IEEE INFOCOM

MAGPRINT: Deep Learning Based User Fingerprinting Using Electromagnetic Signals

Lanqing Yang[#], Yi-Chao Chen[#], Hao Pan[#], Dian Ding[#], Guangtao Xue[#], Linghe Kong[#], Jiadi Yu[#], Minglu Li [*]

Shanghai Jiao Tong University[#]

Zhejiang Normal University[*]

Outline

- Background
- Motivation
- Preliminary
- Challenge and Methodology
- Evaluation
- Conclusion and Future Work

Background

Smart Devices are everywhere…

Background

Smart Devices are everywhere…

Background

Smart Devices are everywhere…

User identification is IMPORTANT!

Biological Feature Based Solutions

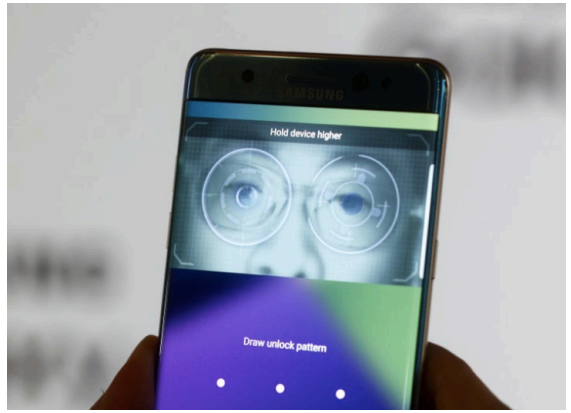
- 2D/3D Face Model

Face ID

- Fingerprint

- Voiceprint

- Iris

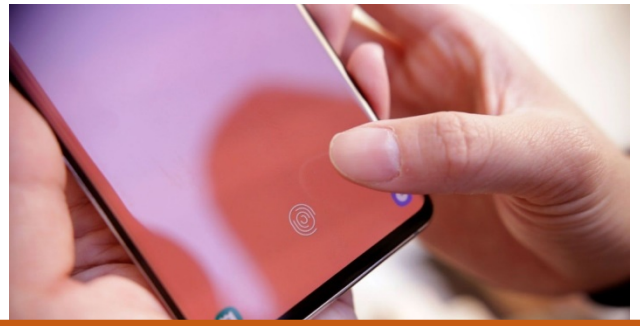


- Heartbeat

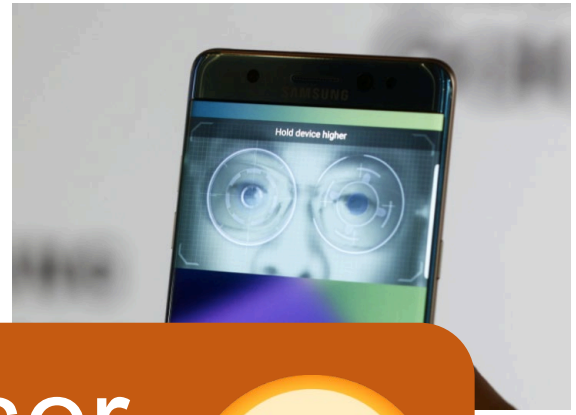
Biological Feature Based Solutions

- 2D/3D Face Model

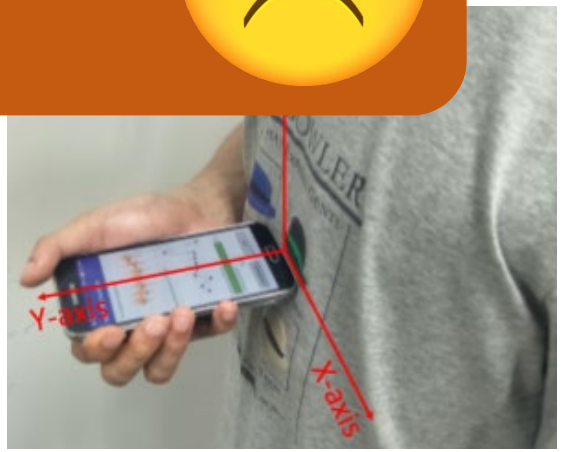
- Fingerprint



- Iris

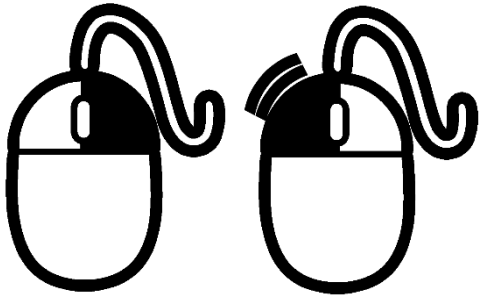


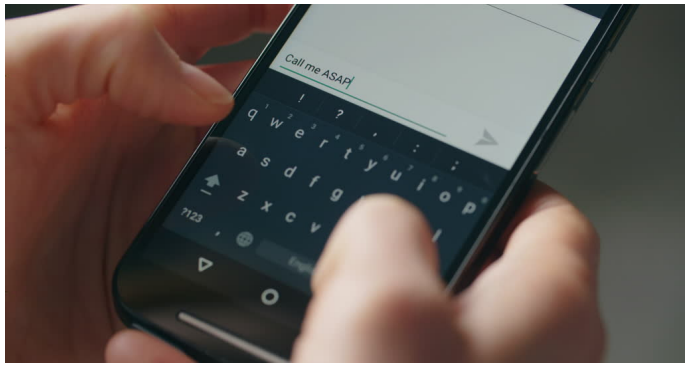
cannot perform continuous user authentication!



User Behavior Feature Based Solutions

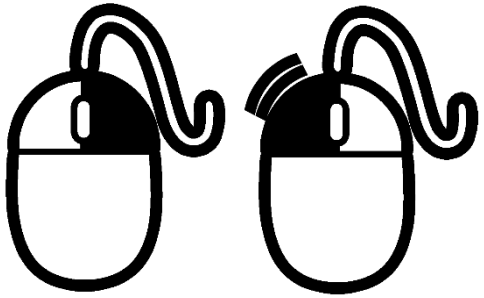
- Typing/Clicking Behavior

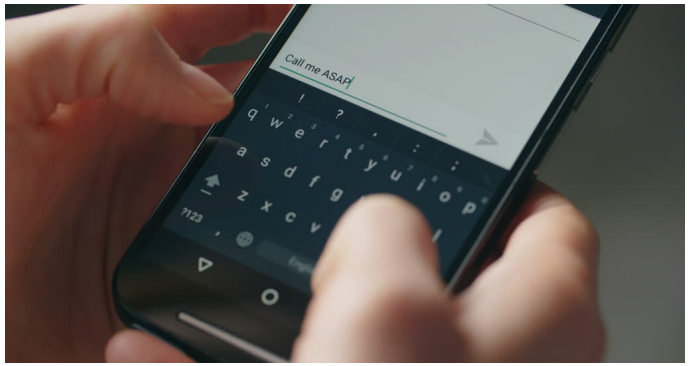




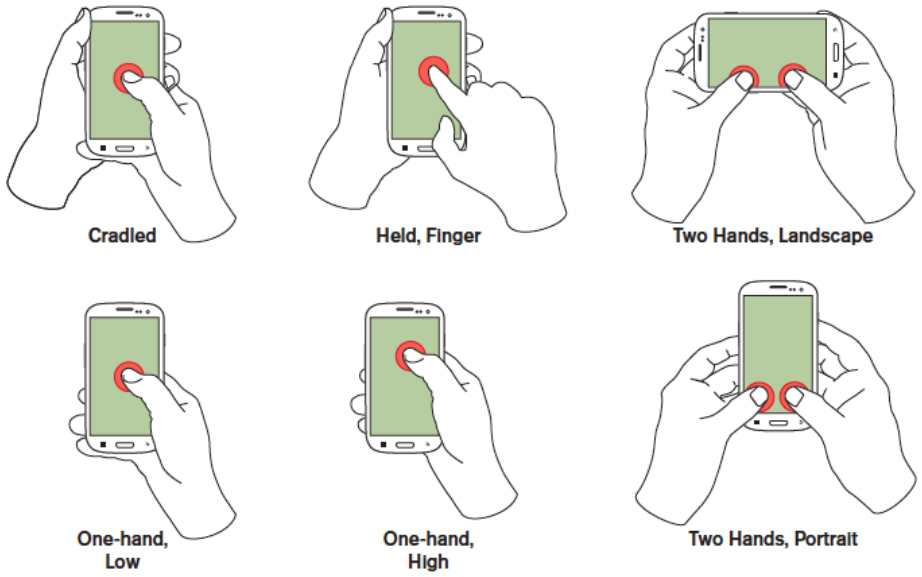
User Behavior Feature Based Solutions

- Typing/Clicking Behavior



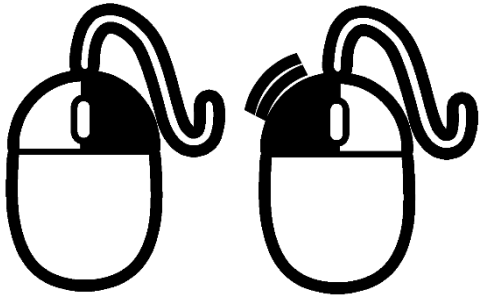


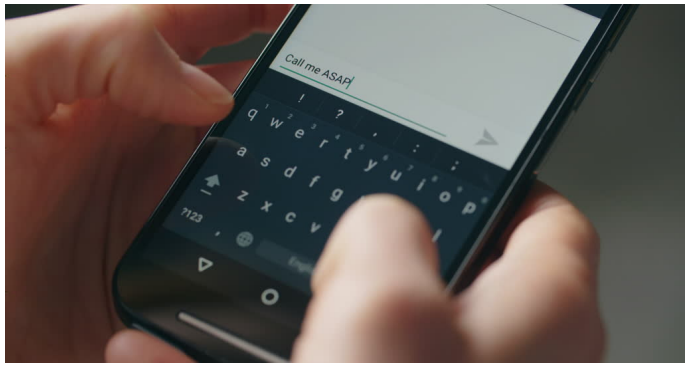
- Holding Behavior



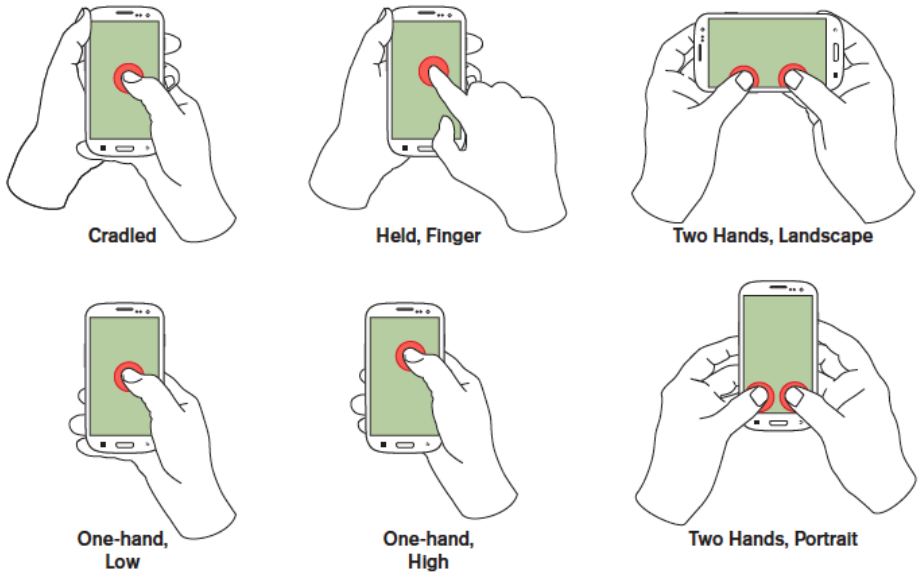
User Behavior Feature Based Solutions

- Typing/Clicking Behavior

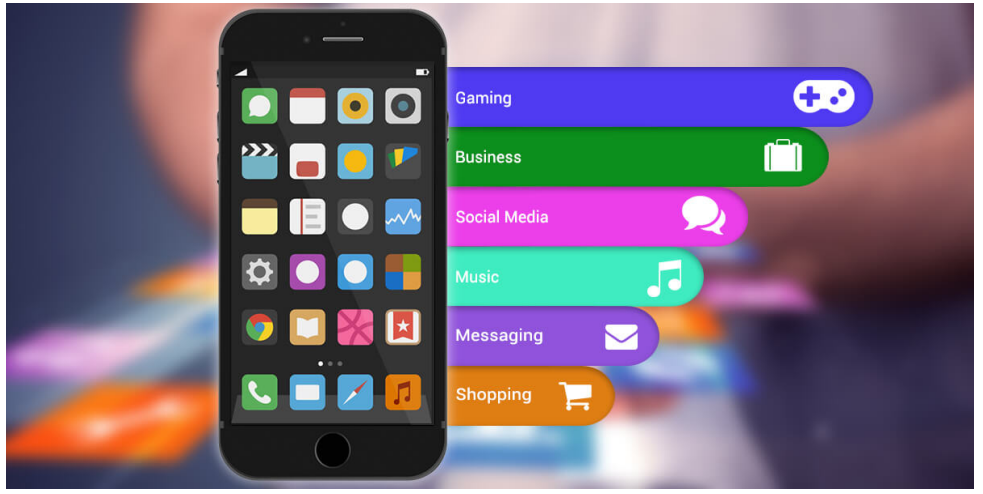




- Holding Behavior

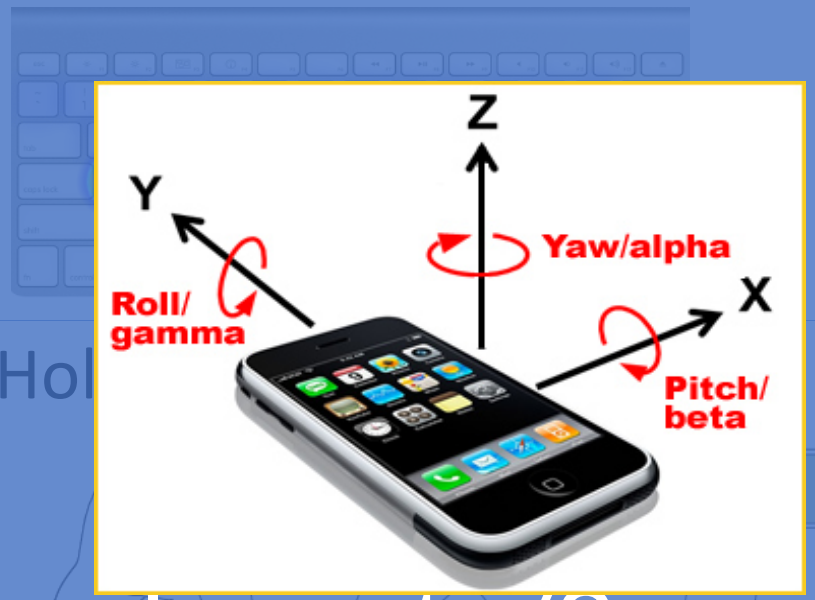


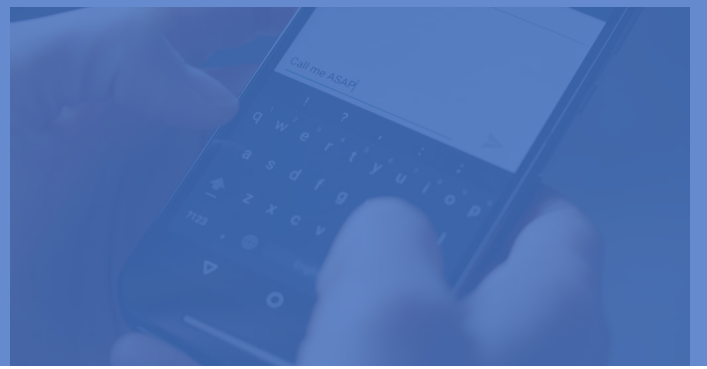
- App Using Behavior



User Behavior Feature Based Solutions

- Typing/Clicking Behavior





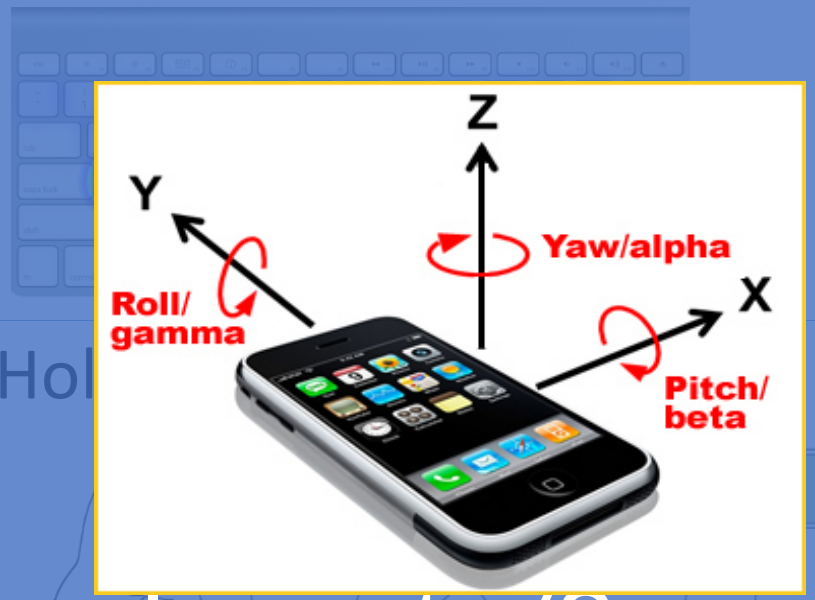
- Hol

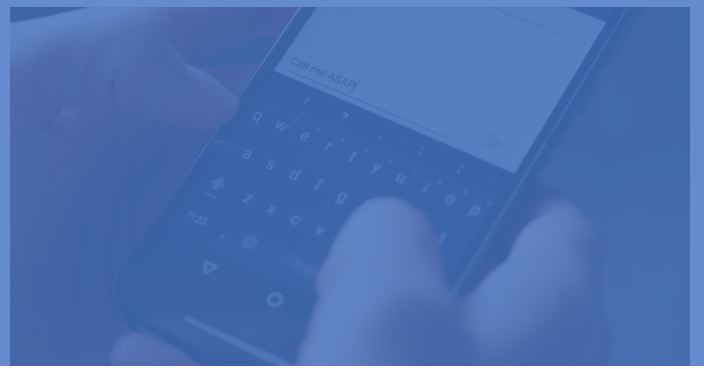
Accelerometer/Gyroscope Data

- App Using Behavior

User Behavior Feature Based Solutions

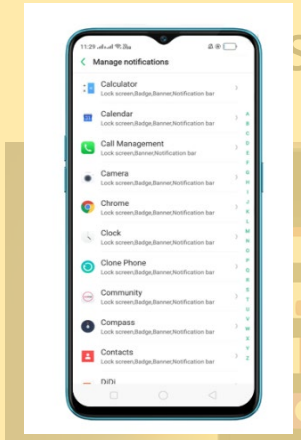
- Typing/Clicking Behavior

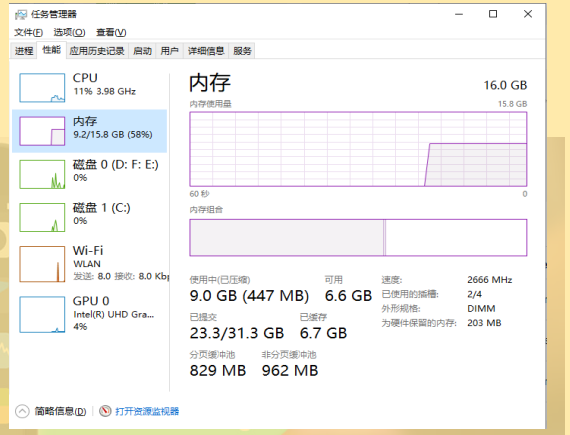




- Hol

Accelerometer/Gyroscope Data

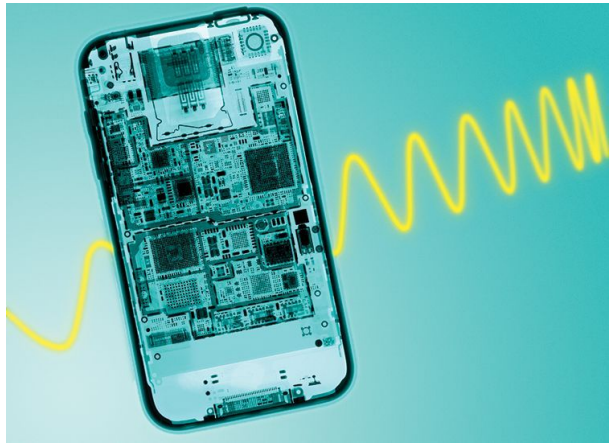




Power Consumption Data
Memory/Cache Data

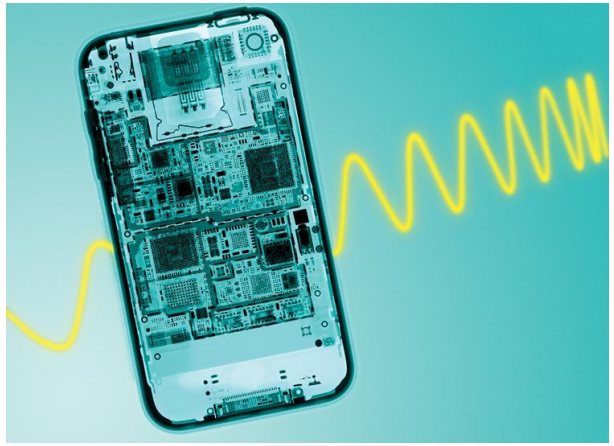
User Behavior Feature Based Solutions

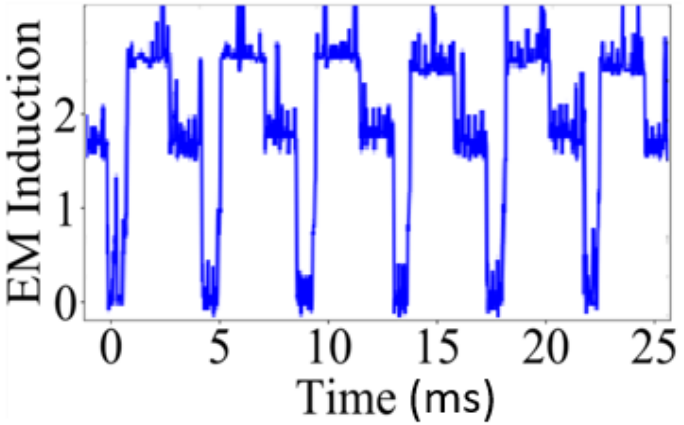
- **Common phenomenon:** Electromagnetic Radiation Signals exit in smart devices



User Behavior Feature Based Solutions

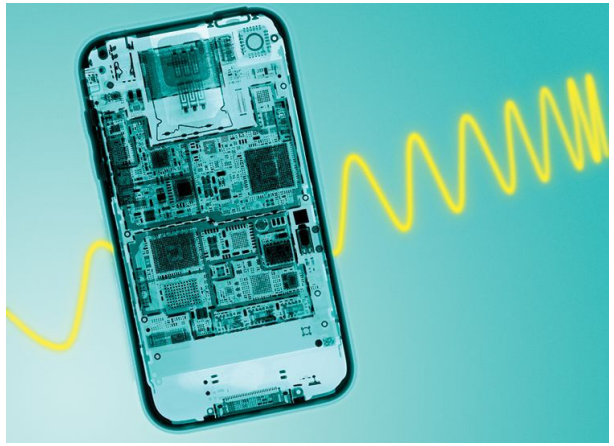
- **Common phenomenon:** Electromagnetic Radiation Signals exit in smart devices

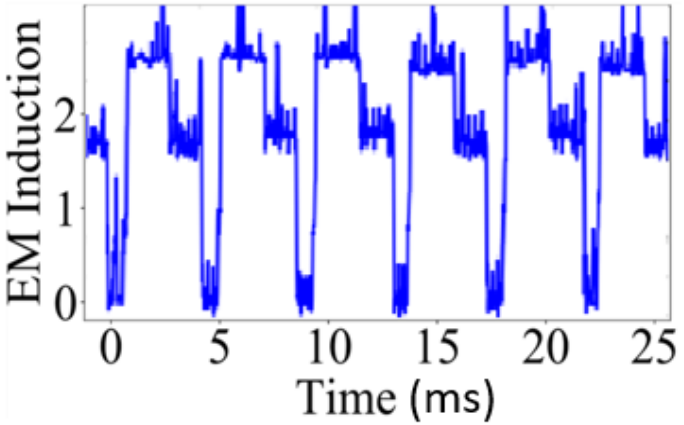




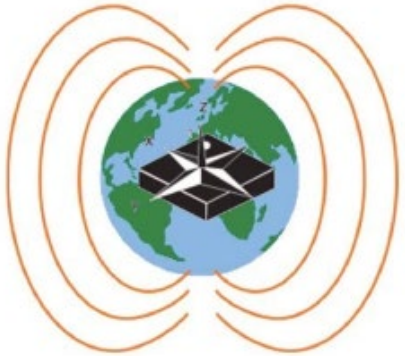
User Behavior Feature Based Solutions

- **Common phenomenon:** Electromagnetic Radiation Signals exit in smart devices



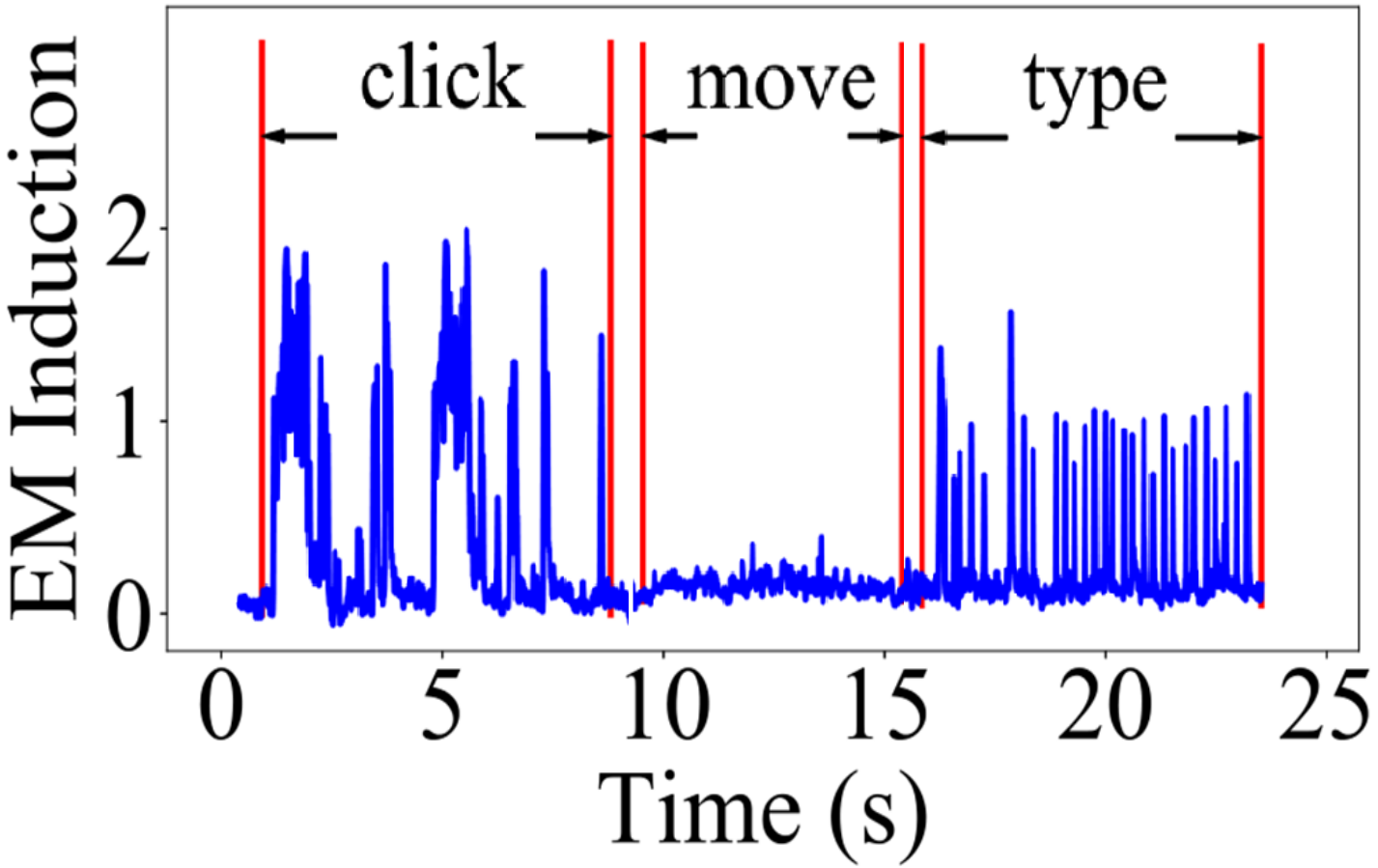


- We propose ***MagPrint***, a novel EM signals based solution using *magnetometer*
- Advantages of ***EM side channel*** :
  - Contain rich user behavior information
  - Data accessibility, and easy to deploy



Preliminary

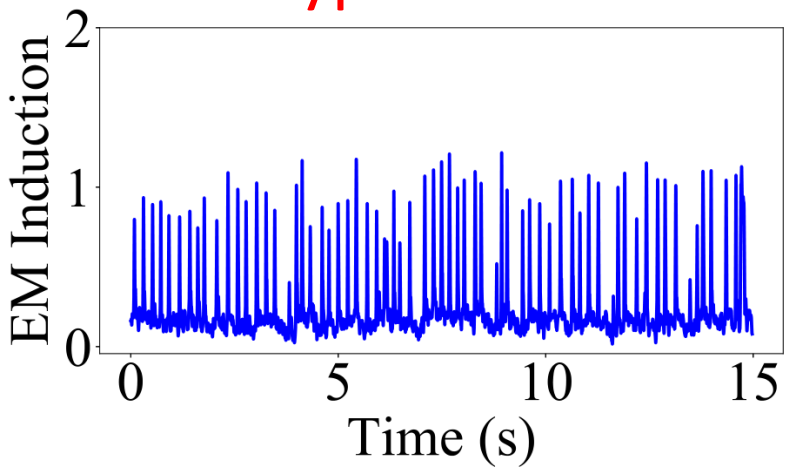
- **Q1:** Detection and distinction of users' operations.



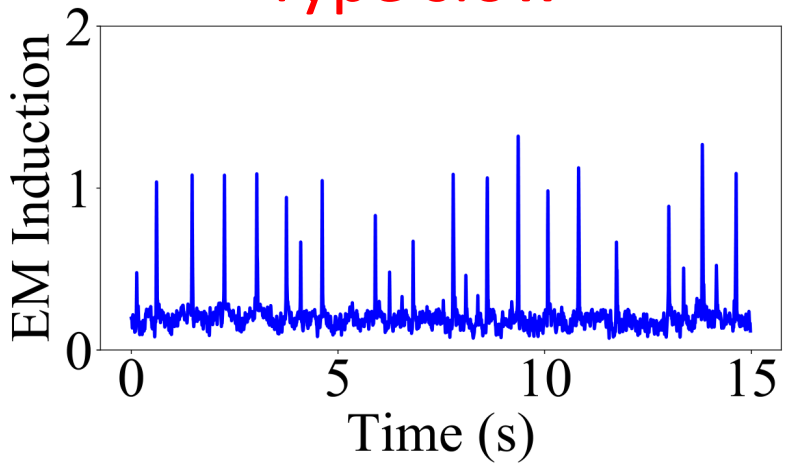
Preliminary

- **Q2:** Distinction of users' operation habits.

Type fast



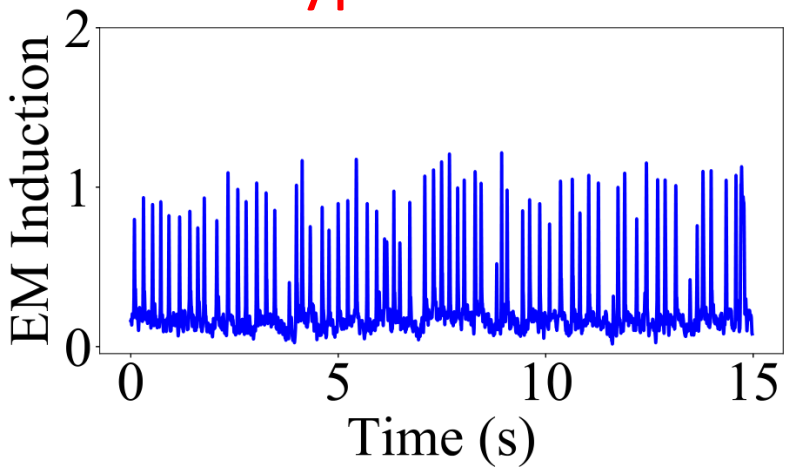
Type slow



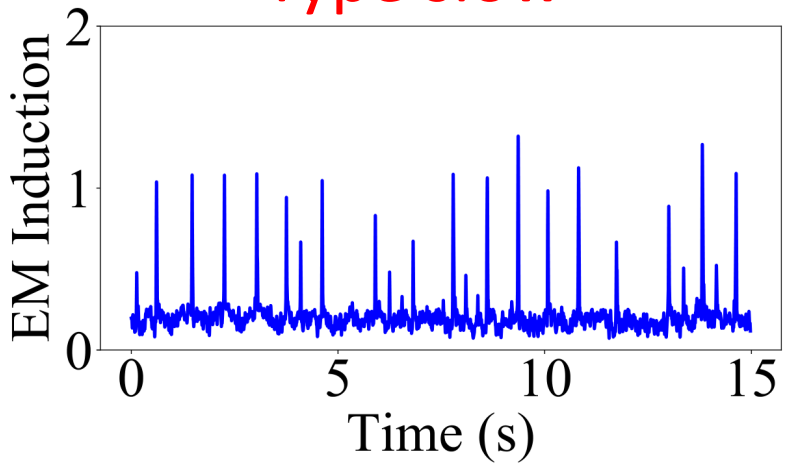
Preliminary

- **Q2:** Distinction of users' operation habits.

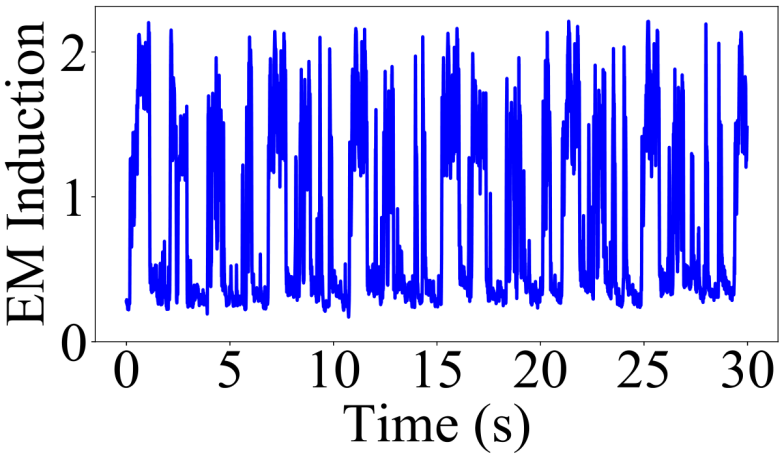
Type fast



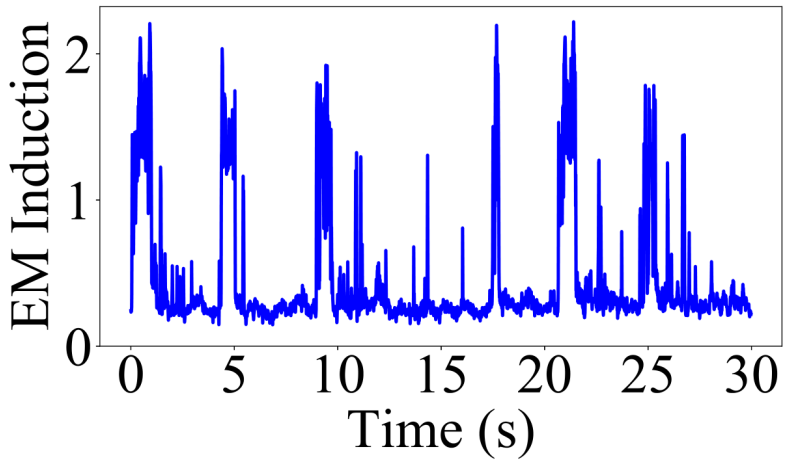
Type slow



Click fast

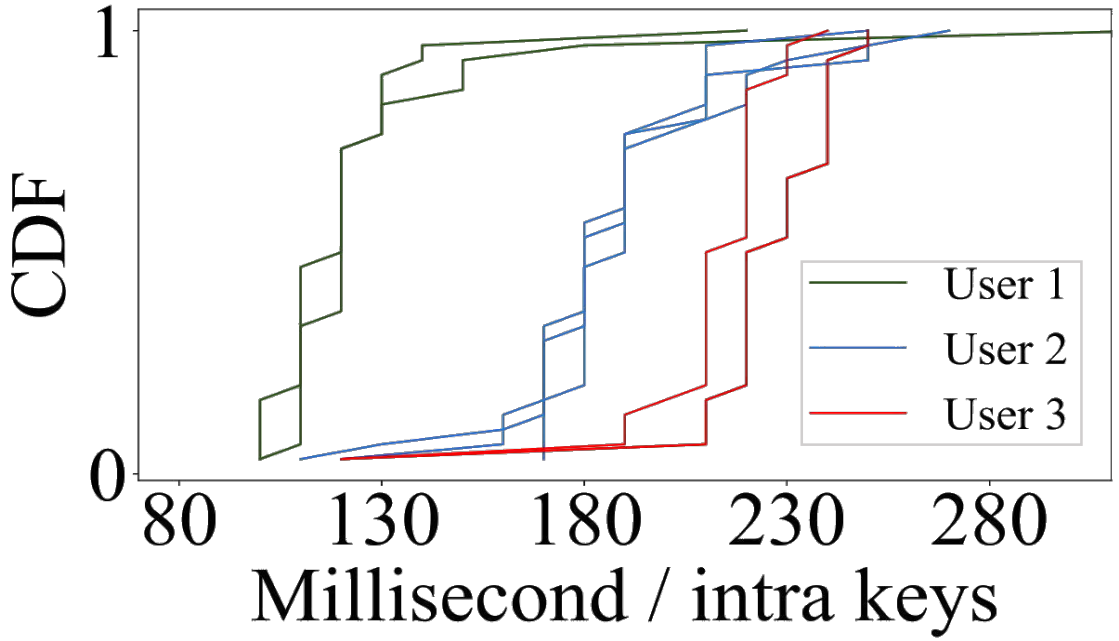


Click slow



Preliminary

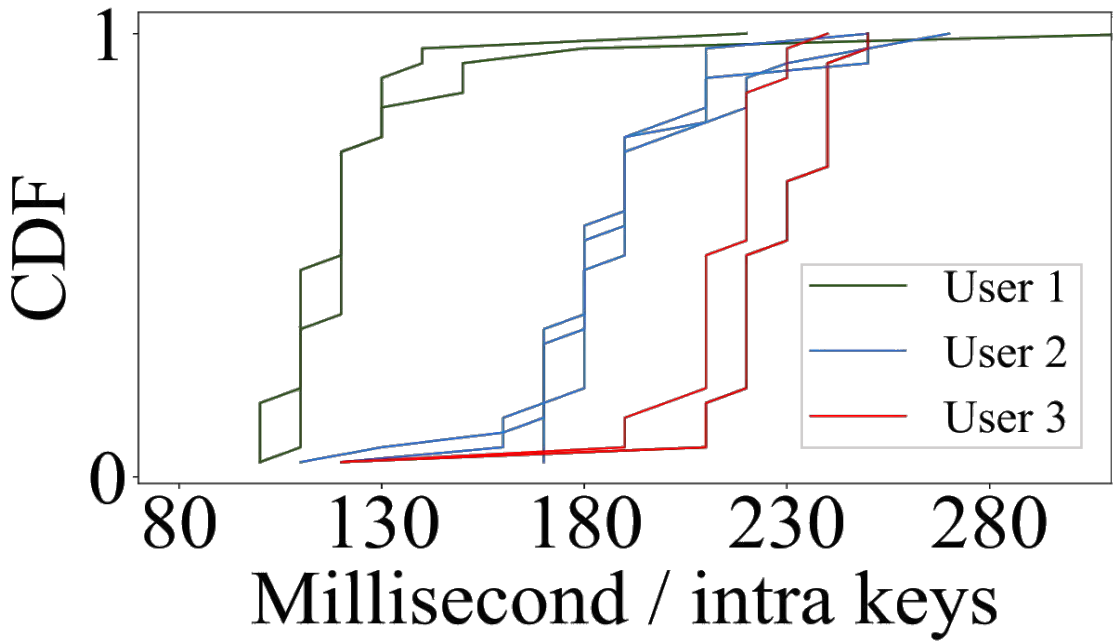
- **Q3:** Consistence over spatial and temporal domain.



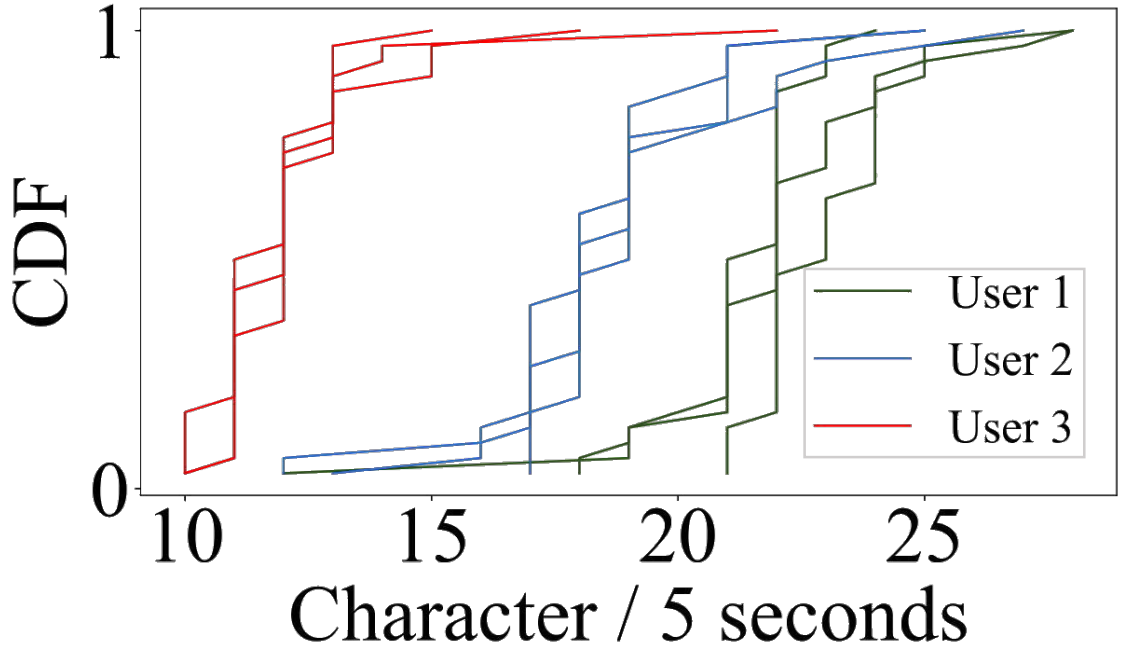
Intra-key interval

Preliminary

- **Q3:** Consistence over spatial and temporal domain.

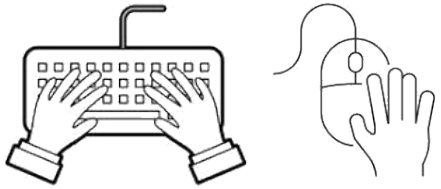


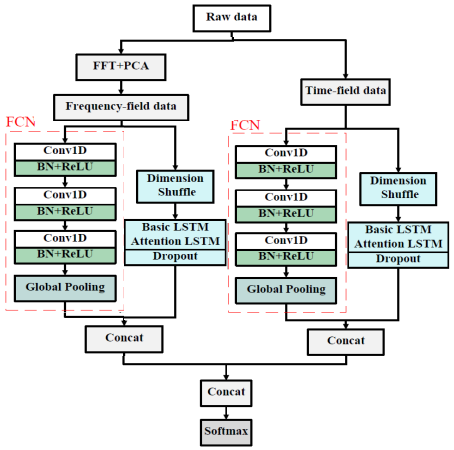
Intra-key interval



Typing speed

System Workflow



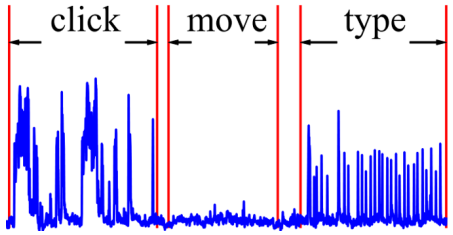


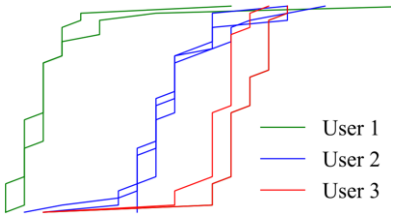
Different users' operations

EM signals of different using habits

Classification Model

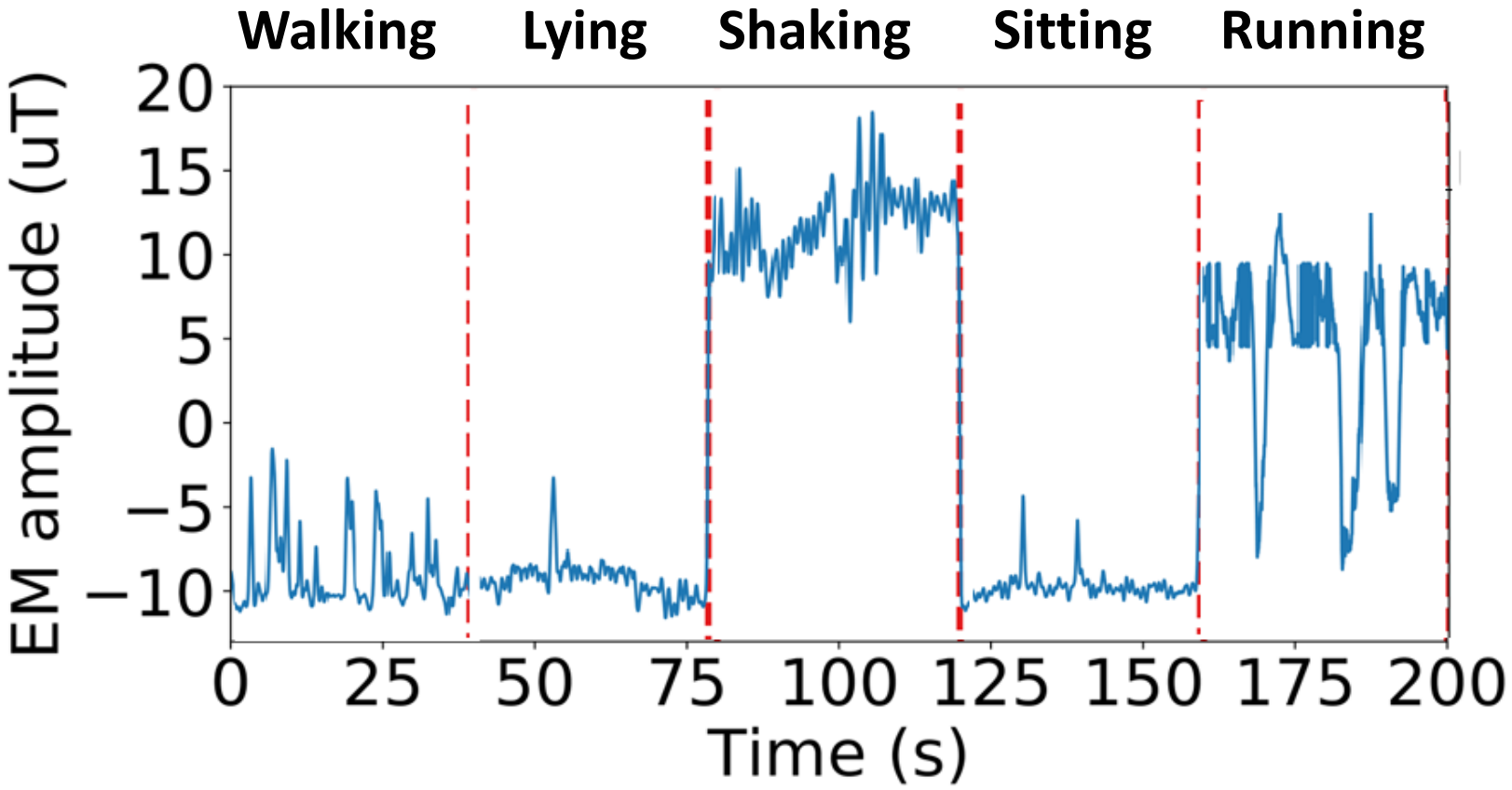
EM Based User Fingerprinting





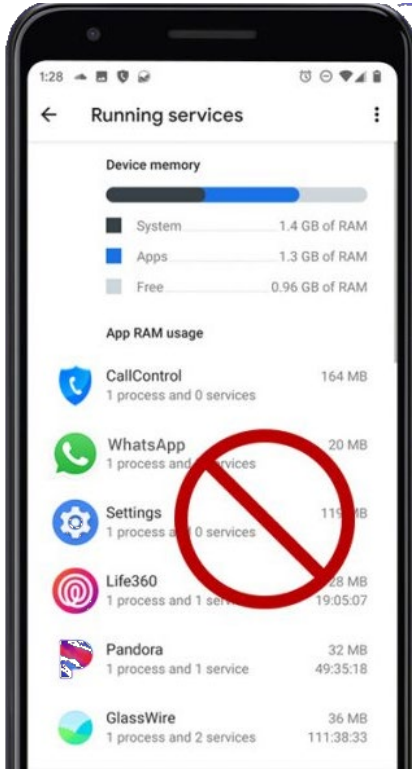
Challenge I —— Noisy EM signal cancellation

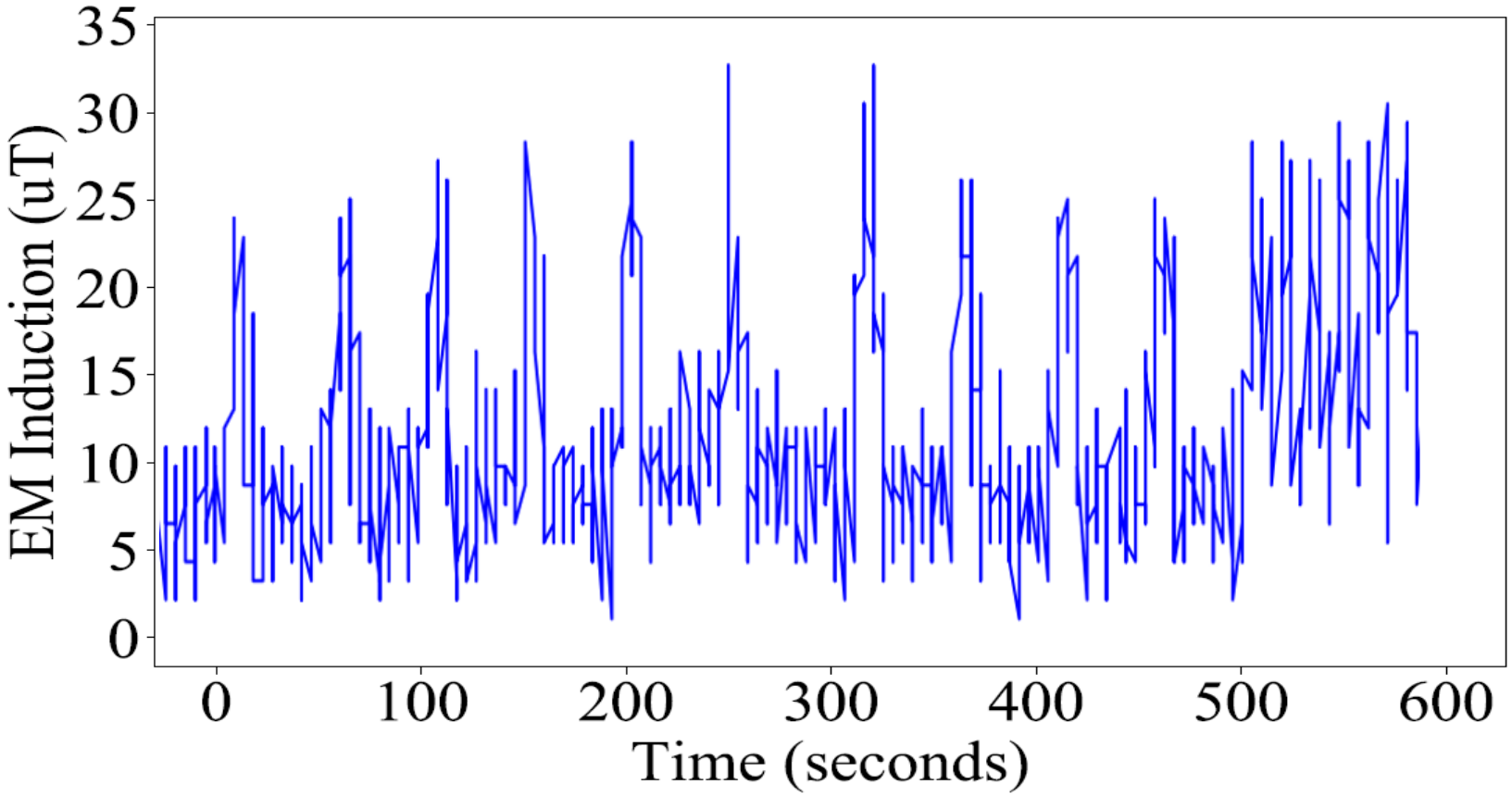
- Noisy EM signals caused by **human movements** because of the geomagnetic signal.



Challenge I —— Noisy EM signal cancellation

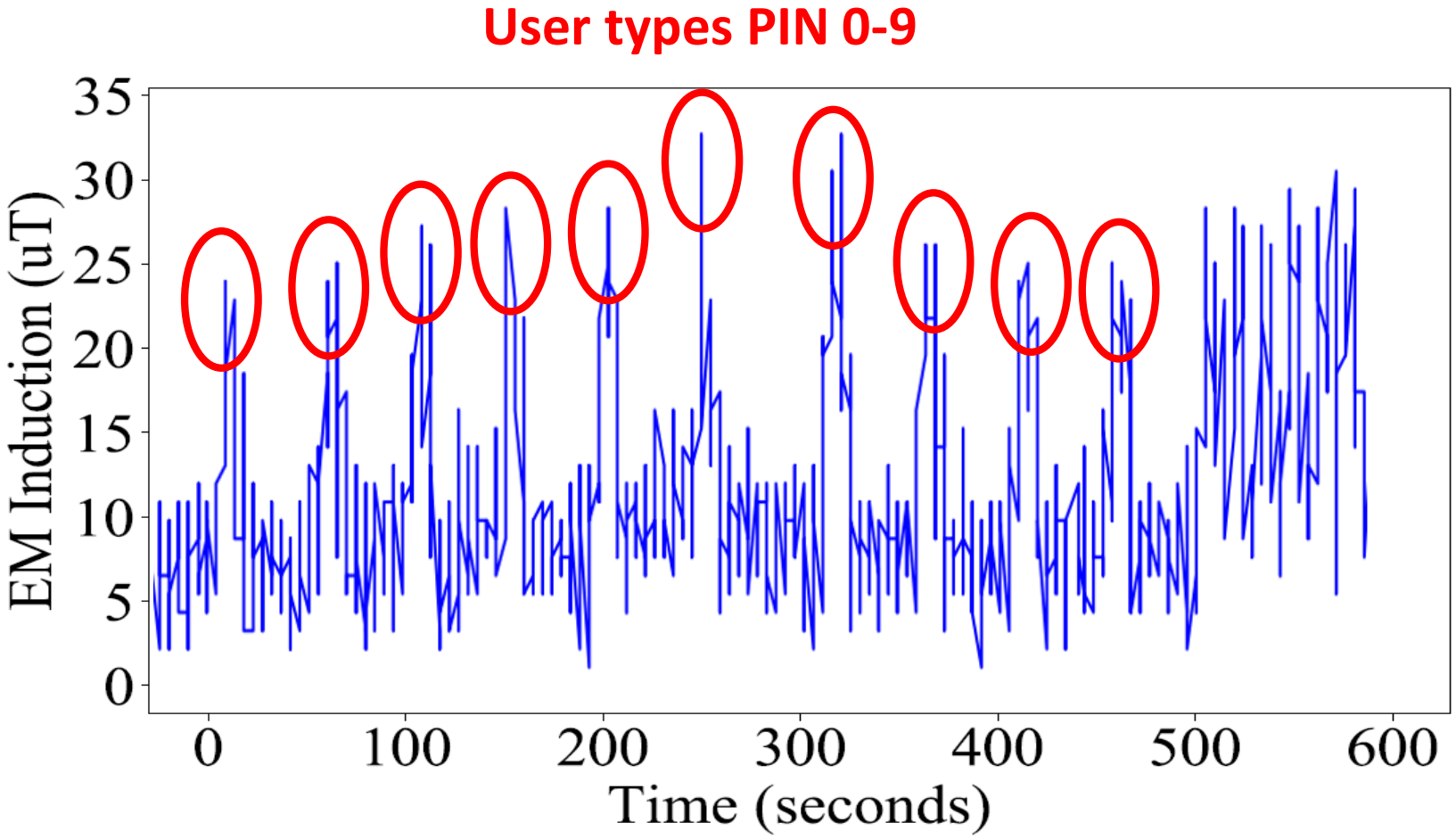
- Noisy EM signals caused by **background running APPs**.





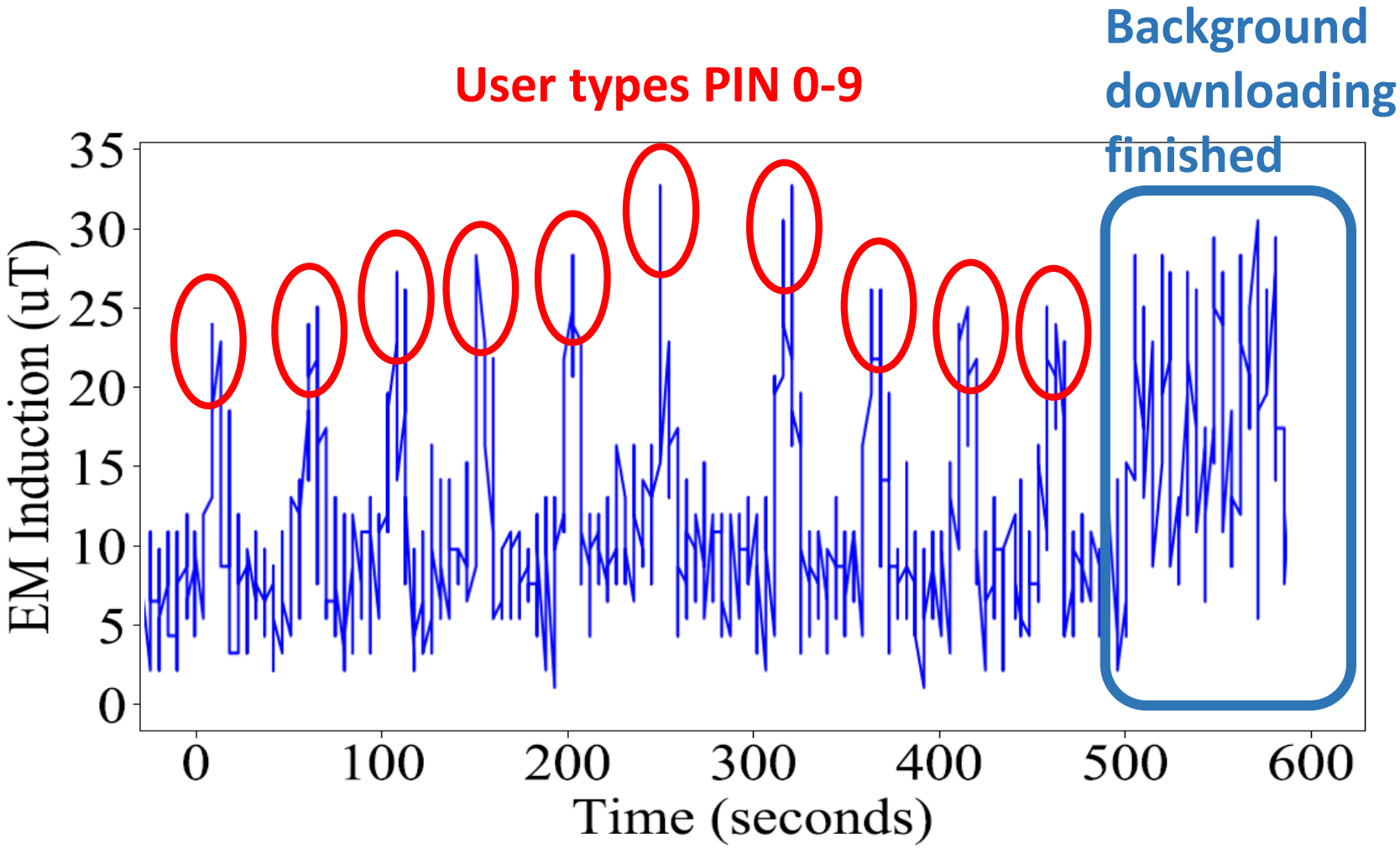
Challenge I —— Noisy EM signal cancellation

- Noisy EM signals caused by **background running APPs**.



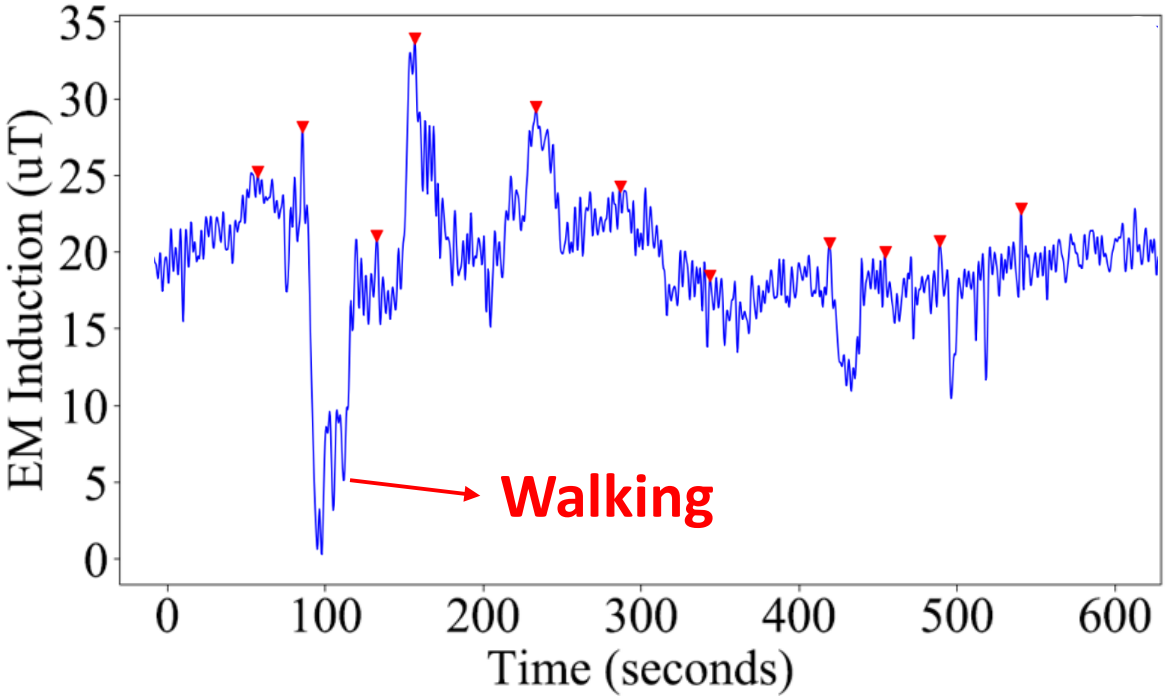
Challenge I —— Noisy EM signal cancellation

- Noisy EM signals caused by **background running APPs**.



Challenge I —— Noisy EM signal cancellation

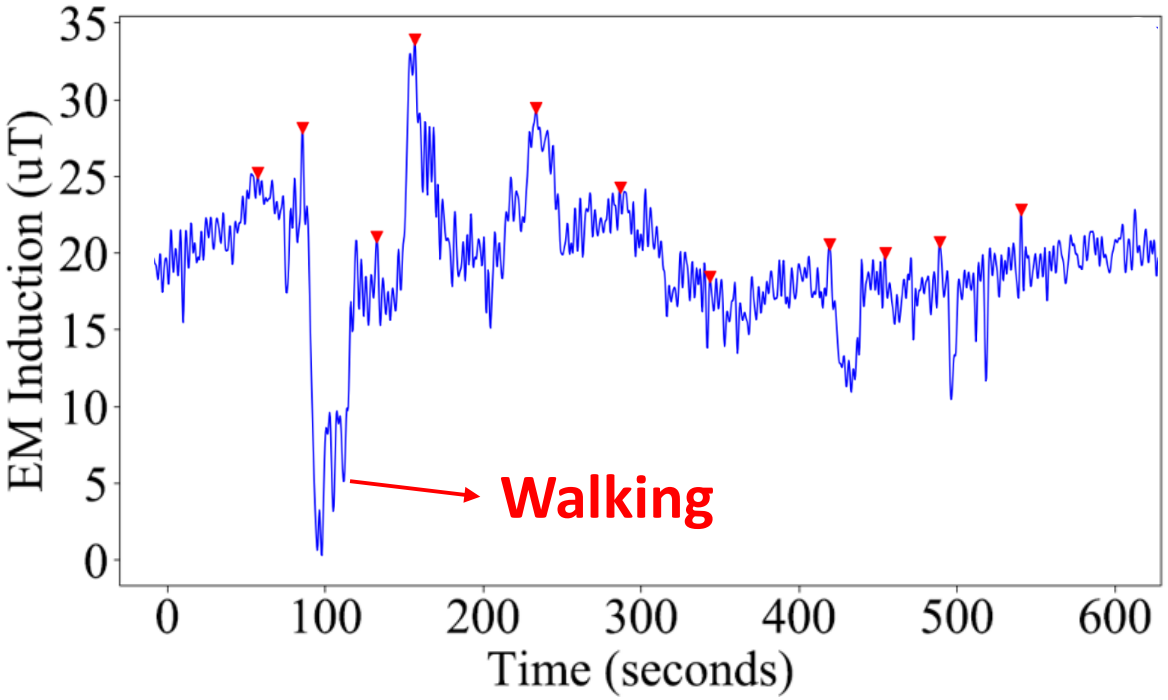
- Filter out noisy EM signals caused by human movement
  - *Low-pass filter* to capture interactions
  - *Gaussian filter* to eliminate random noise

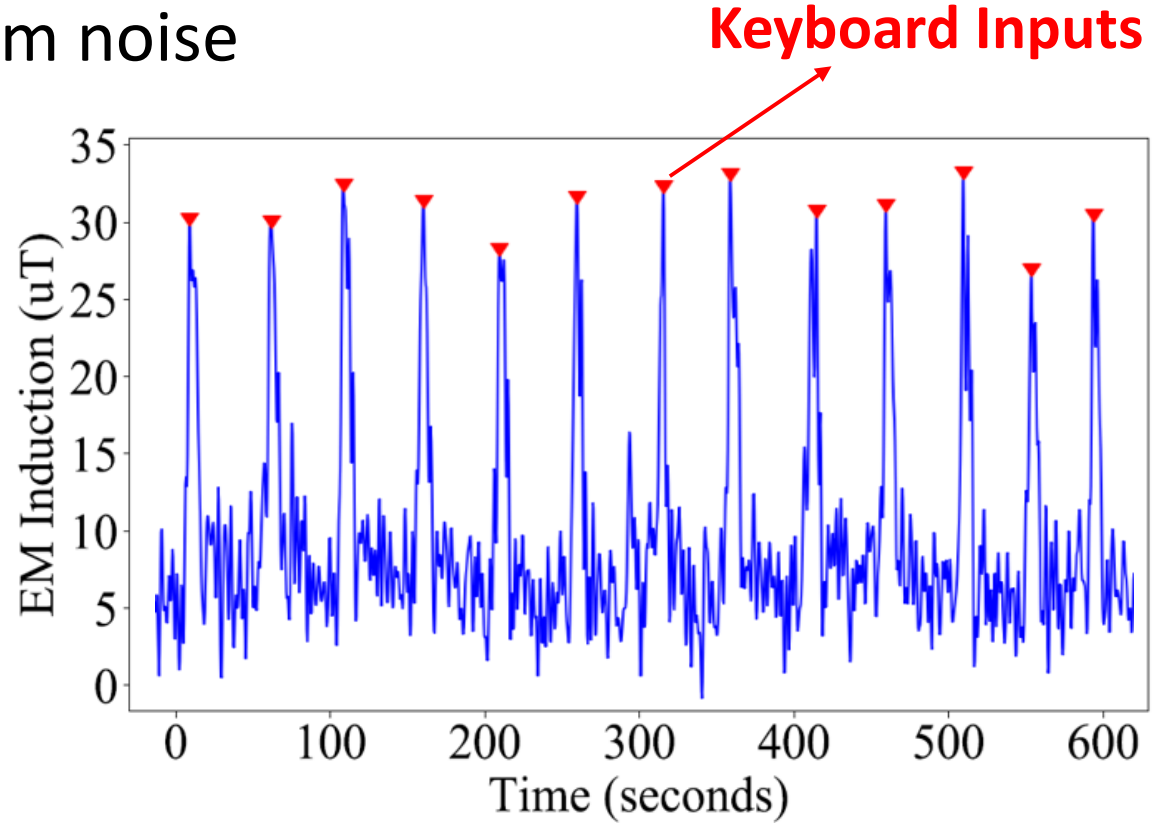


Original EM signals

Challenge I —— Noisy EM signal cancellation

- Filter out noisy EM signals caused by human movement
  - *Low-pass filter* to capture interactions
  - *Gaussian filter* to eliminate random noise

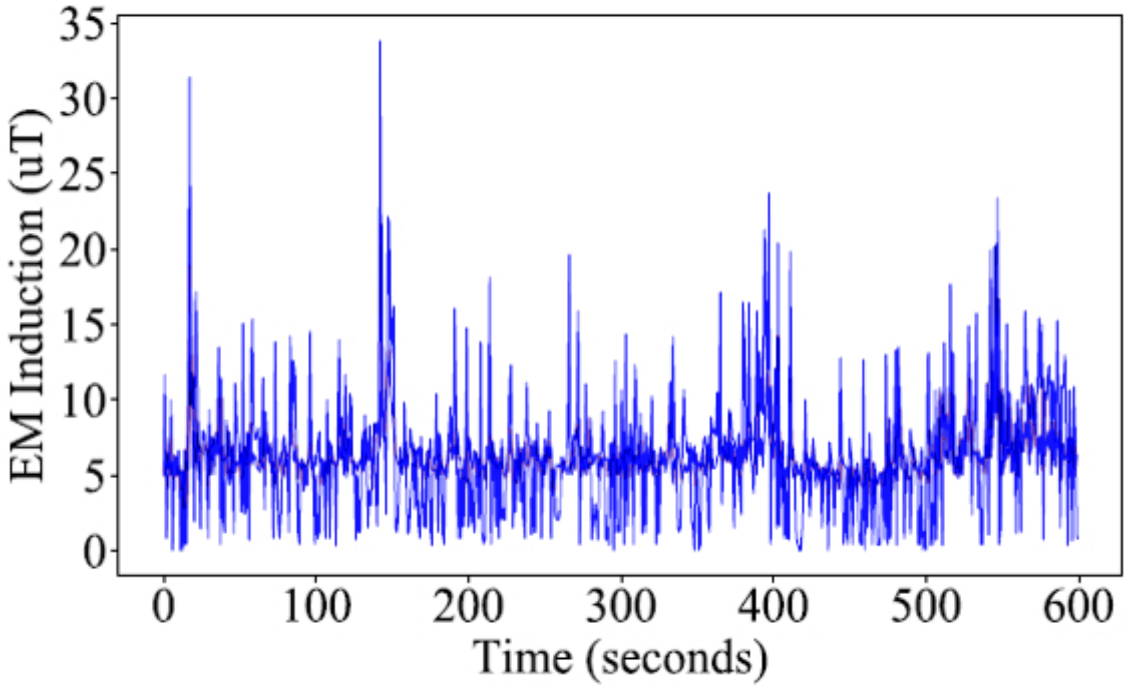




Original EM signals → EM signals after filtering

Challenge I —— Noisy EM signal cancellation

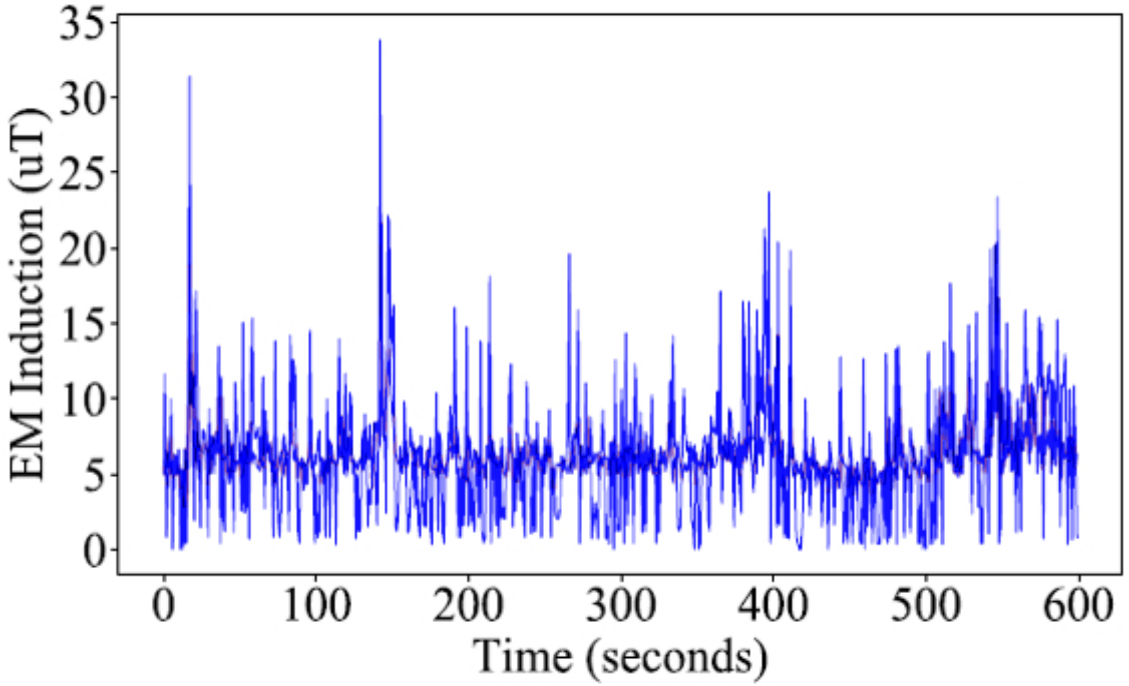
- Cancel the noisy EM signals caused by background running APPs
  - EM signals of Background Running APP change over time.
  - This change is gradual, such as listening to music.
  - 2-layer LSTM regression model is applied to cancel the background APP noise.



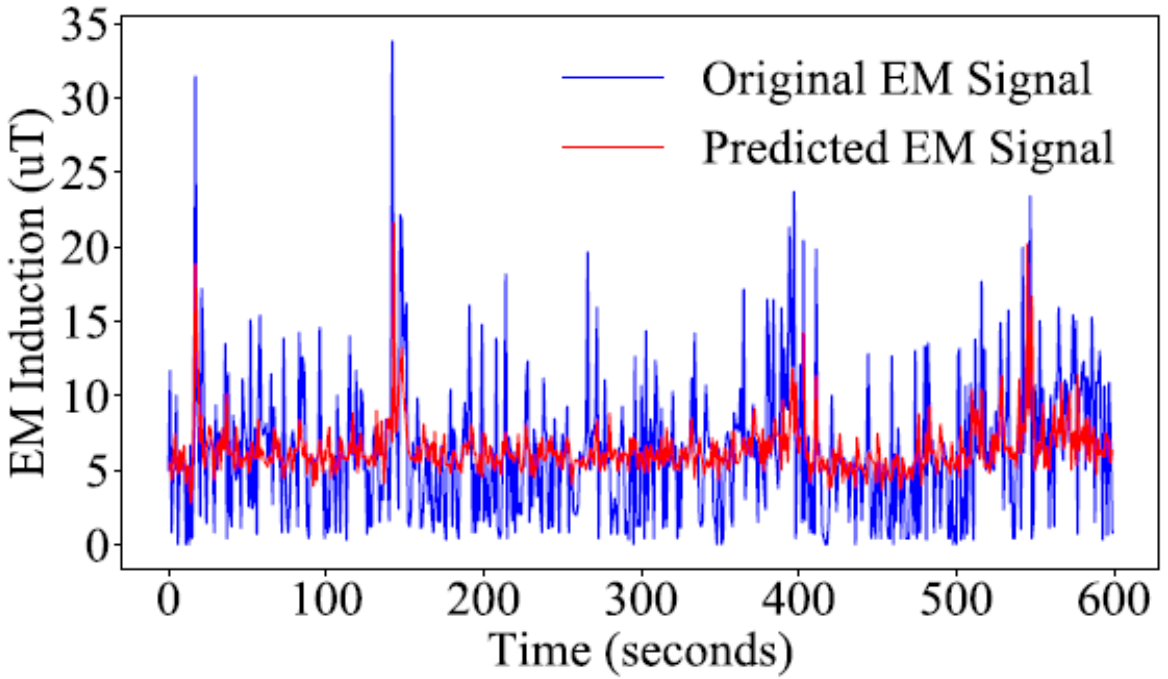
EM signal with background APP noise (listening music)

Challenge I —— Noisy EM signal cancellation

- Cancel the noisy EM signals caused by background running APPs
  - EM signals of Background Running APP change over time.
  - This change is gradual, such as listening to music.
  - 2-layer LSTM regression model is applied to cancel the background APP noise.



EM signal with background APP noise (listening music)



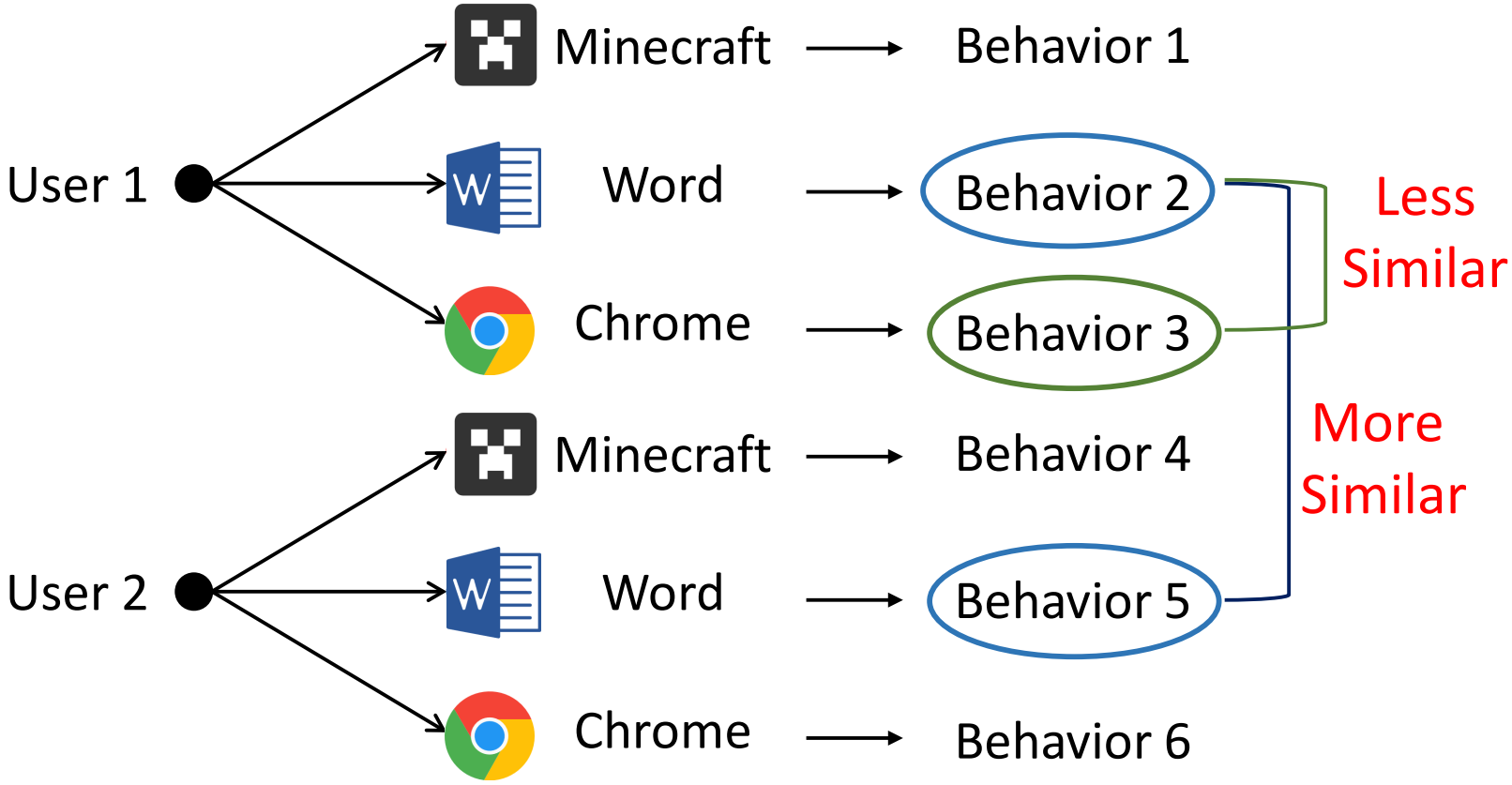
Predicted EM signals using 2-layer LSTM

Challenge II —— Diversity of APPs on the market

Train a model for each APP?

So many unknown/ untrained APPs

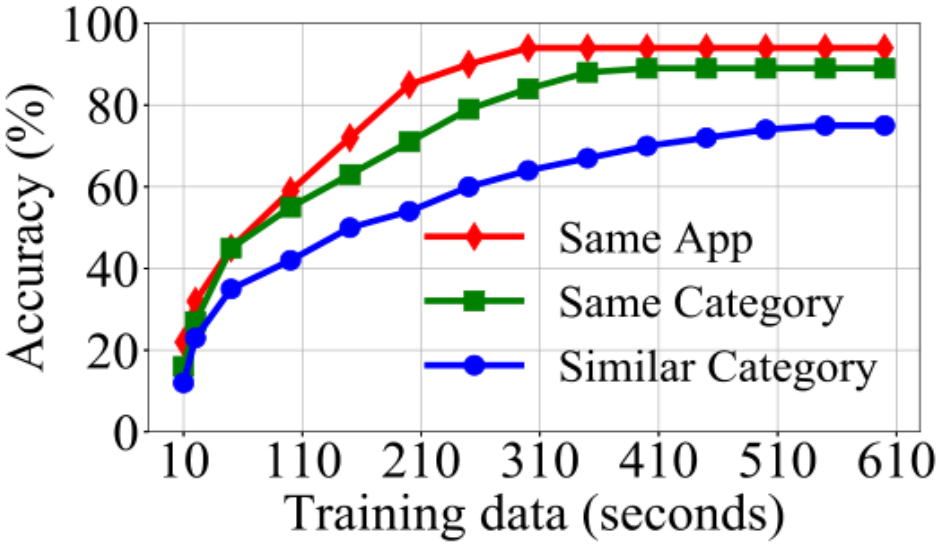
These user behaviors are more related to these APPs themselves, rather than the reflection of user habits.



Classify APPs into multiple categories

Frequency of	Typing	Clicking	Moving
Internet	3	5	5
Business	5	5	3
Communication	5	3	3
Game	1	3	5
Multimedia	1	1	1
SNS	3	3	5
System	3	4	3

APP categories classified by interaction behaviors



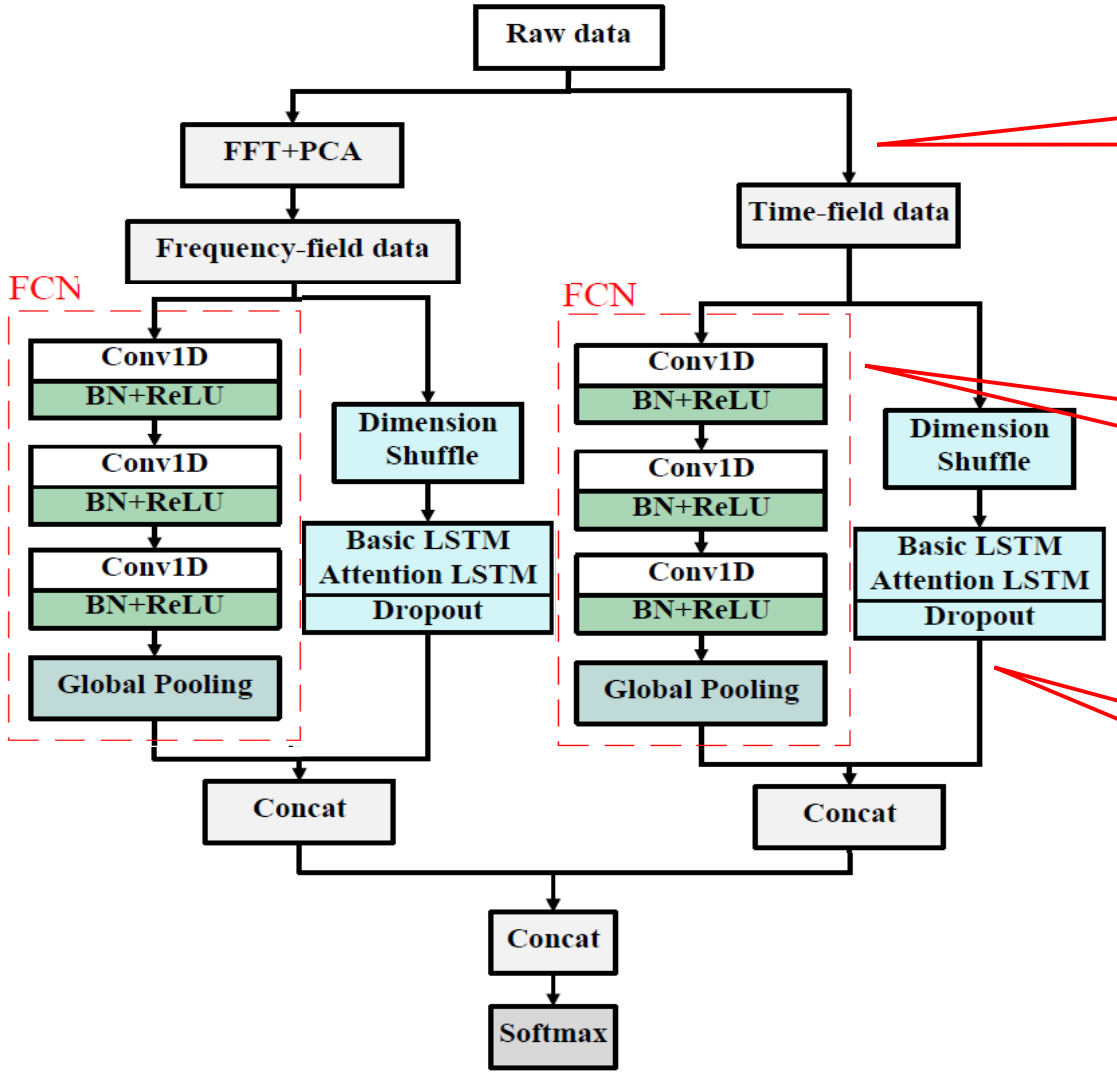
Classify APP into categories can reduce train data needed and remain high accuracy

Input EM signals → Classify into APP category → Using fingerprint model trained on this category → Fingerprint result

Challenge III – Users' Habits Tracking

- Mining users' habits from high-frequency EM signals.
- Users finish interactions in short time, while capturing users' habits need long time range.
- Present users' habits also depends on previous user interactions.
- Users' using habits change over time or mood, and there are also users with similar habits.

Users' Habits Extraction



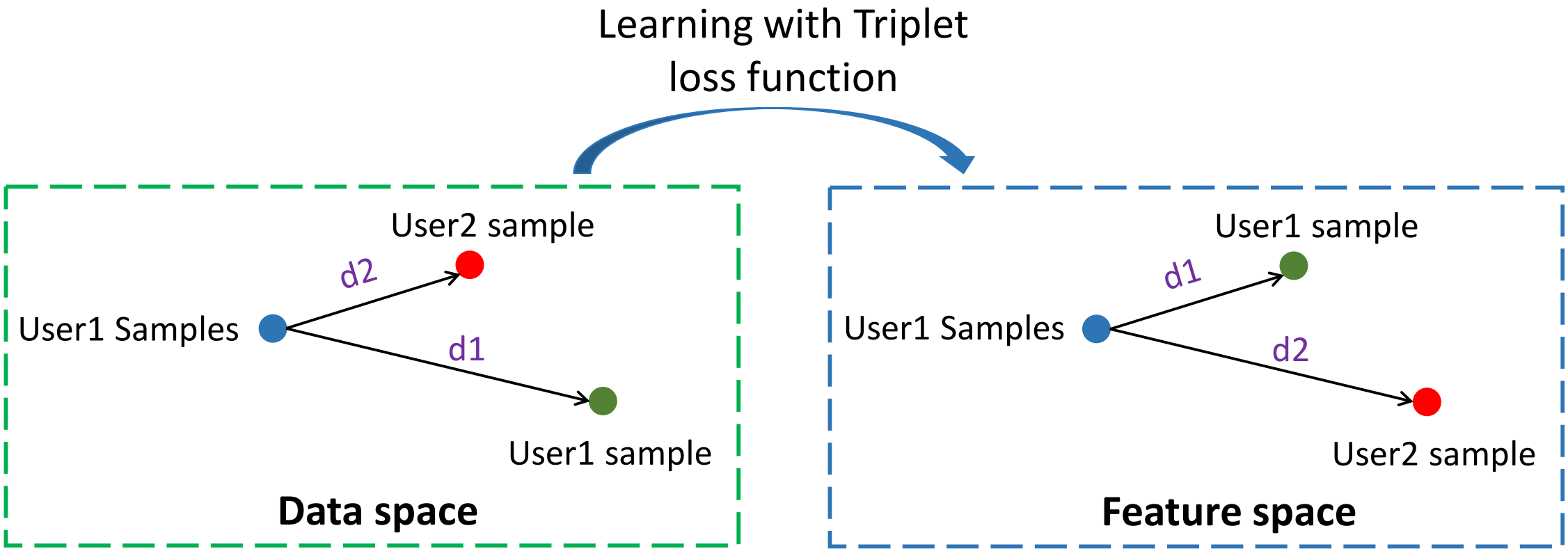
TF-FCN-LSTM Model

Combine of time-frequency domain data as input: fully use of high-frequency data

FCN: Capture short time interval features

LSTM: Track long time interval habits and model dependence on previous observations

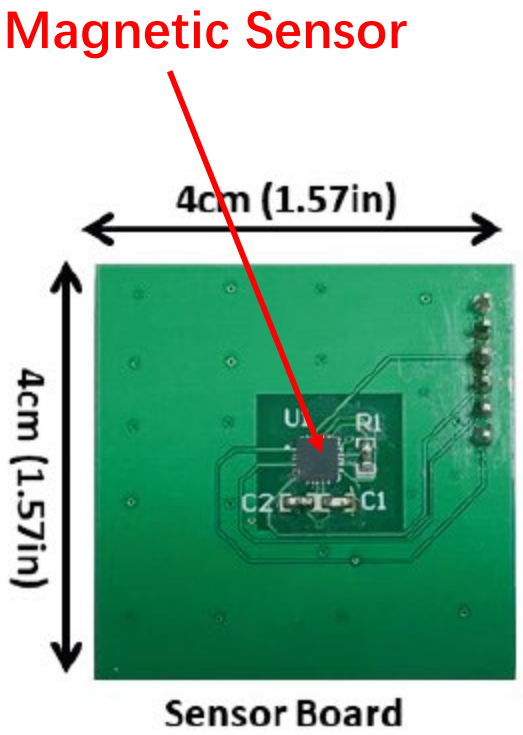
Distinguish Similar User Habits



$$d1 + \alpha < d2$$

$$\boldsymbol{L = \max(d1 + \alpha - d2, 0)}$$

Prototype



Sensor Board

MCU Board

Sensor Chip

Prototype on hand

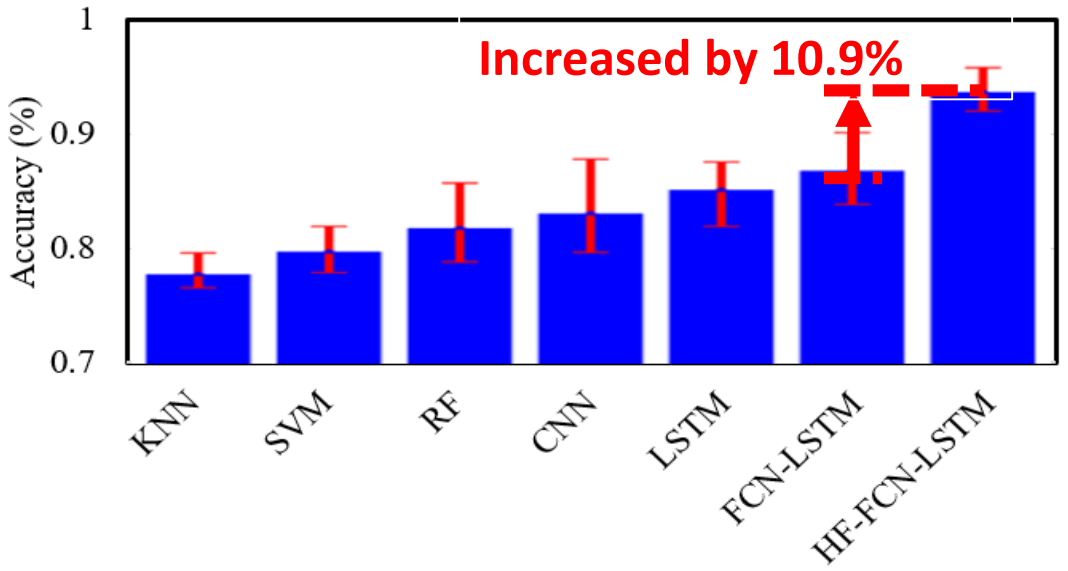
Evaluation

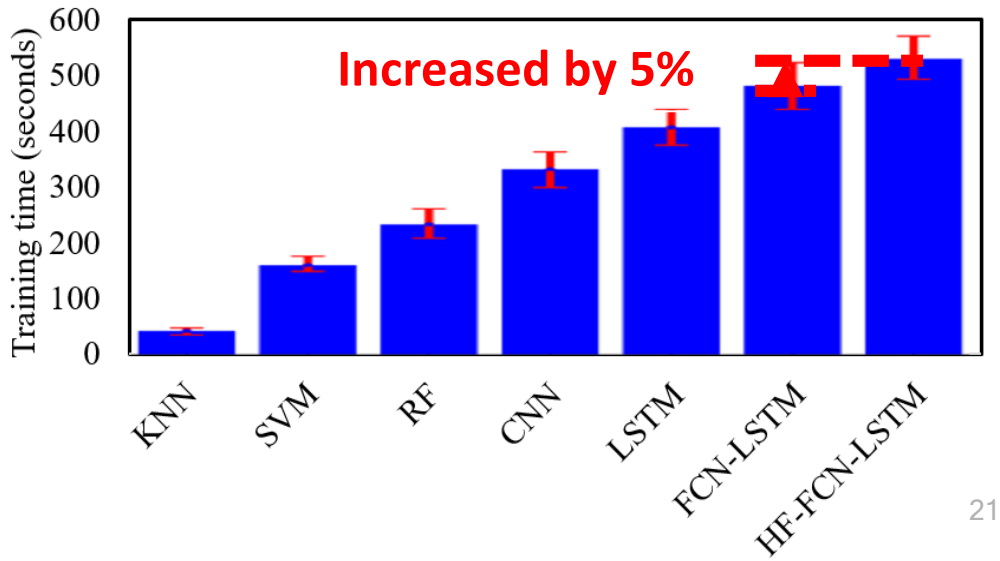
TABLE II: List of 30 Apps collected in the experiments.

App Category	Apps
Internet	Chrome, Firefox, Internet Explorer, Amazon Shopping, Baidu Cloud Download
Business	Microsoft Word, Excel, Power-point, Microsoft Notepad, Adobe Acrobat XI Pro
Communication	Skype, Tencent WeChat, QQ
Game	Zuma, Candy Crush Saga, Minecraft, Plants vs. Zombies, Agar Online
Multi Media	Youtube, Tencent Video, Aqiyi Video, Potplayer, NetEase cloud Music, Windows Media Player
SNS	Gmail, Github, Twitter
System	System Player, System Camera, System 3-D Plot

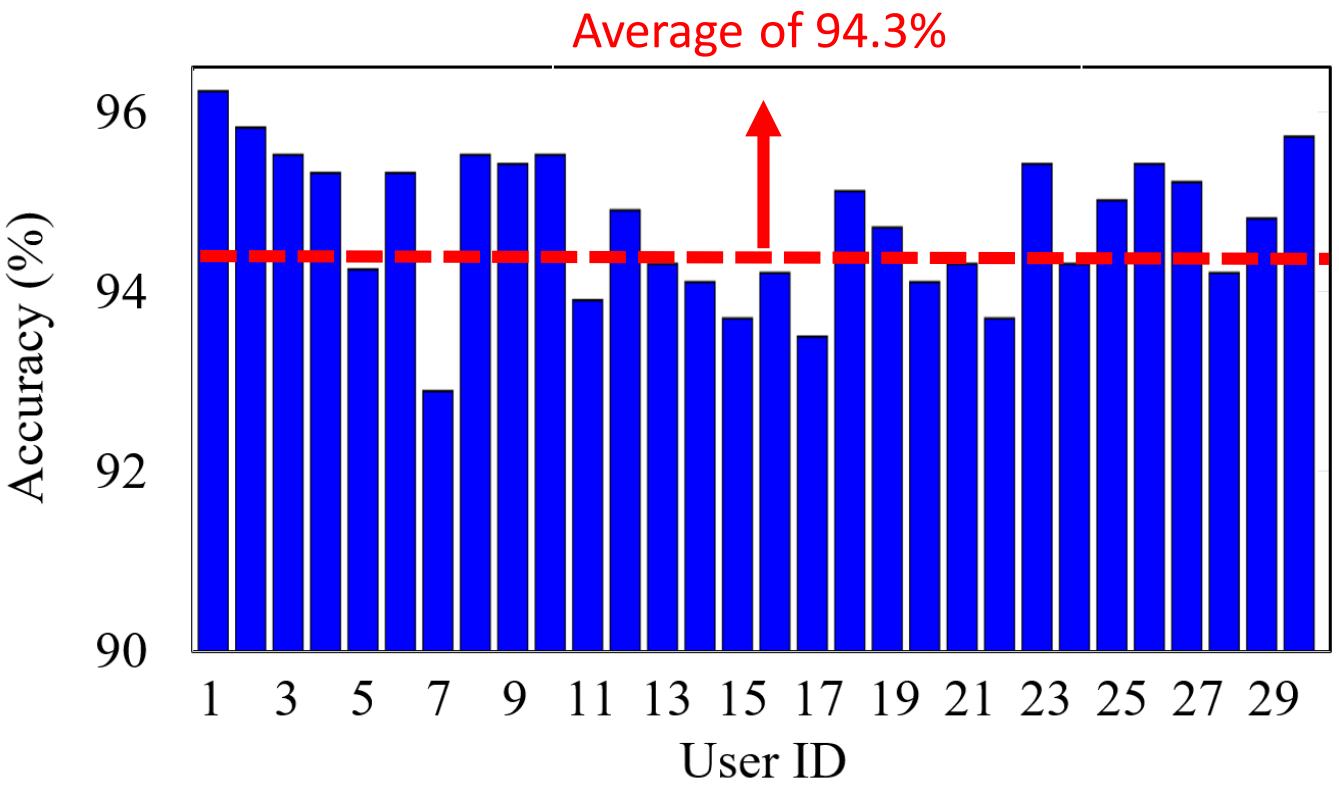
TABLE III: List of 10 devices collected in the experiments.

Model	OS versions	CPU Speed(GHZ)
MacBook Air MQD32CH/A	MacOS 10.13	1.7
MacBook Pro MMGM2CH/A	MacOS 10.13	2.8
Hp ENVY14-J102TX	Windows 10	1.6
Hp 15-be101TX	Windows 10	2.5
Lenovo T440	Windows 10	2.4
ASUS Vivobook 4000	Windows 10	2.4
ASUS FX-PRO	Windows 8	2.4
Samsung 800G5M-X08	Windows 8	2.5
Dell Ins-15PD-7745BR	Ubuntu 17.10	2.3
Acer SF314-52-59TW	Ubuntu 17.10	2.5



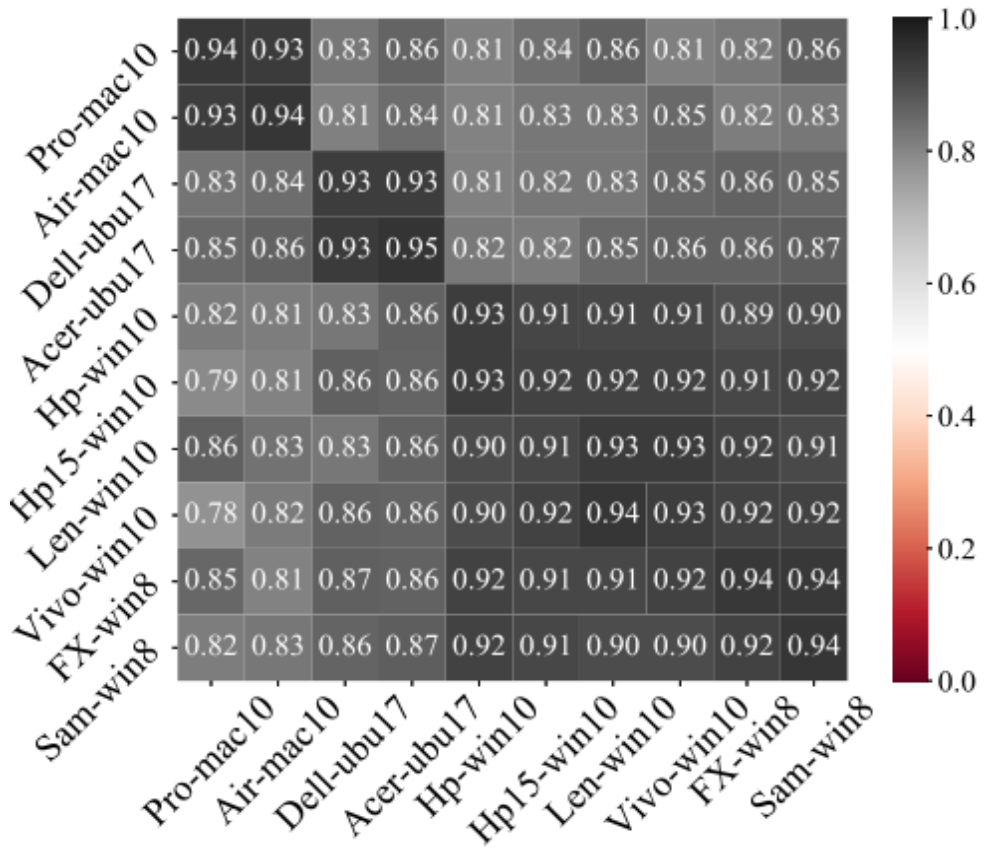


Evaluation



Accuracy across users

Same OS:92.0% Across OS: 83.7%



Leave-one-device-out cross validation

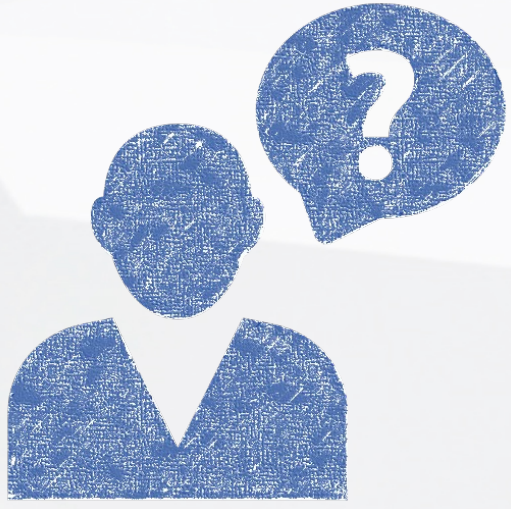
Conclusion and Feature Work

Conclusion

- Propose a novel continuous user fingerprinting method
- Deep learning based user interaction habits tracking
- Easy-to-deploy prototype

Future work

- Expand training set, improve accuracy and robustness
- New scenarios such as energy saving and privacy protection



Thank you !