实时控制系统

作者：gentoo666

原文链接：https://ld246.com/article/1496842872480

来源网站：链滴

许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

<h2 id="1-课程名称">1、课程名称</h2>
实时系统
<h2 id="2-课程目标">2、课程目标</h2>
1、了解电子商务交易的风险点
2、了解电子商务交易中风险点的处理策略
3、利用 Storm 技术开发基于规则判定的风控系统
4、掌握企业中风控系统的一般架构和业务流程
<h2 id="3-背景知识">3、背景知识</h2>
<h2 id="3-1-信用卡的交易风险及常见策略">3.1、信用卡的交易风险及常见策略</stron></h2>
<h3 id="3-1-1-用户逾期风险控制">3.1.1、用户逾期风险控制</strng></h3>
用户主动、被动对正常消费的金额产生逾期
通过滞纳金进行处理
<h3 id="3-1-2-虚假交易风险控制">3.1.2、虚假交易风险控制</h3>
<h4 id="3-1-2-1-配合商家进行虚假交易">3.1.2.1、配合商家进行虚假交易</4>
通过中介公司、皮包公司，在该机构虚假下单，扣除一些的返点。
<h4 id="3-1-2-2-找朋友刷单刷卡">3.1.2.2、找朋友刷单刷卡</h4>
朋友较大金额的购物行为、聚餐、公司聚会的时候。
<h4 id="3-1-2-3-利用系统漏洞进行虚假交易">3.1.2.3、利用系统漏洞进行虚假交易</strng></h4>
案例：1 万元透支额度的信用卡，是怎么被套现 99 万元的
Ø 骗子弄到一台 POS 机，那是 A 银行授权合肥一家商铺的。
Ø 骗子将 10 万元现金，存入陈某信用卡。陈某信用卡原有 1 万元信用额度，加上这 10 万元，某的信用卡额度就到了 11 万元。
Ø 骗子给陈某的信用卡分 10 次发起预授权：112 元、113 元、138 元、137 元、121 元、157、123 元、126 元、137 元、158 元。预授权后，钱被冻结。
　　这里说的预授权，简单来说，就是第三方冻结，也可以算是保证金。比如预授权 158 元，就是帮合肥这家商铺将 158 元冻结。正常情况下，假如交易完成，并且消费者用现金等方式将货款交，那么就可以将 158 元这笔预授权解冻。
Ø 骗子从信用卡中取出 9.9 万元。（一次性取 10 万以上，银行报警系统将对该卡发出预警，银同时将冻结该账户，所以只能取 9.9 万元。）
Ø 骗子将 158 元这笔预授权撤销，信用卡恢复原有额度 11 万元。
　　这里利用了一个漏洞：预授权一撤消，信用卡自动会恢复成完整额度—本案就是 1 万元。
　　接下来，重复上面的程序，每次取出 9.9 万元，再将 1 笔预授解冻，再取 9.9 万元，再解冻…
　　就这样，从 8 月 4 日晚上 11 点 50 分到 8 月 5 日凌晨，骗子总共取现 99 万元。
<h4 id="3-1-2-4-通过支付通道进行套现">3.1.2.4、通过支付通道进行套现</4>
在可以支持信用卡支付的网站上进行购物，下单后取消订单。订单金额会退到用户在网站的账户，然后将资金提现到储蓄卡。
<h3 id="3-1-3-伪造申请信息风险控制">3.1.3、伪造申请信息风险控制</h3>
使用他人身份证信息申请信用卡，然后恶意透支。将恶意透支的风险转嫁给他人。
案例：从发达地区购买西部人员的身份证信息，先办理储蓄卡，伪造账户流水。然后使用流水申信用卡，最后通过以上一种或者几种方式恶意透支信用卡。
<h2 id="3-2-淘宝商家交易风险及常见策略">3.2、淘宝商家交易风险及常见策略</stron></h2>
郑重声明：
以下内容来自互联网，这里只分析现象，不鼓励不支持刷单，请营造良好购物环境。</trong>

<h4 id="3-2-1-淘宝商家刷单">3.2.1、淘宝商家刷单</h4>
<h5 id="3-2-1-1-刷单现状和起源">3.2.1.1、刷单现状和起源</h5>
1、古有“十个淘宝九个刷，还有一个做批发”
2、今有“刷单可能会死，不刷那是必死”，特别是中小卖家
3、某大师说，刷单就像是吃鸦片，吸了会死人的，不吸会生不如死！
当然有些人一直倡导不刷单，倡导各种优化。
<h5 id="3-2-1-2-为什么要刷单-">3.2.1.2、为什么要刷单？ </h5>
本性：人人都想走捷径，每个人都想被破格获取，和中国人凡事都托关系，走后门一个道理，基国情完全适用于商业环境。
现状：
Ø 当我们老老实实做各种内功优化时发现根本不起作用，因为隔壁高手刷出来的数据比我们做内的各项数据都完美，销售额远远超过我们。别人都在刷，没办法，大环境推动着我们去做。
Ø 如果不刷下，如果只靠老客户，那需要浪费多少时间呢？时间成本耗不起，特别是季节性产品女装）。
Ø 活动想尽快报名，不刷下怎么活？
Ø 上了活动，平台不给力，成交不好，下次小二还不给机会，我们怎么活？
Ø 如何应对？小刷怡情，狂刷伤身！
一定要做好内功，做好各种优化，适当补一点，这样才能不死，才能长长久久！
<h5 id="3-2-1-3-刷单的作用-从轻到重-">3.2.1.3、刷单的作用（从轻到重） </h5>
ü 提升信誉——主要以新店为主，买家购物会去参考店铺信誉，在新开店低信誉店下单的可能性相对来说比较低，所以新店大多数都会通过刷单去提升店铺信誉。
ü 刷动态评分——也就是我们常说的 DRS 评分（商品描述、服务态度、货速度）。新手买家可能不懂 DSR 评分的来由，不怎么去考虑，但老买家肯定会去考虑评分的问题因为这是除信誉外，衡量一个店铺的重要标准。而且很多活动也要求动态评分高的才能通过。不过刷分也只能起到一点点作用，并不是长久的法子。最主要的是还是产品，服务等因素。再配合一些辅助段来提高评分，这只是略提一下。当然，有需要的朋友也可以这样操作。
ü 刷退款时间——跟刷评分一样，也是刷数据，骗骗淘宝，请人拍下不点货就直接申请退款，申请好之后就立刻处理掉退款。反正退款率不影响，而且又可以降低退款时间。
ü 提升宝贝销量——提升宝贝销量的好处非常多。
l 活动需要!都是要求有一定销量，一定好评才可以去报名的。
l 破零!买家都是有从众心理的，零销量的宝贝，图片再好，描述再棒。也很难让顾客下定决心购。
l 提升转化率!销量高，好评多的产品，购买者云集。
l 提升点击率！销量高，付款人数多，点击率肯定大一些，对排名至关重要！
l 高手过招，卡位，干死竞争对手必备！SEO 搜索优化的朋友应该都知道自然搜索排名，7 天销量与 30 天销量，都是一项很重要的因素。
l 销量高、排名好，可以获取更多亲睐，包括官方资源！
ü 刷直通车点击、转化降低 PPC——很多新人朋友不理解，直通车点一下要花钱的，还有人专门去刷这个，那不是很浪费？这是新人的疑惑，但了解直通车的朋友一定知道，击率和转化率是提升直通车质量得分的最重要的两个因素，提升直通车点击率转化率可以为直通车推广省掉很多钱。但这也仅限刚开直通车的时候刷，长时间没效果，那要考虑产本身和图片点击效果的问题了。
ü 活动辅助刷销量——这里说的活动，主要是官方的活动（聚划算、天天价）。大家去看聚划算（参考服装类目为主），有卖的好的，有卖得差的。行业中流传着这么一句话参加聚划算的商品，根据开团前 10 分钟销量，可以看出一上午能卖多少件。根据开团前两小时的销，能看出一天大概能卖多少件。聚划算的顾客，都是参团，图便宜来的。绝大多数人的从众心理是非强的，销量高的产品会引起顾客的强烈购买欲望，也非常容易冲动的去下单，即使是不喜欢的产品（要是说女性，女性购物，冲动性是非常强的）。而销量低的产品，即使再喜欢，也会犹豫再三是否要买。
所以，建议各位在参加官方活动，开团时不妨请人拍个百八十件，对活动会起到不一样的效果。在这里就有人反映了，官方活动数量卖完了系统就会下架了，请人拍了百八十件，后面拿什么卖给其

顾客？ 这个其实很简单，等销量引爆到一定程度，就可以让你请拍下的人申请退款，现在退款率是不响店铺排名的。
参加聚划算活动的朋友就要仔细一点了，因为聚划算活动要入库，由良品仓代发货，请人拍的订，有可能会被良品仓发走，所以大家可以考虑让拍的人购买多款产品，一般良品仓是不发这类的订单。具体操作方式，可以根据活动情况做改变。
刷单的作用还是非常多的，暂时只总结了以上这些。以后想到了，再做补充（部分借鉴）
<h4 id="3-2-2-刷单处理策略-降权的因素">3.2.2、刷单处理策略-降权的因素</h4>
<h5 id="3-2-2-1-成长趋势">3.2.2.1、成长趋势</h5>
宝贝各方面成长的速度是否符合逻辑。
例如，比如你的宝贝排名在几十页后，每天通过这个页面成交确实几十笔，这种成长趋势就是诡的，系统严查的。刷单一定要根据关键词的排名逐渐提升。
<h5 id="3-2-2-2-点击率">3.2.2.2、点击率</h5>
点击率是判定违规的重要维度，也是卖家常常忽略的维度
比如：关键排名在 50 页，每天差不多 300 展现，而你的点击量确是 100 多，远远超过行业 点率，毫不疑问，刷的嫌疑。
<h5 id="3-2-2-3-转化率">3.2.2.3、转化率</h5>
与同类目同层级的均值相差不大是最稳当的宝贝转化率，突然超出或低于太多都会对宝贝的权重生影响。转化率稳定高于一切，千万别忽高忽低！
<h5 id="3-2-2-4-硬件信息">3.2.2.4、硬件信息</h5>
一定要物理硬件，淘宝太简单就可以查询出来了，别在傻乎乎的去用云服务或者没有任何修改的 PS 刷了，灭你就在瞬间！
<h5 id="3-2-2-5-快递环节">3.2.2.5、快递环节</h5>
能够查询到的快递时间和你发货的时间、顾客确认收货的时间是否匹配，不存在时间错误，这是统重要监控的环节，能够直接看卖家是否有录入假单号的嫌疑。
再者，物流重量和发货地是不是常用发货地，购买空包单号的要注意了！
<h5 id="3-2-2-6-时间段访客数和成交">3.2.2.6、时间段访客数和成交</h5>
非正常时间和地域交易的宝贝，同一天中的不同时间段，访客数都会有一定的虚假性，对于系统说，是不是稍微有点诡异呢
<h5 id="3-2-2-7-页面访问时间和深度">3.2.2.7、页面访问时间和深度</h5>
单品页面停留时间一定是淘宝审查的重点，在正常情况下，一个宝贝会带给其它页面至少一次以的点击。
<h5 id="3-2-2-8-旺旺聊天">3.2.2.8、旺旺聊天</h5>
聊天不是根本，喜欢静默下单的顾客为数不少，看你的宝贝页描述是否已经诠释了他当时购买时所有问题。聊不聊由你！
<h5 id="3-2-2-9-小号问题-黑号封杀">3.2.2.9、小号问题，黑号封杀</h5>
说到黑号，淘宝现在严打比较厉害，淘宝的严打反而让刷单更安全了，淘宝会限制小号登陆，让小号的商家中垃圾小号死的差不多了。当然如果说到号的问题，商家基本无能为力，只能要求周不 5 不过 15 了，防止刷手号变成黑号！
刷客号不稳定，若你的小号都是异地登录或未满月的，该小号在注册时，不要忽略了淘宝已经将的电脑信息、 IP 地址记录在案。若你的刷客号是刷手买来的，还没有稳定就直接开刷，这样的刷客在超过一定比例的情况下，也会被淘宝发现，从而降权处理。
个人观点：淘宝不会花那么多功夫去查号的问题，比如现在秒刷依然存活！
<h5 id="3-2-2-10-买家行为分析">3.2.2.10、买家行为分析</h5>
刷手的行为，比如是不是货比了，是不是秒开，是不是刷单前一定要去某些网站验证小号的安全
是不是多次同一 IP 登陆不同的号购买你的产品等等
<h5 id="3-2-2-11-手机刷单问题">3.2.2.11、手机刷单问题</h5>
手机刷单不会比 pc 端权重高，在 2015 年 2 月份淘宝小二官方已经证实， 手机端安全问题目前无法证实，个人观点，可能会安全一点，因为手淘是新鲜事物，特别还涉及到通信问题，检测有漏洞理之中。
<h5 id="3-2-2-12-流量入口的问题-个人感觉-">3.2.2.12、流量入口的问题（个人感觉）</h5>
很多大神都说淘宝只会检测单品的转化率，我不这样认为，如果这样的话直接访问的流量也可以

和转化率吗？那就是天方夜谭，也许只有你自己信！
淘宝的防作弊一定是单通道的，某个关键词的转化率或者点击量超高，我都能看出来数据异常了淘宝工程师都是傻子吗？
<h2 id="3-3-京东商家交易风险及常见策略">3.3、京东商家交易风险及常见策略</h2>
郑重声明：
以下内容来自互联网，这里只分析现象，不鼓励不支持刷单，请营造良好购物环境。
案例(来自网络)：
我只记得京东没上市前小二找我做业绩，扣点 3%，现在上市了，不能那么明显，怎么弄，你做 10w，我给你返 4w，自营的更狠，开秒刷机一天十几万单眼睛都不眨一下。现在啥行情我不知道，也问我自己做的哪家店，反正是 TOP，被小二知道不好。这行情还被抓，我只能呵呵了！
中国现在的电商环境不好，刷单是避免不了的问题，京东的品牌团、硬广、商务舱一圈测试下来都亏得一塌糊涂，回到原点还是刷成本最低，当然，这也分类目，我只说自己的经验。今天讲讲刷单基础篇，因为京东有时候刷单不是了排名流量，不过等大家到那级别自然就知道是什么原因了。
不管是京东还是淘宝或者其他平台，换位思考下，为啥给你排名，很简单，你产品好买家喜欢，平台也有钱赚，那就是好产品。所以现在淘宝很流行的持续增长刷法绝对是行通的，基本原理就是尽量模拟一个真实的持续增长的产品，给系统一个错觉——【这是个好产品】。
原理很简单，回归各平台，既然是模拟一个好产品那每个平台侧重的权重不一样的，好评率、停留时间、客单价、销量、收藏量等等等等。
对京东来说，目前销量权重无疑还是排在第一位的，类目排名默认的都是销量排名，不过这里要注意下：京东 7.8 月份就开始改版，部分类目出了一个综合排序，我刚才翻了下男女鞋、部分服装类目都已经是综合排序了，这个算是好事，京东亏了这么多年，现在开始朝更健康方向发展了，不过这要一个时间和过程，综合排序的权重销量仍然是第一的，然那么多商家一个产品刷了几十万进去还不得去京东总部去。后续会怎样，大家自己琢磨。
销量权重最大，不过可不是销售额，当然我有次为了完成小二业绩一款直接刷了十几万，没天这款就冲到第一页去了。不过这有个前提，那就是小二睁只眼闭只眼，现在单笔销售额的权重有多我不敢试，被抓不划算，在京东刷单请记住：不要太明显！
<pre><code class="highlight-chroma">所以现在主流的刷法还是以销售量和客单价为主，一单刷几件，京东要挣钱，你的客户同样的产在你这一次买1000，别人家买500，你说京东在哪挣钱多？以商人的思维去做京东会很简单，刘强东一名成功的商人，是商人就好办，有利益什么都可以谈。
</code></pre>
除了公认的销售量和客单价这俩权重外，京东有一个容易被忽略的权重，那就是买家晒单，我自经过测试每十个评价 1 个晒单效果是比单纯评价要好的。当然权重所占总比例不是很大，这也是大家到几十个评价就能排到前几名的原因，销量权重最大！至于其他的，停留时间、收藏量等权重各不相，我比较懒没有系统的测试，只抓最重要的几个权重打天下。如果要想利益最大化，一定要执行和测，测试自己类目适合自己的刷法。
销售量权重是有时间周期的，京东的排名每天晚上 10 点一更新，系统重新计算，而且是以结算单为准，切记，不是销售量。做类目排名销售量一般计算的是 7 天，关键词的每天一计算，所以一般过的单我们是要在七天内确认收货才能达到最大的效果。
目前我认识的几个比较好的同行刷法一般是两种，一种是连刷几天然后在某一天全部确认收货，种刷法特别适合做类目排名。我一般用的是第一天刷，隔两天就确认收货，排名的增长每天都看得到而且可控，被抓风险也低。
还是那句话，刷单不要太明显，有钱就去放单，没钱的改换 IP 的还是要换，换 IP 工具自己淘宝刷单账户自己淘宝。有实力就去做类目排名，京东客户比较懒，2.3 页的流量和第一页的没法比，款、价格、描述都合适，冲到第一页分分钟就是订单啊。没实力的去做关键词排名，刷关键词就好，收

方法二选一。一般时间周期都是 7 天，也就是说你不管做类目还是关键词排名，执行到位 7 天就够了

新人会问了，新店没流量怎么去测试产品，呵呵，看你眼光了！我没啥眼光，所以前期做主推款了不少冤枉钱，后期有流量基础就好做了，拿去测试就好，放到关联里哪个好卖卖哪个，一推一个准

<pre><code class="highlight-chroma">这里**再教新店一个省钱的办法，刷基础评价用店铺优惠券刷**，首页链接放到某个角落里，满50减300问题不大，能省一笔扣点，不过切记，做几个基础评价就好，多了被抓别怪我没提醒过你，至刷排名就不要用券，意义不大。
</code></pre>
刷单只是方法，产品一塌糊涂没有核心竞争力在京东刷单就是找死，京东扣点不是所有人的吃得消的，所以，新手们，听哥哥一句劝，做流量前，给自己一天时间，看看店铺修上档次不，关联、闭环做好没，主推款市场上再比比扶不扶得起，库存跟不跟的上。
<h2 id="3-4-京东白条-淘宝花呗交易风险及常见策略">3.4、京东白条、淘宝花呗交易风及常见策略</h2>
据《证券日报》深入调查后发现，这些中介往往会收取不菲中介服务费，一般 10%-30% 比例，至更高。一些所谓的“中介”机构通过各种网络渠道发布消息，招揽有套现意愿的用户，并联系提供现业务的商家，三方隐蔽合作，试图躲过花呗及白条风控，实现套现。
个人用户套现意愿者-------中介-------商家（刷单）
个人用户套现意愿者-------机构-------商家（刷单）
个人用户套现意愿者-------中介-------商家（刷单）
<pre><code class="highlight-chroma">常见的诈骗分子通过蚂蚁花呗及京东白条套现方式大致分为几种类型：
</code></pre>
l 账号被盗，不法分子利用被盗账号套现;
l 骗取客户信息，冒名申请蚂蚁花呗及京东白条进行套现;
l 账户转借他人，被利用套现还款纠纷频发;
l 自己刷单赚取差价的套现行为;
l 配合中介合伙套现，反被骗取个人信息。
很多消费者参与花呗与白条套现之后的结果是套现不成，反倒掉进骗子们设下的陷阱里。 在打套现的行动中，京东也有所动作。据了解，在这 90 单中，京东的违规交易拦截系统拦截了其中 95% 以上的交易，而那名钻空者已被公安机关带走。不仅如此，蚂蚁花呗更为了打击套现清理上上千家涉套现的不法商家。
案例一：京东白条“天网”系统精准识别”撞库”，保护客户账户安全

 近日，京东金融“天网”风控系统预警发现一个北京客户的账户在多个设备终端登录,该账户次下单购买实物订单套现均被“天网”系统预警拦截，失败未果后转而给一个湖南的手机号充值。由该账户之前多次触发“天网”系统预警，案件升级至反欺诈案件调查人员进行处理，调查人员随即拨了被充值的电话号码，接电话的人一听到是京东打来的电话后立即挂断，这立刻引起了京东金融风控队的重视。
经过调查，该号码持有者是一名湖南男子，他是一名计算机狂人，依靠黑客技术从某个网站上窃用户账号及密码信息，然后到其他网站进行撞库，于是发生了本案例中的实物订单被拦截转向手机充的尝试，被白条“天网”系统抓了个正着。据了解，不法分子通过撞库进行登陆支付等尝试行为，都被“天网”风控系统察觉，并纳入敏感账户信息库，当该账户再次使用时便会被自动追踪，若证实不本人操作，白条风控便会启动风控拦截。
<pre><code class="highlight-chroma">以上信息来自公开资料。
</code></pre>
案例二：京东白条“天网”系统嗅出猫腻，坚决打击商家中介合伙套现行为

 炎炎夏日，一家京东商城第三方商家，被监控到有异常白条交易订单陆续产生，异常原因在夏天陆续不断有京东白条用户在其店铺购买羽绒服，每个账户买好几件，价格也明显高出市场价格。店铺监控来看，销量呈爆发性增长，并多数使用京东白条支付。这些异常行为同样被“天网”系统进预警，吸引了案件调查人员的关注。经调查，该第三方商家通过互联网发帖介绍，提供配合套现服务

招揽有套现需求的不良用户，引导用户到该店用京东白条下虚假订单，按订单金额收取“套现服务费。
案例三：通过平台进行套现
<pre><code class="highlight-chroma">在互联网上以QQ群组为例，搜索“京东白条套现”的关键字，会出现诸多以此为业的商家。而些商家打出各种京东白条套现、商品代收等广告和攻略，甚至与极少数不良第三方卖家联手，以虚假单为用户提供所谓京东白条套现服务。
</code></pre>
更有甚者，网络中介提供所谓的强开白条技术，要求这些安全意识淡薄的用户提供身份证、银行等机密个人信息包开京东白条，结果用户被中介欺骗，进而出现账号被盗、被骗等情况。
<h2 id="3-5-滴滴打车及企业其他交易风险">3.5、滴滴打车及企业其他交易风险</h2>
l 电商搞活动，发代金券，如何通过技术手段保证这些代金券不被黄牛抢了去；
l 秒杀活动，如果保证不被个别人通过多个小号、或者工具自动秒杀；
l 发红包，红包抵扣现金。
如何知道访问你的网站的是一个真实的人，而不是一个机器或者是刷子；
央广网北京 10 月 10 日消息 据中国之声《新闻晚高峰》报道，近日，海淀检察院以涉嫌诈骗罪准逮捕了全国首例通过“滴滴打车”软件进行刷单套现案件的嫌疑人常某。
　　常某的丈夫唐某是一名出租车司机，其在运营拉客过程中得知可通过领取滴滴打车优惠券方刷单赚钱。常某得知后花钱向他人购买了刷单软件并学习刷单技术。随后，常某在滴滴打车平台上注司机账户领取平台发放的打车优惠券，然后通过虚构打车交易事实，再将领取的优惠券向其注册的司账户支付，最后提现完成套现过程。常某供述，其在短短几个月内就通过刷单非法获利 3余元。
　　办案检察官介绍，对于互联网背景下的新型化犯罪行为，全国范围内入罪先例并不多。本案全国首例以诈骗罪对刷单行为人进行入罪定性的案件。
<h2 id="3-6-扩展-百度贴吧风险控制">3.6、扩展：百度贴吧风险控制</h2>
首先用户想要发帖，那么咱先得有个账户吧。那么第一步：注册账号。咱开始先假设大伙都是好，那咱就注册吧，不需要啥门槛，随便填个东西咱就注册了一个账号。注册来注册去，突然发现，咋么多水军呢，10 个人里 8 个不是我们想要的用户，咋办？ 注册加门槛吧！恩加一个图片验证码。图验证码加上，诶？10 个人里有 5 个是水军了。不错有点效果，但是还是不行，咋办？验证码升级！片变成短信验证码！这下 10 个人里只有 1 个是水军了，恩 效果不错。咱就开始发帖吧！！
<pre><code class="highlight-chroma">作为一个重视用户体验的产品，咱要满足用户的需求。用户想发啥就让他发啥吧。唉唉唉？这帖怎么回事？ “包小姐13XXXXXXXX” 包小姐是谁？**这么发不是等着警察叔叔来抓么！**还得做点制，恩，咱把带包小姐3字的帖子给过滤了。恩 效果不错，包小姐、李小姐刘小姐都过滤了一遍。突，妈蛋人家不写字了，开始发色情图片了。这咋办？ **没事咱技术实力强！咱弄个黄色图片识别.....这样不断的拉锯，加语义识别、加文本分析、加ocr识别、加行为识别、加人工审核。**终于贴吧变了现在的样子，能过滤掉绝大部分的虚假帖子。但是依然会有一些虚假信息没有被干掉，但是我相信一个反欺诈的同学都在不断的为了让更少的人被骗、让骗子不在有可乘之机而努力着。

借用罗永浩的一句，因为我们在不断的努力，我们让这个世界美好了一点点。就是这样。
</code></pre>
<h2 id="4-电商交易风险类型总结">4、电商交易风险类型总结</h2>
<h2 id="4-1-电子商务风险分析">4.1、电子商务风险分析</h2>
<h3 id="4-1-1-互联网络的开放化带来的数据破坏风险-拖库-">4.1.1、互联网络的开放化来的数据破坏风险（拖库）</h3>
电子商务是以互联网络为平台的贸易新模式，它的一个最大特点是强调参加交易的各方和所合作伙伴都要通过 Internet 密切结合起来，共同从事在阿络环境下的商业电子化应用。在电子商务环境商务交易必须通过互联网络来进行，而互联网体系使用的是开放式的 TCP / IP 协议，它以广播的形式行传播。容易受到计算机病毒、黑客的攻击，商业信息和数据易于搭截侦听、口令试探和窃取，给企的数据信息安全带来极大威胁，如遭破坏或泄密，将会给电子企业、商户造成巨大的损失。
<h3 id="4-1-2-系统软件安全漏洞带来的风险-软件开发漏洞-乌云网-">4.1.2、系统软件</h3>

全漏洞带来的风险（软件开发漏洞，乌云网）</h3>
由于现阶段广泛应用的主流操作系统和数据库管理统是从国外引进直接使用的产品。核心技术还是使用引进的版本。这些系统安全性存在系统漏洞等不危及信息安全的问题，例如：Windows 操作系统中存在着的漏洞和陷门，就不断引起世界性的“冲波”和“震荡波”，存在极大风险。系统软件安全漏洞带来的风险主要来自操作系统软件和数据库管系统软件的安全漏洞。操作系统软件处于硬件和上层应用的中间环节，可以提供对网络系统、数据库应用软件、用户的认证管理等，提供全方位的保护。没有作系统的保护，就不可能有网络系统的安全也不可能有应用软件信息处理的安全性。由于操作系统是唯一紧靠硬件的基本软件，其安全职能是其软件安全职能的根基；另外，数据库作为信息的聚集体，是电子商务系统的核心部件，由于数据库的全在很大程度上依赖于数据库管理系统，而数据库管理系统在操作系统下都是以文件形式进行管理的因此入侵者可以直接利用操作系统的漏洞窃取数据库文件，或者直接利用操作系统工具来非法伪造、改数据库文件内容，从而危及到电子商务交易的数据安全。
<h3 id="4-1-3-来自社会的外来入侵风险-钓鱼网站-">4.1.3、来自社会的外来入侵风险(鱼网站)</h3>
电子商务容易被来自社会上的不法分子通过互联网络非法入侵，主要表现形式是黑客和病毒等对子商务系统的文件和数据的篡改和破坏，是一种社会道德风险。黑客通过闯入他人计算机系统进行破，这些人利用电子商务系统和管理上的一些漏洞，进入计算机系统后，破坏或篡改重要数据，盗取机与资源，控制他人的机器，清除记录。设置后门，给电子商务系统带来灾难性的后果。而计算机病毒人为编写的一组程序，可以攻击电子商务系统的数据区、文件和内存，以致使计算机的硬件失灵，软瘫痪。数据破坏，系统崩溃，给企业和商户造成无法挽回的巨大损失。
<h3 id="4-1-4-电子商务本身内部监管漏洞带来的风险-刷单风险-">4.1.4、电子商务本身部监管漏洞带来的风险（刷单风险）</h3>
电子商务本身如果缺乏约束机制，责权不明，管理混乱、安全管理制度不健全等是引起电子商务统安全风险的头号风险根源。如果没有严格的可操作性的内部管理制度，容易造成当系统出现攻击行或受到其它一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警而且，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对系统的可控性与可查性。
<h2 id="4-2-电子商务交易运行的风险">4.2、电子商务交易运行的风险</h2>
<h3 id="--4-2-1-信用风险----">**4.2.1、信用风险 **</h3>
传统商务交易一般使用以纸为介质形式的手写签名或证明文件等方式来证明或确认商务的交易，该说比较容易辨认真伪，操作显得比较容易。而在基于互联网络为交易平台的电子商务形式下，参与业交易均在互联网上进行，双方并不存在与传统商业模式的见面、磋商、谈判、监证、签署文件等问，这就需要通过一定的技术手段相互认证，如数据加密技术、数字签名、数字证书等技术来保证电子务交易的安全。在电子商务环境下，由于电子报表、电子文件、电子合同等无纸介质的使用，无法使传统的签字方式，从而在辨别真伪上存在新的风险，电子商务的成功与否取决于消费者对网上交易的任程度，电子商务的信任风险实质是由网络交易的虚拟化造成的，首先是买方信用风险。在网络中个可以任意伪造信息，可以伪造假信用卡骗取卖方商品。从而给卖方带来风险。然后是卖方信用风险，于信息不对称的原因消费者不可能全部掌握商家商品信息。卖方商品信息不完全、不准确或商家过分导消费者从而误导消费者购买行为；另外，卖家单方面毁约。不履行交易，也会对买方造成损失。所电子商务应用过程中遇到的信用风险问题，是值得关注的问题。
<h3 id="--4-2-2-法律风险----">**4.2.2、法律风险 **</h3>
电子商务在交易过程中存在法律风险，由于电子商务是在网络间进行的，电子商务交易可以看作无纸贸易，是一个虚拟环境的交易，当前对这些虚拟交易的法律监管却并不完善，这些问题使得电子务认证、交易会有不受法律保护的风险。另外，电子商务贸易还存在知识产权的风险，网络是个开放平台，资源在网络中的传播是畅通的。在网络中资源的共享性使得有知识产权的资源受保护的力度被低，因此可能带来电子商务交易的知识产权纠纷等法律的风险问题。
<h2 id="4-3-控制风险的对策">4.3、控制风险的对策</h2>
<h3 id="--4-3-1-加强技术保证-确保电子商务信息的安全----">**4.3.1、加强技术保证，确保电子务信息的安全 **</h3>
针对电子商务依靠互联网络平台来开展的网络开放性的特点，特别是要针对互联网体系使用的是放式的 TCP / IP 协议，给企业信息和数据安全带来的极大威胁的安全隐患。对如何保障企业的信息数

和重大商业机密，是确保开展电子商务的企业的重要技术保障和前提条件，只有高度重视电子商务的息安全，才能保证其运行安全，这就需要有强大的技术安全保障措施，不但要制定完善的技术保障措，更要严格执行制度，才能确保电子商务信息的安全。例如：我们在企业内部网和互联网之间要加一防火墙，防止黑客或计算机病毒的袭击。保护企业内部网中的机密商业信息数据。另外，利用现有的息新技术将数字签名技术应用于电子商务的身份认证，可以防止非法用户假冒身份，从而保证电子支的安全，增强电子商务信息的安全保障措施是电子商务顺利开展的重要技术保障。
<h3 id="--4-3-2-健全内部控制制度----">**4.3.2、健全内部控制制度 **</h3>
实行电子商务的商户，在内部管理制度上应健全相应的规章制度，例如：制定制度来规范和约束工的行为，根据其工作的重要程度，确定该系统的安全等级。制订相应的机房出入管理制度对于安全级要求较高的系统，要实行分区控制，限制工作人员出入与己无关的区域。对操作规程要根据职责分和多人负责的原则，各负其责，不能超越自己的管辖范围；制订完备的系统维护制度，对系统进行维时。应采取数据保护措施。如数据备份等。另外制定人员激励机制也很重要，应建立人员雇用和解聘度。及时对工作人员进行评价，制定奖惩制度，调动工作人员的工作责任感和积极性。
<h3 id="4-3-3-加强复合型人才的培养">4.3.3、加强复合型人才的培养</h3>
实现电子商务环境是当今全球经济一体化、信息化时代的一种发展趋势，重视复合型人才的培养电子商务成功与否的决定因素。所谓电子商务的复合型人才是指要求电子商务管理人员既要有计算机识，还要有管理理论和商务、金融、法律等知识。对电子商务管理人员进行培训，通过学习现代电子络技术，将经济、金融、法律、网络有机地结合。对商务交易、金融活动的网络化、数字化有比较深的认识，加深对电子商务环境下的风险认识和防范。从而提高员工适应电子商务的工作能力和创新能，更好地开展电子商务这一新兴的贸易模式。
<h2 id="5-电商交易风控系统-需求分析">5、电商交易风控系统-需求分析</h>
<h2 id="5-1-业务问题">5.1、业务问题</h2>
由于公司业务的发展，开发了一种类似信用卡的的产品，如京东的白条、淘宝的花呗，旨在方便户购物时的支付环节。这种产品根据用户的信用额度可以提供一定额度的资金，仅仅用作用户在网站购物使用。
信用：消费记录，征信报告，支付宝好友，余额宝
主要问题：
l 由于用户的信用额度是根据用户在网站的基础信息、行为信息以及少量外部信息计算而来（<strng>用户信用评分），虽然能够给予一定的信用评分来标记这个用户是否可能违约。但是由基础信息和行为信息本身就有造假和被污染的可能，所以对用户的行为购物行为进行风险控制就是业面对的一个很重要的问题。
l 由于用户在很多网站上注册的账号密码一致，用户在 A 网站丢失的信息可能会被黑客拿过来撞，如果撞库成功之后，就会对交易有影响。
l 账号被盗，不法分子利用被盗账号套现;
l 骗取客户信息，冒名申请蚂蚁花呗及京东白条进行套现;
l 账户转借他人，被利用套现还款纠纷频发;
l 自己刷单赚取差价的套现行为;
l 配合中介合伙套现，反被骗取个人信息。
<h2 id="5-2-业务需求">5.2、业务需求</h2>
· 为了解决两类问题，期望针对用户的订单进行分析，对触发规则的订单进行风险预警，在紧急况下，直接对订单进行拦截。（两个步骤：先预警，后拦截）
o 用户是否在常用 IP 下单--------三点一线
o 用户是否在常用设备上下单-----一个妹子刷 120 个手机
o 用户收货地址是否是常用收货地址-----快递单号生成器
o 用户收货手机号是否是常用手机号-----用户手机固定
o 用户近期是否修改过登陆密码---------正常的人不会改密码
o 用户近期是否修改过支付密码---------正常的人不会高频修改密码
o 用户近期是否修改过手机号码-----用户手机固定
o 订单是否是货到付款-------------逃逸？
o 订单中指定价格的商品数量是否满足阈值------羽绒服刷单，夏季
o 订单中指定类目的商品价格是否满足阈值------
o 订单的总价值是否达到一定的阈值------------客单价阈值
<h2 id="5-3-功能需求">5.3、功能需求</h2>

o 系统，自动判定，简单的输入和输出。设置规则（由基础的判断条件组成）、查看清单
o 对触发规则的订单信息进行预警（短信或邮件）
o 实时拦截
<h2 id="5-4-数据准备">5.4、数据准备</h2>
<h3 id="5-4-1-用户在网站上的行为数据">5.4.1、用户在网站上的行为数据</3>
<h3 id="5-4-2-用户的基本信息">5.4.2、用户的基本信息</h3>
如账户信息、收货地址、收货手机号码
<h3 id="5-4-3-用户的订单信息-支付信息等">5.4.3、用户的订单信息，支付信息等</strng></h3>
<h2 id="6-功能实现分析">6、功能实现分析</h2>

用户支付一个订单，产生订单支付 MQ（paymentInfo）

通过 Storm 程序消费订单 MQ，对订单进行处理

o 订单处理需要依赖用户的历史数据，比如手机号、收货地址等信息，需将历史数据保存到 Redis 中
o 订单处理需要读取业务人员的配置的规则数据，需要设计表结构存放规则信息
o 订单处理的过程中，需要将实时的订单分解成基础数据保存到 Redis 中
<ol start="3">

将处理的结果存放到 MySQL 数据库中

通过 JavaWeb 程序展示触发规则的订单信息，供业务人员进行操作和处理

<h2 id="7-原形设计">7、原形设计</h2>
<pre><code class="highlight-chroma">产品经理进行原型设计
</code></pre>
<h2 id="8-架构设计">8、架构设计</h2>
<h2 id="8-1-整理架构设计">8.1、整理架构设计</h2>

从支付系统、日志系统、用户系统从获取用户的离线数据，保存到 Hadoop 集群，并对 Hadoop 集群中的数据进行处理，提炼基础数据。然后经基础数据存放在 Redis 中。

从消息中心实时消费支付系统发送出来的支付订单信息，编写 storm 程序对实时订单信息处理。/p>

storm 程序的主要逻辑如下：

从数据库中读取业务配置的规则数据，规则数据从规则配置系统上可视化配置
对订单不同维度的数据进行校验，将触发规则的信息存放到数据库
<ol start="4">
管理平台从数据库获取触发规则的信息进行处理

<h2 id="8-2-功能模块设计">8.2、功能模块设计</h2>
· 数据收集模块 略，详见 Hadoop 基础
· 离线数据处理模块 略，详见 Hadoop 基础
· 消息中心模块，略，详见实时计算基础之 Kafka 增强
· Storm 程序，负责定时读取规则，实时校验
· 数据模型，主要是规则模型，将用户配置的规则信息保存到数据库中，以及将触发信息保存到据库中。
· 报表系统，略
<h2 id="8-3-数据模型设计">8.3、数据模型设计</h2>
<h3 id="--8-3-1-condition-order-monitor----">**8.3.1、condition_order_monitor **</h3>
用户配置的规则信息，一条规则中有多个条件
<h3 id="8-3-2-rule-order-monitor">8.3.2、rule_order_monitor</h3>
分解出针对订单最小判断条件
<h3 id="8-3-3-paymentinfo-order-monitor-订单信息">8.3.3、paymentinfo_order_monitor 订单信息</h3>
<h3 id="8-3-4-products-order-monitor-订单中的商品信息">8.3.4、products_order_onitor 订单中的商品信息</h3>
<h3 id="8-3-5-trigger-order-monitor--rule-order-monitor--触发规则的订单记录">8.35、trigger_order_monitor``rule_order_monitor 触发规则的订单记录</h3>
<h2 id="8-4-Storm程序设计">8.4、Storm 程序设计</h2>
l KafkaSpout 读取数据，需要配置 Topic。
l PaymentInfoParserBolt，规则加载，校验
l SaveInfo2DB，触发信息保存
<h2 id="9-代码开发">9、代码开发</h2>
<h2 id="9-1-项目结构">9.1、项目结构</h2>
<h2 id="9-2-OrderMonitorTopologyMain-驱动类">9.2、OrderMonitorTopologyMai 驱动类</h2>
<h2 id="9-3-KafkaSpout-从Kafka中读取数据">9.3、KafkaSpout 从 Kafka 中读取数据</h2>
<h2 id="9-4-PaymentInfoParserBolt-规则加载-校验">9.4、PaymentInfoParserBolt 则加载，校验</h2>
<h2 id="9-5-SaveInfo2DB-订单信息和触发信息保存起来">9.5、SaveInfo2DB 订单信和触发信息保存起来</h2>
<h2 id="9-6-OrderMonitorHandler-核心操作类">9.6、OrderMonitorHandler 核心操类</h2>