The Abuser Inside Apps: Finding the Culprit Committing Mobile Ad Fraud

Authors : Joongyum Kim, Jung-hwan Park, Sooel Son (KAIST)

Publication : Network and Distributed Systems Security(NDSS) Symposium 2021

Date : 2021. 02.

2021. 08. 19

전자정보공학부(컴퓨터공학)
201950636 / 이주현

전북대학교
JEONBUK NATIONAL UNIVERSITY

Abstract

전북대학교 JEONBUK NATIONAL UNIVERSITY

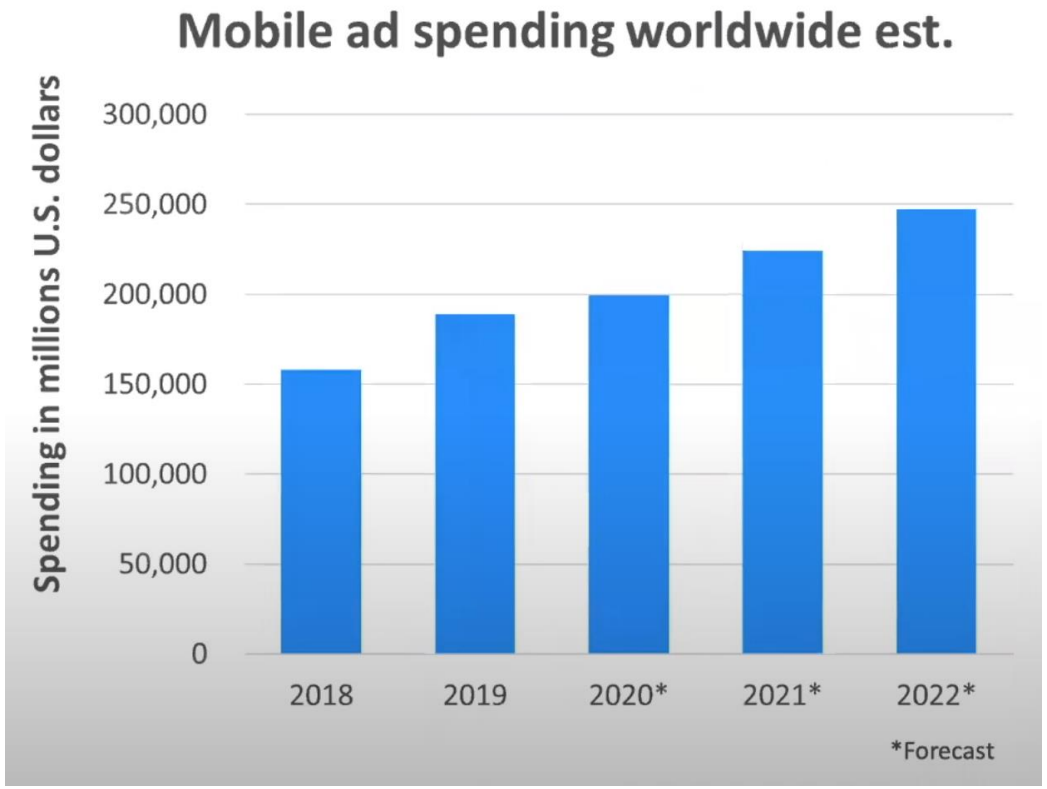
- 모바일 광고 사기는 앱 개발자와 사용자들에게 피해를 입히며 앱 시장 생태계를 훼손시키는 중대한 위협이다.

- 모바일 광고 사기를 탐지하기 위해 동적 테스트 프레임워크를 구현하였다.

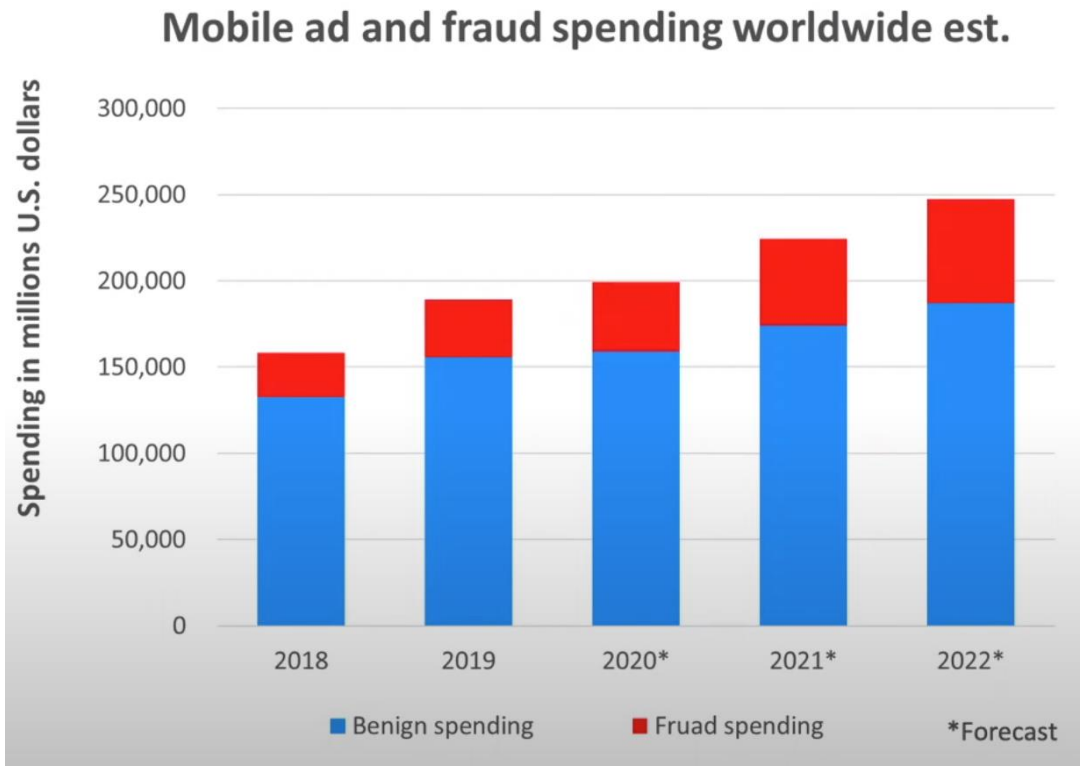
- 사기 행위 탐지는 사용자 상호 작용 없이 발생하는 부정 행위를 식별하는데 초점을 맞추어 실행 과정을 추적 하였다.

- 구글 플레이 스토어의 48,172개 앱 중에서 74개의 앱에서 모바일 광고 사기 행위가 탐지되었다.

- 모바일 광고 시장은 연간 약 200조원 크기로 매년 성장하고 있다.

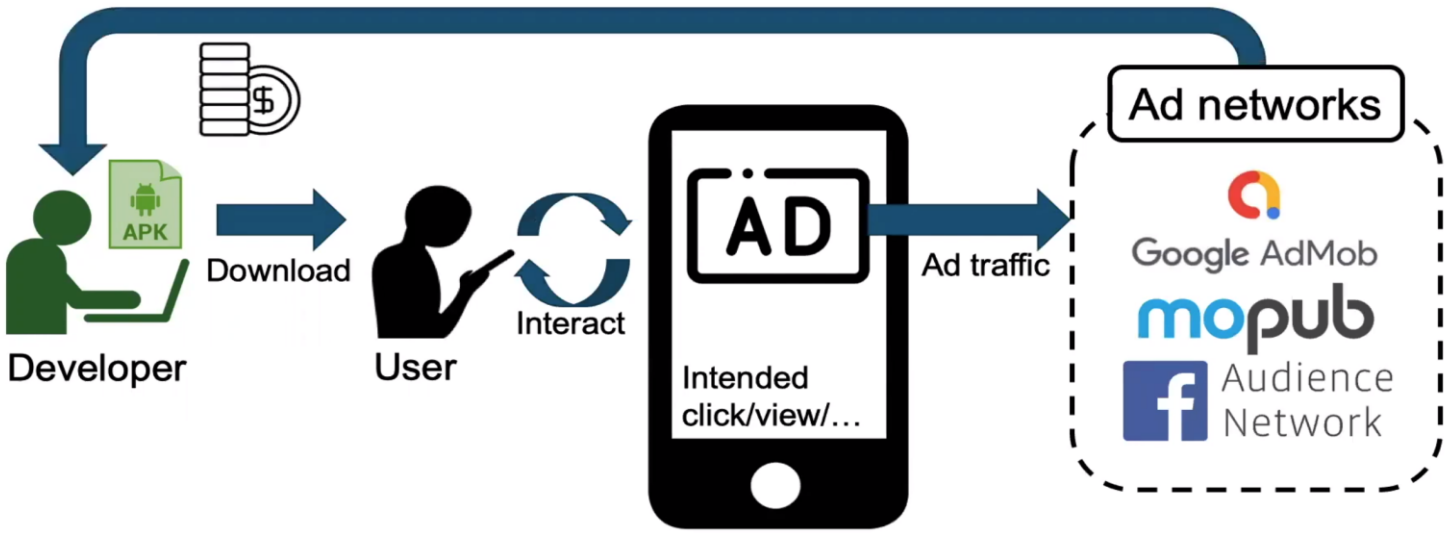


- 모바일 광고 사기를 통해 매년 9-20% 정도의 손실이 발생하고 있다.



모바일 광고 생태계

- **advertiser** : 광고주 또는 광고 대행사로 광고를 기획하고 런칭을 요청한다.
- **service provider** : 광고 서비스 제공자로 광고주 요청으로 광고를 많이 노출시킬 수 있도록하고, 광고 라이브러리를 제공한다.
- **publisher** : 앱 개발자로 앱에 광고 라이브러리를 추가하여 수익을 얻는다.



Background


2018 Korea Advertising MOBIscape 4.0
Latest Update : Nov, 2018
by.MOBI INSIDE
Advertiser
Full Service Ad Agency
Search Agency
FMP
Digital Agency
Media Rep.
DMP
DSP
Ad Network
Influencer Marketing
Retargeting
Ad Exchange
SSP
Analytics
Market Intelligence
Attribution Tracking
Viewability
Publishers
App Player
Pre-registration & Coupon
Reward
Display
Search
Video
Messenger
App store
Community
Social Network
Users
디지털 퍼포먼스 마케팅 에이전시, 모비데이즈
©MOBIINSIDE 2018 Contact : hello@mobiinside.com / www.mobiinside.com/kr

모바일 광고 생태계

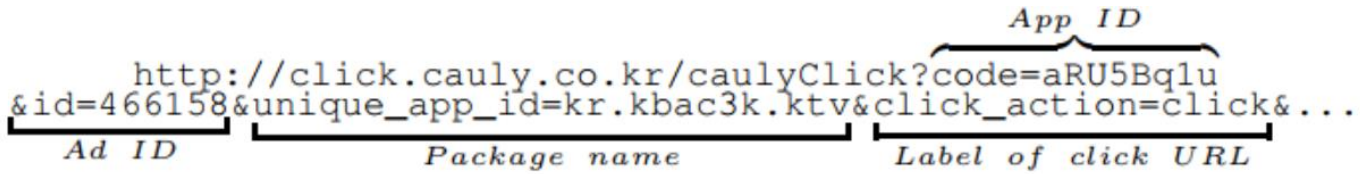
- **CPM (cost-per-mile)** : 노출 수에 비례하여 비용 지불, ($20 CPM : 1000뷰 당 $20 지불)

- **CPC (cost-per-click)** : 클릭 수에 비례하여 비용 지불

- **CPI (cost-per-install)** : 앱 설치 수에 비례하여 광고 비용 지불

Click fraud

- 공격자는 클릭 수를 많이 발생시키기 위해 광고 비용이 발생하는 URL request를 지속적으로 발생시킨다.



Impression fraud

- 광고를 많이 노출 시키기 위해 사용자 화면에서 눈에 보이지 않게 숨겨 놓거나 작게 만들어서 보이지 않는 광고를 만든다.

- 사용자에게 광고를 많이 노출시키지 않으면서 광고 수익을 얻을 수 있다.

광고 사기 탐지 과정

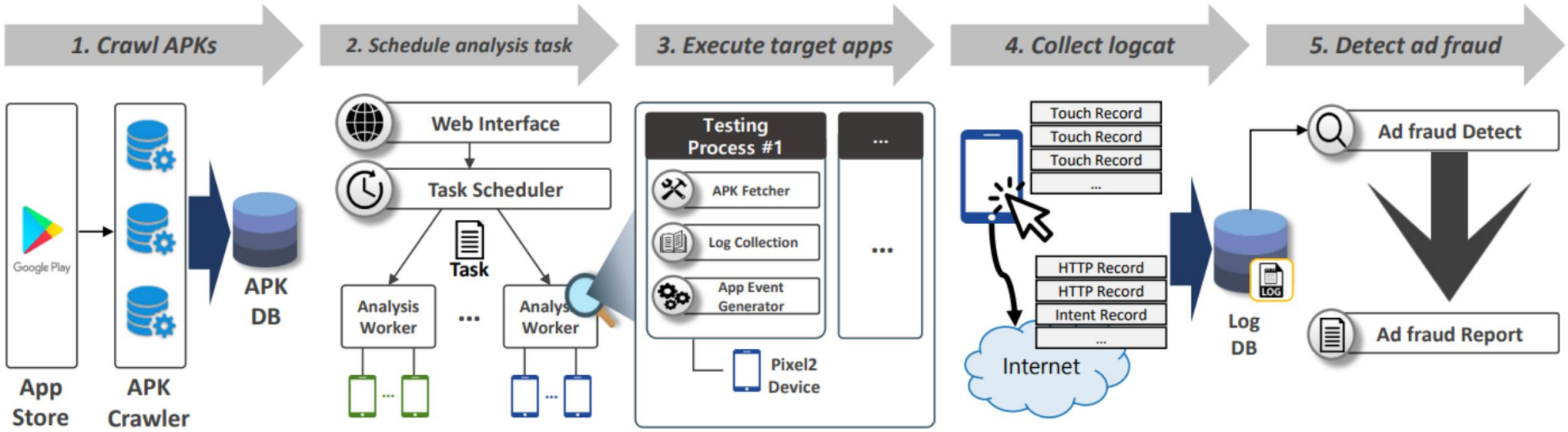


Fig. 2: FraudDetective architecture: A workflow overview of dynamic Android app testing.

Ad fraud activity

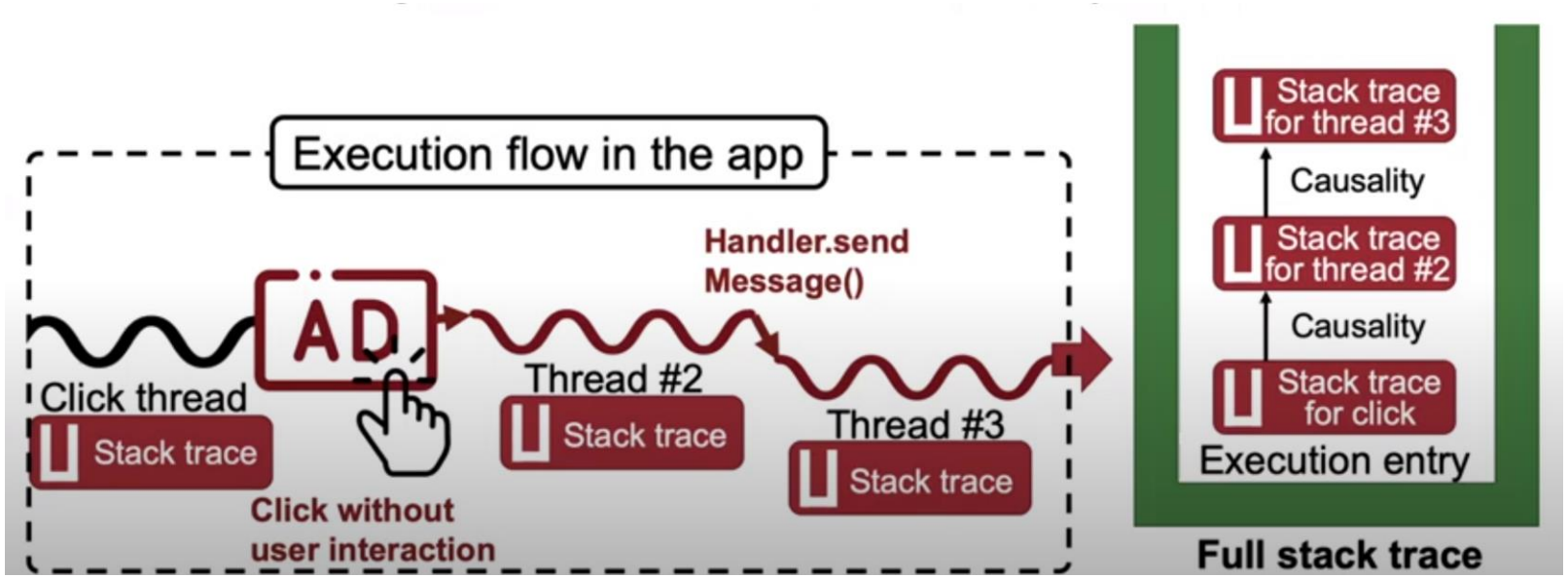
- FraudDetective는 사용자 요청 없이 클릭 URL request를 발생시켜 광고 클릭 수를 올리는 사기를 탐지하도록 하였다.
- 광고 사기 행위를 위해 호출하는 매개 변수와 안드로이드 API 호출 작업을 분류하였다.

Sink method name
android.app.Activity.startActivity()
android.app.ContextImpl.startActivity()
android.app.Fragment.startActivity()
android.content.ContextWrapper.startActivity()
java.net.HttpURLConnection()
org.apache.http.client.methods.HttpRequestBase.setURI()
android.webkit.Webview.loadUrl()
android.webkit.Webview.reload()
android.webkit.Webview.goForward()
android.webkit.Webview.pageUp()
android.webkit.Webview.pageDown()
com.android.webview.chromium. WebViewContentsClientAdapter.onLoadResource()

TABLE I: Sensitive Android APIs that invoke ad fraud activities.

Full stack trace

- 앱 실행과정을 추적하여 광고 사기가 호출되는 방법을 보여준다.



Full stack trace

- com.libraryc 에서 터치 이벤트 핸들러를 강제로 호출한다.
- 터치 이벤트가 발생하면 dispatchTouchEvent를 통해 View 인스턴스로 전달되어 광고가 노출된다.

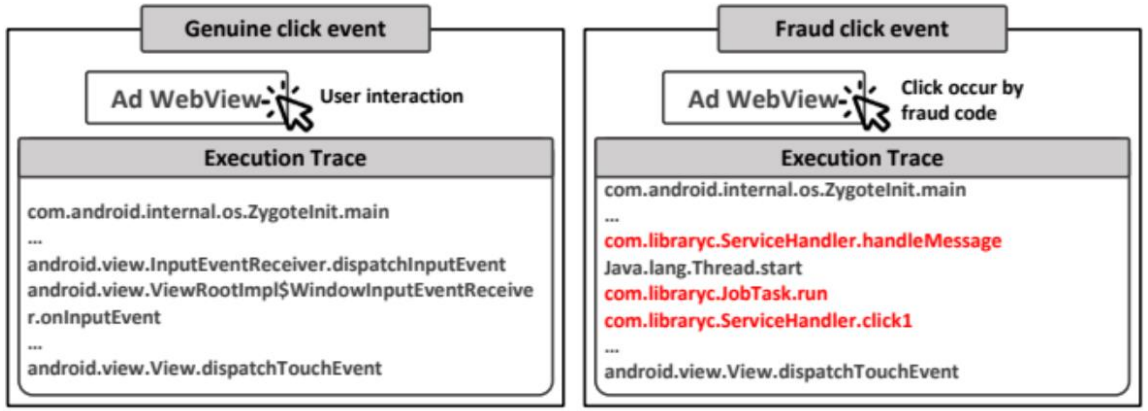


Fig. 3: Examples of two stack traces: One triggered by a genuine user touch and the other triggered by a forged touch event.

Types of Ad Fraud Activities

Type-1

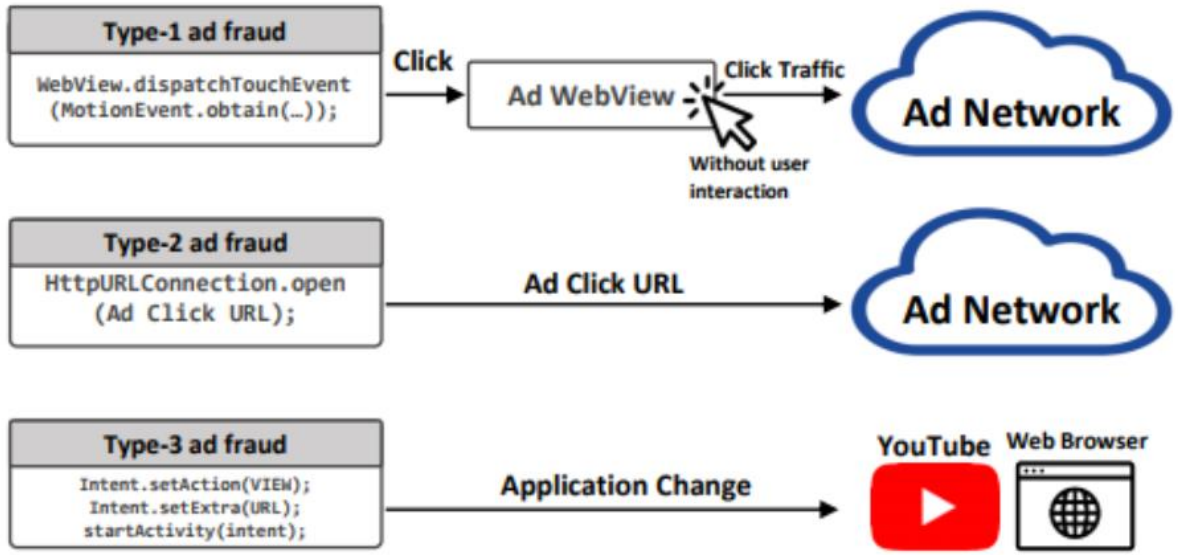
- URL request를 발생시킬 때 dispatchTouchEvent 호출에 사용자 정의 내부 클래스가 있는지 확인한다.

Type-2

- 사용자와 상호작용 없이 전송된 URL request를 확인한다.

Type-3

- 다른 앱을 호출하는 intent를 찾는다.



- 구글 플레이 스토어에서 48,172개의 앱을 다운받아 검사하였다.

# of download	~5K	5K ~ 100K	100K ~ 500K	500K ~ 1M	1M ~ 5M	5M ~ 10M	10M ~ 50M	50M~	Total
# of apps	7,368	10,828	8,573	5,311	8,793	3,877	2,426	996	48,172

- 74개 앱에서 34,453번의 광고 사기 활동을 탐지하였다.

Type	# of records (# of apps)	Responsible module		
		Module	# of apps	Ratio
Type-1	0 (0)	App	0	0%
		Library	0	0%
Type-2	34,232 (66)	App	1	1.5%
		Library	65	98.5%
Type-3	221 (8)	App	0	0%
		Library	8	100%

# of download	~1K	1K~ 50K	50K~ 500K	500K~ 5M	5M~ 100M	100M~	Total
# of apps	6	8	16	15	22	7	74

Conclusion

전북대학교 JEONBUK NATIONAL UNIVERSITY

- 본 논문에서는 동적 테스트 프레임워크를 제안하여 광고 사기를 탐지하도록 하였다.

- 사용자 이벤트와 광고 사기 행위 활동 사이에 풀 스택 추적으로 모델링하였다.

- 제안한 FraudDetective를 통해 74개의 사기 광고 라이브러리를 사용하는 앱을 탐지하였다.

Q & A