Demystifying the Underground Ecosystem of Account Registration Bots

Ongoing work presentation

Yuhao Gao - Nov/12/2021

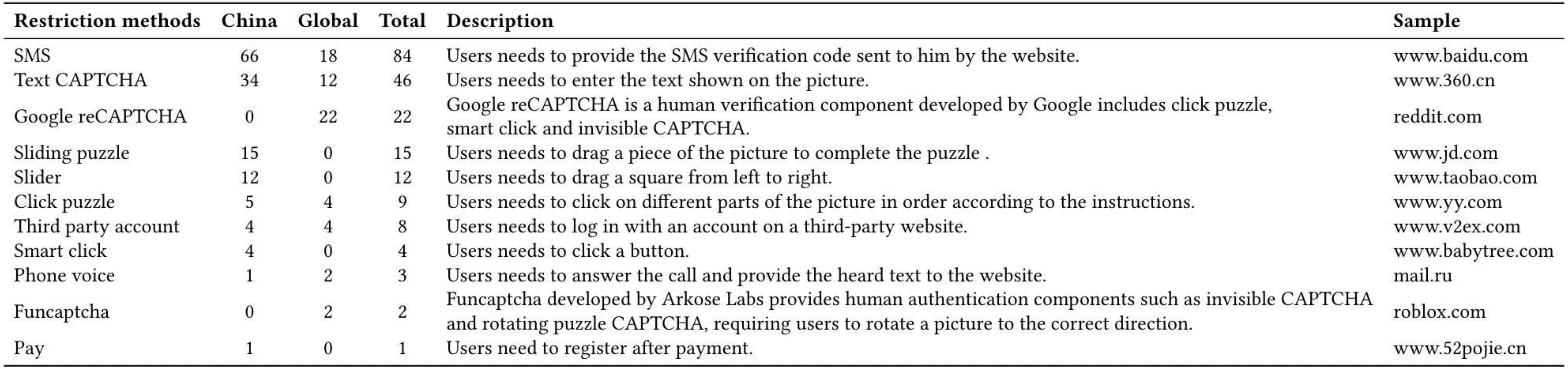
1.Background & Preliminary Study

1/3 Existing Malicious Register

- A numerous amount of malicious accounts (zombie accounts) on the internet
    - Especially the online society websites (e.g. Facebook twitter Weibo)
- A variety of uses of malicious accounts:
    - Fake likes and hits (e.g. Facebook)
    - Abuse of promotions (e.g. Amazon Taobao)
- Lack of register limitation??

1.Background & Preliminary Study

2/3 Human Verification methods used by top websites*

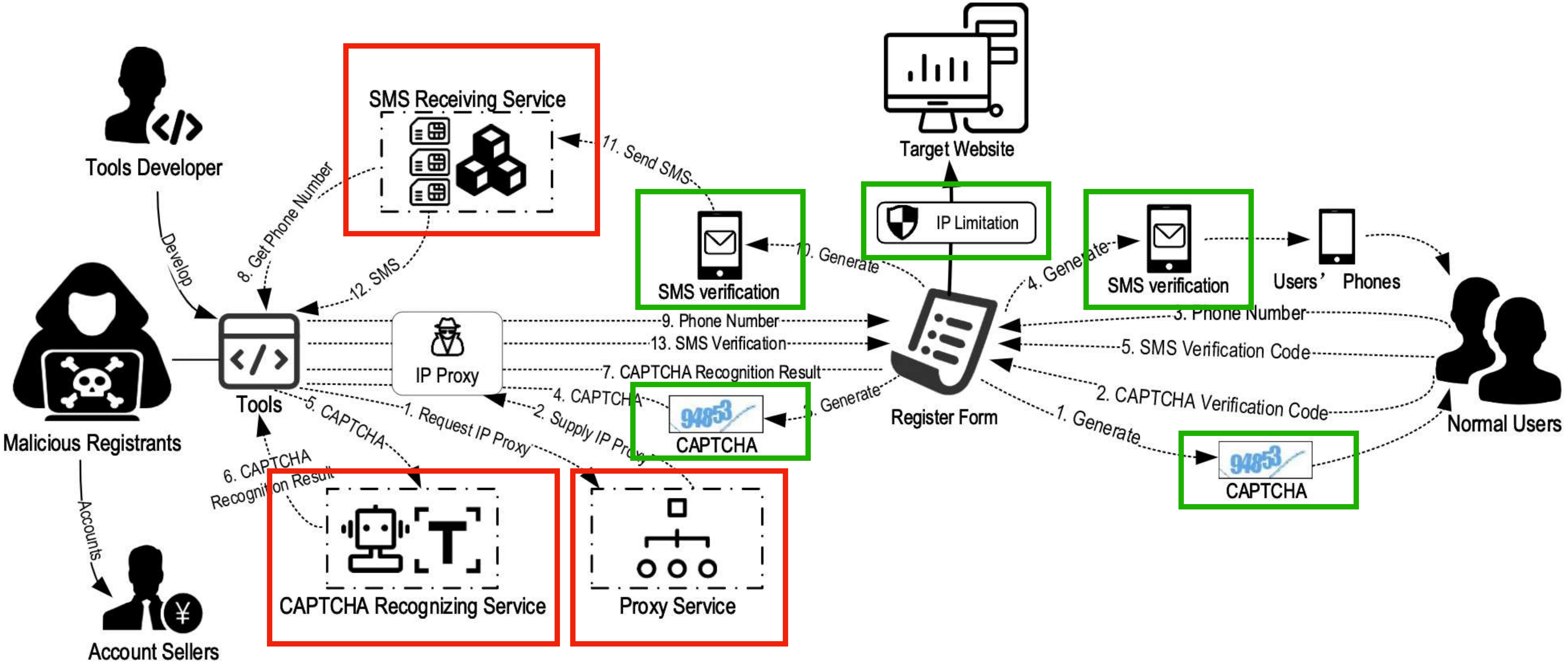


Restriction methods	China	Global	Total	Description	Sample
SMS	66	18	84	Users needs to provide the SMS verification code sent to him by the website.	www.baidu.com
Text CAPTCHA	34	12	46	Users needs to enter the text shown on the picture.	www.360.cn
Google reCAPTCHA	0	22	22	Google reCAPTCHA is a human verification component developed by Google includes click puzzle, smart click and invisible CAPTCHA.	reddit.com
Sliding puzzle	15	0	15	Users needs to drag a piece of the picture to complete the puzzle .	www.jd.com
Slider	12	0	12	Users needs to drag a square from left to right.	www.taobao.com
Click puzzle	5	4	9	Users needs to click on different parts of the picture in order according to the instructions.	www.yy.com
Third party account	4	4	8	Users needs to log in with an account on a third-party website.	www.v2ex.com
Smart click	4	0	4	Users needs to click a button.	www.babytree.com
Phone voice	1	2	3	Users needs to answer the call and provide the heard text to the website.	mail.ru
Funcaptcha	0	2	2	Funcaptcha developed by Arkose Labs provides human authentication components such as invisible CAPTCHA and rotating puzzle CAPTCHA, requiring users to rotate a picture to the correct direction.	roblox.com
Pay	1	0	1	Users need to register after payment.	www.52pojie.cn

* Top 100 websites from the Alexa Top List

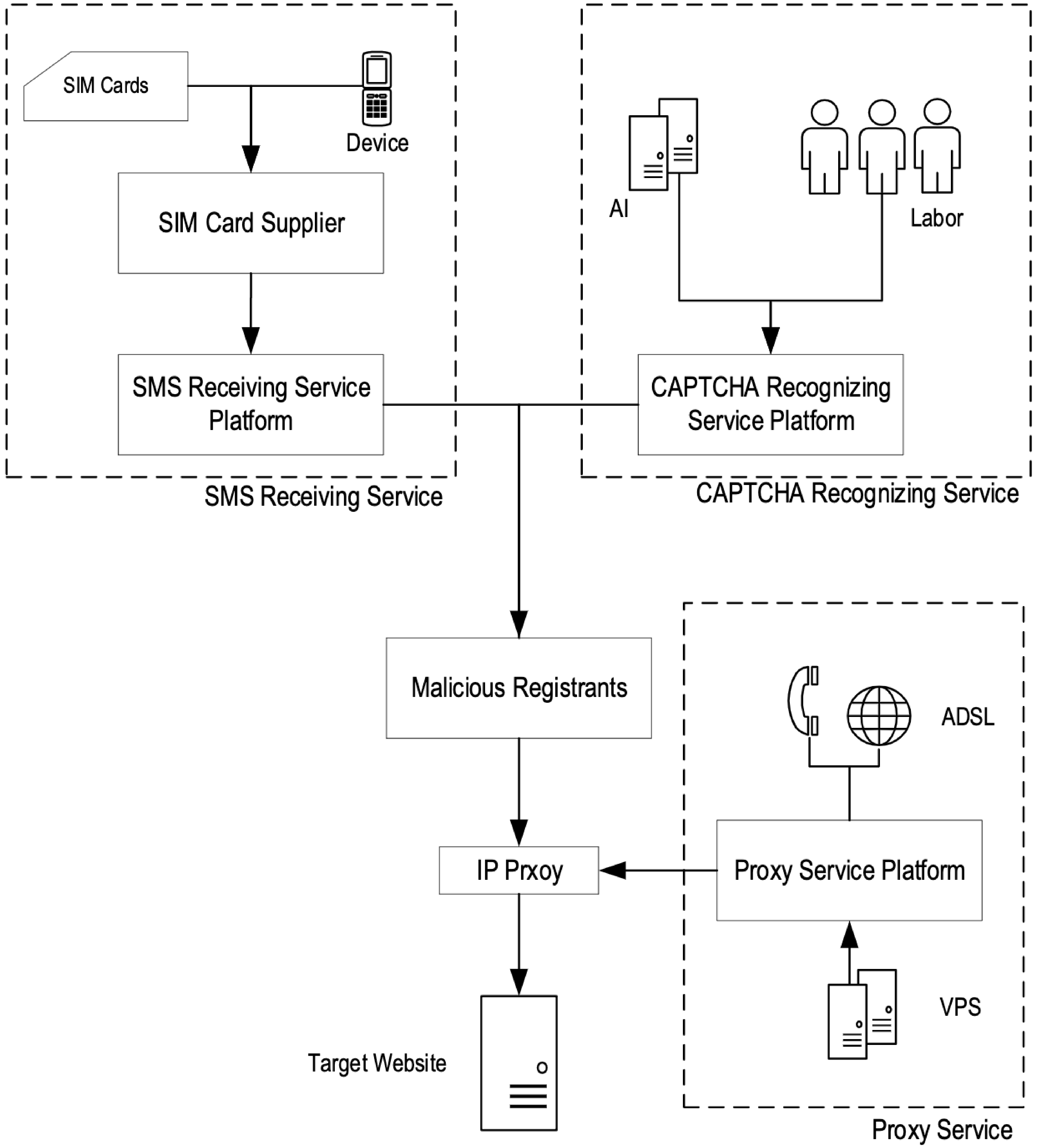
1.Background & Preliminary Study

3/3 The ecosystem of malicious registration



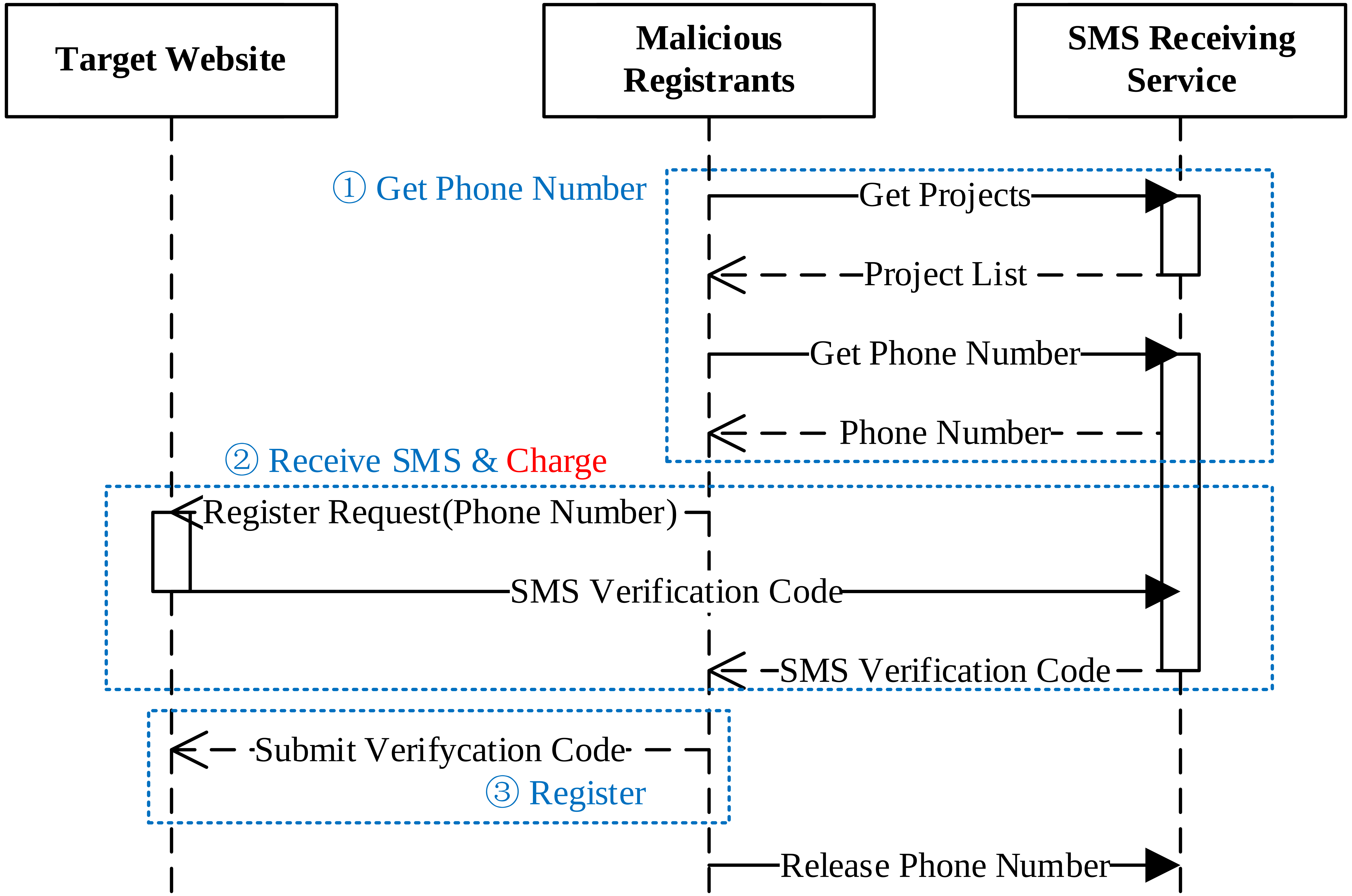
2.Demystifying Anti-human Verification Services

Overall



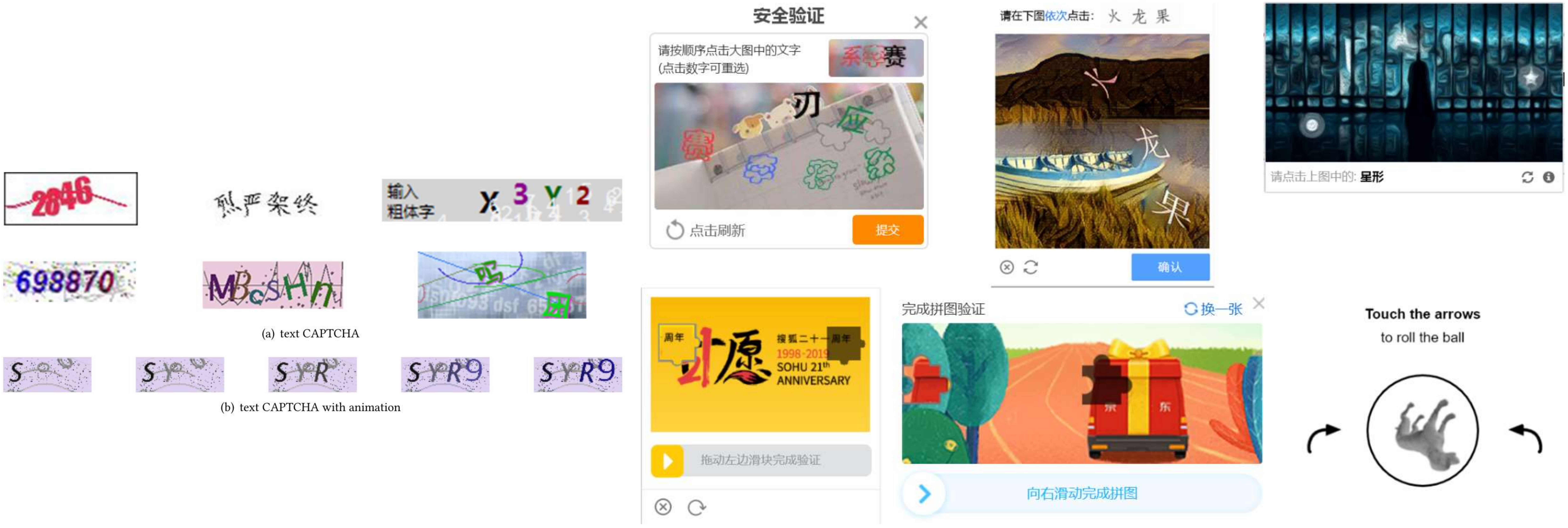
2.Demystifying Anti-human Verification Services

1/3 SMS Receiving Service



2.Demystifying Anti-human Verification Services

2/3 Captcha Recognizing Service



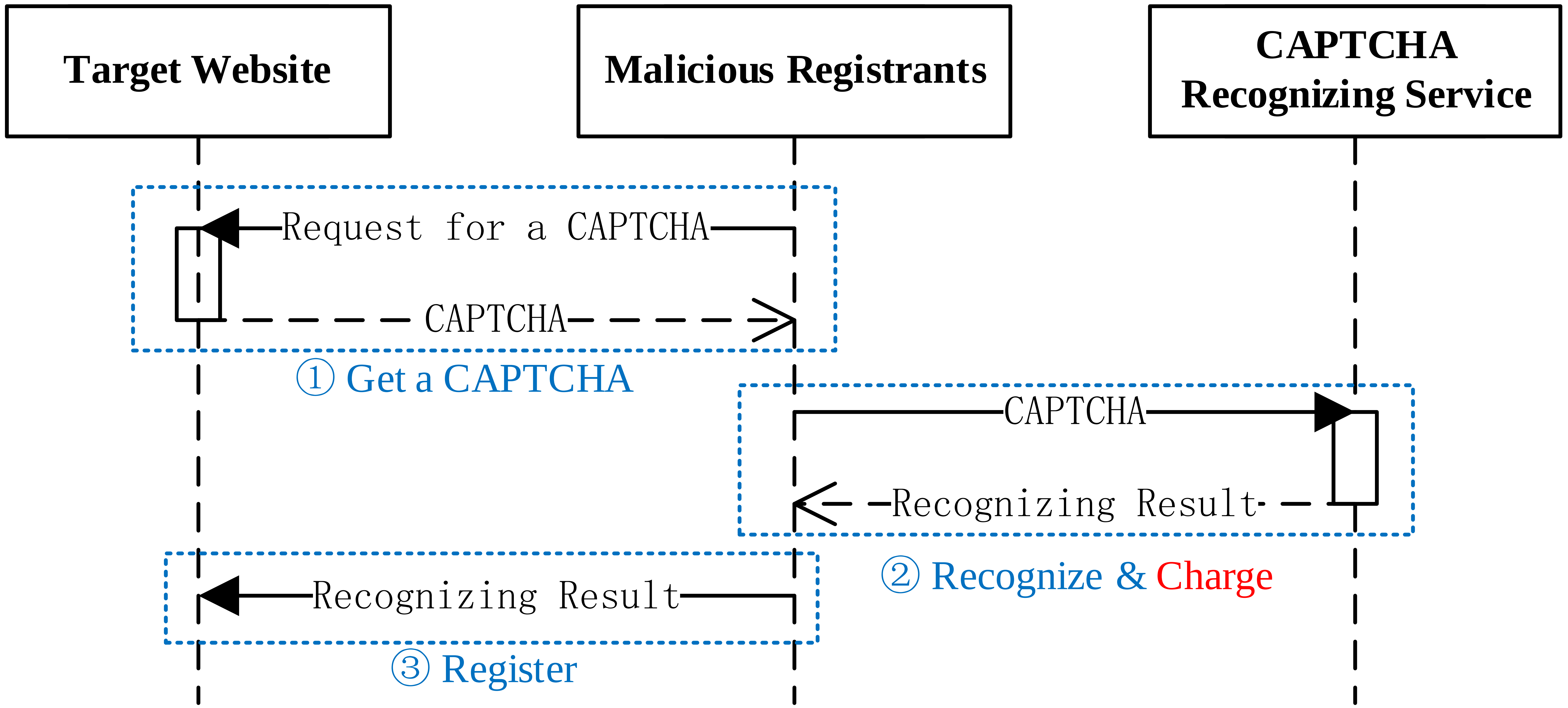
(a) text CAPTCHA

(b) text CAPTCHA with animation

(c) interactive CAPTCHA

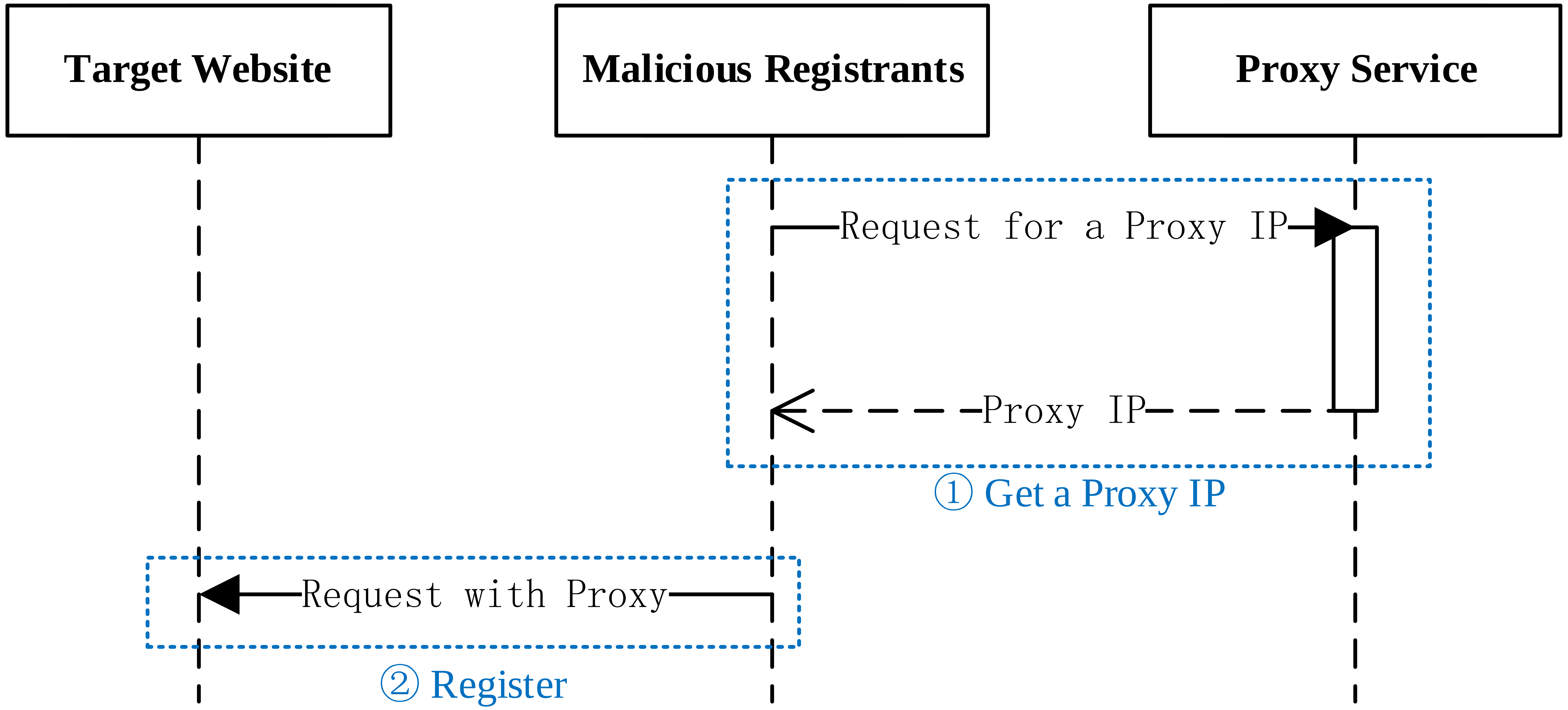
2.Demystifying Anti-human Verification Services

2/3 Captcha Recognizing Service



2.Demystifying Anti-human Verification Services

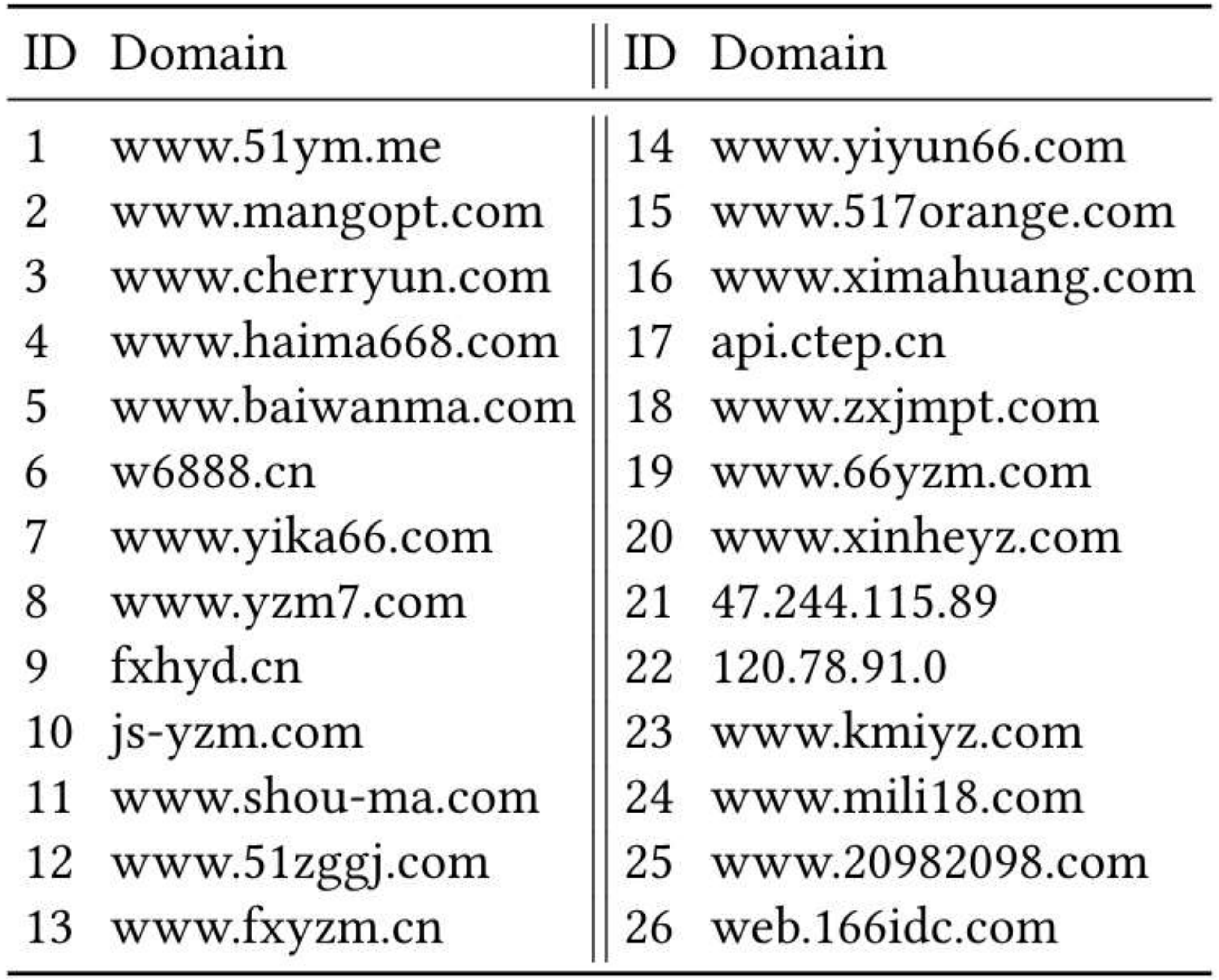
3/3 Proxy Service



3.Measurement of Anti-human Verification Services

1/3 SMS Receiving Service

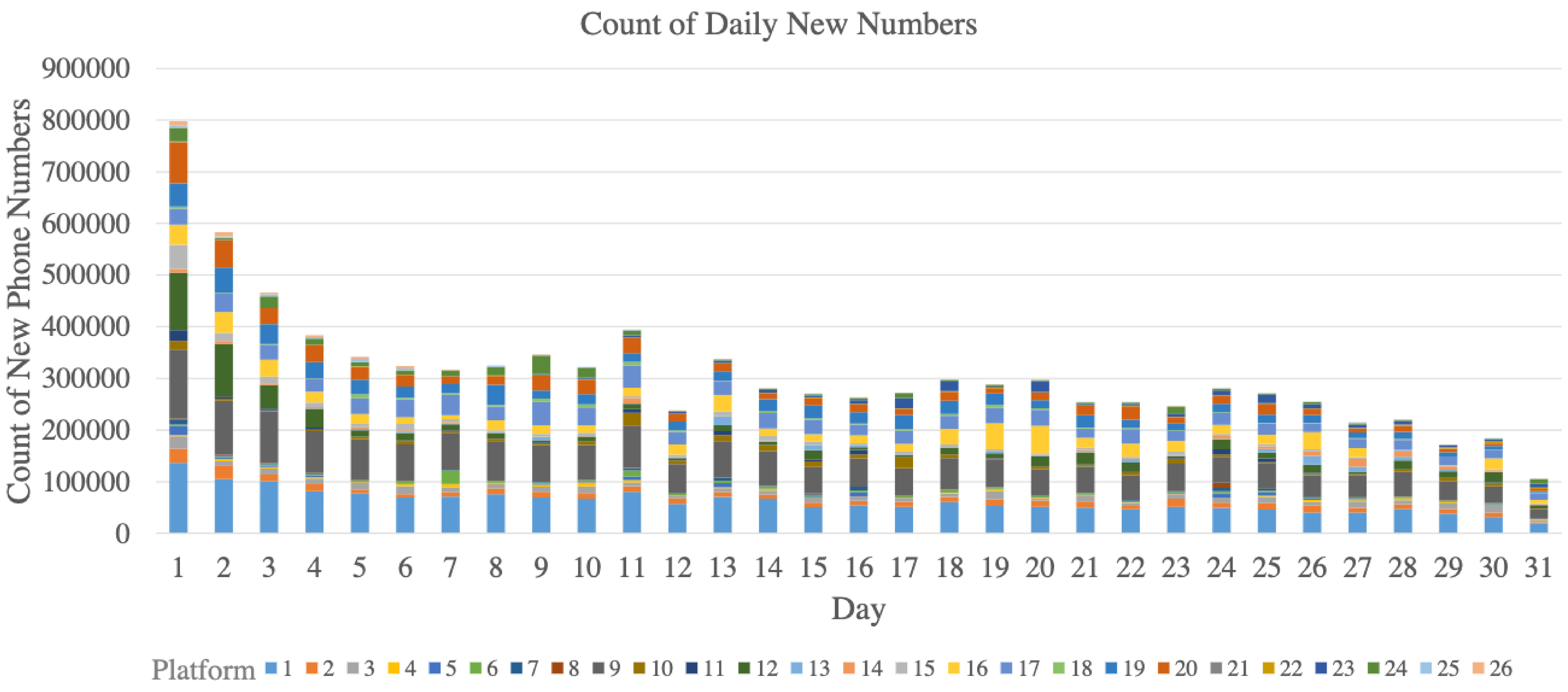
SMS Receiving Service List



ID	Domain	ID	Domain
1	www.51ym.me	14	www.yiyun66.com
2	www.mangopt.com	15	www.517orange.com
3	www.cherryun.com	16	www.ximahuang.com
4	www.haima668.com	17	api.ctep.cn
5	www.baiwanma.com	18	www.zxjmpt.com
6	w6888.cn	19	www.66yzm.com
7	www.yika66.com	20	www.xinheyz.com
8	www.yzm7.com	21	47.244.115.89
9	fxhyd.cn	22	120.78.91.0
10	js-yzm.com	23	www.kmiyz.com
11	www.shou-ma.com	24	www.mili18.com
12	www.51zggj.com	25	www.20982098.com
13	www.fxyzm.cn	26	web.166idc.com

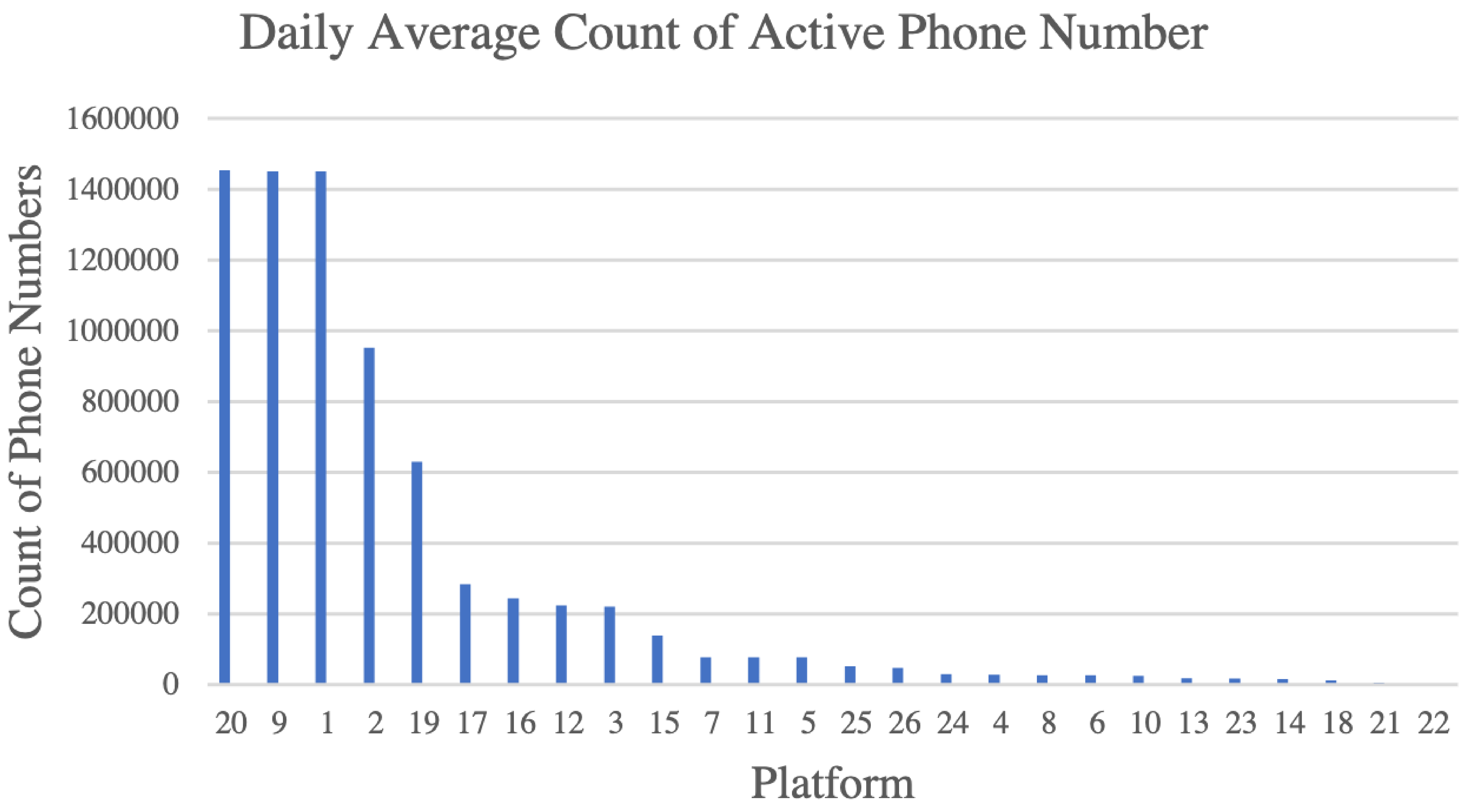
3.Measurement of Anti-human Verification Services

1/3 SMS Receiving Service



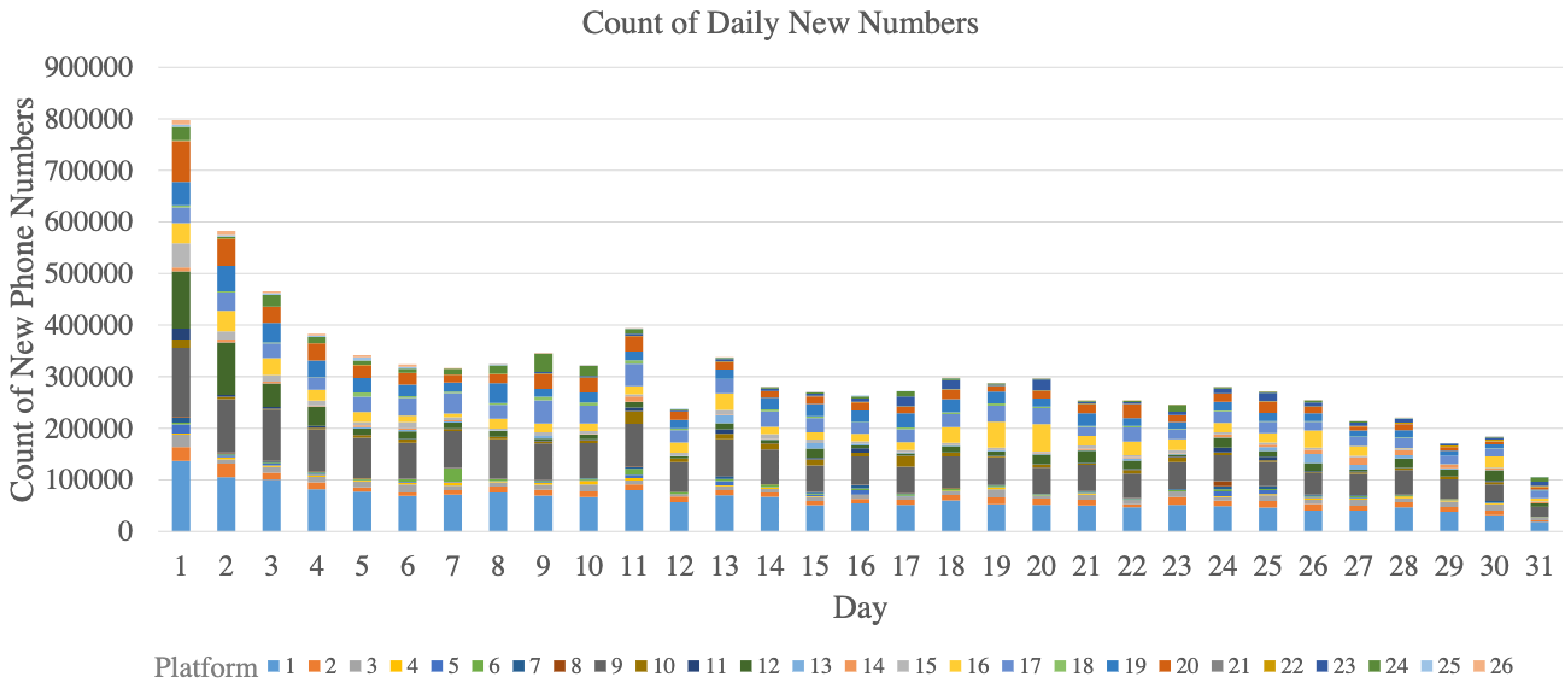
3.Measurement of Anti-human Verification Services

1/3 SMS Receiving Service



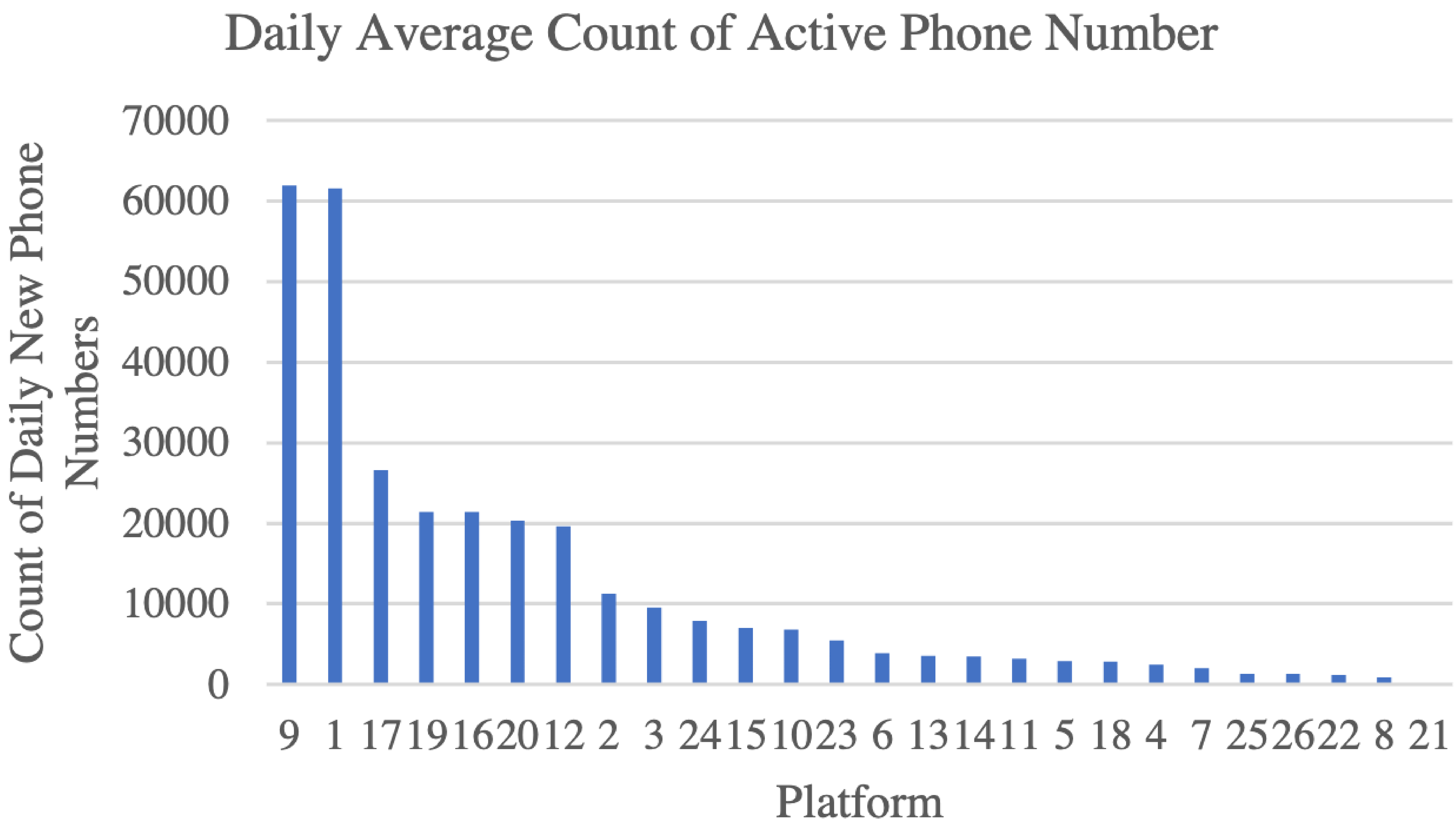
3.Measurement of Anti-human Verification Services

1/3 SMS Receiving Service



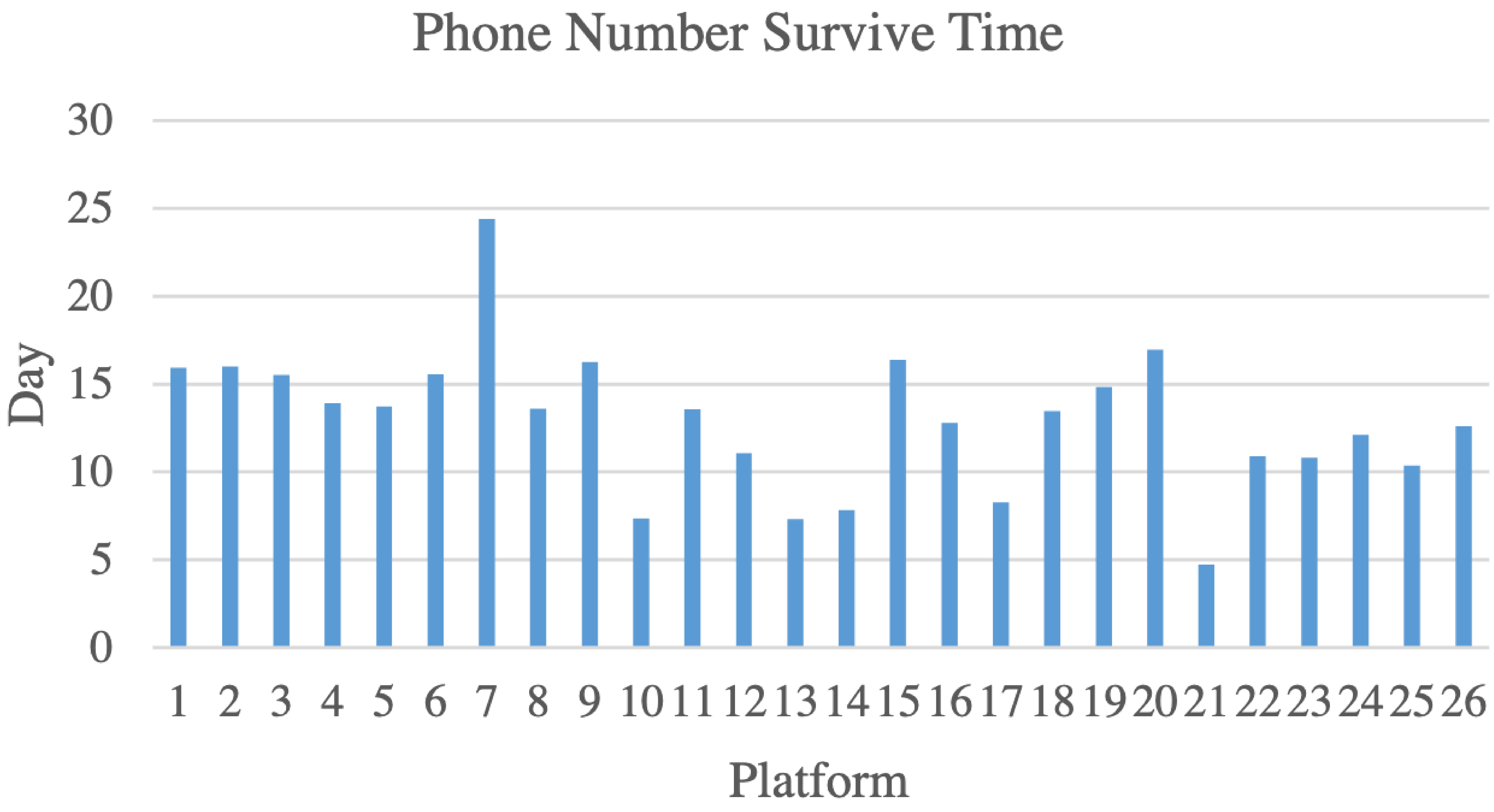
3.Measurement of Anti-human Verification Services

1/3 SMS Receiving Service



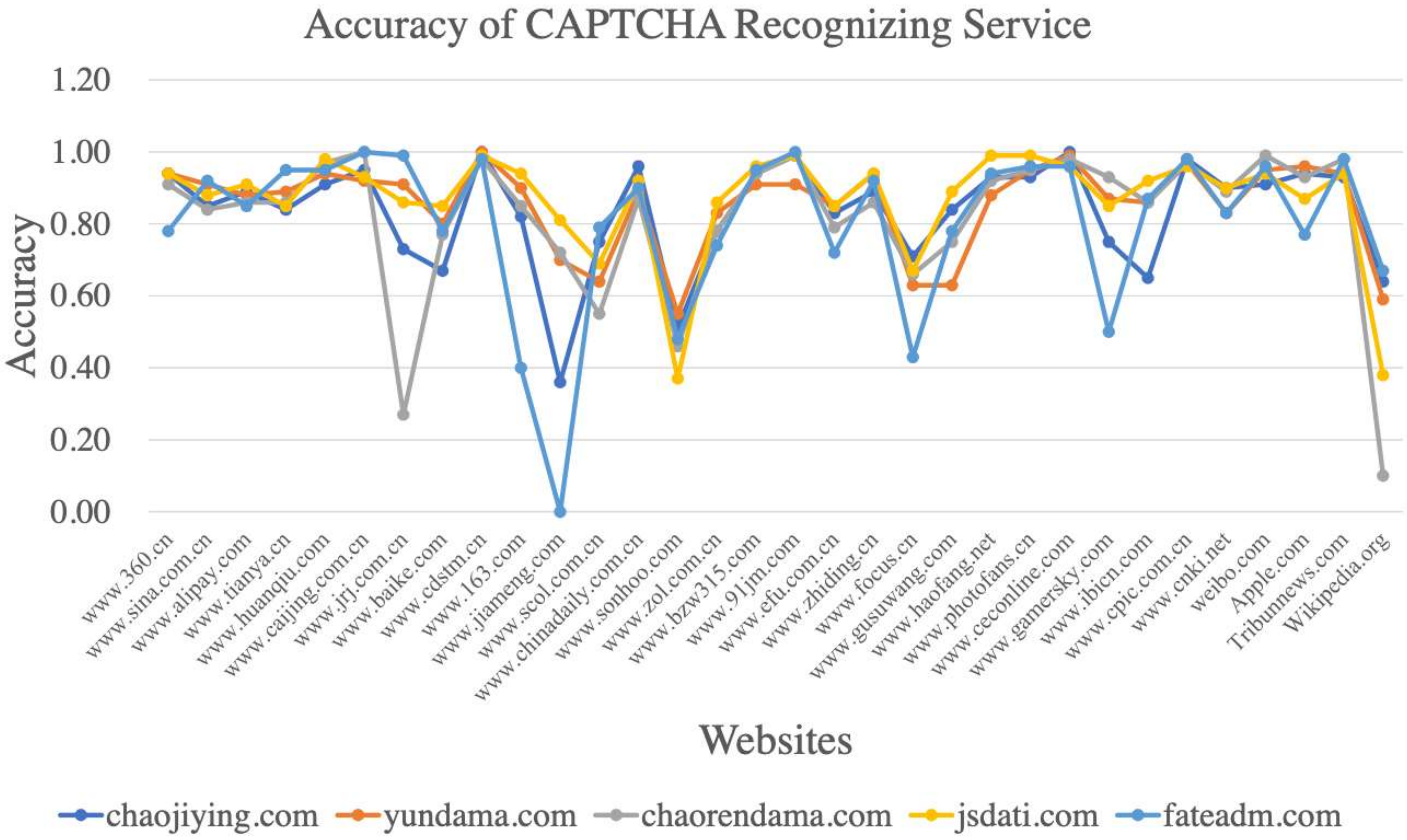
3.Measurement of Anti-human Verification Services

1/3 SMS Receiving Service



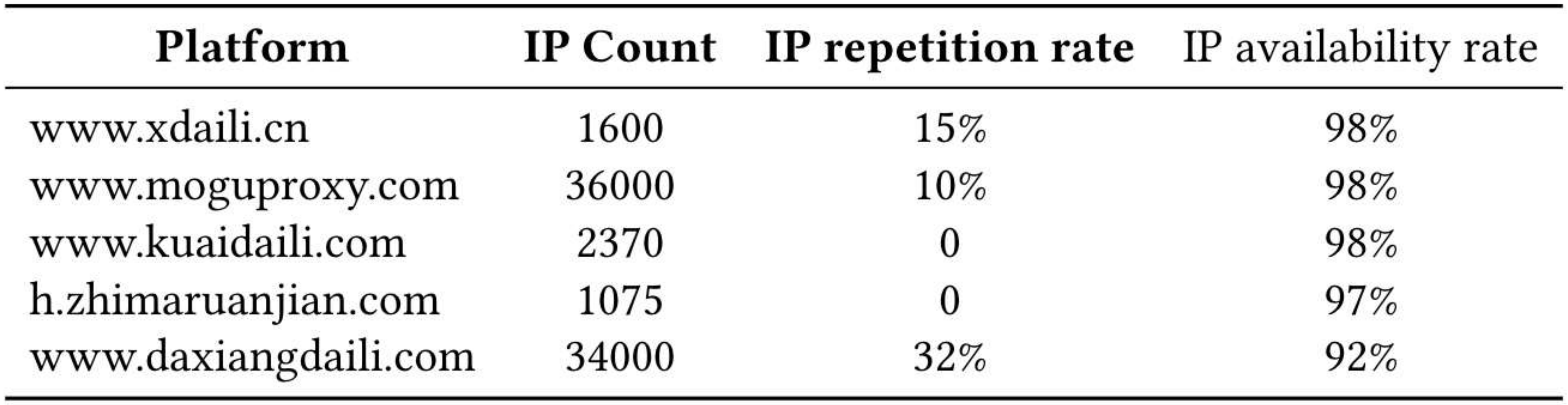
3.Measurement of Anti-human Verification Services

2/3 Captcha Recognizing Service



3.Measurement of Anti-human Verification Services

3/3 Proxy Service



Platform	IP Count	IP repetition rate	IP availability rate
www.xdaili.cn	1600	15%	98%
www.moguproxy.com	36000	10%	98%
www.kuaidaili.com	2370	0	98%
h.zhimaruanjian.com	1075	0	97%
www.daxiangdaili.com	34000	32%	92%

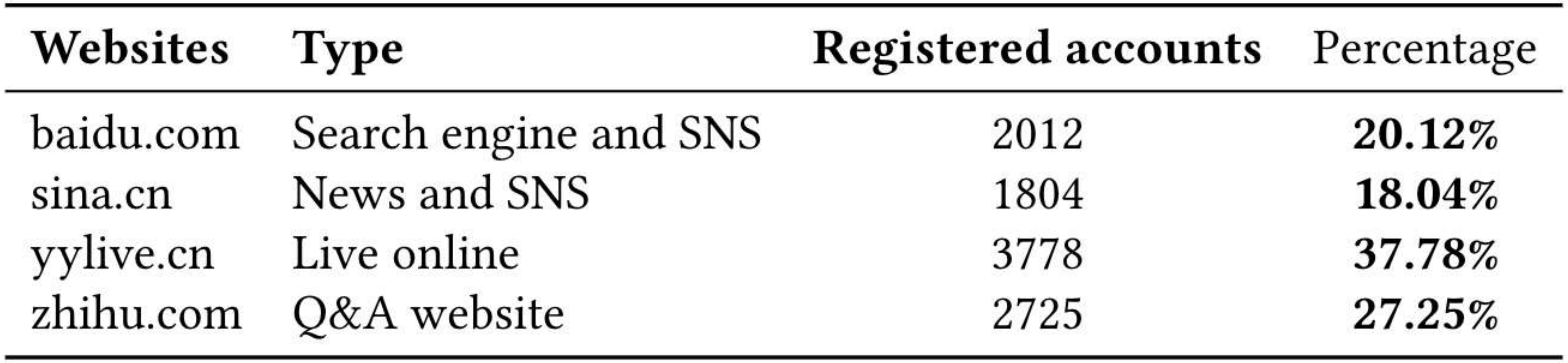
4.Characterizing the Impact

1/3 Automated registration test

We selected **10 websites** with different CAPTCHA types from the **Alexa Top 100** website for testing in consideration of development cost and economic cost. We found that we can use SMS reception service, CAPTCHA identification service, and IP proxy service to help automate registration on these websites.

4.Characterizing the Impact

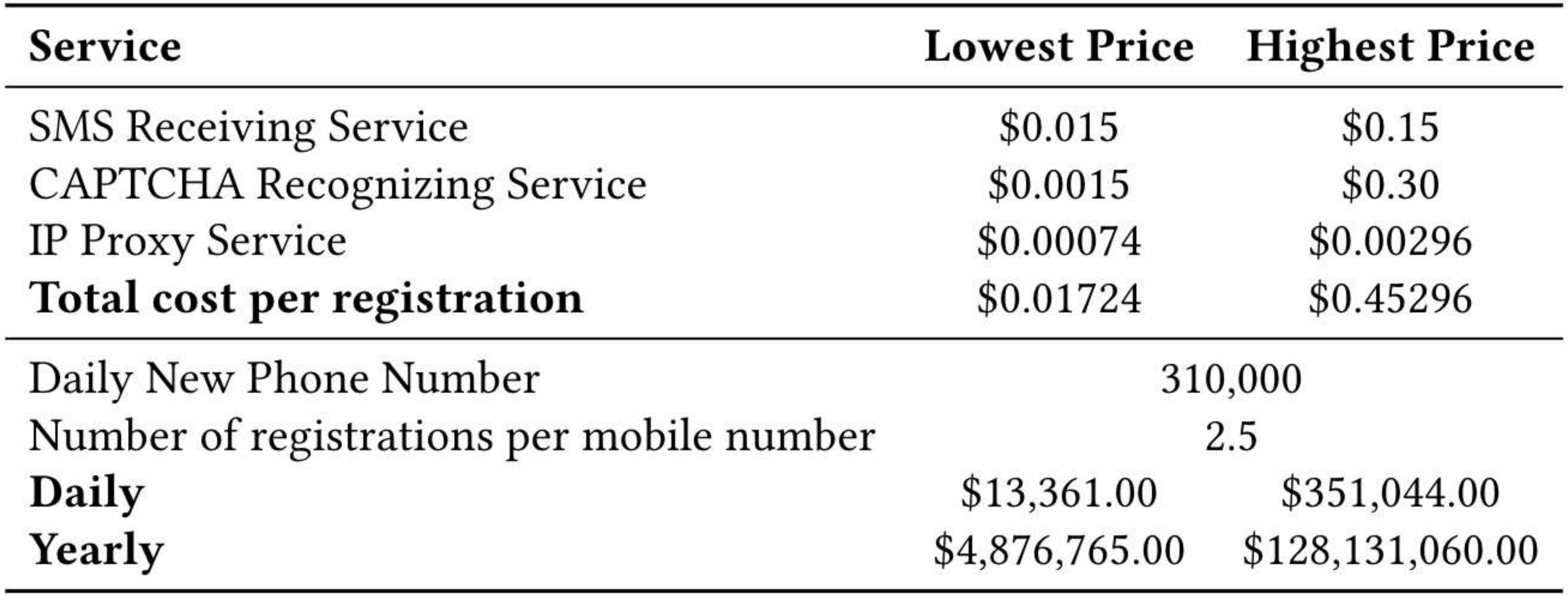
2/3 Registration number evaluation



Websites	**Type**	**Registered accounts**	Percentage
baidu.com	Search engine and SNS	2012	**20.12%**
sina.cn	News and SNS	1804	**18.04%**
yylive.cn	Live online	3778	**37.78%**
zhihu.com	Q&A website	2725	**27.25%**

4.Characterizing the Impact

3/3 Scale estimate



Service	**Lowest Price**	**Highest Price**
SMS Receiving Service	$0.015	$0.15
CAPTCHA Recognizing Service	$0.0015	$0.30
IP Proxy Service	$0.00074	$0.00296
Total cost per registration	$0.01724	$0.45296
Daily New Phone Number	310,000	
Number of registrations per mobile number	2.5	
Daily	$13,361.00	$351,044.00
Yearly	$4,876,765.00	$128,131,060.00

5.Next work

Problems

- 1. Too much manual work
- 2. Some parts of the experiment is not solid enough
- 3. The presentation need to be improved

5.Next work

Objectives

- 1. Use a new automatic tool to evaluate the website security strategies for register (Background)
- 2. Reduce the figures in the measurement of services (e.g. the phone numbers)
- 3. Repeat the experiment of proxy services evaluation for more details with some new scripts
- 4. Conduct an experiment of the website register limitation bypass with a new tool (Impact)
- 5. Conduct an experiment of the account usage for more accurate result of how many these phone numbers are used indeed with a new tool (Impact)