开放环境下
医院互联网服务安全防护体系

浙江大学滨海产业技术研究院
浙江大学计算机科学与技术学院
浙江省现代服务业电子服务工程技术研究中心
李莹 博士 副教授

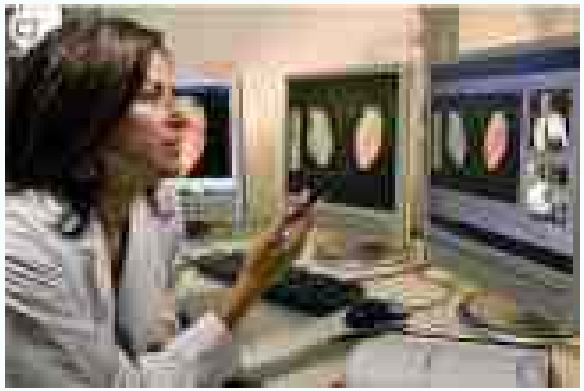
互联网医疗健康服务现状与问题

医院互联网开放服务安全开放解决方案

应用推广与典型医院成功案例介绍

前景

美国互联网+医疗的发展趋势



- **2010年奥巴马医改，将美国医疗体系中消费者、政府、保险公司、及医疗企业多家博弈的情形推上了新的高度**
- **2014年美国互联网医疗的风险投资达到40亿美元约有7000万医生通过互联网为病人提供了医疗服务。**
- **2017 年 5 月 27 日全美 50 个州全部通过远程医疗立法法案（即参议院法案 SB1107 及众议院法案 HB2697），互联网医疗达到爆发时代。**

美国“互联网+医疗”正如火如荼地进行,迸发出前所未有的“火花”

前景

中国互联网+医院的发展需求和必然趋势

- 2015年，国务院办公厅，全国医疗卫生服务体系规划纲要（2015-2020）
- 2015年，习近平主席出席第二届世界互联网大会，“乌镇互联网医院”
- 2016年12月26日 - 中共中央、国务院已经印发《“健康中国2030”规划纲要》”
- 2017年，国家卫计委官网发布《2017年卫生计生工作要点》

开放是医院提供医疗健康服务和运作发展的必然趋势！

现状

中国互联网医疗健康服务的蓬勃发展

在资本的推动下，通过免费的互联网模式，中国医疗健康互联网应用蓬勃发展，APP下载过亿。

现状

互联网医疗健康服务需要和医院信息化系统对接

院前服务

- 预约挂号
- 智能导诊
- 候诊叫号

院中服务

- 健康宣教
- 移动医护
- 远程医疗
- 电子病历
- 云影像
- 健康档案
- 多学科联合会诊MDT

公共服务

- 移动支付

院后服务

- 出院随访
- 慢病管理

绝大多数的互联网医疗健康服务，都需要和医院内部信息化系统对接，才能真正实现线上-线下服务闭环，否则就是“隔靴搔痒”！

大事件

医疗信息安全事故频发，卫计委将规范互联网诊疗活动的开展

医院安全事故回顾
山东临沂某医院的官方网站被黑，因网站安全措施低，导致被治疗患者轻易入侵。
安徽某医院的5767例新生儿治疗视频被发布在视频网站，因信息系统未做防范导致外泄。
天津某医院的官方网站被篡改，跳转其他网页，因安全防护低，导致网络木马轻易篡改。
广州某医院的统方被窃取，因业务系统弱口令，导致第三方技术人员轻易获取，进行倒卖。
深圳某医院官方网站被攻击，遭到攻击者金钱勒索，因防范措施低，导致攻击者通过任意入侵工具。
福州某三甲医院患者信息被频繁窃取，因开放端口过多导致被技术人员利用，进行频繁窃取。
浙江某医院的医护人员信息被公开，因业务系统接口开放过多，尚未做安全防范措施导致APP用户可以任意查询。
江苏某医院的10W条患者信息被公开倒卖，因业务数据未做脱敏措施，导致第三方接入厂商获取全部信息。
……

基于安全监管的考虑，卫生主管部门颁布方案，将实现严格准入管理，明确互联网诊疗活动的实施主体只能是医院。

疑问

医院
准备好了吗

？

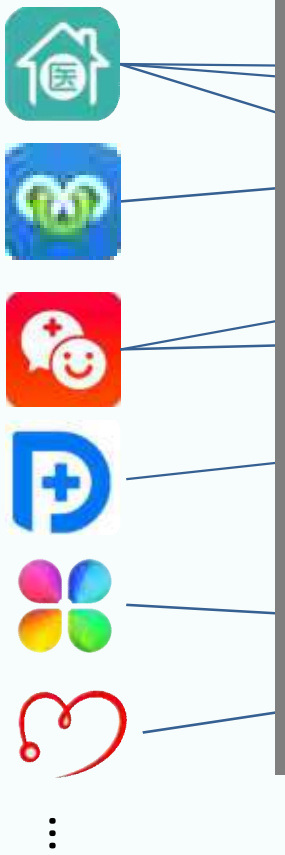
现有问题

一、安全问题

问题一

安全问题：互联网应用的访问行为缺乏实时监管

各类互联网应用



对医院来说：是个黑盒子

1、风险不确定
2、过程不透明
3、行为不可控
4、记录不可查

无法管控非法分子获取数据行为

- HIS系统
- LIS系统
- PACS系统
- EMR系统
- HRP系统
- CDR系统
- ……
- 财务系统

医院信息系统厂商

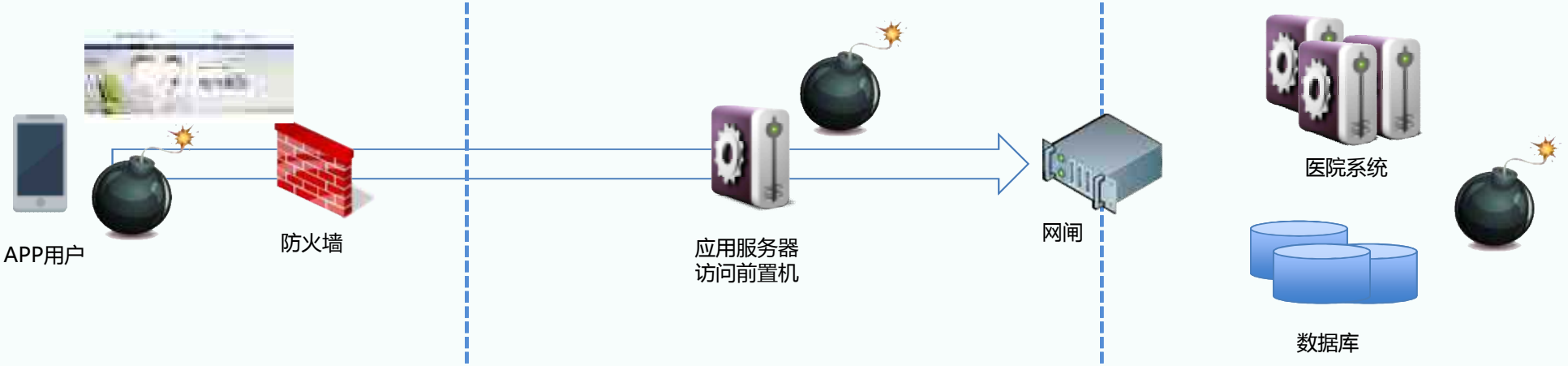
安全问题

针对现有医院网络架构的攻击手段

攻击手段：
1、 SQL注入
2、APP反编译
案例：

攻击手段：
1、网络抓包
2、端口监听
案例：

攻击手段：
1、DB漏洞
2、OS漏洞
案例：



篡改网站发布反动信息

伪装患者获取非授权的数据

对核心数据的窃取、删除、修改

互联网

DMZ区域

院内局域网

攻击手段

常用的各类攻击手段和攻击效果

①
逆向工程
APP反编译

②
SQL注入

③
网页篡改

二、架构问题

问题二

架构问题：传统医院信息化系统不能支撑互联网级访问需求

互联网应用，每秒万以上的用户同时访问，响应时间不超过5秒

医院有100个窗口，每次操作需30秒时间，院内信息系统可支撑每分钟200个用户访问。

三、模式问题

问题三

模式问题：周期长，成本高，医院难以自建互联网服务

医院能否自建互联网医疗应用？
（技术、成本、经验）

申请

医院协调，厂商自行沟通

院内系统

HIT厂商

接口费成为部分医院信息系统厂商主要收入来源：
每个应用5w～100w

App厂商

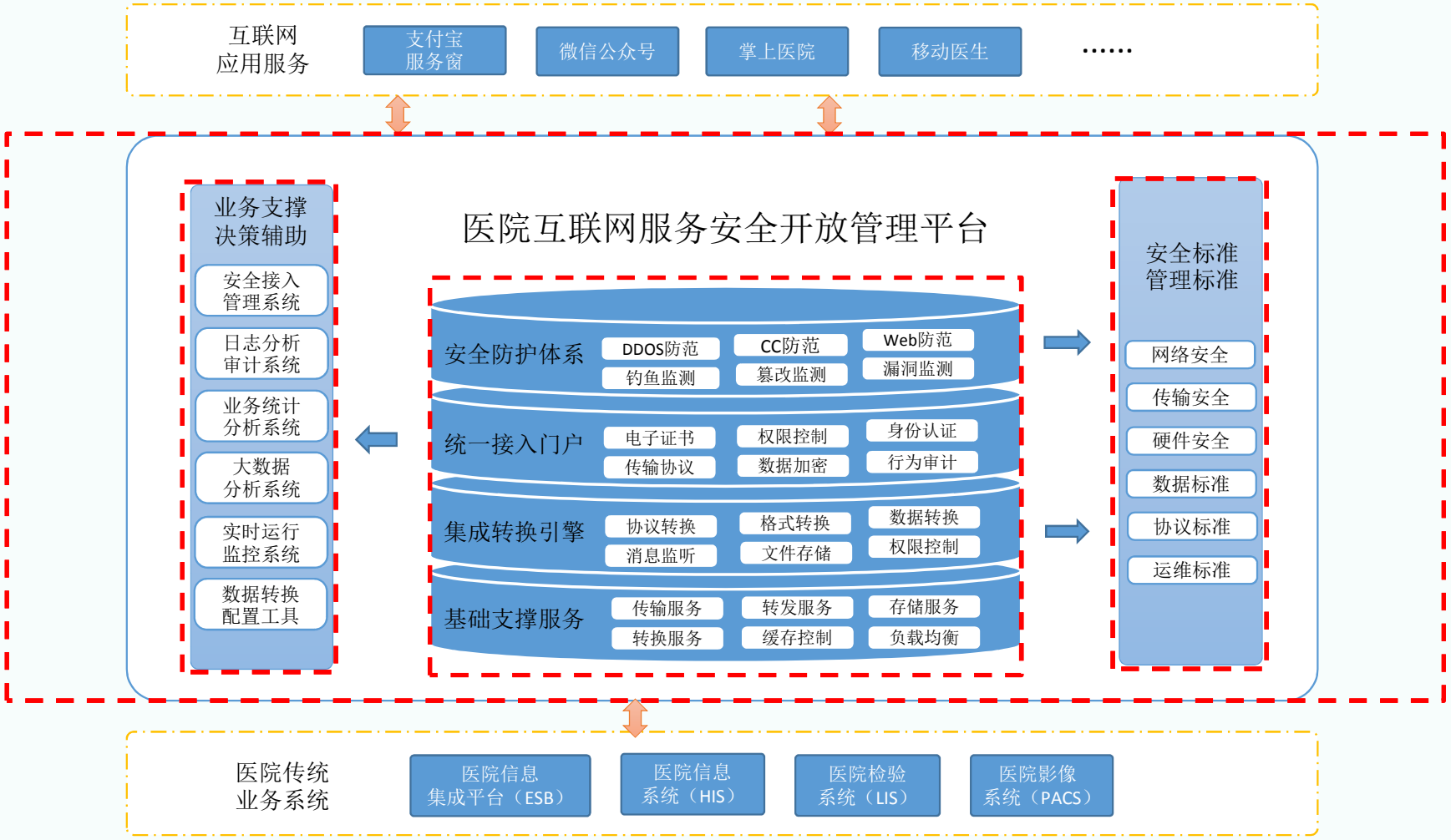
现阶段，所有费用基本由APP厂商承担，医院不用付费

接口费—互联网应用难以承受之重

- 互联网医疗健康服务现状与问题
- 医院互联网开放服务安全开放解决方案
- 应用推广与典型医院成功案例介绍

方案

形成开放环境下医疗健康服务安全防护整体解决方案



一体化安全防护服务

解决开放环境下医院信息安全与隐私保护问题

域名防护

针对医院互联网域名的安全防护体系

- 网站防护
- CDN加速
- 防DDOS攻击
- 防CC攻击
- 防WAF攻击
- 防网络木马
- 防钓鱼程序
- 防网络抓包
- 永久在线
- 用户数据报表
- 可视化安全防护

零部署　　百G DDOS防护能力　　大数据安全防护

终端防护

针对互联网医院移动终端的安全防护体系

设备安全	内容安全	应用安全	交易安全
• 登记(Enroll), 开通和配置设备，设置移动策略 • 识别唯一及持久的移动设备ID • 远程定位, 锁定及擦除丢失或被盗的设备 • 加强设备安全遵从性: 密码, 加密,	• 拷贝、粘贴和共享限制 • 数据本地存储的安全区 • 安全访问医院邮件、日历和联系人信息 • 安全访问医院内部网站和网络	**软件开发生命周期** • 集成开发环境 • 应用静态扫描 **应用保护** •应用程序包装 •信息防篡改 •运行时风险检测 •白名单/黑名单应用	**访问** •移动接入管理 •API 连接 **交易** •移动欺诈风险检测 •跨渠道欺诈检测 •浏览器安全/ URL 过滤

终端安全的管控

- 移动应用涉及环节多，网络不可控，需要完善的移动安全策略和方案
- 帮助医院将IT管理能力从传统的 PC 延伸到移动设备和移动应用APP

通过对移动终端设备的管控，确保设备、应用和数据使用安全，有效预防终端安全问题

行为审计

针对互联网访问行为的实时审计和监控

互联网医院会面对各种来自外部的攻击，需要对数据访问行为进行实时分析，及时阻断异常的请求，保障信息系统安全。

异常访问实时审计

- 传统的防火墙能够阻断Ddos等病毒攻击，但对以窃取用户数据为目的的黑客行为，需要更智能的算法，结合自动/人工的审计方式，来进行判定

通过对异常访问的行为审计，及时阻断非法的访问请求，保护数据不被故意窃取

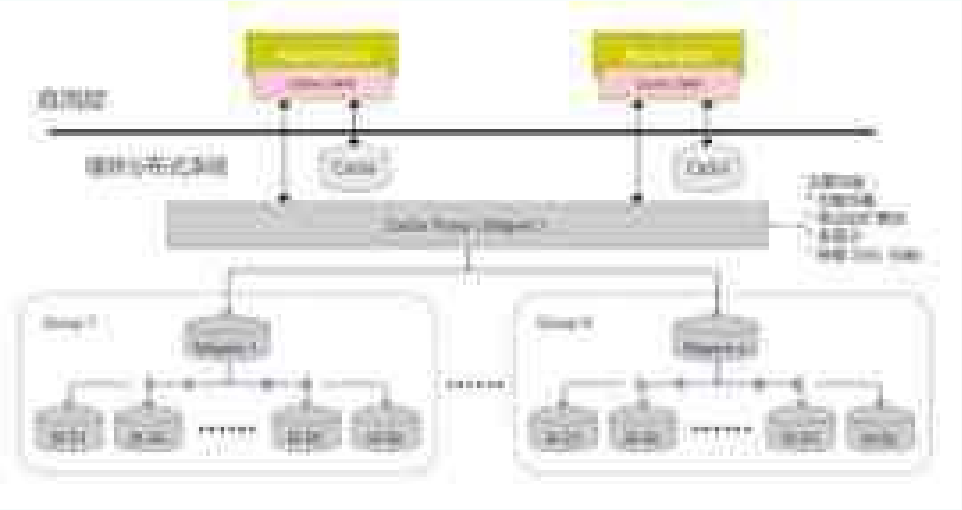
分布式集成架构

解决高并发互联网访问下医院信息系统稳定问题

行为审计

分布式缓存技术解决性能瓶颈问题

医院内部信息化系统，不能应对来自互联网的高并发访问冲击，需采用分布式缓存技术来构建缓冲层，来保障内部系统的可靠运行。



分布式应用协同架构

- ZooKeeper为分布式应用提供一致性服务的软件，提供的功能包括配置维护、域名服务、分布式同步、组服务等，它封装好复杂易出错的关键服务，将简单易用的接口和性能高效、功能稳定的系统提供给用户。

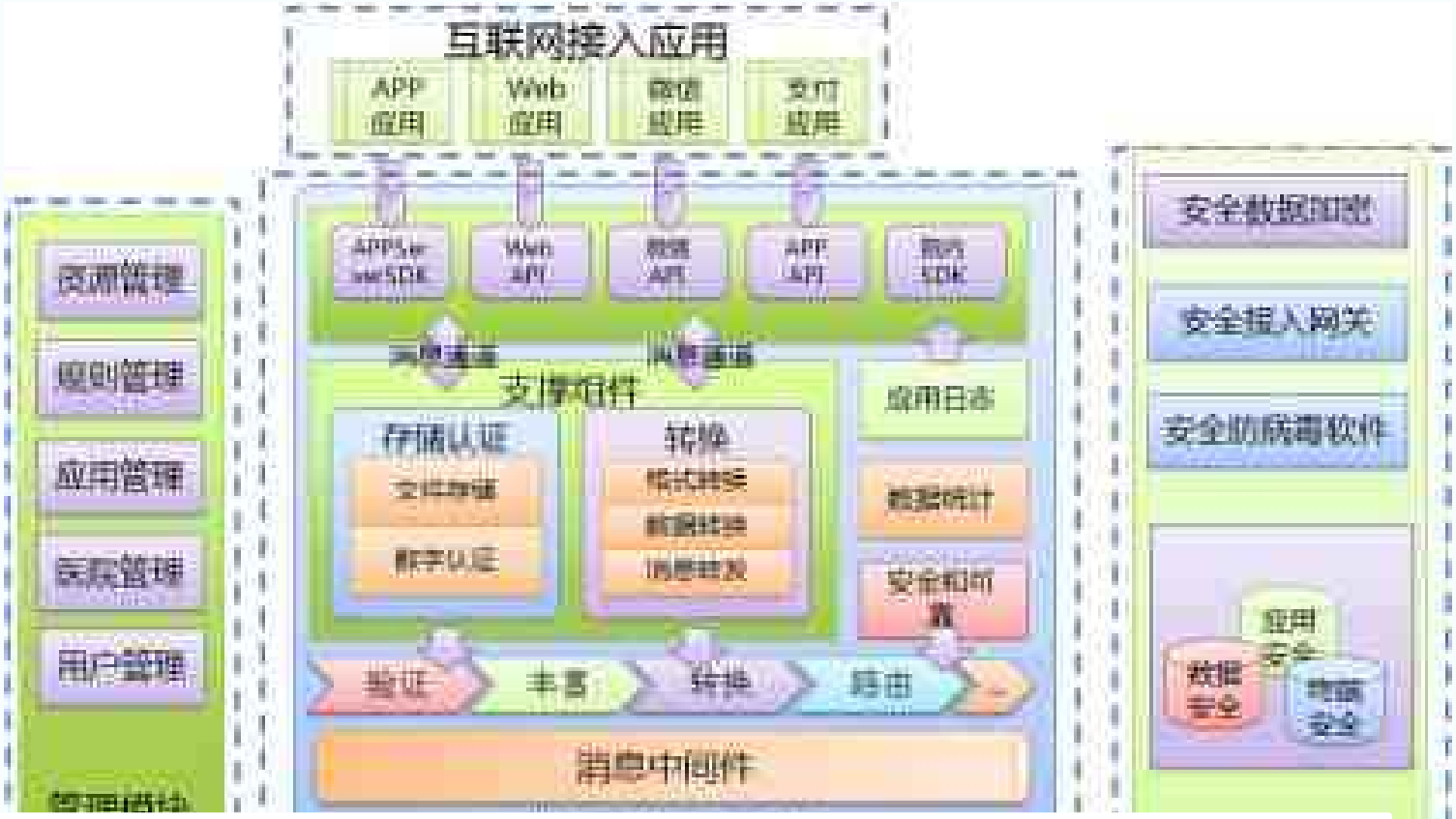
通过分布式技术构建访问缓冲层，避免互联网高并发访问对内部系统的性能冲击，保护医院信息系统的可靠运行

信息集成

医院轻量级信息集成与接入引擎技术

信息集成与接入管理

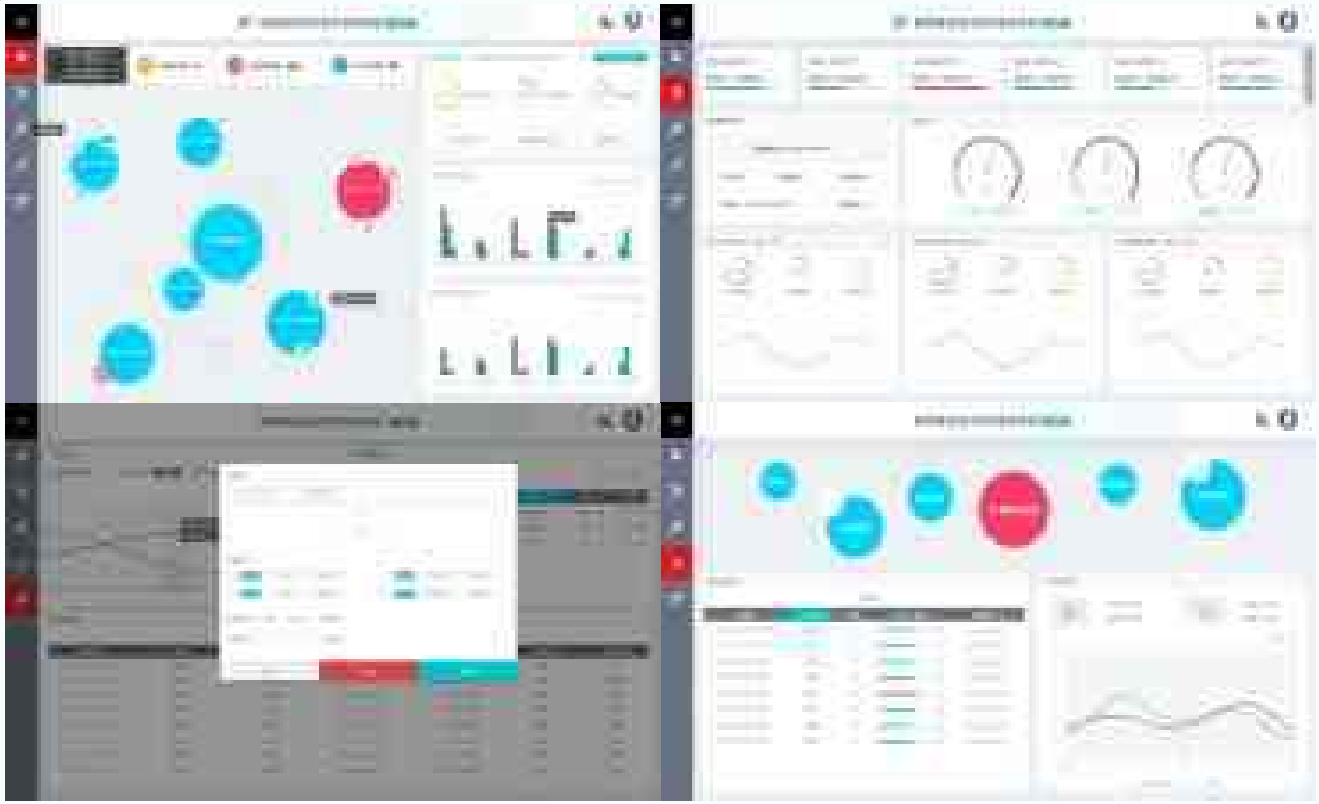
- 多种类型的应用接入方式
- 格式转换和隐私信息过滤
- 不同类型的通讯协议转换
- 消息的推送、订阅和分发
- 数据加解密和防篡改保护
- 分布式的文件数据存储
- 集群服务，防止单点故障



通过信息集成与接入引擎，提供互联网级架构支撑，保障互联网医院的运行可靠性

运维监控

针对医院互联网开放服务的实时运维监控



- **实时监控服务**
  - 服务器环境监控
  - 系统服务运行监控
  - 系统服务异常报警
  - 互联网APP应用监控
  - 异常行为分析报警
  - 访问日志审计分析
- **架构管理**
  - 分布式集群部署
  - 支持动态扩展
  - 杜绝单点故障
  - 7×24可靠运行

为医院提供对互联网服务的自主运维能力！

一体化开发管理工具

解决医院互联网医疗健康应用开发和管理问题

资源开放

针对医院信息化资源开放的标准化管理工具

- **标准模型库**
  - 70项HL7消息模型
  - 53项共享文档模板
  - 20项电子病历模板
  - 58项数据集标准
- **可视化编辑**
  - 数据映射配置
  - 数据赋值公式
  - 命名空间管理
  - 规则编译调试
  - 模型发布和版本管理

为医院带来基于图形界面的技术规范管理能力！

应用管理

针对医院信息资源、互联网应用和第三方厂商的管理

- **服务管控**
  - 注册审核
  - 接入认证
  - 流程审批
  - 证书发放
  - 资源授权
  - 运营监管
  - 黑名单管控
- **AAAA管理**
  - 统一用户管理
  - 统一认证管理
  - 统一授权管理
  - 统一审计管理

让医院摆脱对软件厂商的技术服务依赖！

统计分析

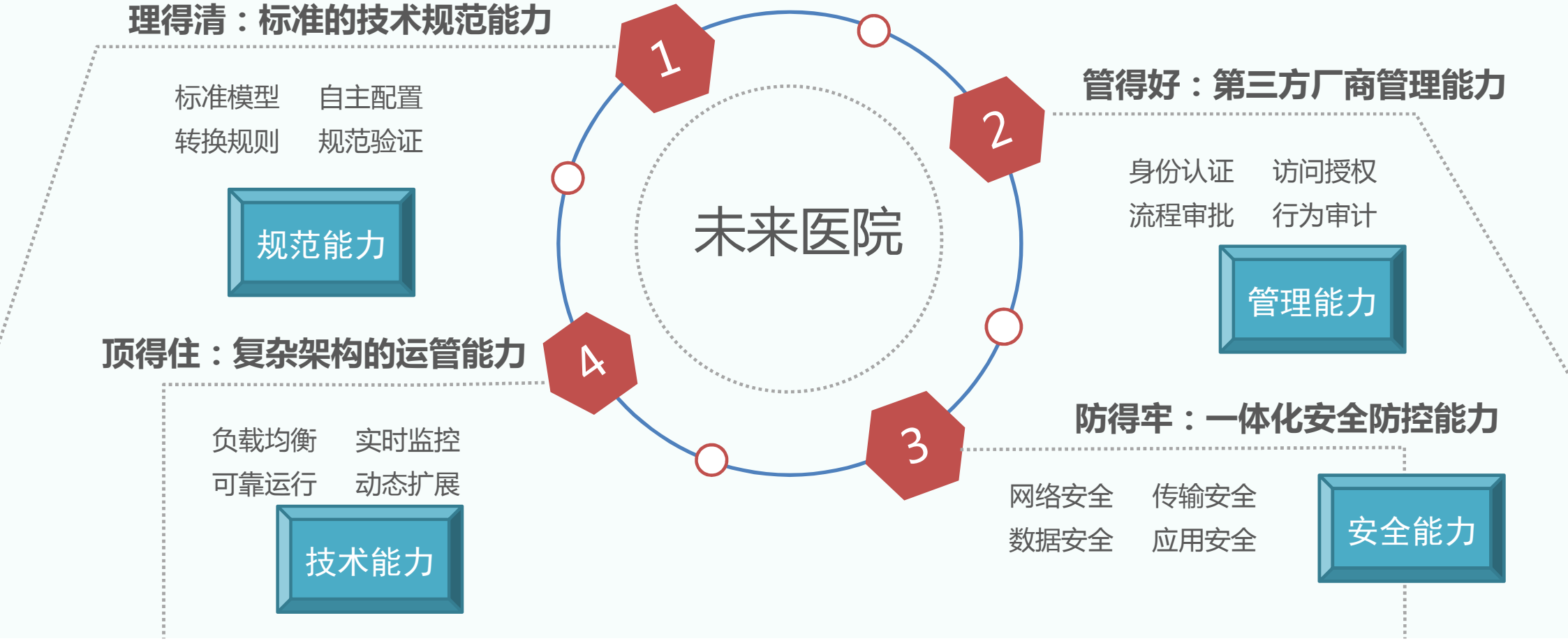
针对医院互联网服务访问情况的统计分析

- **应用统计分析服务**
  - 日统计报表
  - 月统计报表
  - 年度统计报表
  - 同比环比分析
  - 接口调用分析
  - 数据频率分析
  - 自定义报表分析

为医院提供对互联网服务的业务统计分析能力！

能力

互联网时代医院开放服务需要的四大能力



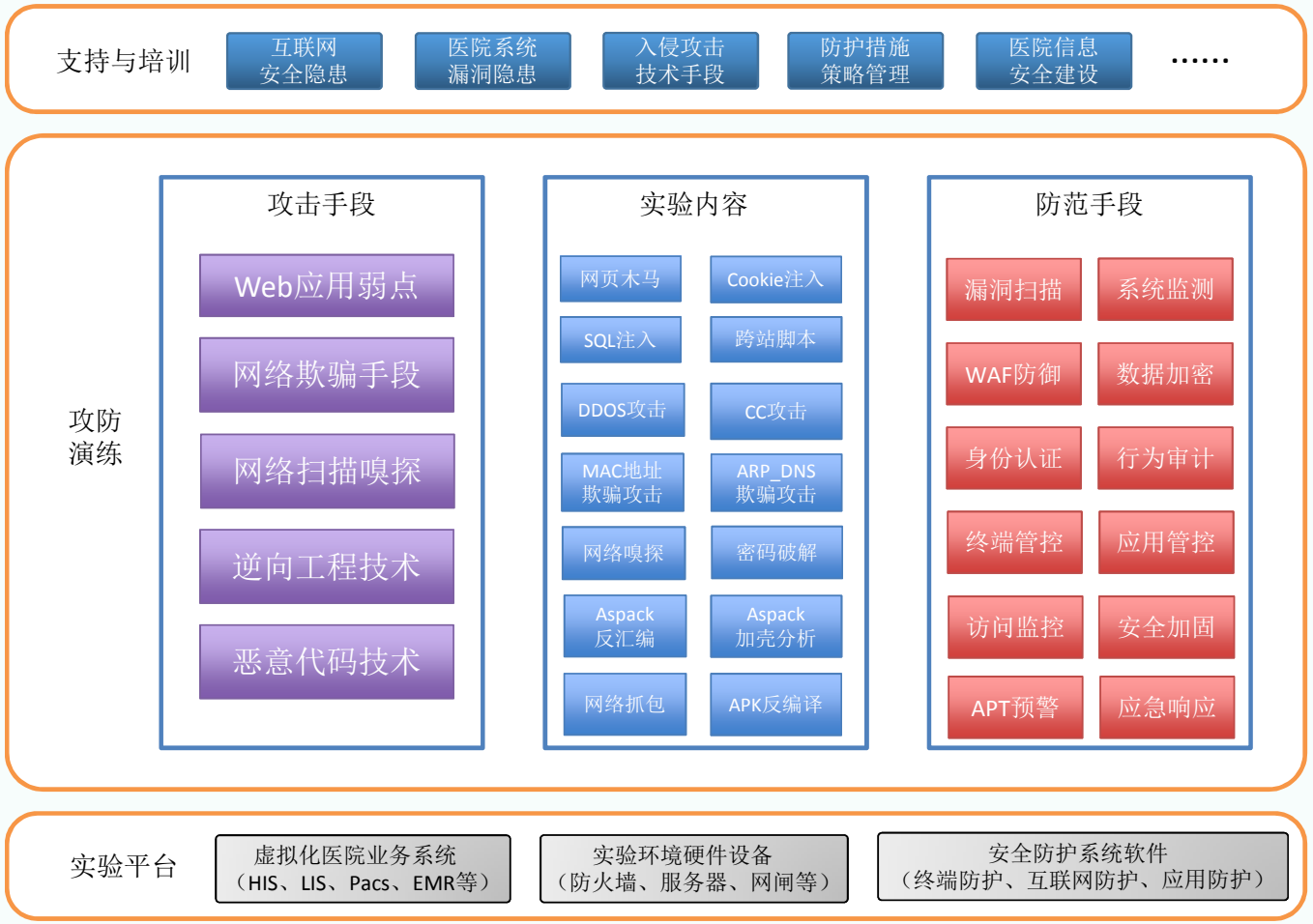
互联网医疗健康服务现状与问题

医院互联网开放服务安全开放解决方案

应用推广与典型医院成功案例介绍

攻防演练

浙江大学建设“互联网医院攻防演练实验室”



- **教学实践**
  - 信息安全培训
  - 安全技术培训
  - 技术实训实验
- **安全建设**
  - 信息安全指导
  - 信息安全建设
- **仿真演练**
  - 漏洞扫描演练
  - 入侵攻击演练
  - 防范措施演练

案例

目前合作的医院和厂商

18家医院

33家机构

35个移动互联网应用

案例

成功案例分析

浙江大学医学院附属第二医院
The Second Affiliated hospital of Zhejiang University School of Medicine

总理给医改留下了“两道题”：一是远程医疗的隐私保护、信息安全等，运用网络平台，把优质资源更好地辐射到更多的地区；二是社会办医如何管理好，要鼓励社会资本参与到医疗，同时要加强监管。

专业服务

成立产业化公司提供产品、实施、运维一系列专业服务

在浙江大学工业研究院的支持下成立天津医康互联科技有限公司，专注于提供医院+互联网一体化安全解决方案，满足医院对互联网应用的管理需求，提供可靠的互联网服务运维管理环境，为医院顺利进入互联网时代保驾护航。

荣获
国家科技进步二等奖
及省部级奖项四项

- 依托**浙江大学计算机学院、浙江大学滨海产业技术研究院**开展创新模式研究和关键技术攻关
- 依托**浙江大学工业技术研究院**提供专业化服务和成果产业化推广
- 团队在平台及数字医疗健康领域，已发表高质量论文172篇，获得发明专利95项，软著27项

Thank You

李莹 cnliying@zju.edu.cn