



尚云互联

尚云互聯產品介紹

P2P 连线平台

深圳市尚云互聯技术有限公司
CS2 Network



成功的P2P平台

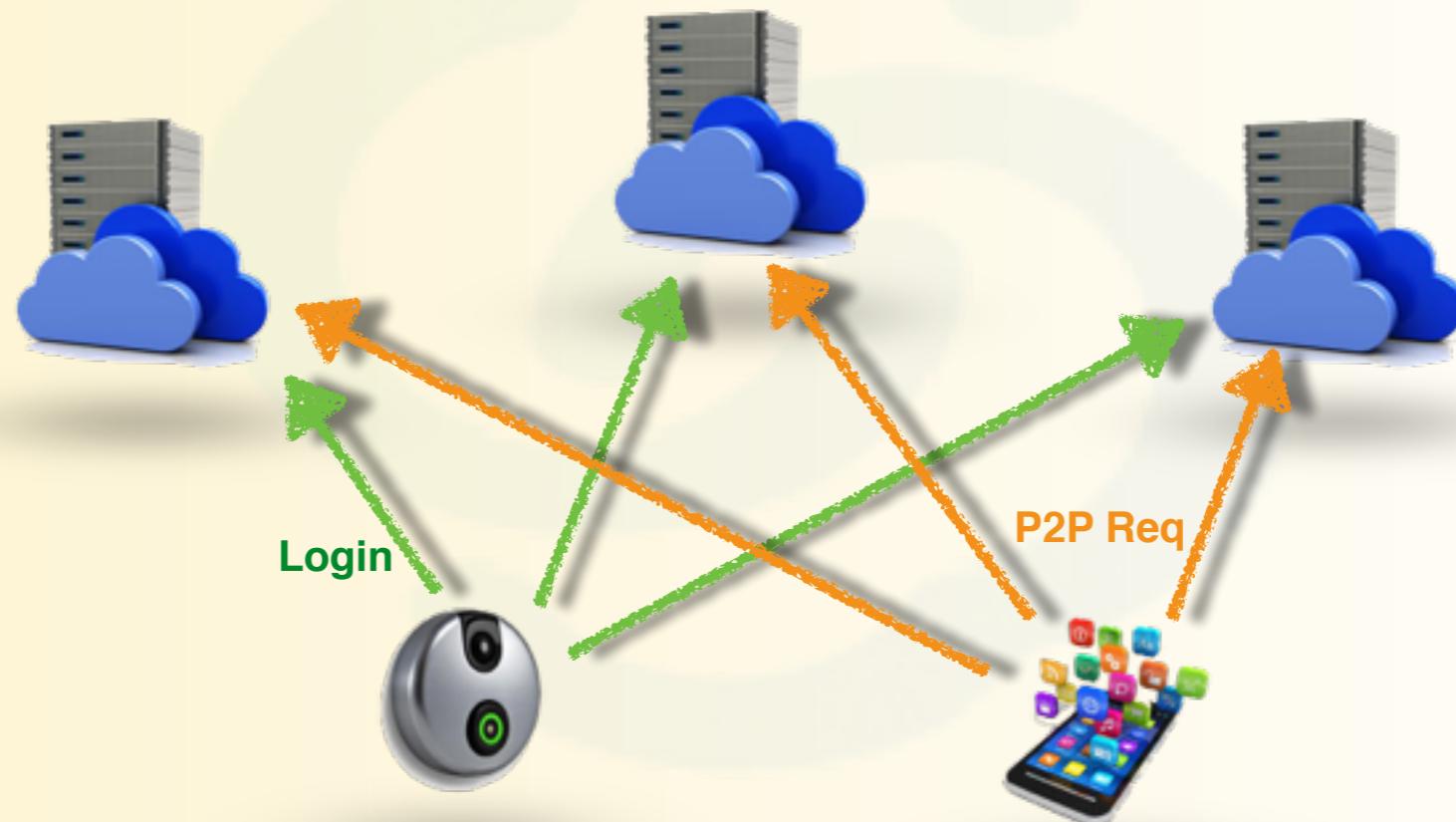
- 尚云的P2P是长时间经过大量用户验证过的
 - 平台的架设套数已达100多套
 - 总出货的ID号数量超过500万
 - 因为平台设计缺失而导致的故障事故数为零
- 使用尚云的P2P平台不会让您成为白老鼠



技术面的优势功能

- 完善的备援架构
- 简单易上手的API设计
 - 尚云P2P的API函数与TCP Socket几乎一样
- 设备转发功能
- 安全性
 - 共有三道保护机制防止平台遭受假设备的攻击

备援架构



主控服务器最多可以有3台

- 现实的Internet并不是想像中的完美,因此备援是绝对需要的
- 主控服务器彼此独立,且不知道有对方的存在,只要有一台主控,就足以让整个平台正常运行

转发服务器没有理论上的上限

- 可以随时视情况调整
- 调整后立即生效



TCP-Socket-Like API

“尚云的P2P跟TCP Socket API在使用上几乎没有多大的差异”

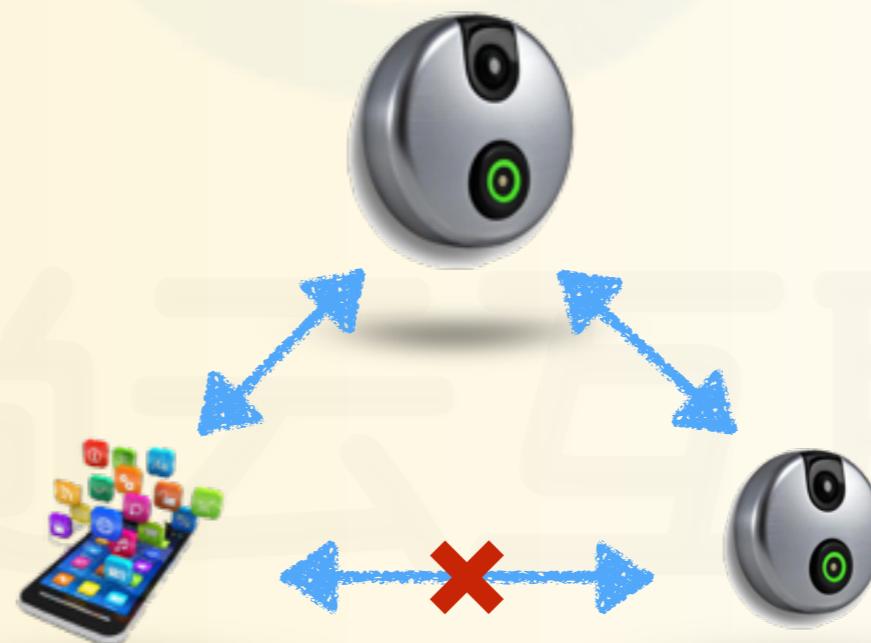
连线流程相似都是Listen() / Connect() / Close()

数据传输都是流的形式, 都保证送达

资料收送函数一样, 收用Read(), 送用Write()

设备转发

1. 使用尚云P2P的智能设备产品, 在网路条件许可之下, 可以充当转发服务器来提供转发服务给别的设备, 先决条件是: 设备转发功能已开启
2. 使用设备当作转发服务器, 可以有效的降低转发服务器的带宽流量(理想条件下可达90%)
3. 设备转发的控制只需要一个API函数: Share_Bandwidth(0 or 1)



安全性

- 所有P2P平台最为棘手的安全性问题是所谓的假设备的攻击方式
 - 假设有某人盗取了您卖出的所有设备的ID号
 - 他可以简单的写几行程序使用这些ID号来登入您的平台, 进而造成该ID号的真正设备无法使用
- 假设备攻击方式不仅是瘫痪正常的设备的使用, 还可能盗取客户的机密, 影响层面可能非常大



针对假设备的攻击尚云的P2P一共有三道防护



三道防护

- 第一道. 尚云的ID号, 包含两个部分
 - 明码: 也就是DID本身, 例如: **ABCD-123456-GHKLM**
 - **DID**是贴在机身外面给用户添加设备用的
 - 暗码: 也就是P2P API License, 也就是跟在DID后面的六位字母**ABCD-123456-GHKLM,PQRSTU**
 - **API License**是P2P库调用的时候用的, 不需要提供给用户
- 第二道. 尚云的P2P的服务器主机地址串为加密过的
 - 即使借由封包监听得知主机地址也无法使用
- 第三道. 用户可以自定义服务器的CRCKey,
 - 没有正确的CRCKey, 即使知道完整的DID以及地址串也无法登入到服务器上

自主掌握

- 尚云P2P平台的服务器是由客户自己搭建, 自己管理, 且营运权力属于客户
 - 尚云仅提供服务器程序, 以及技术手册
- 尚云的P2P平台架构中并没有根服务器
 - 用户所搭建的主控服务器就是整个平台的管理者了
- 尚云的P2P的License为终生有效
 - 一旦购买之后, 即属于用户所有



请与我们联系



深圳市尚云互联技术有限公司

地址: 深圳市龙华新区清祥路1号宝能科技园宝创大厦9栋B座17楼S单元

TEL: +86 755 36600360

FAX: +86 755 36600361

尚雲互聯技術有限公司 42763893

台灣新竹縣竹北市復興二路229號11樓之五

TEL: +886-3-6670428



敬请随时关注尚云互联公众号