日益严重的金融欺诈检测问题

根据Juniper Research的调查，仅在线支付欺诈就将在2018年至2023年间使商户损失超过1300亿美元。所有金融服务中的欺诈事件都以惊人的速度增长。LexisNexis最近的一份报告表明，在过去的一年中，金融服务公司遇到的欺诈尝试显著增加，欺诈尝试的次数翻了一番，欺诈成功率提高了85%。

如何改进

让我们来看一个典型付款，这是由在线支付提供商(例如 PayPal，Venmo，Apple 或 Samsung Pay)进行的，通过这个发现潜在欺诈的示例，我们可以知道为什么很难通过常规分析来发现这种欺诈。

消费者User1创建一个新帐户，即帐户1，该帐户已链接到他们的信用卡。作为设置和双重身份验证的一部分，他们已将其电话号码Phone_number 1和其电子邮件地址Email 1链接到其帐户。User1正在使用设备1(具有注册的电话号码的Apple iPhone 6)并发起付款，即向帐户2支付$ 500的付款1。

到目前为止，传统的金融服务欺诈检测解决方案中没有任何危险信号或警告，因为用户1是全新的用户，具有新的电话号码和电子邮件，并且这些都与过去使用付款服务进行的任何欺诈交易无关。常规分析不会发现任何异常或可疑的内容，并且这种付款不会被标记或拒绝。

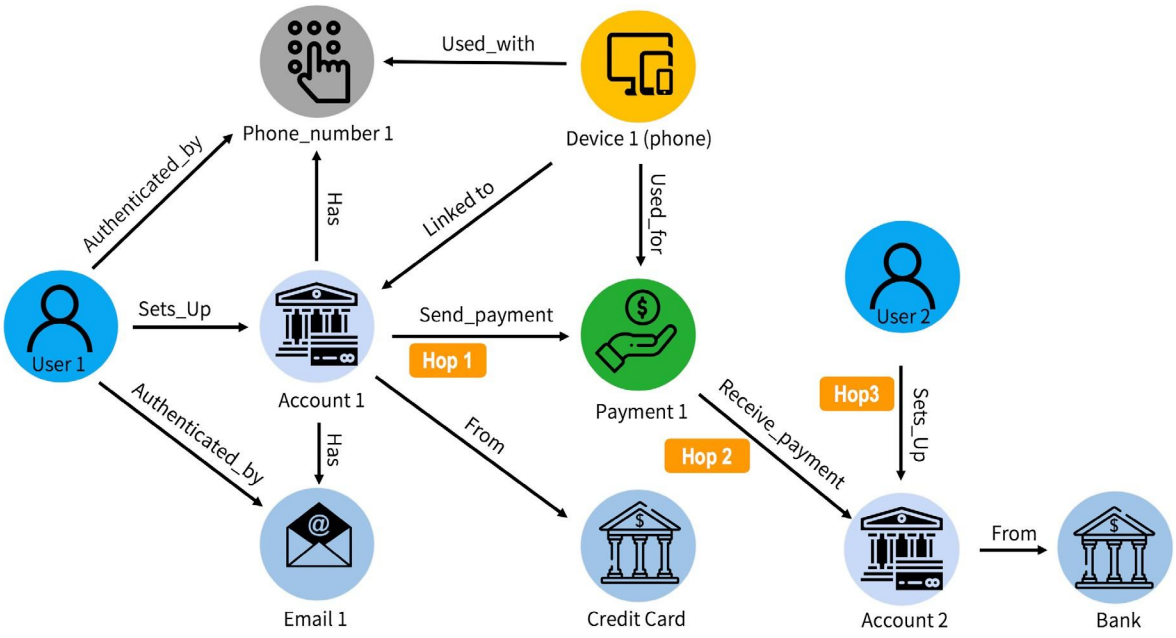

图1-三跳分析未发现欺诈行为

利用高级分析功能对金融服务进行欺诈检测

TigerGraph的高级分析功能可以实时发现与先前欺诈的关系，从而拒绝付款交易。向帐户2付款的接收者帐户属于用户2，该用户已使用电话号码2对帐户进行身份验证。电话号码2与设备101（三星Galaxy S3设备）一起使用。对先前的欺诈交易和相关设备的历史记录的分析表明，设备101与电话号码101一起使用来建立帐户101。帐户101发起了付款101，后者被发现是欺诈的，因为帐户101由被盗的信用卡提供资金。

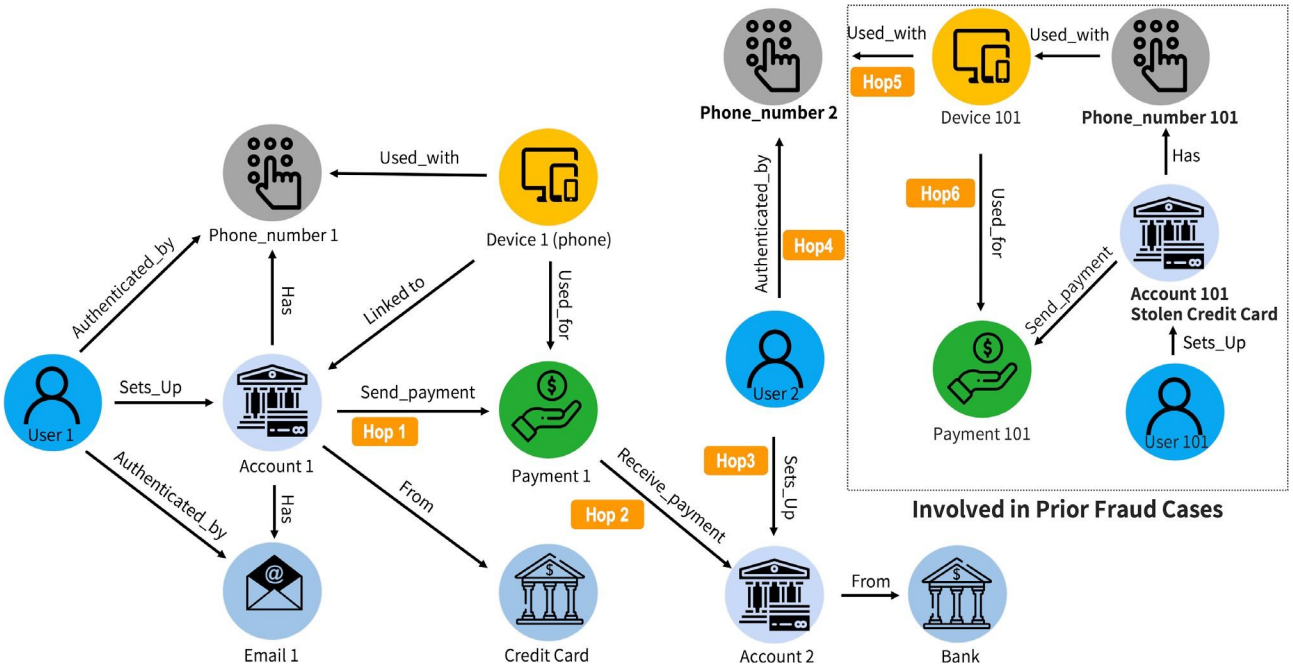

图2-使用TigerGraph进行六跳分析后检测到欺诈行为

提供实时欺诈检测需要三种高级分析功能：

- **交易或可变数据基础结构**-由于付款1是由用户1发起的，因此高级分析解决方案必须能够从付款网关接收它并将其附加到发送方（帐户1），收件人（帐户2）中亚秒级的响应时间。下一步是对连接的数据（图）运行六跳或连接查询。
- **实时深层链接遍历**-高级分析必须运行六跳或连接查询，从用户1开始付款（第一跳）开始，遍历到帐户2（第二跳），然后到达拥有帐户2的用户2（第三跳），然后是与帐户一起使用的电话号码2（第四跳），找到与电话号码2一起使用的设备101（第五跳），　最后从去年（第六跳）遍历到欺诈性付款101。该解决方案必须能够以每秒数千甚至100,000+次的付款量达到高峰！
- **实时计算和更新连接的数据（图）**-最后，为了返回具有亚秒级响应的答案，高级分析必须支持计算，例如查看付款的信任度以查看是否欺诈行为，并执行更新操作，例如将新用户，用户1和用户2标记为可能与欺诈有关的帐户，这些帐户可能需要进行调查，然后才能发送或接收付款。

利用TigerGraph改进金融行业的欺诈检测

基于关系型数据库的传统解决方案可行吗？

传统欺诈检测解决方案主要依赖于对单个业务实体的行为分析，例如客户、公民、设备、医生或医疗保健提供商，从其行为中发现异常模式。欺诈者越来越狡猾，他们建立合成身份网络，将合法信息（如身份证号、姓名、电话和实际地址）与该合成网络相结合。

他们使用通过合成身份创建的虚假帐户进行欺诈，每个欺诈者帐户在外观和行为上都与合法帐户非常相似，这极大增加了传统欺诈检测解决方案检测出欺诈的难度。检测欺诈需要超出个人帐户行为范围，随时间分析帐户组或实体之间的关系，而这通常需要结合来自第三方来源的信息。基于关系型数据库构建的传统欺诈解决方案在设计上无法解决这一挑战。

TigerGraph如何为企业打造反欺诈解决方案？

通过深度关联分析检测欺诈

以一个难以检测的医疗保险欺诈为例，基于关系型数据库构建的传统欺诈解决方案由于固定的模式而难以融合来自第三方的新数据源，并且需要与计算密集型数据库关联，因此无法实现深度关联分析。

为了检测其中的隐藏关系，TigerGraph 通过8 次跳跃来执行深度关联查询，并将其与第三方知识存储库数据（如地址和电话号码）相结合，可以准确地查找到串通。

通过实时分析检测欺

欺诈检测对时间有效性非常敏感。在检测到欺诈之前，每过去一分钟、一小时、一天，您的组织以及您的客户都会遭受更多损失。TigerGraph的实时反欺诈解决方案可以解决这一挑战。

以中国移动某省公司为例，该公司使用 TigerGraph 来分析预付费用户的呼叫模式，以实时检测电话欺诈。当潜在欺诈者呼叫时，用户将收到实时提醒，高可能性的欺诈呼叫将重定向到中国移动的呼叫中心以进行调查。

通过机器学习改进欺诈检测

在电信总呼叫量、医疗和政府福利索赔数据或金融服务支付交易中，经证实的欺诈事件很少，不到 1%。因此，机器学习模型没有足够的训练数据，导致无法提供高准确性的欺诈检测。

拥有原生并行架构的 TigerGraph 专用于解决这一挑战。同样以中国移动某省公司的电话欺诈检测为例，TigerGraph 对每部电话创建了超过 118 项特征属性，通过对 4.6 亿部电话相关联属性的分析，将这些电话区分为可信号码或嫌疑号码。与此同时，它新产生的 540 亿条数据，可以作为训练数据为机器学习算法的自我提升提供支持。 这使得通过机器学习进行欺诈检测的准确性大幅提高，并同时降低了误报率和漏报率。

“到2023年，图技术将促进全球30%企业的快速决策场景化。需要图还是不需要？这已不再是个问题，一定是需要。”

Mark Beyer
Gartner公司副总裁、杰出分析师

TigerGraph 基于互联数据进行高级分析和机器学习

我们的部分客户

AMGEN · intuit · wish · STATE GRID CORPORATION OF CHINA · opencorporates · 中国移动 China Mobile · Paganti's · IPPEN DIGITAL PLATTFORM · Kickdynamic

“一旦我们把一切都建立在图中，我们就可以实时地对变化做出反应。图是我们所做一切的中心。”

Jay Yu博士
Distinguished Engineer and Architect,
Intuit

“使用TigerGraph，我们可以将数据源连接在一起，并在数据中建立以前无法建立的连接。我们现在可以回答过去20年来我们认为不可能提出的问题。”

Harry Powell | 数据与分析 总监
Jaguar Land Rover

认识 TigerGraph:

- 唯一的企业级可扩展图数据库，比竞争对手快40-300倍；
- AI和ML解决方案的基 础平台；
- 支持高并 发的OLTP和OLAP负载；
- 类SQL的图查询语言（GSQL）加速解决方案落地
- 支持本地部署和云部署：Google GCP，Microsoft Azure，Amazon AWS；
- TigerGraph的成熟技术支持欺诈检测、反洗钱、客户360、统一ID、供应链、知识图谱、个性化推荐、人工智能和机器学习等应用。

中国官网：www.tigergraph.com.cn
关注我们：微信，LinkedIn，哔哩哔哩
联系我们：sales_cn@tigergraph.com

几分钟即可免费开始图分析：tgcloud.io

TigerGraph Cloud，一个为敏捷团队构建的，基于云的、易于使用的图数据库即服务。

入门套件	概览
COVID-19 分析	检测感染中心并跟踪潜在传播者的移动
客户360 –归因和参与度图	创建客户旅程的实时360度视图，以了解归因和参与情况
网络安全威胁检测	通过检测相互关联的事件，设备和人员来阻止网络安全威胁
企业知识图谱（企业数据）	分析包括投资者和主要利益相关者在内的公司数据
企业知识图谱(Crunchbase)	带有初创公司、创始人和企业的Crunchbase数据特征的知识图谱示例
实体解析/统一ID（MDM）	通过属性和关系分析来识别，链接和合并诸如客户之类的实体
欺诈和洗钱检测	多种类型的欺诈和洗钱模式
GSQL 101	介绍TigerGraphs强大的图查询语言
医疗保健图（药物相互作用）	针对药品的公共（FAERS）和私有数据的医疗保健示例
医疗保健–推荐网络，Hub（PageRank）和社区检测	分析会员（患者）处方建立推荐网络，确定最有影响力的处方者（医生）并发现相关的处方者社区的情况
机器学习与实时欺诈检测	用于实时检测欺诈并生成基于图的特征以训练机器学习解决方案的移动行业示例
网络和IT资源优化	网络和IT资源图，用于建模和分析硬件中断对工作负载的影响
推荐引擎（电影推荐）	使用公共数据构建的基于图的电影推荐引擎
社交网络分析	用于理解和分析关系的社交网络示例
供应链分析	涵盖库存计划和影响力分析的示例

https://www.tigergraph.com.cn/product/cloud/starterkits/

微信：TigerGraph

TigerGraph.com.cn/link/