

# Online Fraud Detection with AI

Yanhui Wang (wangyanhui@360.cn)

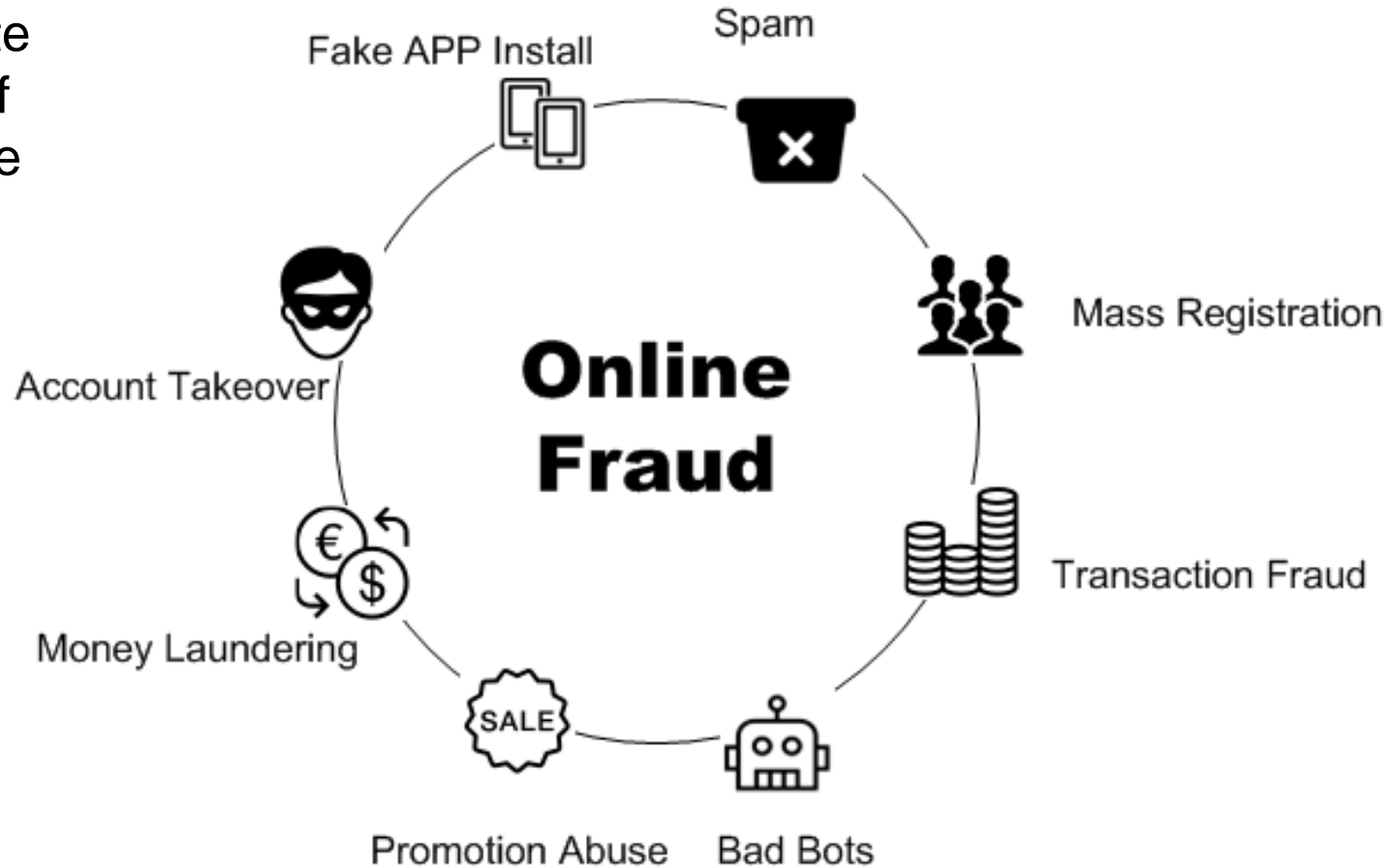
# AGENDA

1. ONLINE FRAUD
2. FRAUD DETECTION WITH AI
3. THE CHALLENGE IN THE FUTURE

# 1. ONLINE FRAUD

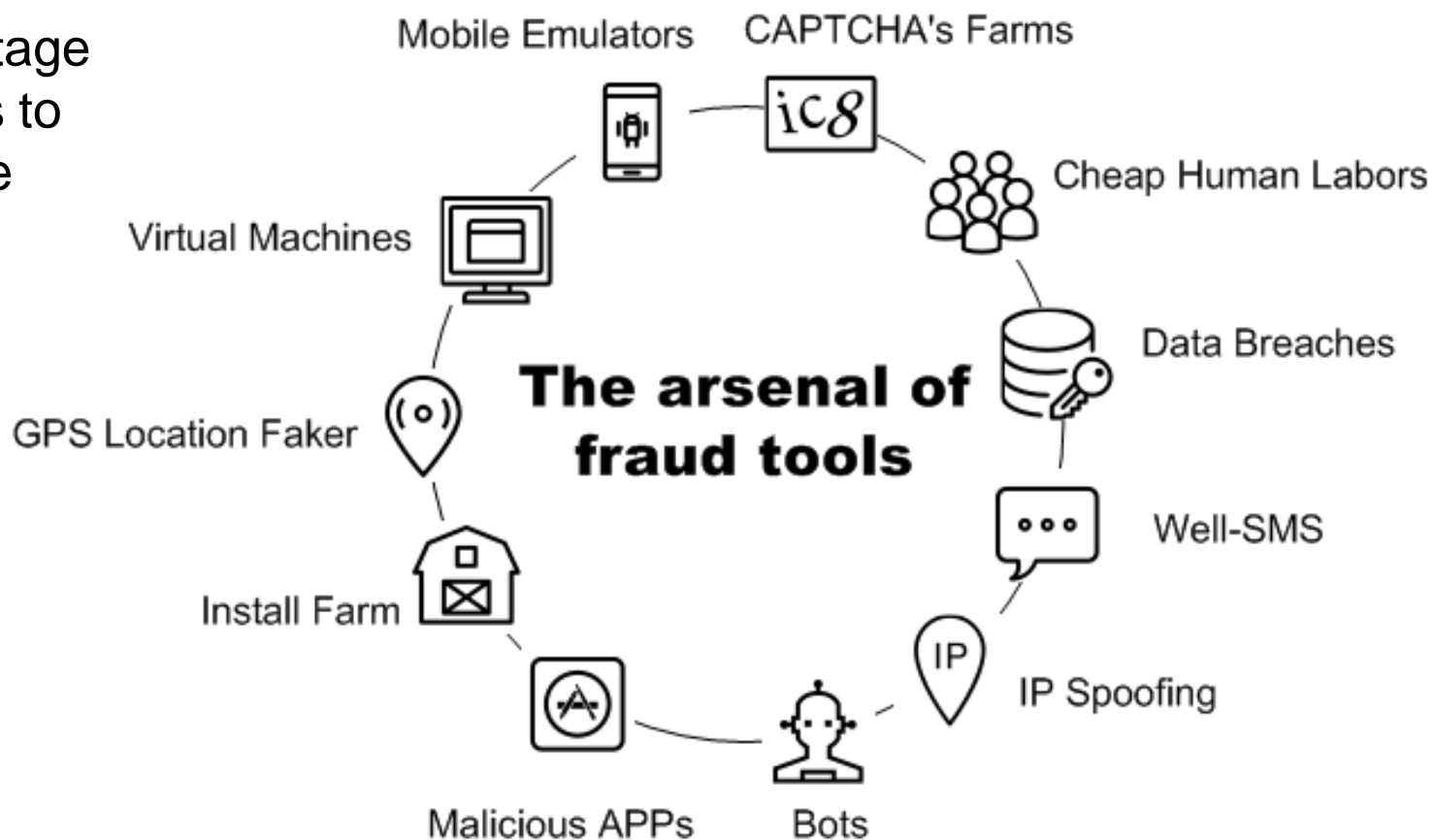
# 1. ONLINE FRAUD

Online fraud is quite popular because of the growth of online services.



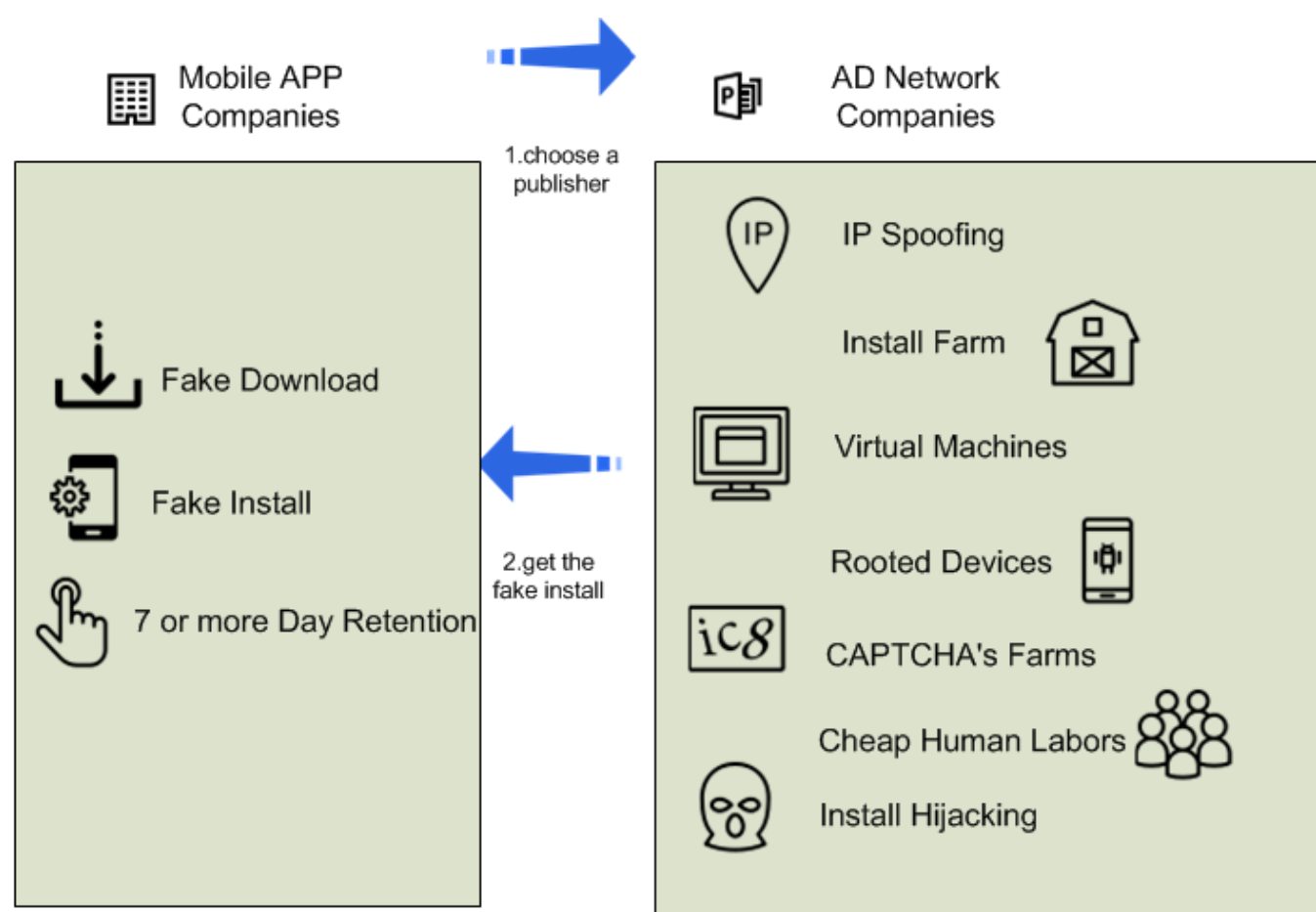
# 1. ONLINE FRAUD

Bad actors take advantage of various technologies to make profits and evade detection.



# 1. ONLINE FRAUD

A typical Scenario of online fraud-User Acquisition Fraud which means fraudsters trick advertisers into spending money on fake users and fraudulent traffic.

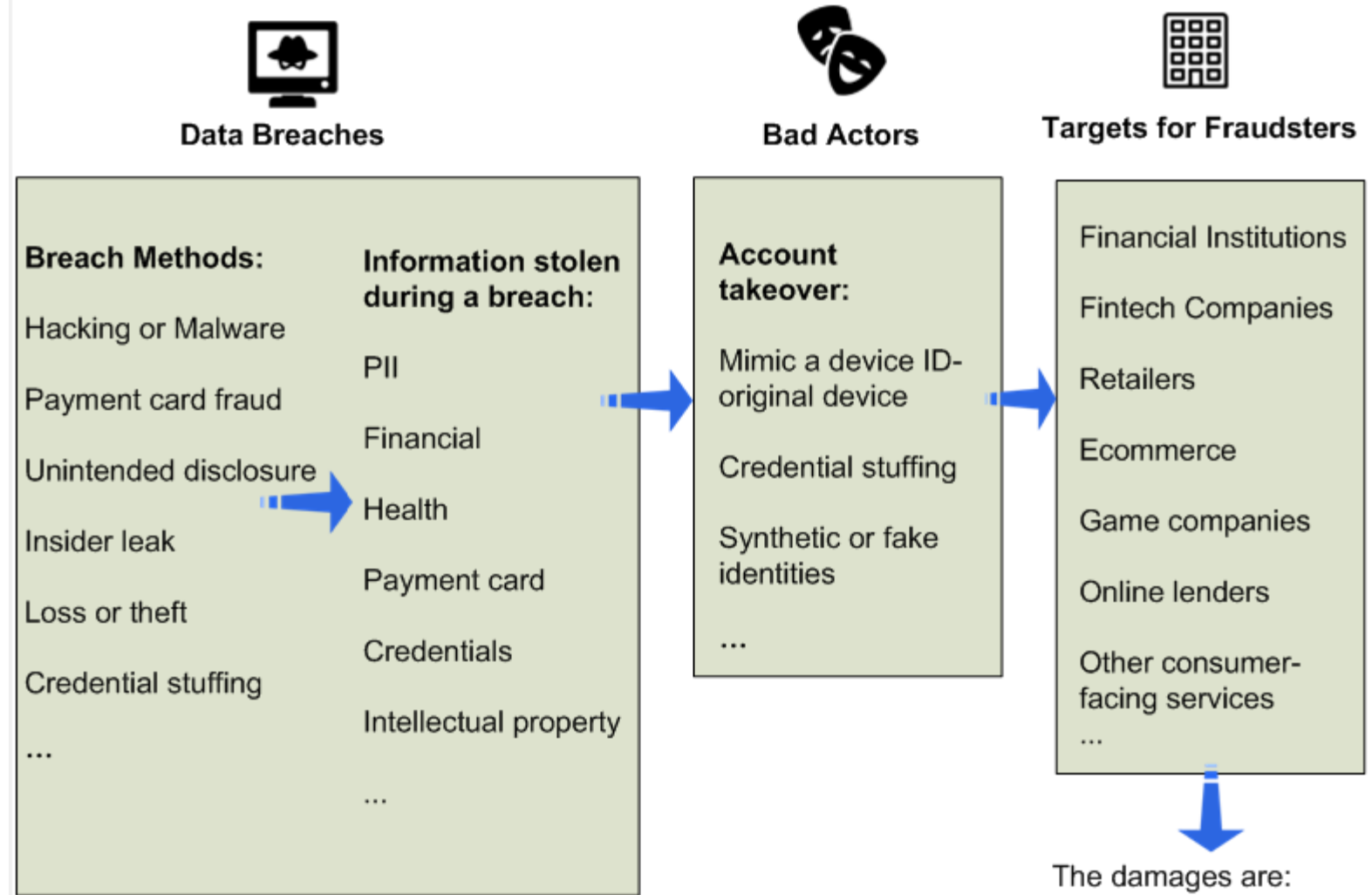


The damages are:

- (1) reputation degrade
- (2) loss in ad revenue
- (3) a stagnant user base

# 1. ONLINE FRAUD

A typical Scenario of online fraud-account takeover fraud, where a fraudsters takes over an account using an account holder's online credential.

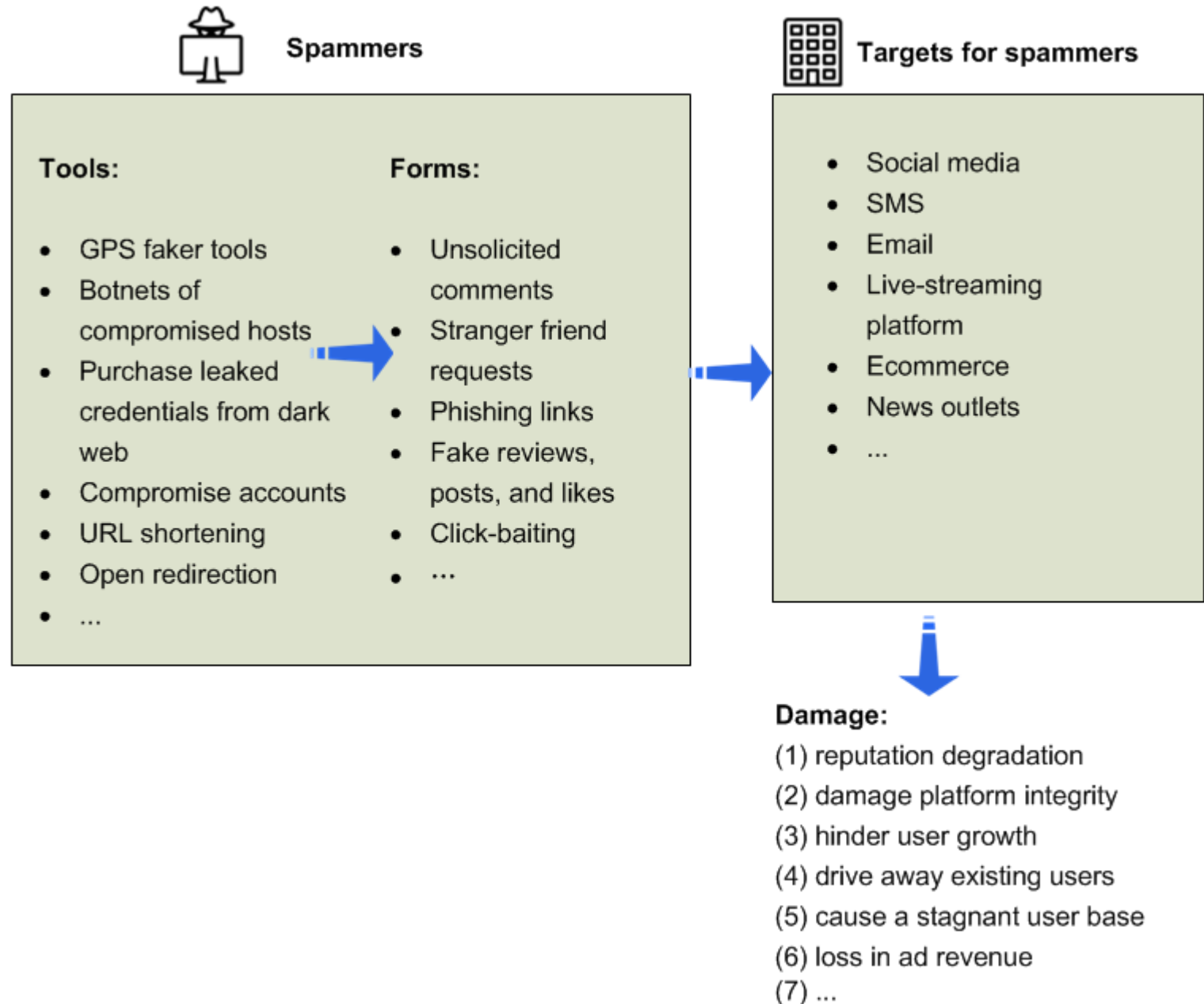


The damages are:

- Financial loss
- Reputational and brand damage
- ...

# 1. ONLINE FRAUD





A typical Scenario of online fraud-spamming, which is the use of messaging systems to send an unsolicited message (**spam**), especially advertising, as well as sending messages repeatedly .





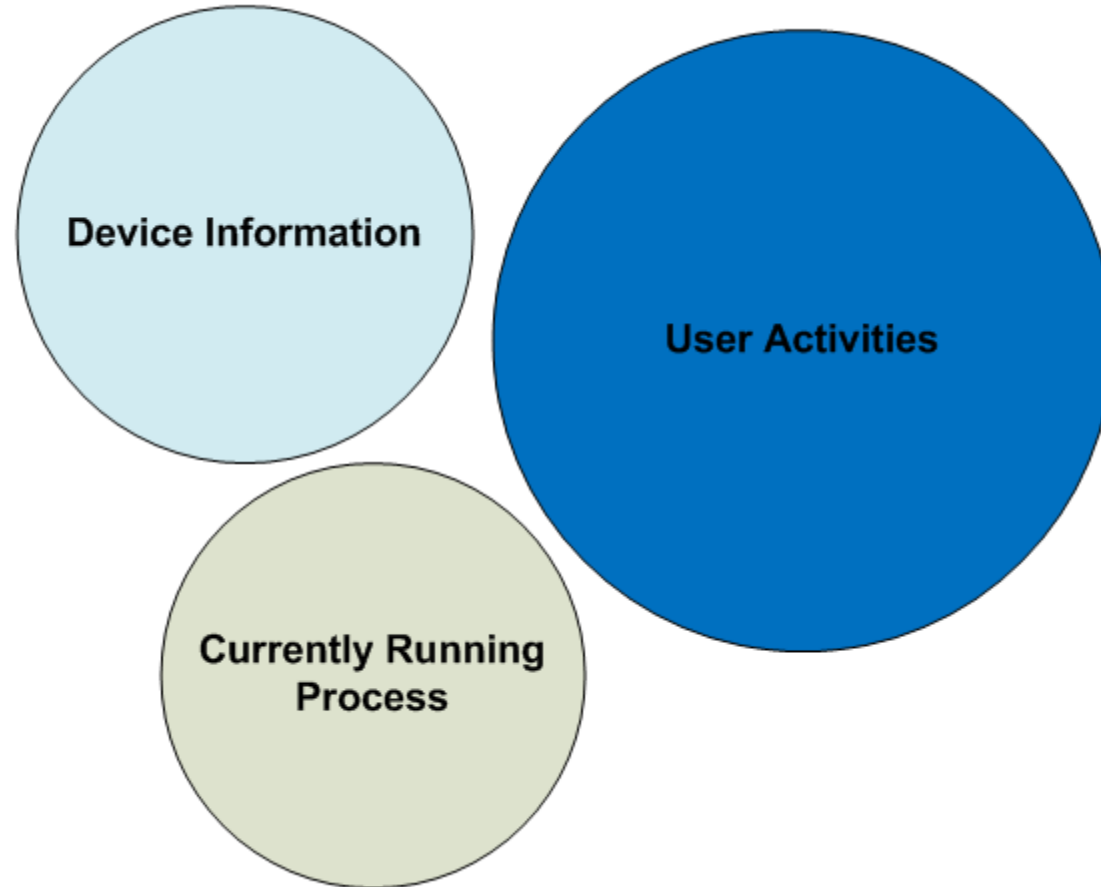
## 2. FRAUD DETECTION WITH AI

# THE TRADITIONAL METHODS TO COMBAT FRAUDSTERS:

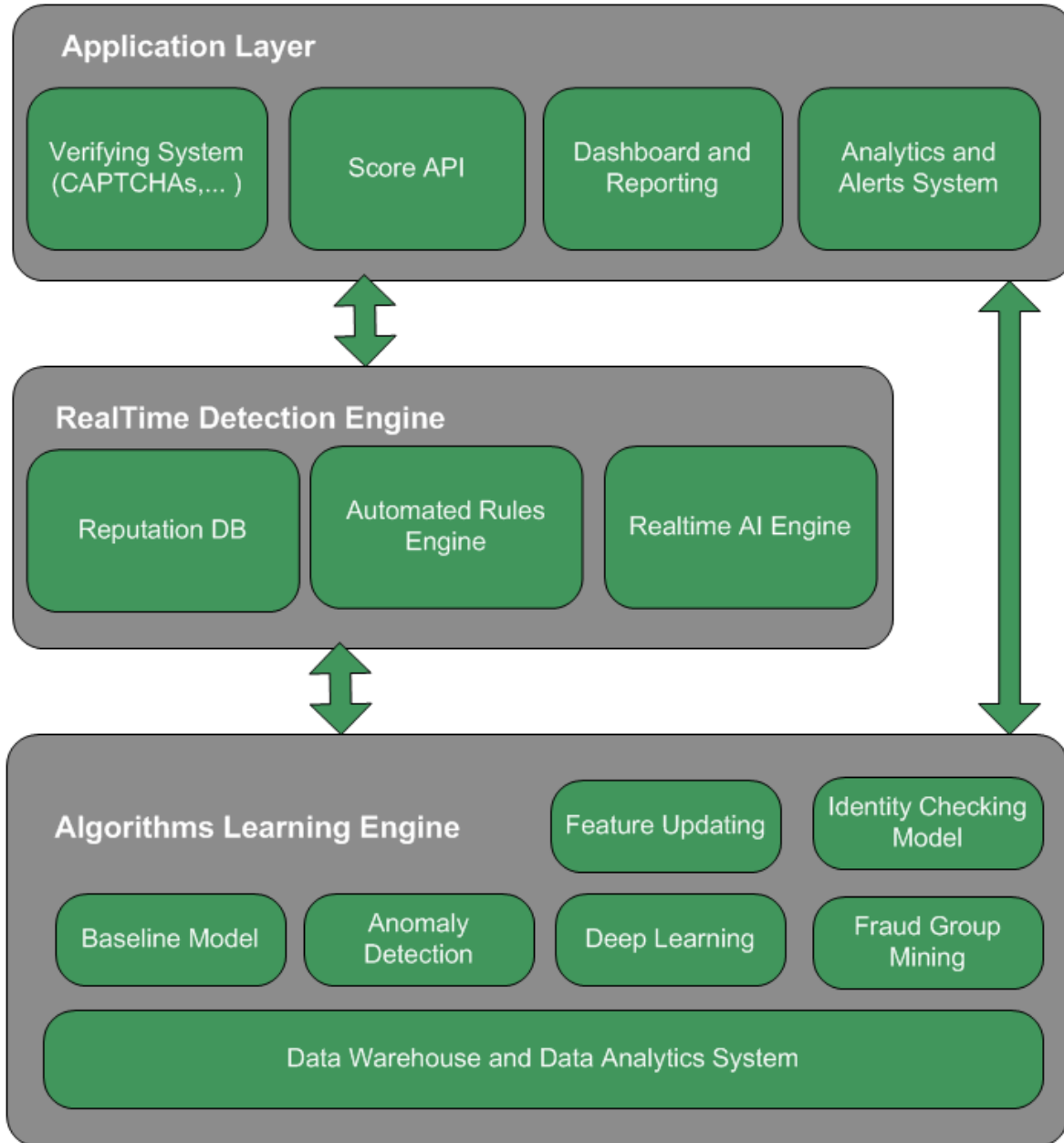
Methods	Techniques	Disadvantages
 <b>Device Fingerprinting</b>	Device id, biometrics, smartphone sensors, GPS, gyroscope, accelerometers, WiFi networks...	Mobile device flashing, Jailbroken/rooted devices,...
 <b>ID Verification</b>	CAPTCHAs, SMS, email verification, two-factor authorization (2FA), three-factor authorization(3FA, including phone number, Identity number, name)...	Various anti CAPTCHAs tools, Modem Pool, stolen credentials, synthetic or fake identities, fake phone number...
 <b>Reputation lists</b>	IP, device, user accounts, phone number, email, etc.	Mobile device flashing, IP agency,...
 <b>Rules Engines</b>	Black lists (e.g. IP addresses), negative lists, weighted scoring mechanisms, business rules, etc.	Simulate real users' activities in the services

# THE INFORMATION WE CAN USE:

User activities are the best features which is hard to be mimicked by fraudsters.



## Realtime Fraud Detection Platform(RTFDP)



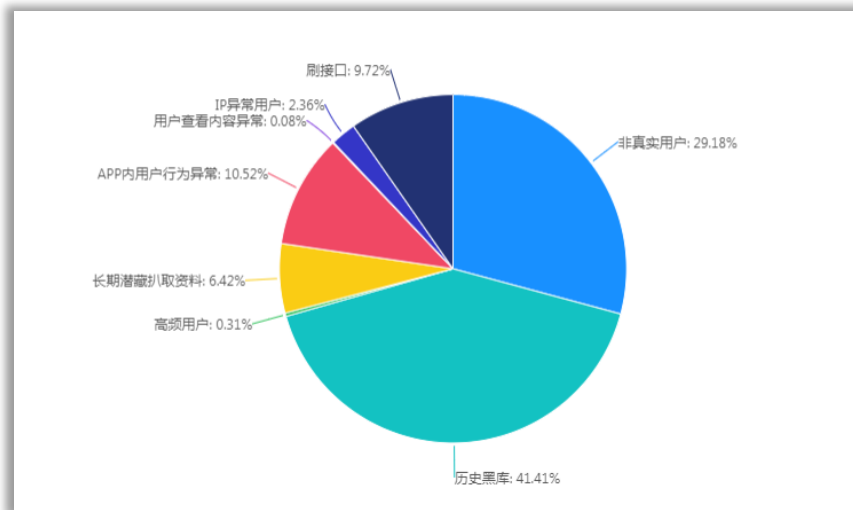
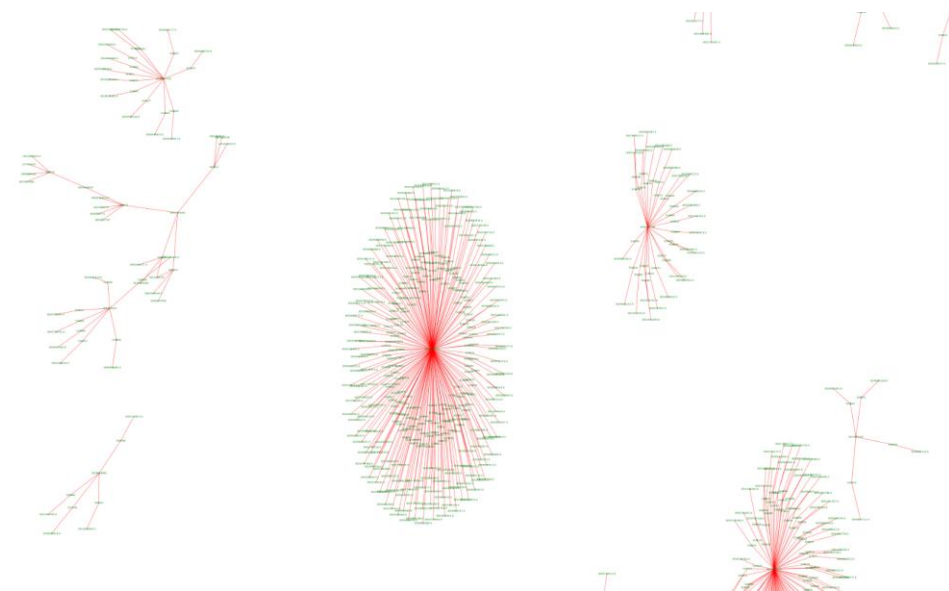
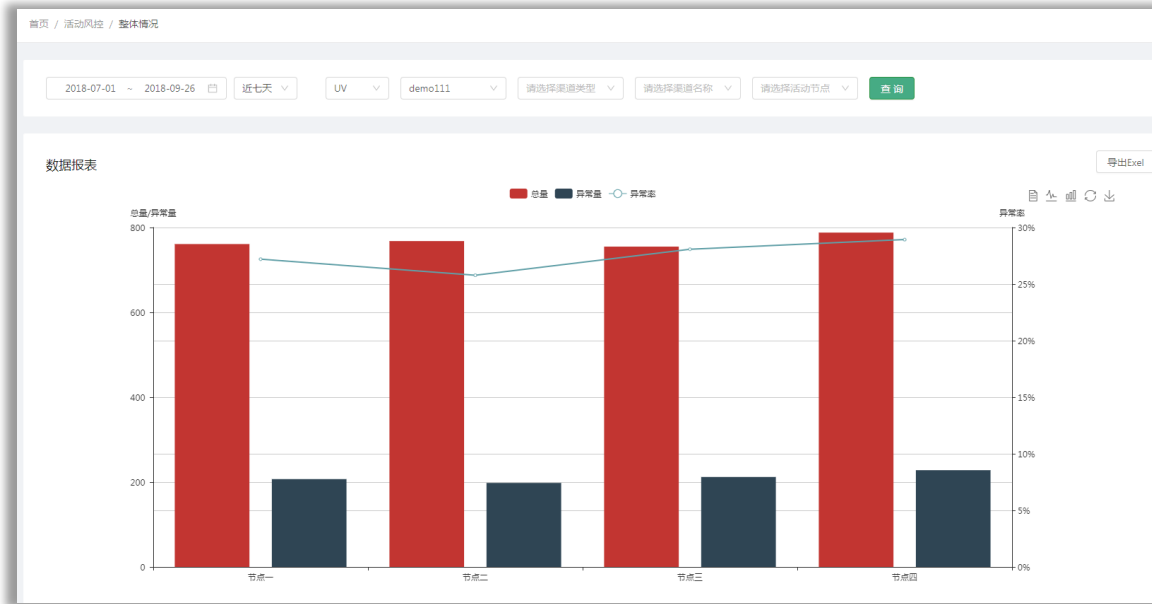
## RTFDP

This platform consists of three layers: Algorithms Learning Engine, RealTime Detection Engine, and Application Layer.

We store all the historical activity information about a user, and judge whether the user is a bad actor whenever he/she generates a new activity.

We credit every user with a score which is range 0 and 1, and the service provider can take measures to block the bad actor correspondingly.

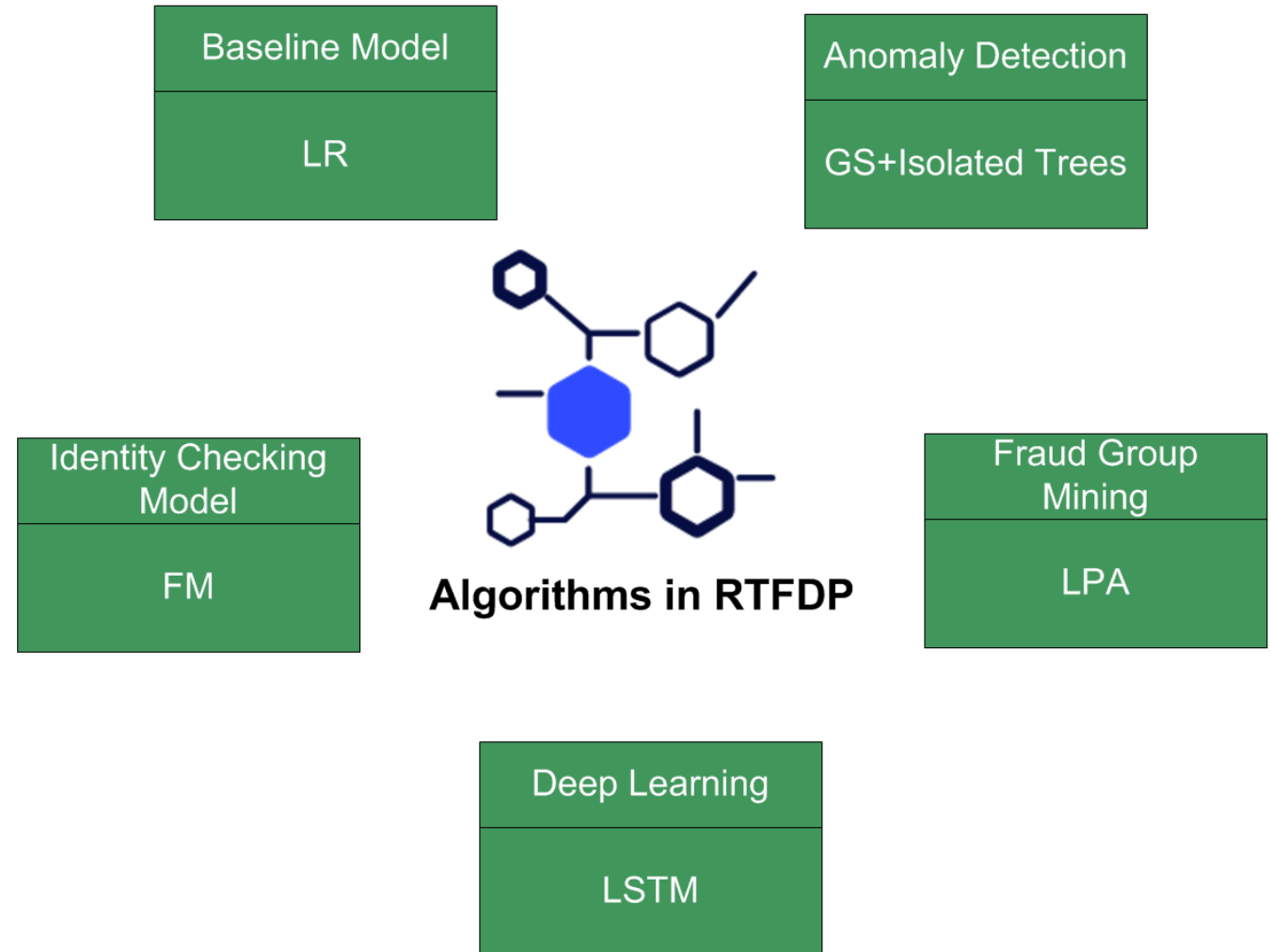
# DASHBOARD AND REPORTING



# THE ALGORITHMS IN RTFDP:

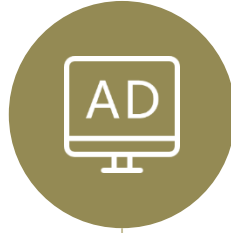
The Algorithms in RTDP include:  
LR, GS+Isolated Trees, FM, LPA,  
LSTM.

We are now researching on using  
more AI algorithms to detect more  
Fraudsters, such as  
CNN+LSTM+CRF.



# SOLVED PROBLEMS:

This system can solve these problems effectively.



User Acquisition Fraud



Bad Bots



Marketing Campaign



Fake App Install



Account takeover



Fake traffic

## WHAT WE FOUND IN OUR ONLINE SERVICES ARE:



Bad Bots: 0.5% of the UV in an app are bad crawler bots.

Fake APP Install: over 60% APP install from DSP is fake.

Spam: 20% posts in our live streaming platform are fake.

Device info: fraudsters tend to use older devices because of low costs.

Location: most of bad actors in China are located in Guangdong province.



### 3. THE CHALLENGE IN THE FUTURE

### 3. THE CHALLENGE

- Cyber attackers are constantly devising new techniques to evade security defenses.



- They use the latest mobile hacker tools and cloud technology to impersonate legitimate users. They even begin to use AI to emulate real users' activities.

- Increasing data breaches make it easier for fraudsters to commit various frauds. With all compromised credentials and PII, bad actors can act as legitimate users.

- Fraudsters have begun to use real users to cheat by offering online lucrative jobs. These users are real users, but they are not our targeted users.

# Thanks