中国金融反欺诈技术应用报告

研究机构　零壹财经 · 零壹智库

联合发布　Maxent猛犸反欺诈

零壹财经 · 零壹智库　　maxent 猛犸反欺诈

一

金融欺诈现状

一、全球网络安全形势严峻

世界

网络犯罪是当今商务世界的头号威胁，每年它造成的损失超过4000亿美元[1]。

2017年第一季度全球网络攻击创下新高，超过1.3亿次，增速超过了2016年交易的增速。2016年，以英国为例，英国金融犯罪防范和反欺诈非盈利机构Cifas的国家欺诈数据库和内部人员欺诈数据库共录得325000条欺诈记录，该机构的会员单位共防止了超过10亿英镑的损失。

中国

全球身份欺诈最高发的地区[2]。

仅2015年下半年到2016年上半年，中国网民因垃圾信息、诈骗信息、个人信息泄露等遭受的经济损失人均达133元，总体经济损失高达915亿元[3]。仅电信诈骗一项，2015年中国电信诈骗发案59.9万起，造成经济损失约200亿元，2016年上半年，电信诈骗发案28.7万起，造成损失80余亿元[4]。

2016年遭遇网络安全事件的用户占整体网民的70.5%，其中，网上诈骗是网民遇到的首要网络安全问题[5]。

[1、2] 来自ThreatMetrix

[3] 资料来源：中国互联网协会、中国互联网协会12321网络不良与垃圾信息举报受理中心联合发布的《中国网民权益保护调查报告（2016）》

[4] 公安部官网，《人民日报：电信诈骗既要能打，也要能防》，2016年9月21日， http://www.mps.gov.cn/n2255079/n4876594/n5104076/n5104079/c5497482/content.html

[5] 资料来源：中国互联网络信息中心《第39次中国互联网络发展状况统计报告》

二、金融欺诈事件频发、规模巨大

2015年全球银行卡欺诈率约为7.76BP（每万元中发生的欺诈金额占比），实际造成的欺诈损失为4.17BP，美国和欧洲地区的银行卡欺诈率分别为14.19BP和5.29BP，欺诈损失率分别为7.86BP和1.38BP。

截至2015年底，中国

银行卡欺诈率
1.99BP

欺诈损失率
0.13BP

银行卡欺诈金额总计
1392.6亿元

银行卡欺诈损失约
87亿元

2016年中国信用卡欺诈损失排名前三的欺诈类型为伪卡、虚假身份和互联网欺诈，与2015年一致。其中，伪卡损失占比较2015年继续上升；2016年借记卡欺诈的主要类型为电信诈骗，互联网欺诈损失金额排名第二位[1]。

宜人贷在2016年第三季度财务报告中透露，当季针对7月欺诈事件额外计提了8126万元（1219万美元）特殊风险准备。该次欺诈事件发生后，宜人贷立即暂停了相关极速借款产品的审批、推行了更为严格的申请及审批要求，于当月底重新上线了该类产品。

猛犸反欺诈称，据其观测，金融科技欺诈交易的比例在7.6‰，欺诈笔数达30万笔；推广领域欺诈交易的比例在15%，推广中刷量欺诈量达数千万次。

[1]资料来源：中国银行业协会，《中国银行业产业发展蓝皮书》

三、金融欺诈涉及业务环节多、手段多样、隐蔽性强

[1]资料来源：中国银行业协会，《中国银行业产业发展蓝皮书》

四、金融欺诈移动化程度不断增加

世界

2016年，全球[1]

重大数据泄露事件达980个

其中，来自移动设备的欺诈60%，同比上升170%

中国

截至2017年6月，中国

网民规模达
7.51亿

手机网民规模达
7.24亿

手机支付用户规模达
5.02亿

网民手机网上支付的使用比例
69.4%

相应地，金融欺诈呈现出移动化趋势[2]。

[1] 资料来源：http://finance.caixin.com/2017-07-18/101118068.html
[2] 资料来源：中国互联网络信息中心

五、金融欺诈组织化程度不断增加

欺诈呈现出产业链化的特征。

围绕着欺诈的实施，形成了

专业的技术开发产业、

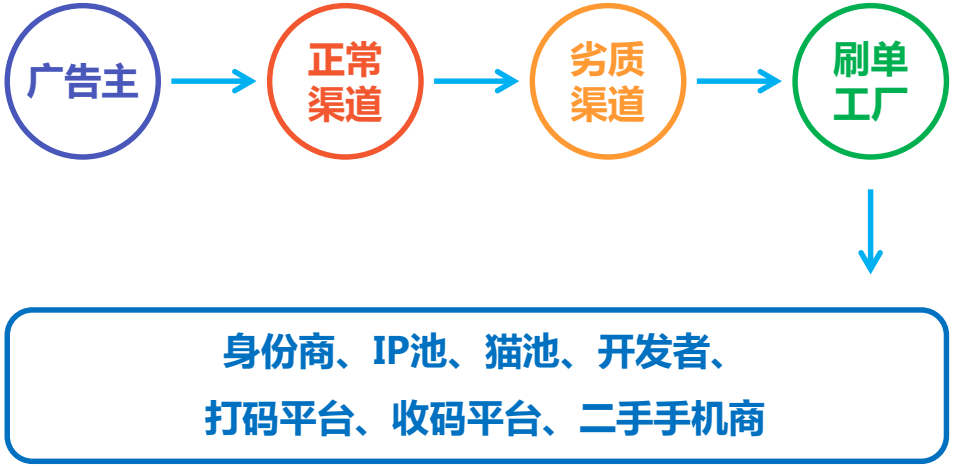
身份信用包装和虚假身份提供产业、

业务漏洞发现和欺诈方法传授产业。

各产业间通过网络通讯工具匿名交流，组织松散，但又合作紧密。

数十亿对账号密码关系为地下黑色产业链所掌握,他们通过撞库、刷库造成的账号被盗,占到整体被盗账号的80%,而盗号所衍生的黑产业链年获利超百亿元。据测算,中国“网络黑产”从业人员已超过150万,市场规模高达千亿级别[1]。

以推广刷量为例，



[1] 资料来源：《电子商务生态安全白皮书》

六、新兴金融科技公司愈来愈被欺诈者重视

金融科技业务交易频繁、实时性强、数据量大、客群下沉，相比于银行等传统金融服务机构，金融科技公司可能更容易受到攻击，欺诈者可能会利用这一点将从暗网获得的数据变现，尤其是P2P贷款和欺诈性汇款方面。

传统金融机构系统开发能力强、经验丰富、人力储备充足，新兴金融科技公司硬件和软件设施资源有待积累，更易受到攻击。

金融科技面临的欺诈更多是一种社会工程学上的攻击，而非纯技术攻击，攻击者会采用各种手段伪装身份和信用信息。金融科技面临的欺诈技术手段主要集中在联网设备的伪装上，欺诈分子经常利用各种手段掩盖联网用设备的真实信息，达到伪装身份的目的。

七、金融科技面临的欺诈规模不断增加

2017年第一季度
金融服务领域被拒绝的交易
相较于2016年增长了

40%

数字钱包和在线汇款不断发展，
数字钱包交易的
年同比增长幅度为

80%

相关僵尸攻击的
年同比增长幅度为

180%

预计到2020年，
在线支付欺诈预计将达到
256亿美元。

而针对数据泄露而言，
预计到2019年，其经济损失
在全球范围内将达到

2.1万亿
美元[1]

[1]资料来源：http://finance.caixin.com/2017-07-18/101118068.html

二

金融反欺诈
进入人工智能时代

一、金融反欺诈技术的流程

二、金融反欺诈检测的两种路径

利用外部数据

建立欺诈者黑名单

服务商核心能力 掌握和处理数据的能力

局限性

1.失效速度可能会很快

2.预测力有限

只有欺诈行为发生后才会进入黑名单，那么每台设备至少有一次欺诈的机会。

3.与企业具体业务场景结合有限

外部数据能够覆盖一些常见的欺诈场景，但各个企业的业务场景都有各自的特点，面临的欺诈威胁和对欺诈的处置策略也不尽相同。尤其在金融领域，风控是业务的核心，更不可能完全依赖于外部数据。

利用内部数据

从自动行为模式学习到自动异常检测

1.终端特征检测：检测内容包括设备类型信息等等。

现有的常用的技术是设备指纹技术。

设备指纹通过获取上网设备属性的多层次信息(设备的协议栈、OS、浏览器以及硬件特征等)、

为设备生成的不依赖本地ID的唯一ID，用以标识设备，这一ID相当于入网设备的“身份证”。

2.交易特征检测：IP地址检测等

服务商核心能力 算法

局限性

1.提高欺诈识别率，降低错报率，改善用户体验

防止“好”用户因被识别为“坏”用户而被拒绝服务。

2.降低人工审核工作量

使得人工只需要审核高风险的交易，以节省原本需要花在低风险、低回报的交易上的时间。

3.预测力较好

通过风险评分，给出欺诈概率。通过机器学习技术，分析客户自有数据识别和预测异常行为。

4.与业务场景紧密结合

根据自身业务场景，以内部数据为核心，结合各方数据纳入算法中，能够为特定业务场景得出反欺诈结论。

资料来源：Maxent猛犸反欺诈

三、设备指纹技术的“派别”

主动式

技术方法

主要通过SDK或JS代码在设备上主动收集设备特征信息，如种植cookie

准确度 较高，接近100%

应用范围 因隐私和安全性而受限

特点

1.所取特征均暴露于客户端，欺诈者可轻易通过一些一键新机等工具篡改相应特征信息，从而使指纹无效；

2.不能实现App和移动网页间、不同浏览器间的设备识别。

被动式

技术方法

基于通信协议栈特征识别，仅收集用户允许的公开信息，不种植cookie

准确度 存在技术壁垒，只有少数公司准确度较高

应用范围 对用户隐私保护度较高，应用范围较广泛

特点

1.完全工作在服务器侧，一些无法植入SDK或JS的场景也可使用；

2.跨Web/App,跨浏览器识别；

3.不侵犯用户隐私，避免了被App Store下架的风险

混合式

在识别率、应用场景和对抗性三个方面平衡主动式与被动式

资料来源：Maxent猛犸反欺诈

四、人工智能[1]在金融反欺诈中的应用

人工审核

效率低下

静态规则

措施：IP地址/DID频次限制

易规避

易被欺诈者以IP代理池或者一些一键新机的工具规避掉

多误伤

由于移动网络的特性，共享IP很普遍，容易误伤到正常用户

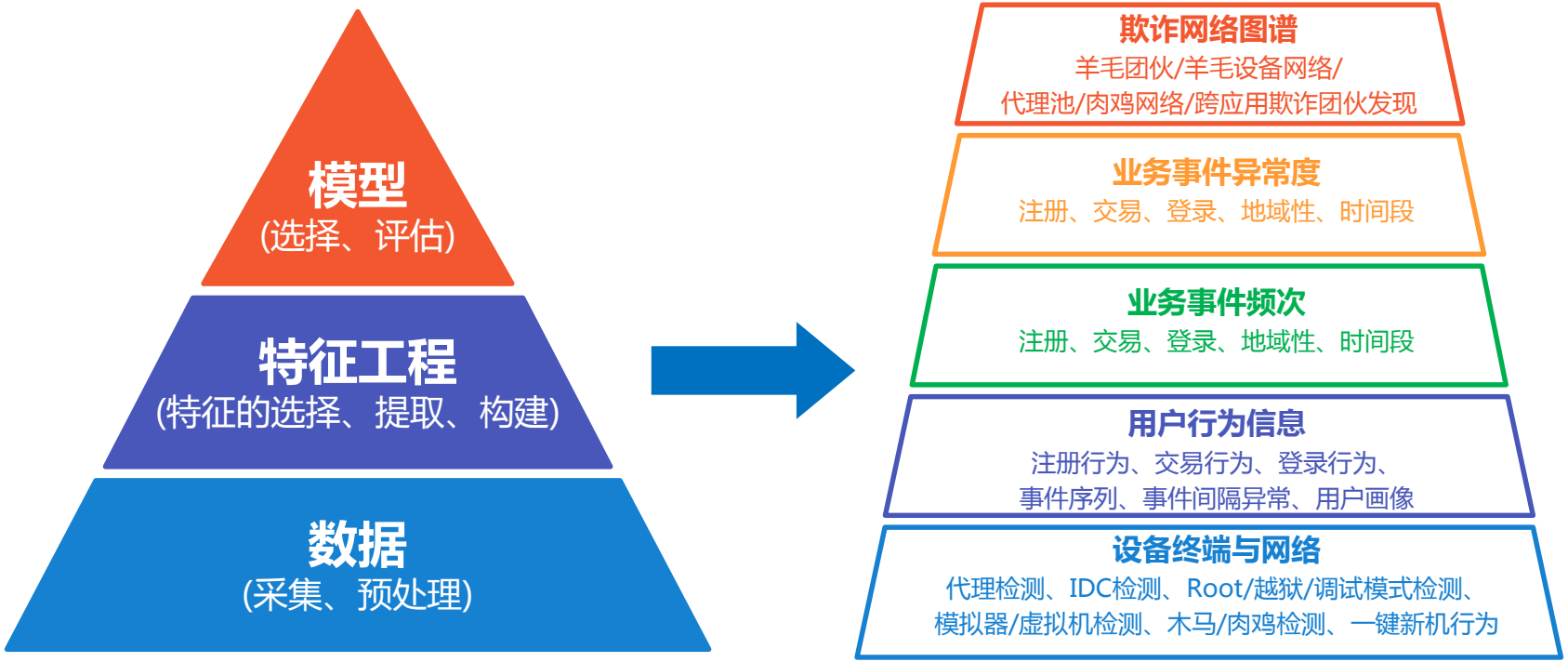
机器学习

在线欺诈呈现出实时在线、隐蔽性强、数据动态、标注稀缺、手法多变等特性，传统的基于信誉度名单和静态规则的系统很难应对；

单纯的监督式学习方法由于很大程度上依赖于标注数据也很难奏效。

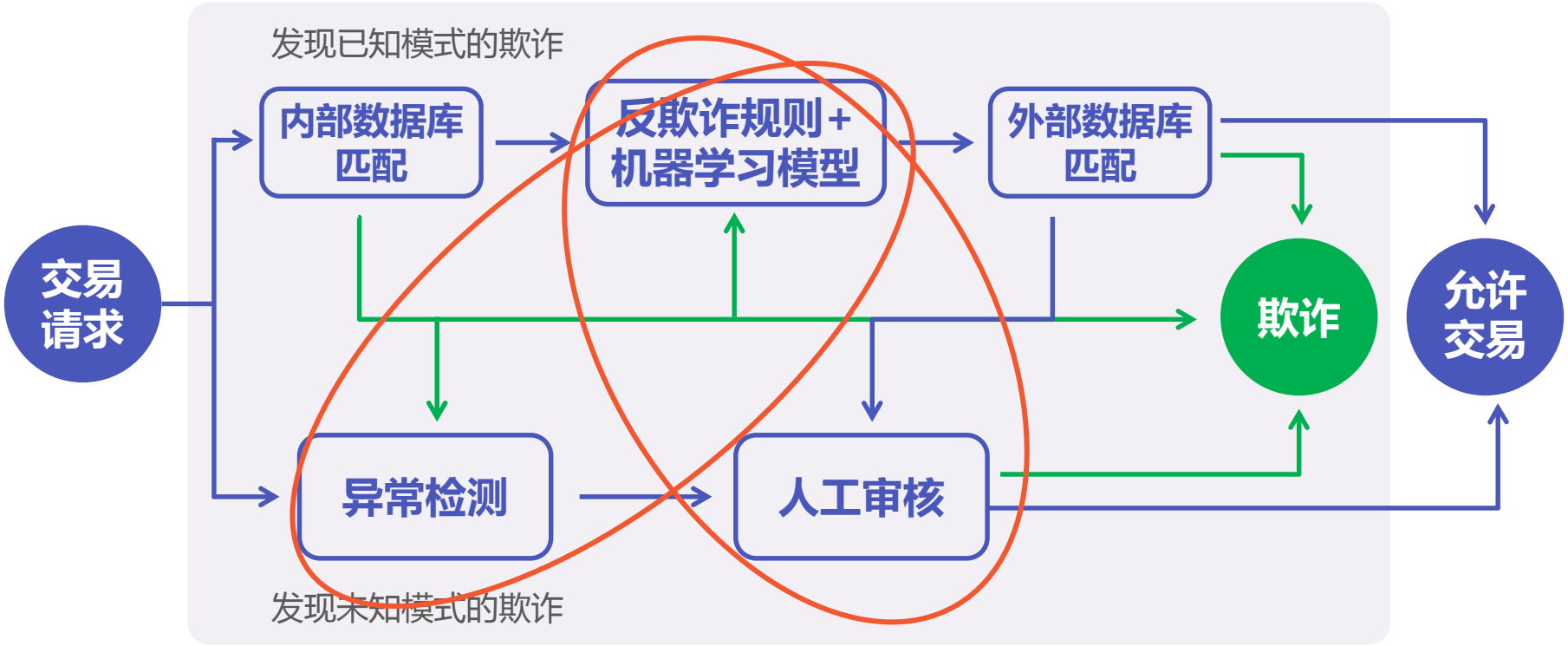
[1]人工智能：研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的科技，常见的人工智能技术是机器学习，机器学习又有有监督式、半监督式和无监督式等多种算法。

五、机器学习技术在金融反欺诈中的应用



数据和特征定义机器学习上限，模型逼近真实上限。

五、机器学习技术在金融反欺诈中的应用



资料来源：Maxent猛犸反欺诈

三
公司案例

案例一、Maxent猛犸反欺诈

1、基本情况

成立时间：2014年11月

总　　部：上海

业务模式：

人工智能反欺诈SaaS服务平台

2015年1月，
数百万元，天使轮
投资方：
伽利略资本

2016年初，
数千万元，A轮
投资方：
祥峰资本

2017年3月，
5000万元，A+轮
投资方：
DCM、祥峰资本

资料来源：Maxent猛犸反欺诈，零壹智库整理

案例一、Maxent猛犸反欺诈

2、技术

(1)机器学习

猛犸反欺诈针对在线欺诈这些特性，采用非监督式和监督式学习相结合的方式打造了一套基于多层动态模型的风险评分体系和决策系统。

1. 依托于专利的设备指纹技术进行设备及身份识别。
2. 基于非监督式学习的异常检测，将数据分解为正常趋势，随机扰动和异常情况三个部分，并在此基础上做到设备、网络和用户三个层面上的“千人千面”。
3. 基于生成式概率模型的特征学习，形成了统一的多层特征模型。将各个维度的特征统一成一种“单位”，方便模型和人工对欺诈风险进行综合评估，规避传统的静态规则的灵活性差的问题。
4. 基于图学习的欺诈网络识别，利用高效的图聚类和社交网络算法，对欺诈网络进行动态的实时识别。

案例一、Maxent猛犸反欺诈

2、技术

(2)图特征

在用户使用在线服务时，用户，设备，和账号等实体通过行为和业务时间比如注册，交易，相互关联从而构成了一张网络，也称为图。由于欺诈者往往团体作案，所以若将他们的行为表现在图上，通常会呈现出高度一致性和聚集性。这与正常用户分散的、不统一的行为模式明显不同。图特征有助于识别欺诈。

猛犸反欺诈对图特征的使用主要体现在以下几个方面：

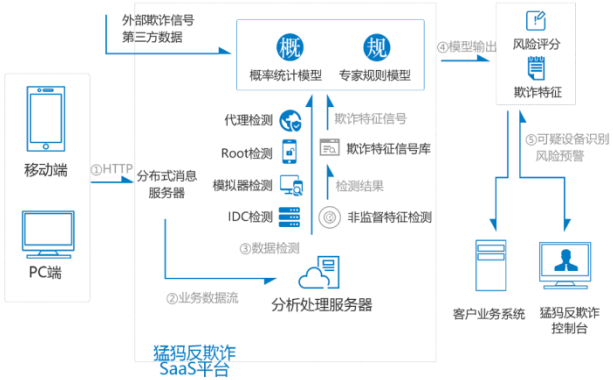
1. 利用算法，使用图聚类的方法，挖掘二度网络的聚集模式，从而完成对欺诈网络的发现。
2. 在图上使用半监督学习的方法，通过图中各点的连接关系，对少量标注样本进行传播和放大，从而通过算法自动地获得更多的标注样本。在这些“新”标注数据的基础上，使用监督式学习的模型，以取得更大成效。
3. 利用图数据库，以可视化的方式提供设备、用户等的关联图谱，辅助人工决策。

案例一、Maxent猛犸反欺诈

3、产品与服务

猛犸提供金融行业、电商行业和营销推广反欺诈解决方案和两大产品。

猛犸ID系统



猛犸反欺诈SaaS平台

案例二、Sift Science

1、基本情况

成立时间：2011年

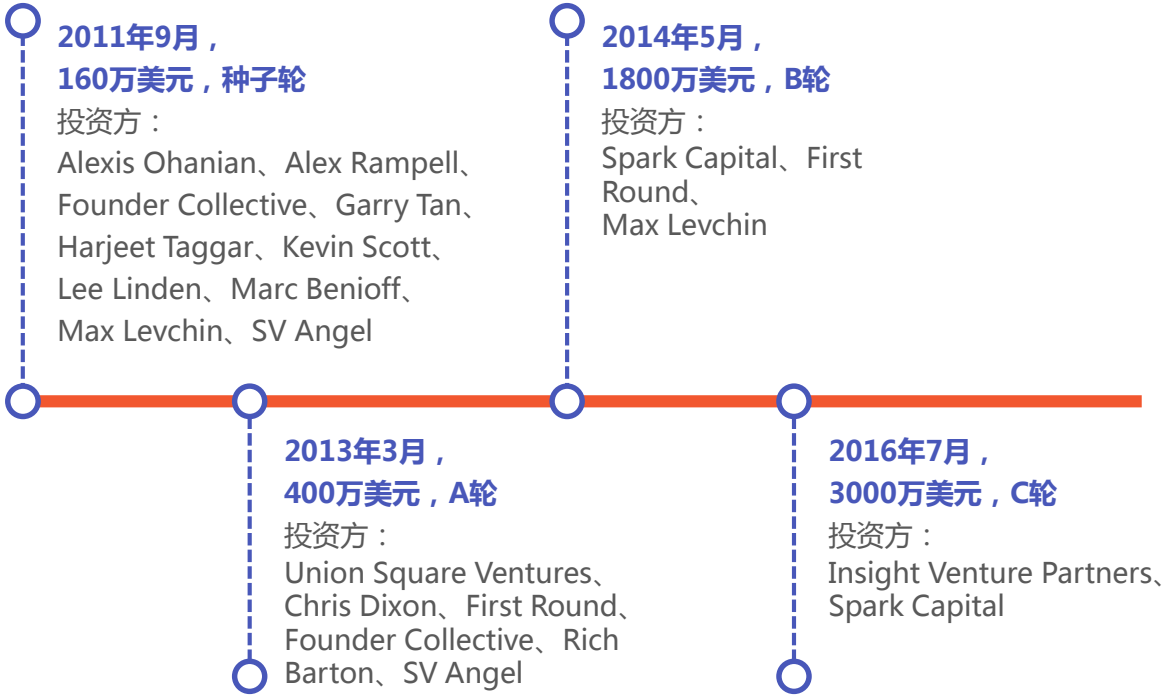
总　　部：加州 旧金山

业务模式：

人工智能反欺诈服务商

提供解决方案的行业：

电子商务、数字产品、按需服务业、平台或社区、旅游、票务、汇款、支付网关、SaaS



资料来源：Crunchbase，零壹智库整理

案例二、Sift Science

2、产品与服务

Sift Science的产品通过可视化仪表盘呈现给用户，呈现内容包括各项欺诈的概率评分、用户定制的数据和欺诈类型等信息。

Sift Science的产品功能建立在其机器学习系统——信任平台（Trust Platform）上，该平台每天监测着6000多个站点和app，收集、分析和从数亿起事件中学习。

资料来源：Sift Science官网，零壹智库整理

案例三、ThreatMetrix

1、基本情况

成立时间：2005年

总　　部：加州 圣何塞

2、基本情况

ThreatMetrix向电子商务、银行和证券经纪、支付和借贷、保险、旅游、政府、医疗、媒体和游戏等行业提供数字身份识别、反欺诈和网络威胁防范服务等解决方案。

资料来源：Crunbase，零壹智库整理

四
金融反欺诈趋势展望

一、人工智能被持续关注，应用不断深化

目前，人工智能已上升至我国战略层面高度，金融监管当局对人工智能亦高度关注。

2016年5月	2016年11月	2017年6月27日	2017年7月20日
发改委、科技部、工信部、中央网信办制定《“互联网+”人工智能三年行动实施方案》，提出到2018年，打造人工智能基础资源与创新平台。	国务院印发《“十三五”国家战略性新兴产业发展规划》提出“加快人工智能支撑体系建设”、“推动人工智能技术在各领域应用”。	央行印发《中国金融业信息技术“十三五”发展规划》，推出积极推进区块链、人工智能等新技术应用研究。	国务院印发《新一代人工智能发展规划》，提出鼓励金融行业应用智能客服、智能监控等技术和装备，建立金融风险智能预警与防控系统。

二、云计算应用或迎来“国家队”

监管层对云服务的认可不断增强。

2016年

银监会牵头制定《中国银行业信息科技“十三五”发展规划监管指导意见（征求意见稿）》，指出“积极开展云计算架构规划，制定云计算标准，联合建立行业云平台，主动实施架构转型”。

2017年6月27日

央行印发《中国金融业信息技术“十三五”发展规划》，提出稳步推进系统架构和云计算技术应用研究。

2017年7月5日

银监会被传出就银行联合设立互联网金融云服务平台公司与银行沟通，银监会要求每家银行的出资金额不低于2000万元。云平台可以帮助银行处理网上支付，贷款审批，为客户提供定制化的金融产品，并且通过整合海量客户数据来控制风险防范欺诈。云计算反欺诈或迎来“国家队”。

SaaS的发展尤其值得关注。

三、生物识别技术已有应用，有待完善

目前，生物识别技术在反欺诈领域已经有所应用：

艾克飞(Equifax)

2017年3月

与Jumio和Paycasso合作推出解决方案Document Verifier

该方案能在数秒之内识别出金融产品的申请人的身份是不是真实的，方式是通过智能手机或安装有网页摄像机的设备比对人脸和护照或驾照的照片。这一自动化的技术能识别超过200个国家的官方文件是否存在篡改或异象。

益博睿（Experian）

2017年4月

和技术服务商BioCatch合作。

通过个体打字速度和用鼠标浏览网页的方式等行为特征进行金融产品的在线反欺诈。上述机构称行为特征对识别欺诈者利用“暗网”中被盗窃的身份信息、通过自动化程序脚本进行欺诈的行为尤其有效。BioCatch时任副总裁Frances Zelazny举例称，欺诈者相较于普通用户填写生日和名字等身份信息可能较慢，但由于熟悉相关表格的架构，填写其他问题可能较快。

环联（TransUnion）

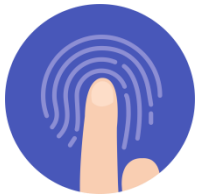
2015年4月

宣布正在和南非声纹识别服务商OneVault合作开发“声音银行（Voice Bank）”，当时环联呼叫中心向该项目提供了3万个声纹。

2014年，环联还和生物识别服务商ImageWare Systems在反欺诈业务上达成了合作。2016年，ImageWare Systems联合环联在亚马逊云服务（AWS）平台上推出了生物认证管理SaaS服务，该服务支持包括人脸识别、声纹识别和指纹识别在内的多种生物识别方式。

三、生物识别技术已有应用，有待完善

目前主流的生物识别方式各有局限：



指纹识别

指纹传感器价格较为昂贵；部分人无指纹，或由于职业原因指纹可能被损坏；指纹可能被复制，存在安全风险；采集需要对象配合，便捷性差。

人脸识别

容易受到姿态、光照、遮挡、照片清晰度等因素影响。

虹膜识别

摄像头较为昂贵；采集虹膜需要对象配合，便捷性不高。

与身份验证中所使用的显式生理的身份识别手段（比如人脸、指纹、虹膜等）不同，风险评估更多地是使用隐式行为上的一些特征，比如触屏力度、滑屏轨迹、步态等。

这些特征会在访问者无感知的情况下采集，对用户的使用体验不造成干扰，受黑客攻击的可能性也较小。

四、TEE技术开始受到重视

开放环境的使用，使得以下信息暴露于各种攻击之下：

1.个人隐私：联系人、短消息、照片、视频等；

2.企业数据：登陆VPN的凭据等；

3.密钥资源；

4.金融交易中的用户交互数据：交易内容、交易额、用户输入PIN……

可信执行环境（Trusted Execution Environment，TEE）是存在于移动设备主处理器内的安全区，确保敏感数据在可信的环境里得到存储、处理和保护。TEE有能力对经授权的安全软件（所谓的“可信应用程序”）进行安全的执行，因此可通过实施保护、保密性、完整性和数据访问权限，提供端到端的安全性。随着苹果Apple Pay的普及，TEE逐渐为人所知。

人民银行《关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》要求，打造可信手机支付执行环境，针对手机木马病毒、虚假短信、伪基站等欺诈手段，鼓励手机厂商综合运用SE、TEE等新技术提供硬件级安全保护，提升支付敏感信息防护能力和支付交易安全强度。

国内大型企业，如阿里巴巴，华为等，也积极参与国际上TEE标准的制定以及国内TEE在移动支付安全中的应用探索。

五、区块链技术受到持续关注

区块链是一种由多方共同维护，以块链结构存储数据，使用密码学保证传输和访问安全，能够实现数据一致存储、无法篡改、无法抵赖的技术体系 。

区块链技术正在被不断地应用于反欺诈中，尤其是在身份验证领域。该领域已经出现一些专门的服务商，如Chainalysis致力于为银行设计区块链反欺诈系统。

谢谢

关于我们

作者

孙爽

零壹财经

零壹财经是专业的新金融成长服务机构，建立了媒体+数据+研究+智库的独立第三方服务架构，拥有新媒体、零壹智库等服务平台。
零壹财经是中国互联网金融协会成员、北京市网贷行业协会发起单位并任宣传教育专委会主任单位、中国融资租赁三十人论坛成员机构、湖北融资租赁协会副会长单位、微金融50人论坛特邀成员机构、跨界创新组织COIN执委机构。

零壹媒体

零壹财经具备专业的新金融媒体服务平台，包括新金融门户网站（01caijing.com）和强大的自媒体平台，为新金融提供专业的内容建设和传播服务；旗下包含“零壹财经”、“爱有财”、“零壹融资租赁简报”、“P2P日报”、“金羊毛工作坊”、“消费金融观察”、“fintech前线”、“零壹研究”等自媒体品牌。

零壹智库

零壹智库是零壹财经旗下新型的研究服务平台，坚持独立、专业、开放、创新的价值观。包含零壹财经华中新金融研究院，零壹研究院等研究机构，并建立了多元化的学术团队，通过持续开展金融创新的调研、学术交流、峰会论坛、出版传播等业务，服务新金融机构，探索新金融发展浪潮。

关于我们

零壹研究

零壹研究院以数据和案例为基础，进行新金融前沿理论和实务研究。零壹研究院数据中心（零壹数据）已建成Fintech、P2P借贷、众筹、融资租赁等新金融领域的强大数据库，形成了可动态量化分析的数据产品。

华中新金融研究院

华中新金融研究院是成立于武汉、面向全国、沟通国际的学术交流平台，包含融资租赁研究中心、汽车金融研究中心、金融科技投融资研究中心等垂直研究中心。由武汉市金融工作局担任指导单位，中央财经大学银行业研究中心主任郭田勇教授担任研究院院长。

零壹融资租赁研究中心

零壹融资租赁研究中心（简称“零壹融资租赁”）是华中新金融研究院旗下新锐的融资租赁研究机构，运营专业的融资租赁垂直媒体，关注和探索融资租赁与互联网的结合。为融资租赁从业者和使用者服务：提供及时的专业资讯、深度解析、研究报告和高质量的线下活动。服务载体包括：零壹融资租赁网（www.01leasing.com），微信公众账号“零壹-融资租赁简报”等。

关注我们

零壹财经

爱有财

零壹融资租赁

P2P日报

金羊毛工作坊

消费金融观察

Fintech前线

零壹研究

免责声明

零壹财经

www.01caijing.com

市场推广

岳军（北京）
18612238376
yuejun@01caijing.com

刘锐（上海）
18917865380
liurui@01caijing.com

张安基（深圳）
18688826809
zhanganji@01caijing.com

余旖旎（武汉）
15871761031
yuyini@01caijing.com