带来了不小的负担，在频繁的更改中系统质量也难以保证。

换个角度看，其实还有更好的交互方式：当风控要保证账户操作环节的安全，可以让用户中心直接与风控系统对接。即业务系统调用用户中心，用户中心再调用风控透传风控所需参数，而风控的决策也通过用户中心返回给业务后台。这样的好处是只需要用户中心与风控对接一次，业务系统甚至不需要明显感知到风控的存在。同样的道理，与商户中心、支付环节的交互也可以采取类似的设计方法。这样的改造相当于把风险控制的“责任”从业务方移交给了中间件，即由中间件来保证提供安全的服务。这样理顺系统模块间的关系，从而降低整体开发成本。

运行成本

业务接入风控系统后，尤其关心运行过程中的是否会有问题。风控系统要尤其关注以下这些方面：

- 服务稳定性
    - 隔离部署：在对接的众多后台服务流程中，哪些是核心流程、哪些是非核心流程，需要隔离开防止相互影响。
    - 依赖降级：风控策略需要实时依赖大量外部数据接口和存储，依赖越多稳定性问题发生的概率越大，相应的熔断、降级机制不可缺少。
    - 限流防刷：业务尤其是高风险业务随时可能因爬虫、恶意攻击而造成流量突增。系统需要具备识别和拒绝这些恶意流量的能力，而不是放任其消耗业务后台和风控系统的计算资源。为了做到这一点，风控系统不应仅位于业务系统的调用下游，而要在全局流量入口处插入反爬防刷模块来实现整体控制。
- 服务性能
    - 风控与业务对接可以大致分为两类：
      ① 同步控制接口，返回风控决策并由上游实时处理。
      ② 异步信息收集接口，主要目的是收集数据提供风控决策依据。异步接口可以显著减少上游服务的阻塞时间。
    - 最初风控策略硬编码在代码中，对运行过程的优化也以人为调整代码为主，但策略调整频繁，运行优化无法跟上策略调整，而且策略复杂度提高后，人为优化代码也不再现实，因此需要在运行时动态决定运行策略才能达到最好的优化效果。这点通过规则平台来完成，**将在后文中“规则平台”中介绍。**
- 风控运营
    - 风控策略不可能做到完全精确，为了降低业务损失很多情况下要以牺牲一部分用户体验为代价，因此完善的用户运营保障不可或缺。这在后文的“运营系统”中会提到。

挑战二：变化快

具备感知风险和控制风险的能力后，**实现风控策略**就是第二个关键问题。最初的策略可以很简单，比如此时我们认定：“穿黑衣服的是坏人”。类似策略运行一段时间后会出现有意思的现象：“坏人会逐渐换上其他颜色衣服”。这也很好理解，攻击者不会持续做无效的攻击浪费资源，而是会转向其他进攻手段。这样旧策略反而只会影响到一部分正常用户——观察到的结果是策略准确率下降。这样的情况无法避免，因为——**风控工作经验二： 风控是一项长期的对抗性工作。**

那么我们首先要加强**策略健壮性**。还用上面的例子，攻击者很容易发现后台针对黑衣人的策略。但如果策略复杂一些，识别“穿黑衣服而且戴黑帽子的人”有问题，那么策略被暴露的概率就低了很多。但这会影响策略的覆盖面，所以需要更多的策略形成策略网共同作用。假设极端一点，把能想到的识别要素都用上，制定策略也就变成了模型训练问题，通过机器学习来制定策略会有更好的健壮性。不过这只是理想情况，现实并没有这么乐观。风控所面对的真实场景中正样本和负样本数量差距悬殊，而且攻击模式在持续变化，导致这并不是稳定的算法问题。所以实际工作中人工介入制定专家规则并与算法策略结合使用是更有效的方法。

涉及到长期对抗的工作，**效率高低**将是对抗效果的决定性因素。风控需要多种角色配合，典型如：开发者建设系统、策略制定者制定规则策略、产品角色把策略应用到合适的场景。让这些角色并行不悖就是工作的理想高效状态。“规则平台”就是我们用来达到这一状态的秘密武器。

规则平台

为了解耦**系统开发**和**策略开发**，需要让策略执行过程标准化。我们把策略划分成几个层次：

- **场景**：对应规则集合，一个场景包含若干条规则。
- **规则**：是最小的决策单元，一个规则包含多个因子。
- **因子**：因子是组成规则的最小逻辑单元。

上下两层之间都是多对多的关系。这样划分后，所有策略都套用标准化的执行过程，并能达到最大程度的配置复用。此外还有一个好处，就是将策略配置从代码中抽离。旧的策略执行过程是用硬编码预先编写好，对执行过程代码调优十分复杂，即使调优也只能针对特定的策略配置。如果策略改变了，原来的优化可能就不再适用。通过配置执行策略后，执行过程也变成动态的。具体来说，运行时会根据请求来决定需要计算哪些场景、规则和因子，每个元素计算且仅计算一次，没有相互依赖的部分放入多个线程并行处理。通过这样的优化，效率和性能得到大幅度提高。

再看**策略开发**和**决策应用**。最初实际工作中这两者耦合在一起不加区分，即针对特定场景开发特定策略。逐渐暴露出一些问题，比如场景会变化、会新增，那原有的策略是否还适用？一个策略是否只能使用固定的决策动作？为了让这两部分工作并行，需要从设计定位上就把两者区分开。即：

- **策略**：是为了识别一些特定的问题，例如“是不是模拟器请求”，“该用户是不是新客”。
- **决策**：是针对场景的应用，如拒绝、验证手机短信等。

规则平台设计让每个场景可以应用不同策略，命中策略后的决策也可以灵活定制，甚至可以配置多个决策，并设置不同优先级。

验证中心

上文中的“决策”代表系统是否信任该请求，风控背后的工作也围绕这个“信任”而展开。拒绝不信任的，放行信任的。但还有不少情况是中间不足以确定的部分，常见的处理方法是需要让用户补充验证信息来辅助判断。最初实现的验证流程是：风控服务识别风险后返回决策给业务系统，由业务系统实现验证的完整交互过程。这样存在两个问题：

- 首先业务方很多，不同的业务需要重复实现验证流程，造成重复开发。
- 其次验证种类有很多，从较弱可信度的短信验证，到较高可信度的银行卡验证等——风控能返回什么样的决策受限于特定场景业务方的实现了什么验证支持。

这些问题对于业务和风控系统造成了不小麻烦。所以我们需要优化这一过程，让验证过程由一个独立的服务——验证中心来完成。业务系统从风控服务获得风险决策，再与验证中心交互完成验证。从风控的角度看，以前的处理方式称作“只管杀，不管埋”，优化后可以称之为“杀埋一条龙服务”。

除了规则平台、验证中心，我们还抽象出了累计服务、处罚中心、算法平台等服务来提升风控对抗效率。

挑战三：我在明，敌在暗

风控与黑色产业的对抗有个天然的不利因素，就是风控团队需要防御所有短板，而对手只需要找到薄弱的环节进攻。面对进攻，我们可以建立相对完善的实时策略体系和工具系统，但如果仅寄希望于实时策略解决所有问题也是不现实的。即使策略再优，黑产、业务、环境都在变化，仍然可能留有漏洞，或者陷于疲于应付的境地。这样的现实需要风控团队视角更宽广一些——**风控工作经验三：要从事中防守扩展到立体事前、事中、事后防御。**

在风险事前，要注意提升防御能力，减少防御短板：

- **风险教育**：在快速发展的业务中，风险控制的核心在于人，要将风险意识和基本概念传递到业务的各个阶段，明确告知风控可以提供的服务。
- **参与业务**：参与到业务的产品流程中，了解高风险业务、活动的规则，预判风险并给予合适力度的干预。
- **数据准备**：打通数据收集流程，制定预警规则、模型策略等。
- **主动防护**：关注业界风险动态，发生行业安全事件后，或重大活动、产品改动上线前，制定有针对性的规

则，甚至采取锁定高危账户、发送预警消息等措施。

在风险事后，要快速响应，灵活管控。客户投诉是风控了解策略效果的最重要指标之一。 针对风险场景，风控还要主动关注异常数据，实现“预警”监控。这些反馈都会进入**运营工作流**做处理。 运营工作流中，尽管各风控产品具体流程不同，都可以划分为初步受理、核查审理、案件处理三个步骤，对应着以下三个系统。

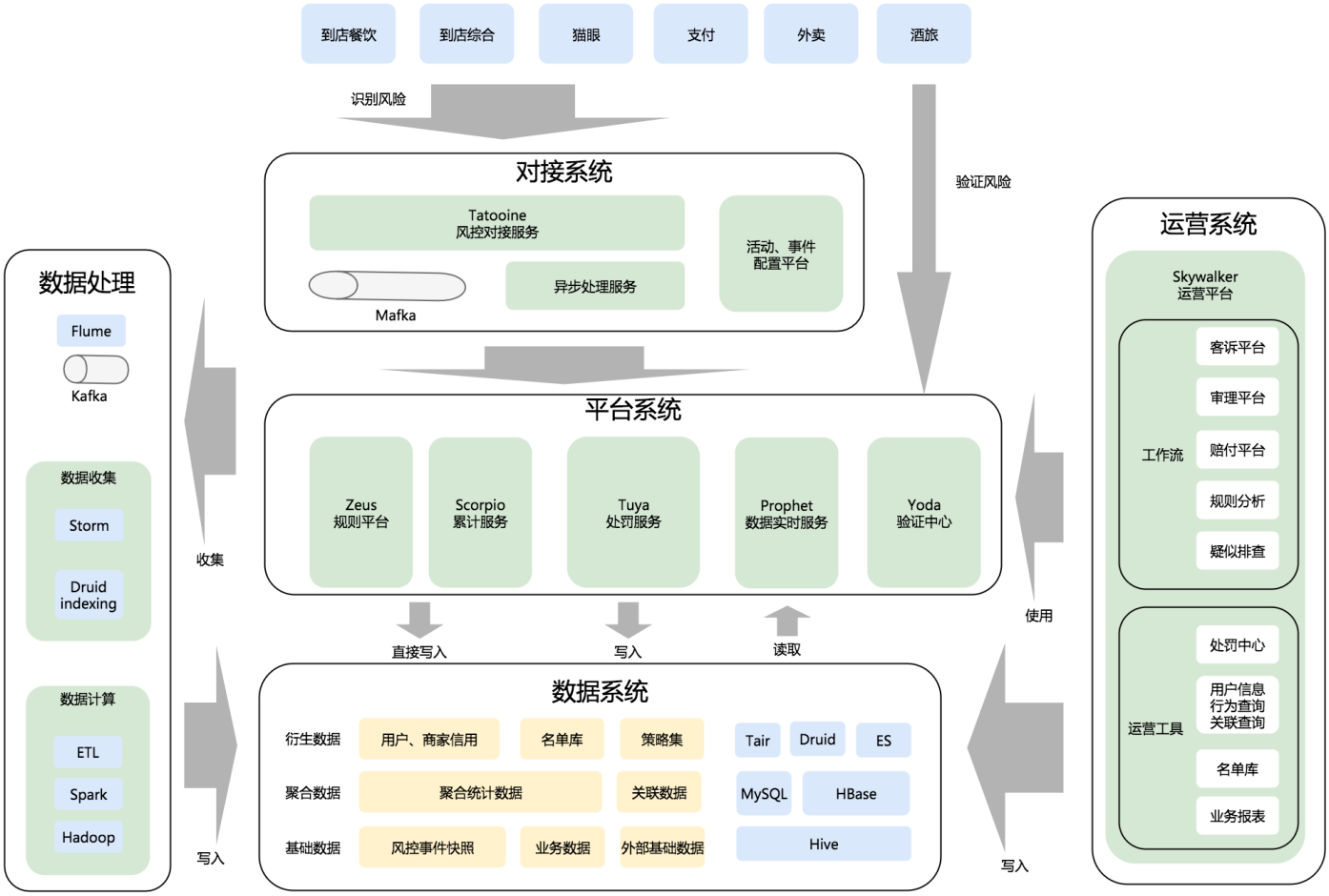
- **初步受理**：主要用作初步筛选案件，决定是否需要进入下一步骤。其流程较为简单，系统的设计目标是让风控运营人员可以便捷的处理案件，因此处理效率是其中的重要衡量指标。
- **核查审理**：用于详细核查案件，通常有多步骤流程，不同角色以其专业视角做判断。核查过程中需要大量数据支持和处理系统支持，因此有了**运营支持系统**。
- **案件处理**：确认且涉及到资金损失的案件需要进入赔付流程。因为涉及到资金赔付，精确的权限管理是系统设计和实现时需要特别注意的问题。

运营平台的意义不仅在于处理案件本身，更在于将处理结果反馈到线上系统中实现风控线上和线下的运行闭环。除了运营平台，逆转信息劣势还要靠完善的数据体系的帮助。风险控制所使用的数据可以这样分类：

- **事件快照**：原始而完整的信息，用于生成聚合数据，也是支持运营查询的主要数据源。
- **聚合事实**：相比于原始的事件记录，更多使用场景更关心聚合的结果，例如某用户、某商家的历史购买次数。经过聚合整理后的数据，是进一步数据挖掘的基础。
- **衍生信息**：指基于事件快照和聚合事实衍生出的理解信息，例如用户的作弊风险、设备的可信程度、黑白灰名单等。这些衍生信息可以适配到各个特定场景中使用。
- **基础数据**：除了直接传递到风控的数据外，风控处理过程少不了需要业务甚至是外部的辅助信息。例如，业务相关订单和活动信息、公认的事实数据、外部辅助决策信息等。

小结

把上面三部分融合起来，可以看到风控系统的全景：



风控之道

从上文三条风控工作原则可以看到，风控系统构建过程各个阶段的关注点从对接质量，到平台效率，再过渡到立体的闭环防御。但即使系统发展到了相对成熟的阶段，与黑产的斗争也远没有结束。为了更好的对抗，我们要从对手身上学习：

- 黑产链条经过长时间的实战优化，分工极为细致。风控团队也应该学习这样的思路，将服务功能切分到细粒度以更好适应变化。
- 黑产对利益极为敏感，甚至很多时候比业务开发者还要了解业务。风控团队只有比对手更了解“主场”——也就是自身业务，才有可能在对抗中取得主动。

如果把风险控制比喻成一场战争，还可以从军事理论中得到借鉴。《孙子兵法·谋攻篇》中的一段描述就十分贴切：“知可以战与不可以战者胜，识众寡之用者胜，上下同欲者胜，以虞待不虞者胜，将能而君不御者胜。此五者，知胜之道也。”类比到风控工作中，风控团队需要考量：

- 控制风险是否现实
- 团队人才质量和数量是否足够
- 团队价值观是否统一
- 对风险是否足够了解
- 是否得到上层支持