ISC 2016

2016 中国互联网安全大会 China Internet Security Conference

协同联动 共建安全+命运共同体

移动终端交互行为分析的身份主动认证与安全感知

沈 超

西安交通大学副教授

智能网络与网络安全教育部重点实验

身份安全、身份认证？
不就是密码、指纹吗？

身份安全得到极大关注

各种智能计算终端（传统PC、云终端、移动终端等）已进入到各行各业，能够存储并访问越来越多的安全和隐私信息，内部人员攻击、密码泄漏、隐私侵犯、身份盗用等造成的国家及各级企业隐密信息泄漏及财产损失已引起各国政府和企业的极大关注。

内部人员攻击

密码泄漏

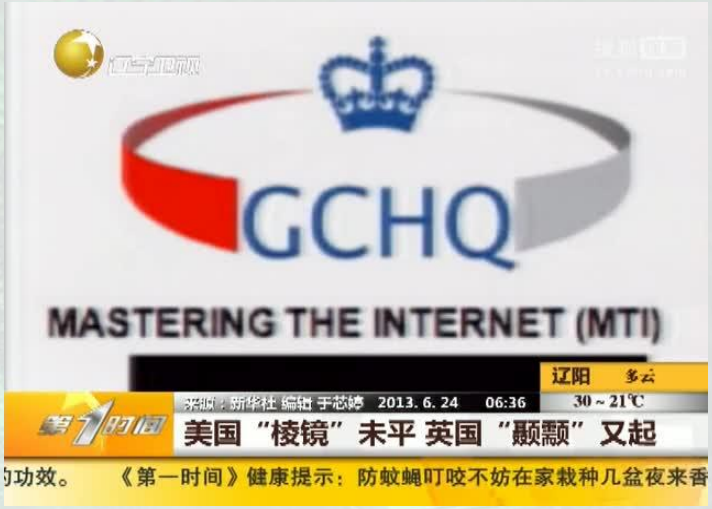
身份安全

隐私侵犯

身份盗用

棱镜门等事件的频发带来的挑战

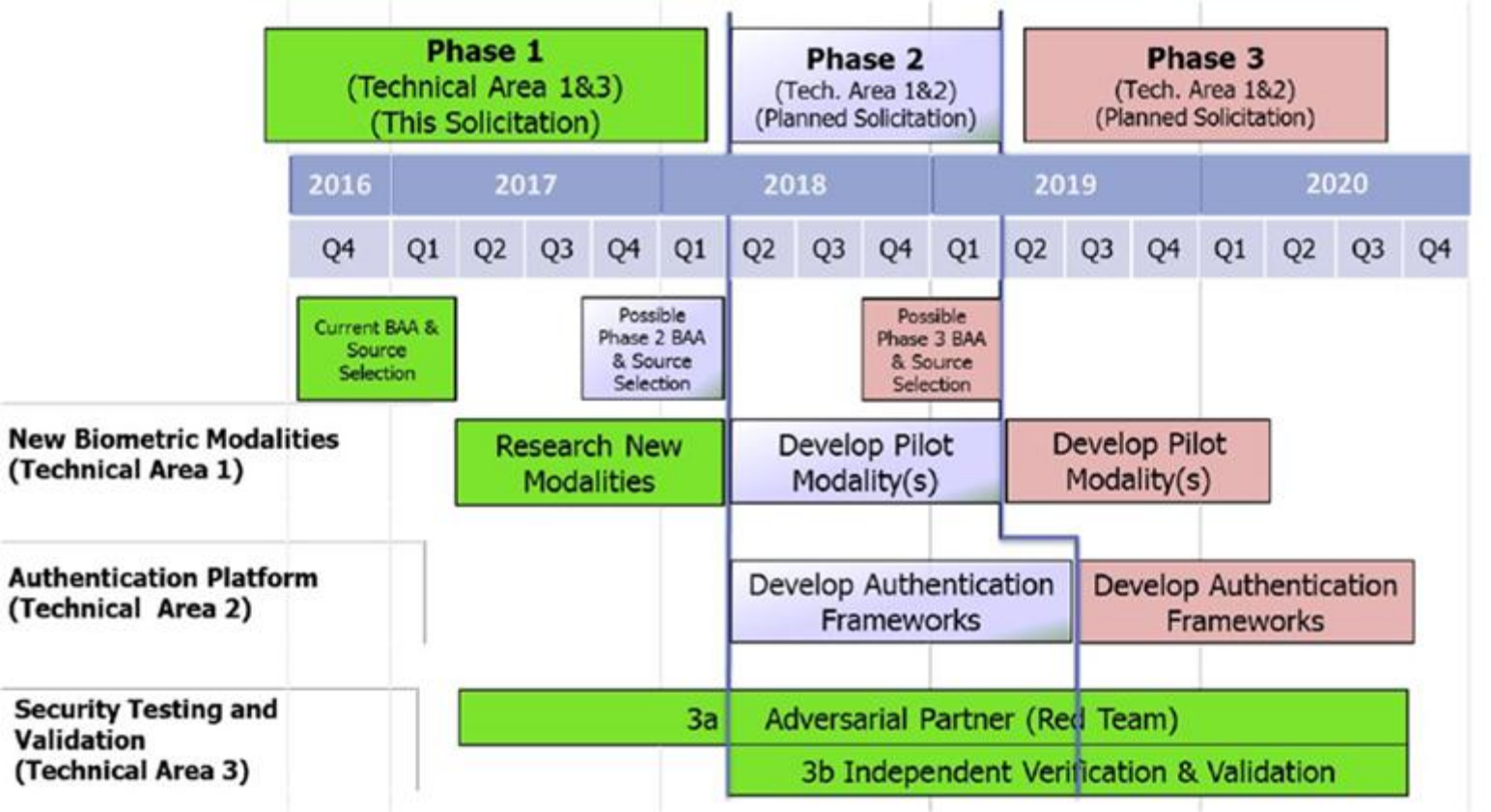
- “棱镜”、“颞颥”事件再次说明由于终端安全信息泄露给国家造成的重大损失
- 需要对终端操作行为进行持续监控，并对操作者身份进行认知
- 需要主动式的身份安全分析方法



- DARPA在2013年12月支持4年期的交互行为测定&主动认证计划
  - 在用户使用计算终端的过程中进行主动式行为监控和身份认知分析
  - 强调不需要用户的配合

DARPA Active Authentication - Continued

- 新的动机：在个人强身份认证信息丢失或被复制（2013年底德国国防部长指纹泄漏）的情况下，能够通过行为分析的方法进行身份的动态识别。
- “斯诺登事件” -> 第二个4年期研究（从2016开始）

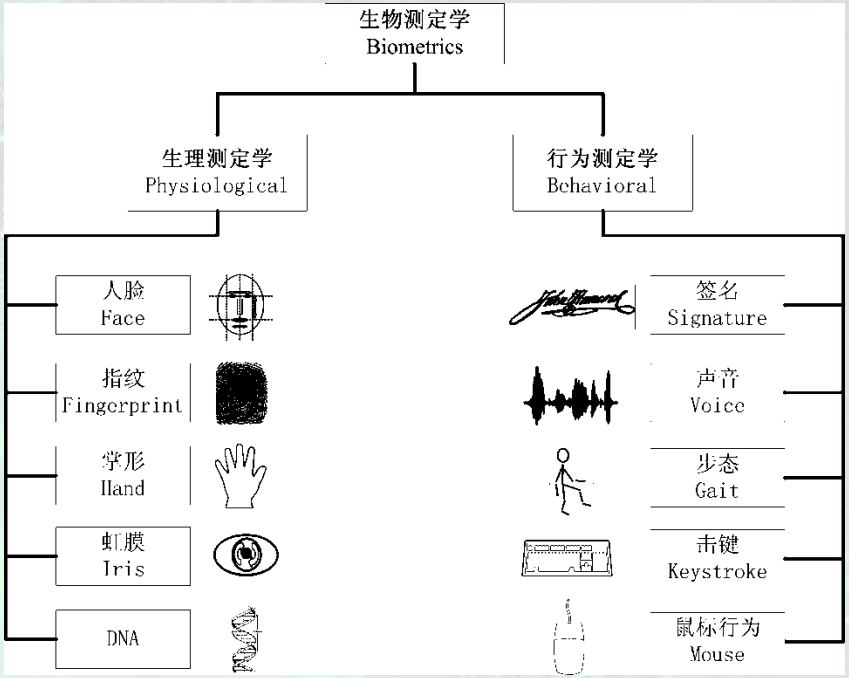


终端交互行为是什么？
进行主动式身份认证和监控？

终端交互行为

□ 生物特征

- ✓ 生理特征（虹膜、指纹等）
- ✓ 行为特征（步态等）
- ✓ 终端交互行为：
  - 鼠标 – 移动模式，曲线特征
  - 键盘 – 敲击节奏
  - 触摸屏&触摸板 – 触摸模式
  - 穿戴传感器 – 交互模式
  - 软生物特征 – 衣服、发型、肤色
  - 可视交互的人脸特征



优点：

- ❖ 终端交互行为直接从人机交互过程中提取
- ❖ 无需记忆或携带，不需要额外的硬件
- ❖ 可无缝融入用户与智能计算终端的交互过程

终端交互行为主动身份认证和认知

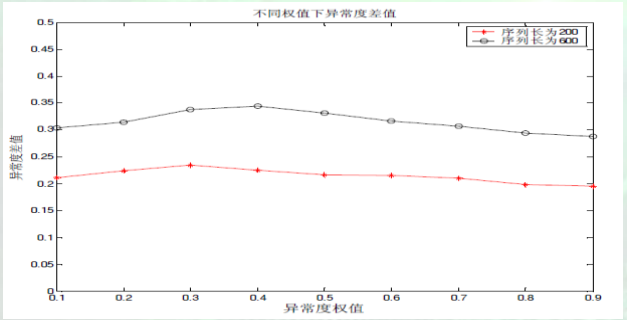
- 终端交互行为安全监控和身份认知
  - ✓ 静默式捕获终端用户操作人机交互设备时所产生的交互行为数据
  - ✓ 结构化描述交互行为并提取稳定的行为表征特征
  - ✓ 监控操作者的身份安全（监控用户的交互行为、持续分析用户的真实身份）
  - ✓ 认知用户的物理身份信息（操作者的性别、年龄、左右手使用习惯等信息）

终端交互数据

	subject	sessionIndex	rep	H.period	DD.period.t	UD.period.t
2	s002	1	1	0.1491	0.3979	0.2488	0.1069
3	s002	1	2	0.1111	0.3451	0.2340	0.0694
4	s002	1	3	0.1328	0.2072	0.0744	0.0731
5	s002	1	4	0.1291	0.2515	0.1224	0.1059
6	s002	1	5	0.1249	0.2317	0.1068	0.0895
7	s002	1	6	0.1394	0.2343	0.0949	0.0813
8	s002	1	7	0.1064	0.2069	0.1005	0.0866
9	s002	1	8	0.0929	0.1810	0.0881	0.0818
10	s002	1	9	0.0966	0.1797	0.0831	0.0771
11	s002	1	10	0.1093	0.1807	0.0714	0.0731
12	s002	1	11	0.0887	0.1660	0.0773	0.0876
13	s002	1	12	0.0911	0.1525	0.0614	0.0824
14	s002	1	13	0.1114	0.1620	0.0506	0.0900
15	s002	1	14	0.0903	0.1871	0.0968	0.0805
16	s002	1	15	0.1169	0.2562	0.1393	0.0739
17	s002	1	16	0.1270	0.1839	0.0569	0.0911
18	s002	1	17	0.1016	0.1799	0.0783	0.0792
19	s002	1	18	0.1056	0.1755	0.0699	0.0781

安全监控

2013年5月18日13:45: 当前为第16次, 当前主动认证的用户身份可靠性为77.42%
2013年5月18日13:50: 当前为第17次, 当前主动认证的用户身份可靠性为82.43%
2013年5月18日13:55: 当前为第18次, 当前主动认证的用户身份可靠性为75.32%
2013年5月18日13:60: 当前为第19次, 当前主动认证的用户身份可靠性为78.97%
2013年5月18日14:05: 当前为第20次, 当前主动认证的用户身份可靠性为88.24%
2013年5月18日13:10: 当前为第21次, 当前主动认证的用户身份可靠性为89.45%
2013年5月18日13:15: 当前为第22次, 当前主动认证的用户身份可靠性为62.42%
2013年5月18日13:20: 当前为第23次, 当前主动认证的用户身份可靠性为76.42%



身份认知分析

操作者的性别为：男

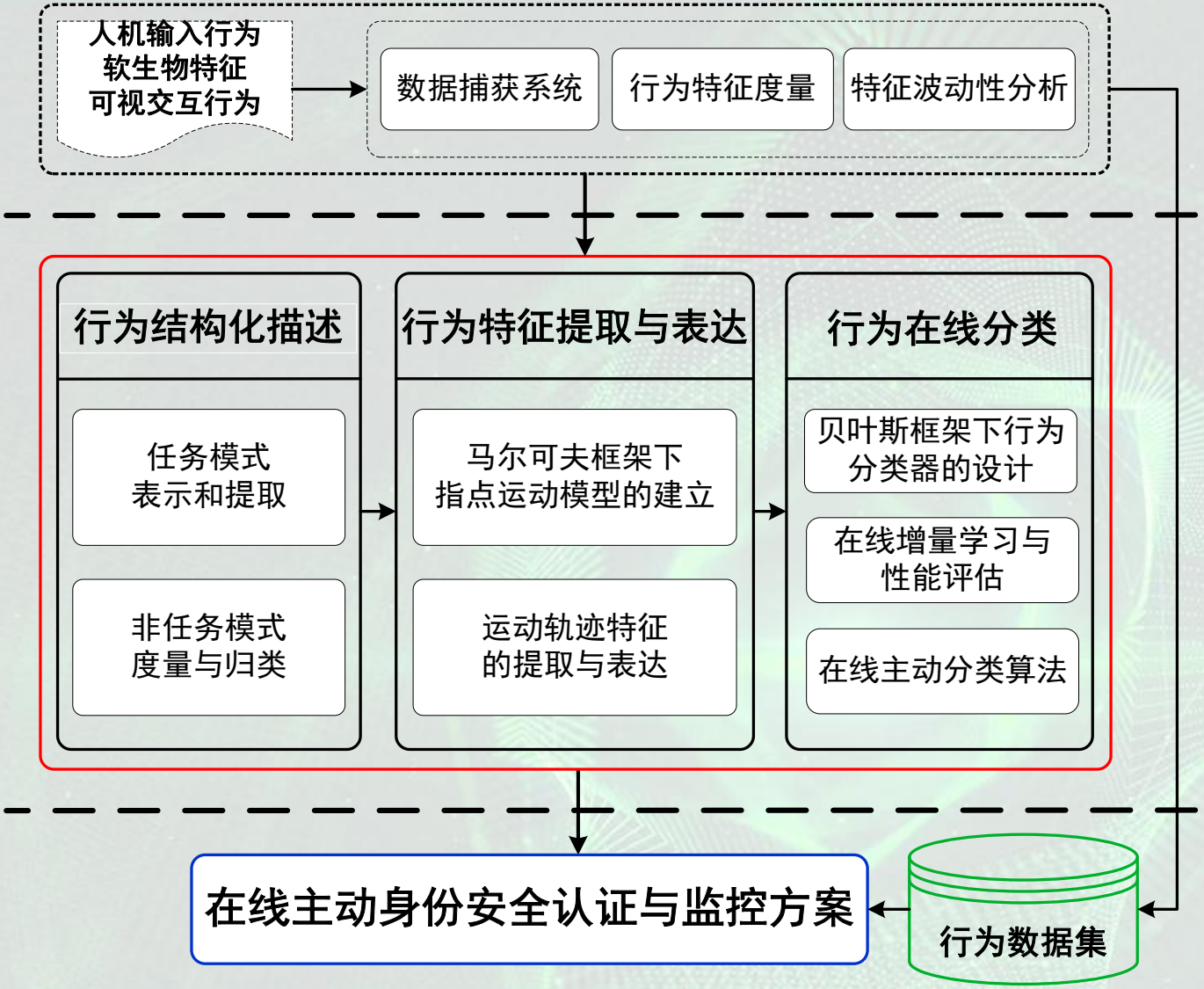
年龄为：20-30

左右手使用习惯：右手

身高：约为170～180

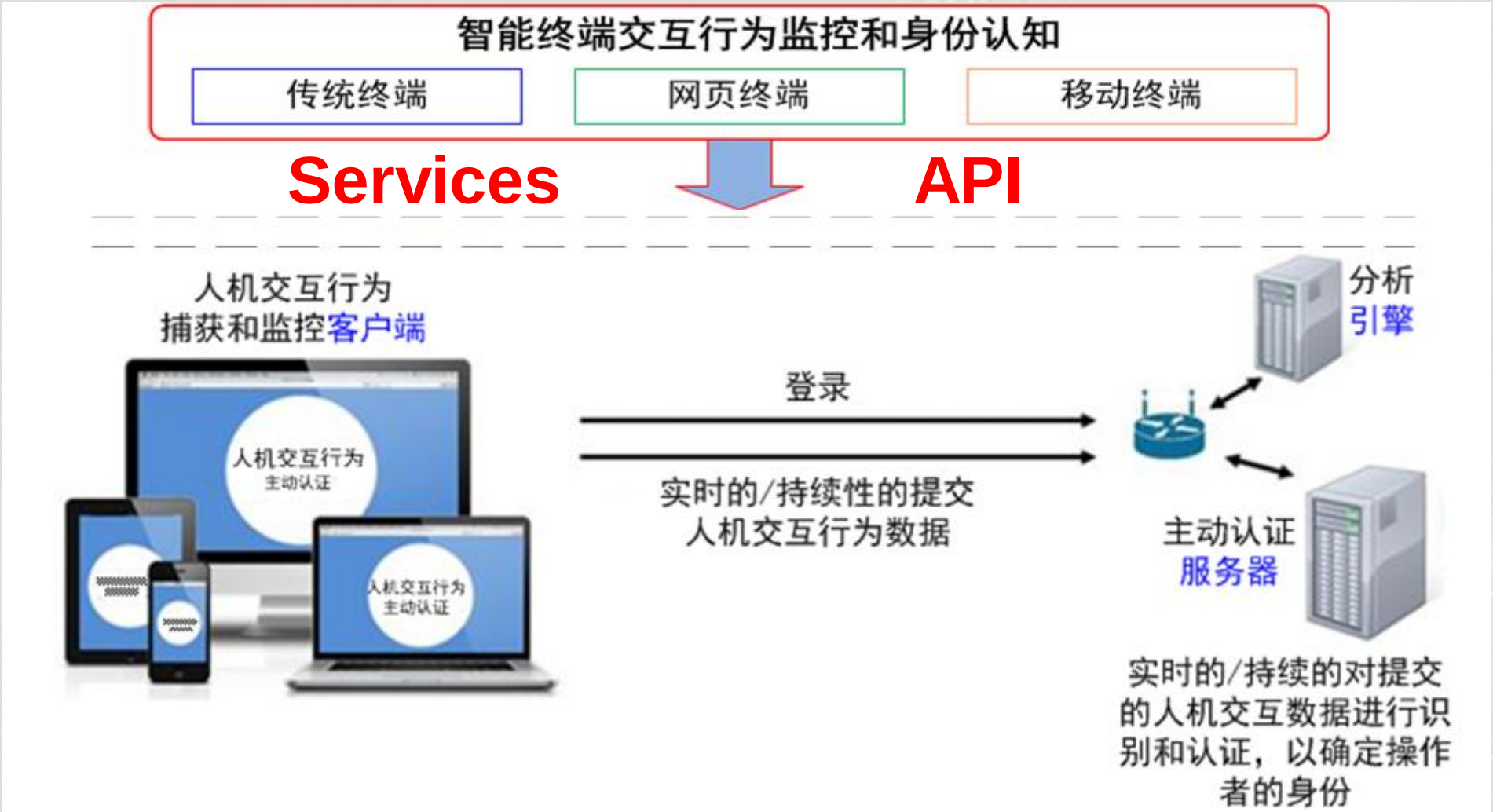
……

技术框架

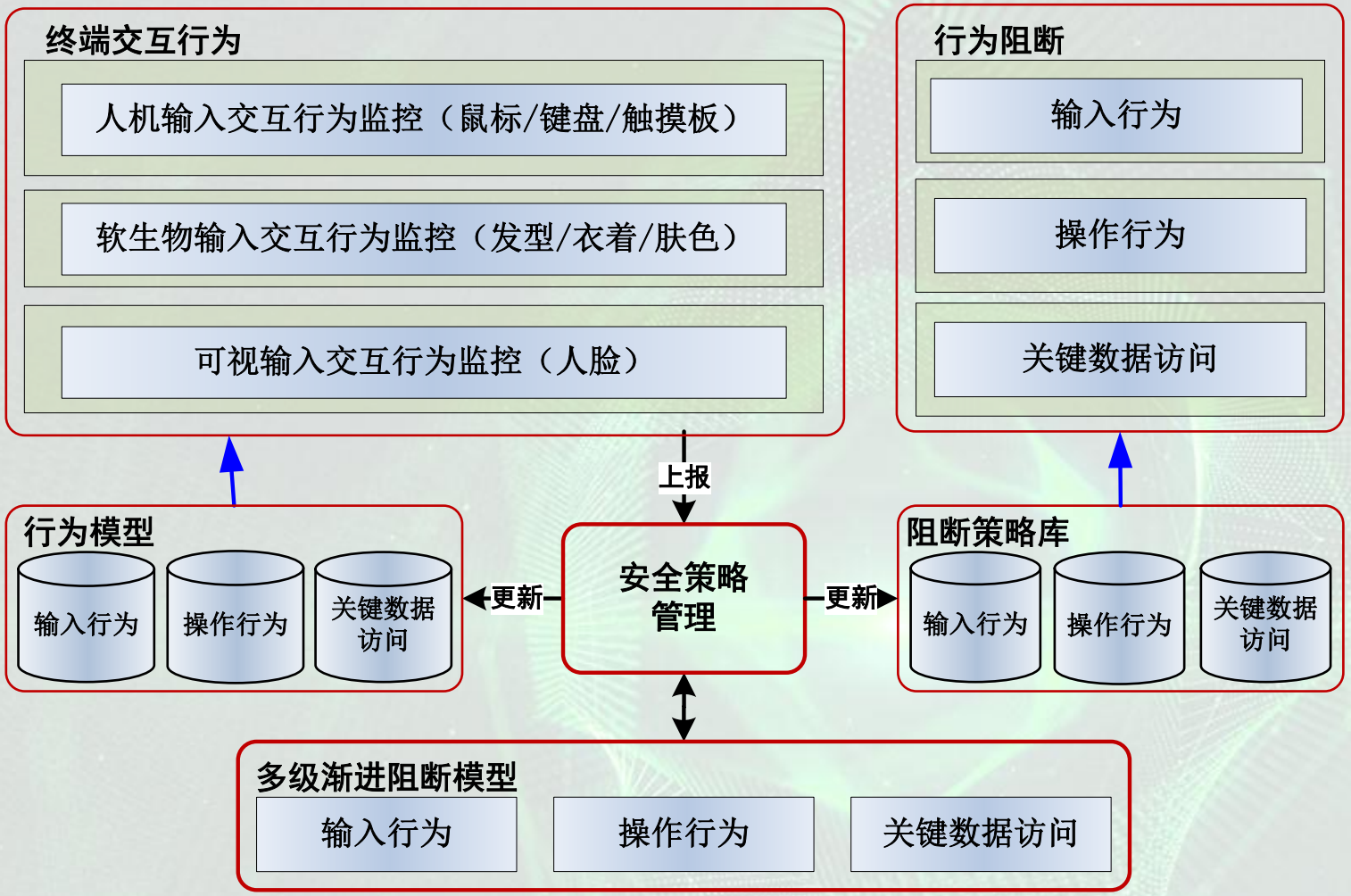

人机输入行为
软生物特征
可视交互行为
数据捕获系统
行为特征度量
特征波动性分析
行为结构化描述
任务模式
表示和提取
非任务模式
度量与归类
行为特征提取与表达
马尔可夫框架下
指点运动模型的建立
运动轨迹特征
的提取与表达
行为在线分类
贝叶斯框架下行为
分类器的设计
在线增量学习与
性能评估
在线主动分类算法
在线主动身份安全认证与监控方案
行为数据集

在PC端、网页端、移动端上都能用吗？

技术方案


智能终端交互行为监控和身份认知
传统终端
网页终端
移动终端
Services
API
人机交互行为
捕获和监控客户端
人机交互行为
主动认证
人机交互行为
主动认证
登录
实时的/持续性的提交
人机交互行为数据
分析
引擎
主动认证
服务器
实时的/持续的对提交的人机交互数据进行识别和认证，以确定操作者的身份

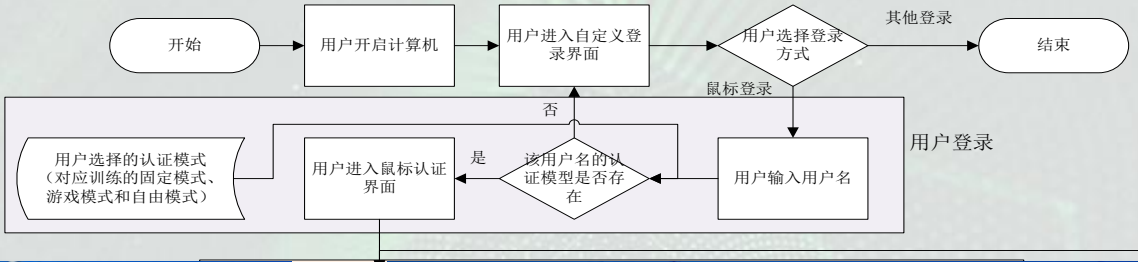
逻辑方案

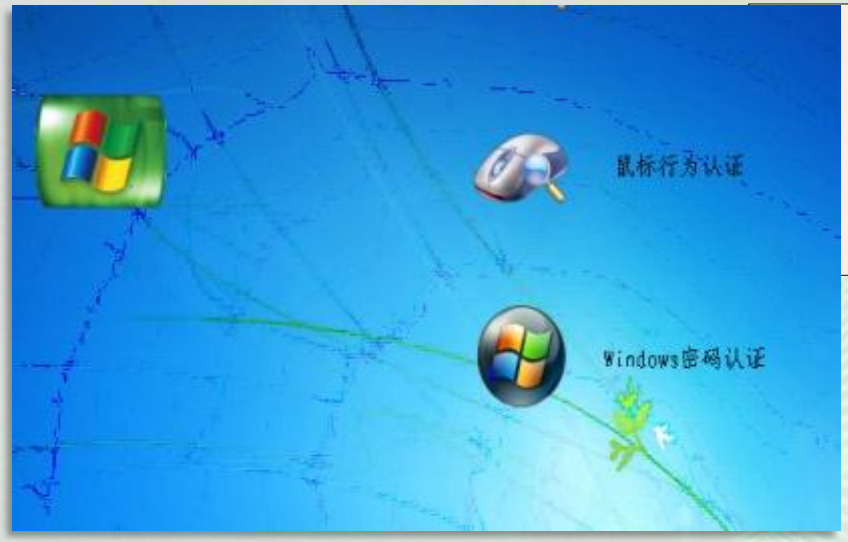

终端交互行为
人机输入交互行为监控（鼠标/键盘/触摸板）
软生物输入交互行为监控（发型/衣着/肤色）
可视输入交互行为监控（人脸）
行为阻断
输入行为
操作行为
关键数据访问
上报
行为模型
输入行为
操作行为
关键数据访问
更新
安全策略管理
更新
阻断策略库
输入行为
操作行为
关键数据访问
多级渐进阻断模型
输入行为
操作行为
关键数据访问

传统终端交互行为的身份认证

- 系统设计

- 系统实现



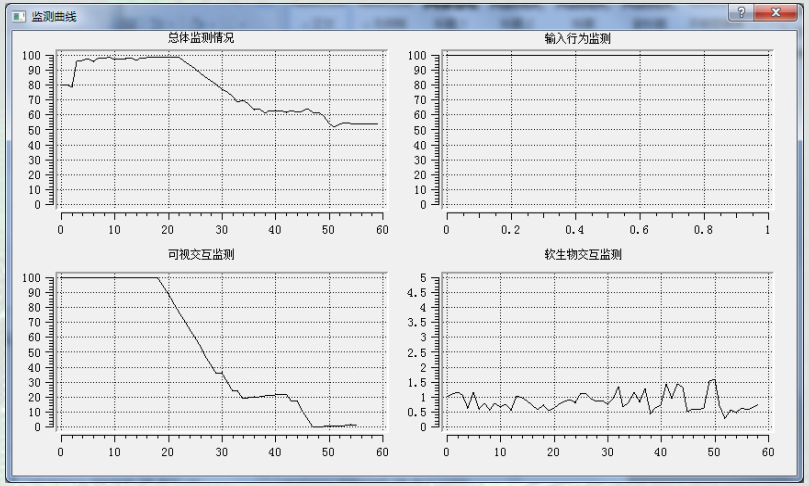


传统终端交互行为的身份监控

- 系统设计
- 系统实现

传统终端交互行为认证与监控

客户端



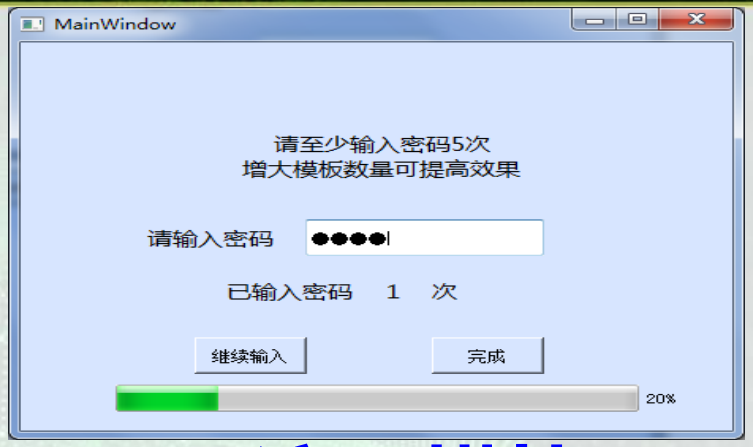
分析引擎

服务器端

加强版-传统终端交互行为的安全认证

传统终端双因素强化认证

客户端



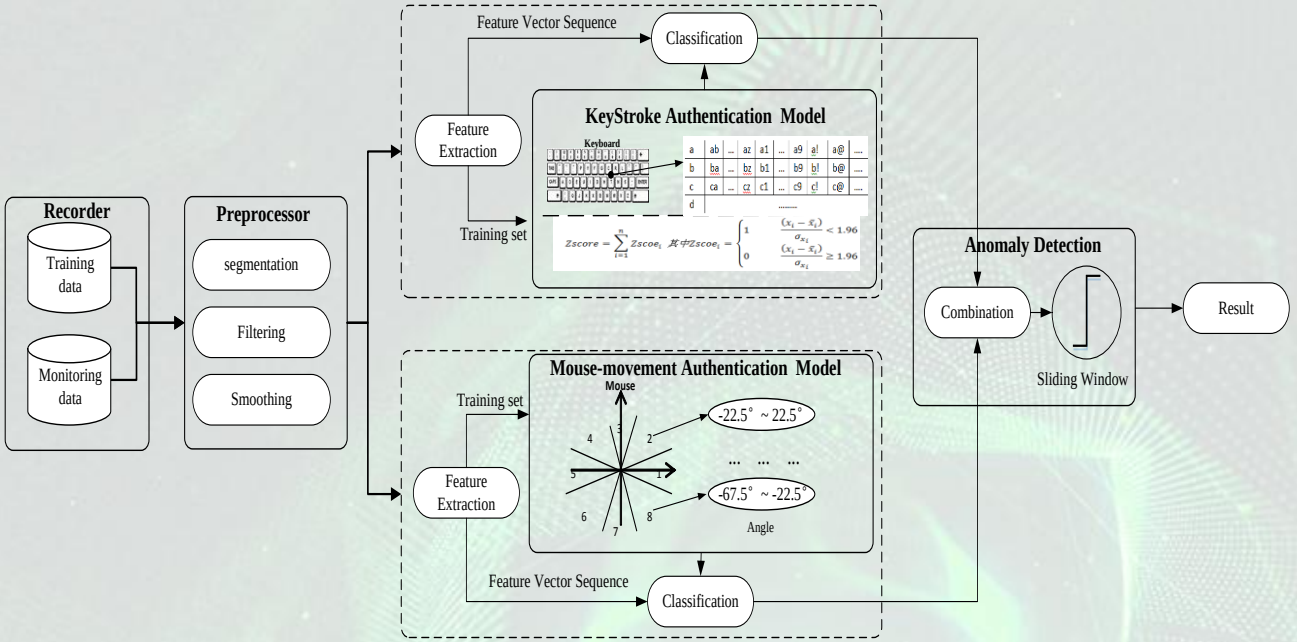
注册模块

服务器端

认证精度在200人的测试集上高达99.99%！

Web交互行为的身份确认与追踪

- 系统设计



- 系统实现

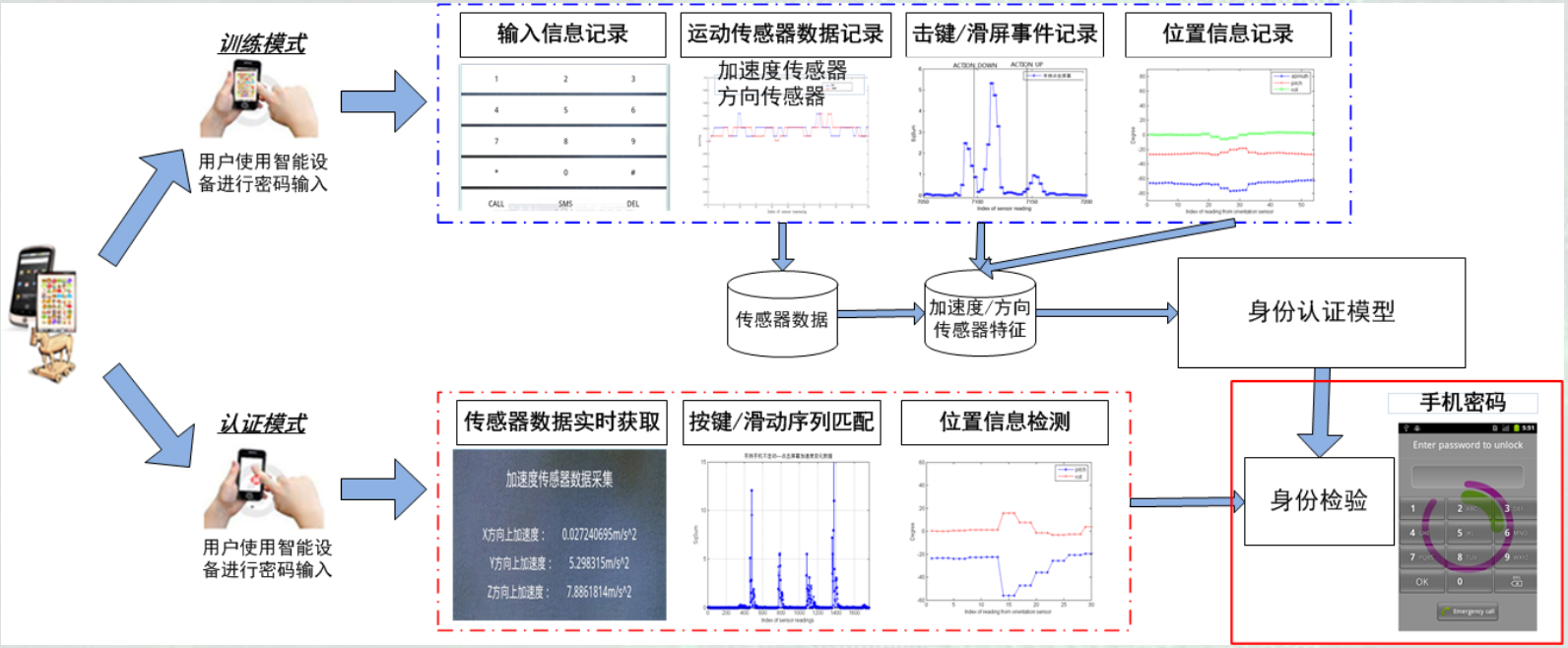
Web交互行为认证与监控（银行）

转帐页面的认证

缴费页面的认证

移动端交互行为/传感器的双因素认证

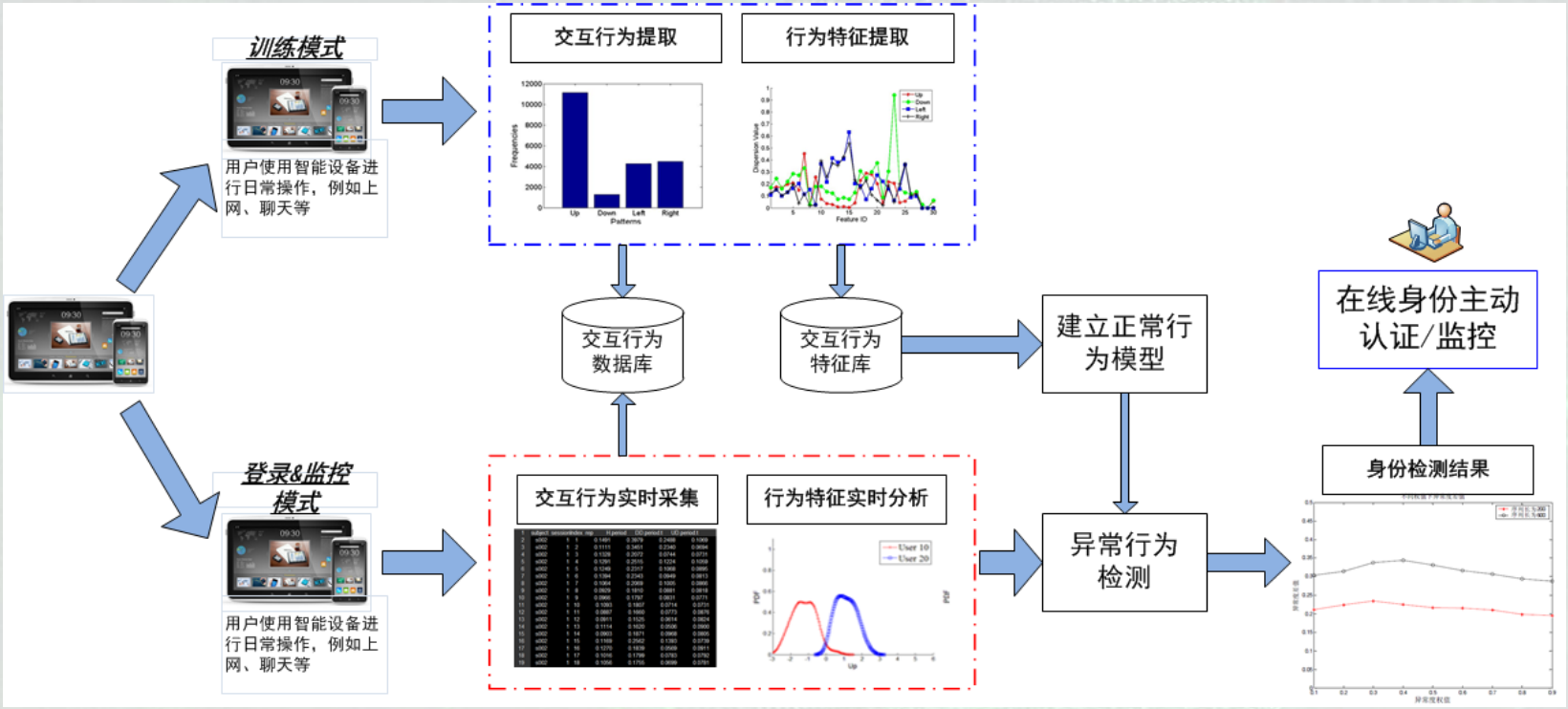
- **关键技术**
  - 输入序列和运动传感器数据的融合技术
  - 传感器的结构化表示技术 & 运动传感器的特征分析与提取
  - 在线学习、认证和更新技术
- **研究框架**



移动端双因素强化认证（手机&平板）

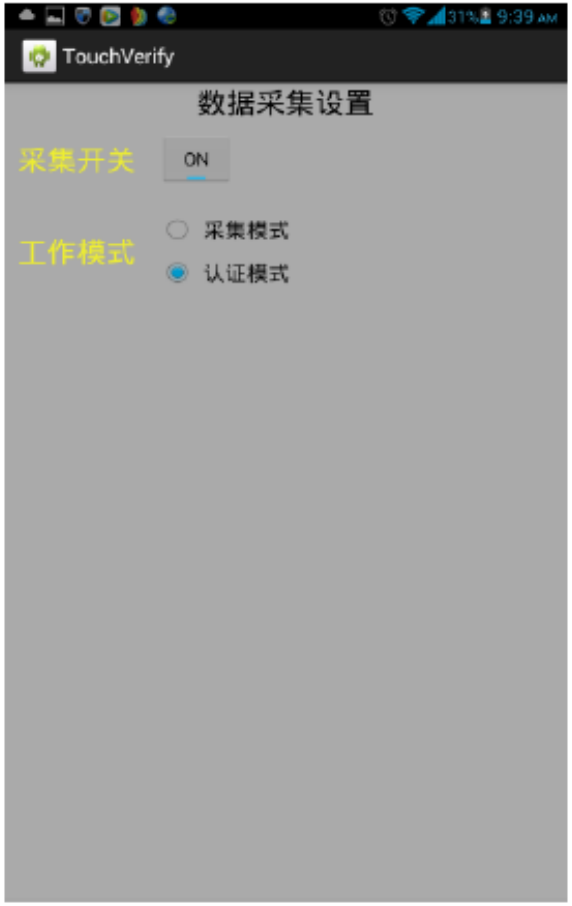
移动端交互行为/传感器的主动监控

- **关键技术**
  - 异构数据的结构化表示和融合技术 & 多源数据的融合建模技术
  - 交互行为的半监督增量学习技术 & 在线主动认证技术
- **研究框架**

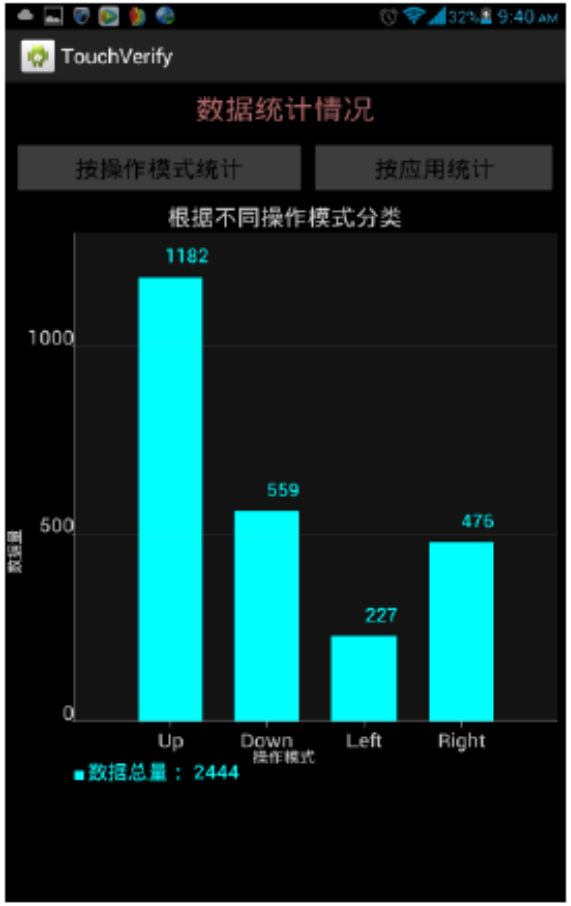


移动端交互行为/传感器的主动监控

（a）主界面

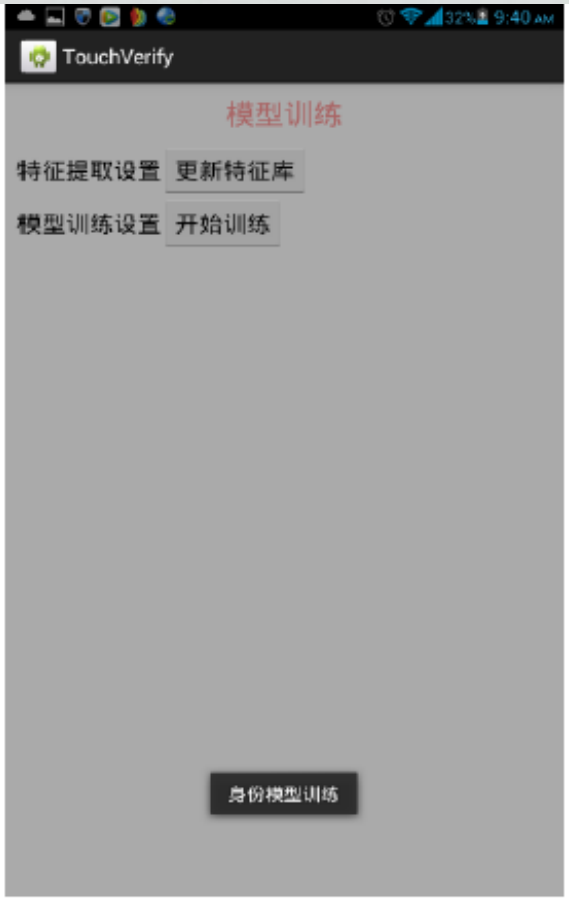


（b）数据采集界面



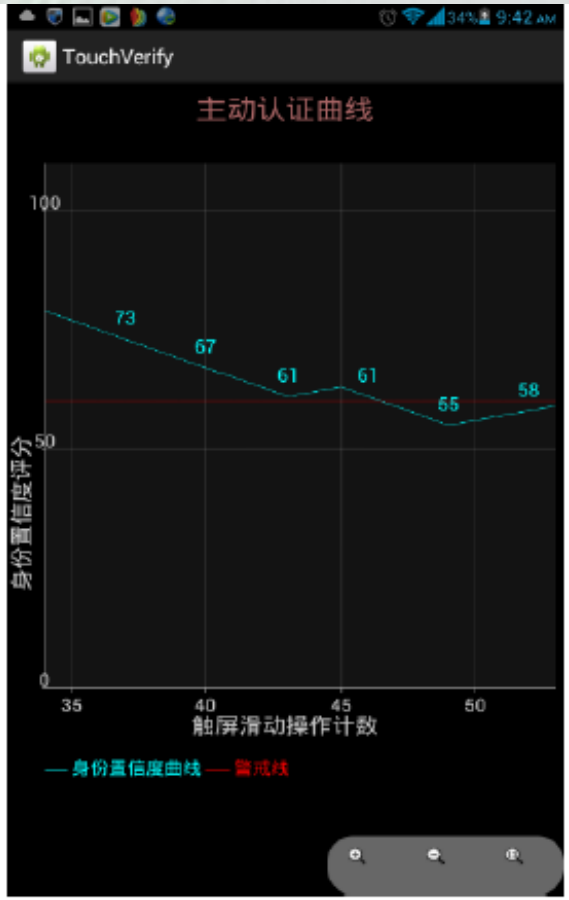
（c）数据统计界面

移动端交互行为/传感器的主动监控



（d）模型训练界面

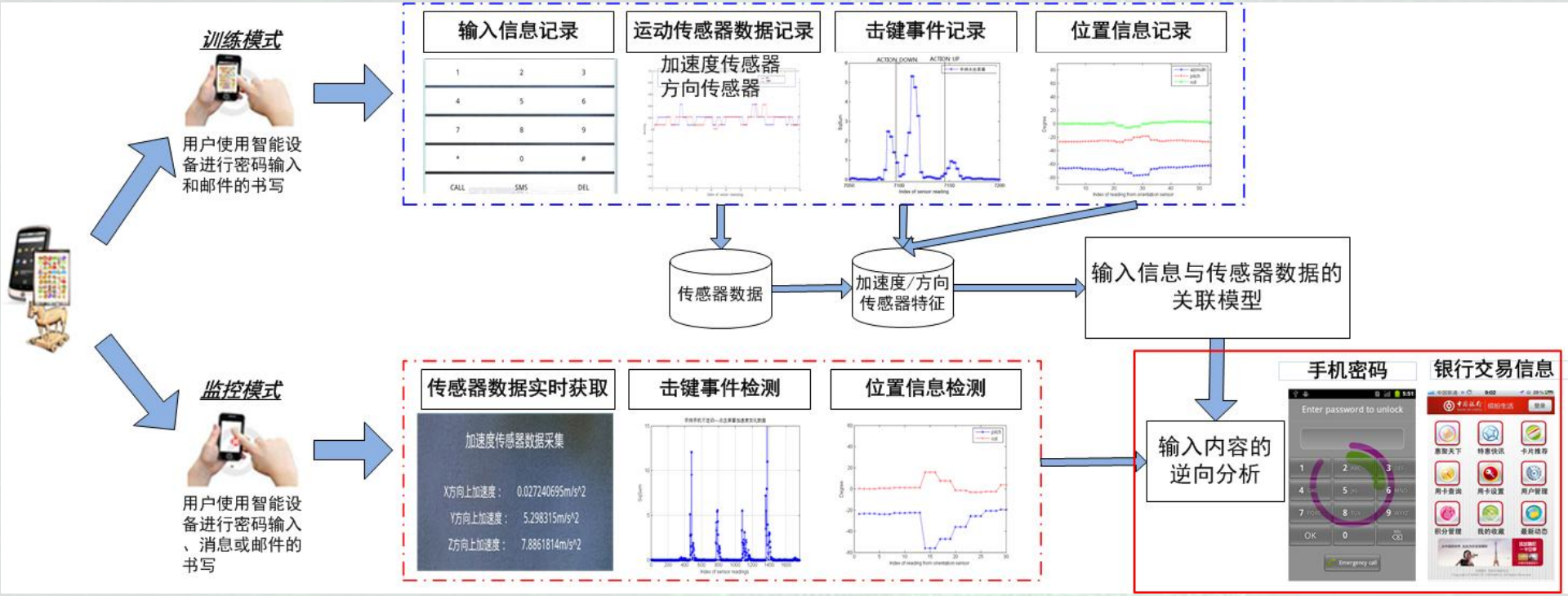
（e）主动认证界面



（f）主动认证曲线界面

移动端交互输入行为的逆向分析

- **关键技术**
  - 基于加速度传感器的输入行为检测技术 & 基于方向传感器的位置感知技术
  - 多源传感器数据的融合表示技术 & 智能终端输入行为的逆向推理技术
- **研究框架**



谢　谢