João P. Vilela

University of Porto, INESCTEC and CISUC, Portugal

Federated Learning for Mobile Privacy

2023-12-07

Joint work with: Alastair Beresford (UCambridge, UK), Ricardo Mendes (UCoimbra, PT), Catarina Gomes, André Brandão, Mariana Cunha (UPorto, PT)

snob-5g.com

cop-mode.dei.uc.pt

1

Research Group: Main Areas & Applications

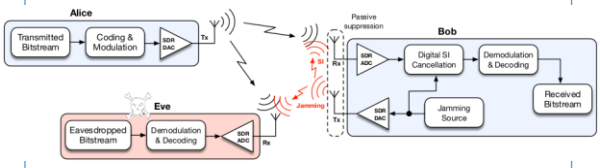
- Security and Privacy @ INESCTEC:
  - Cryptography & provable security, SMC, TEEs
  - Privacy-enhancing technologies
  - Secure distributed systems, decentralized ID management
- Networking @ CISUC, Coimbra:
  - Network security
  - Cloud and edge computing
  - Beyond 5G networks & services (slicing, orchestration, …)
  - Networks and systems management, Network virtualization and SDNs
- Application areas:
  - Smart Cities, Internet of Things, I4.0, Critical Infrastructures, Mobile Devices, ...

9

My Research Areas: Network Security

Wireless Physical-layer Security

- Jamming and Coding for Secrecy



- SDR Implementation & Evaluation

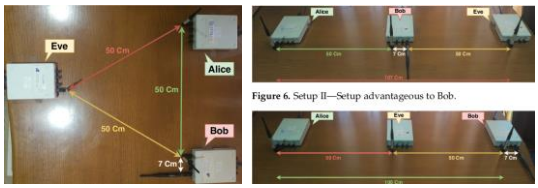
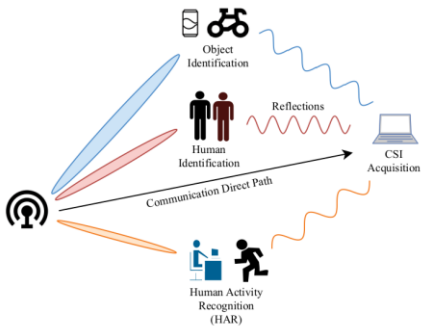


Figure 6. Setup II—Setup advantageous to Bob.

Joint Communications & Sensing

- Cross-domain: Avoid Scenario Dependance
- Privacy Aspects of Passive Sensing

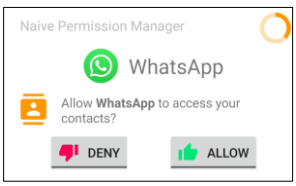


10

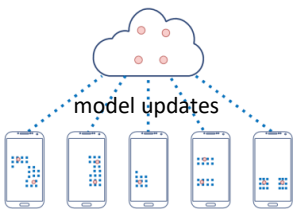
My Research Areas: Data Privacy

Automated Privacy for Mobile Devices

- Prediction of Privacy Preferences

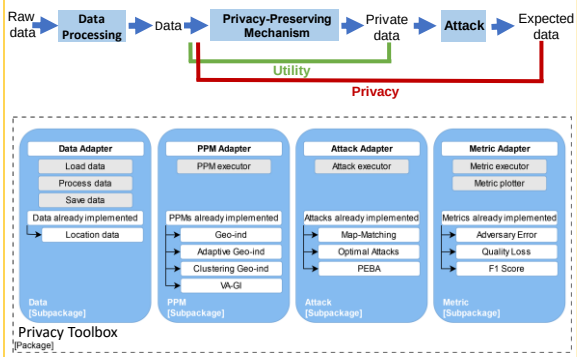


- In a Distributed/Federated Manner



Anonymization Methods for Heterogeneous Data Types

- Location Data
- Face Detection/Recognition



11

The Problem of Privacy in Mobile Devices

Dozens of apps

X

Multiple Configurations

=

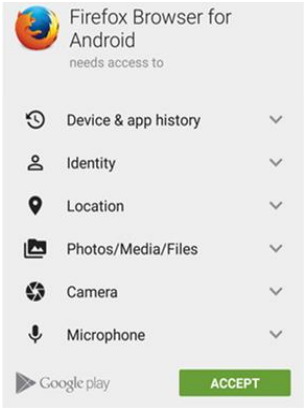
Privacy Loss

5

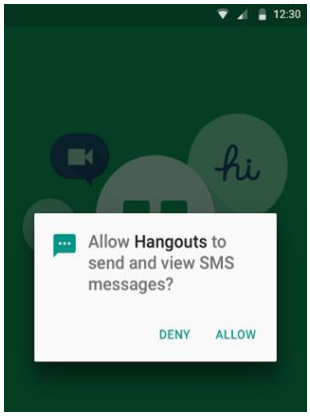
18

Privacy in Mobile Devices

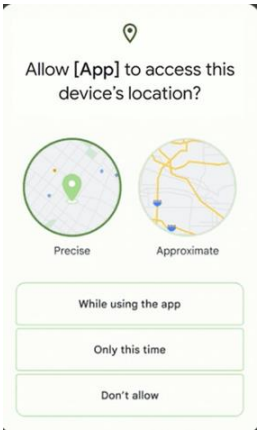
Install-time Permissions



Runtime Permissions (Oct 2015)



Latest Improvements

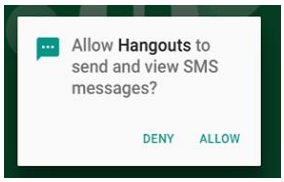


- Location Obfuscation
- "While using the app" (location, camera and microphone)
- "Only this time"
- Auto-reset when unused

6

19

Privacy in Mobile Devices



Runtime permissions allow:

- fine-grained permissions control
- to contextualize permission prompts by the needs of the app

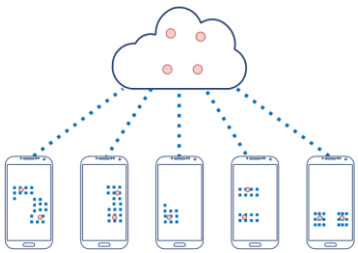
The problem: (hundreds of daily) **automatically accepted permissions**

- **Violate** contextual integrity (preferences of user within context)
- **Contradict** user expectations

7

20

Solution: Automated Privacy Decisions



- Several devices with local info on:
  - Requesting Application
  - Permission
  - Grant Decision

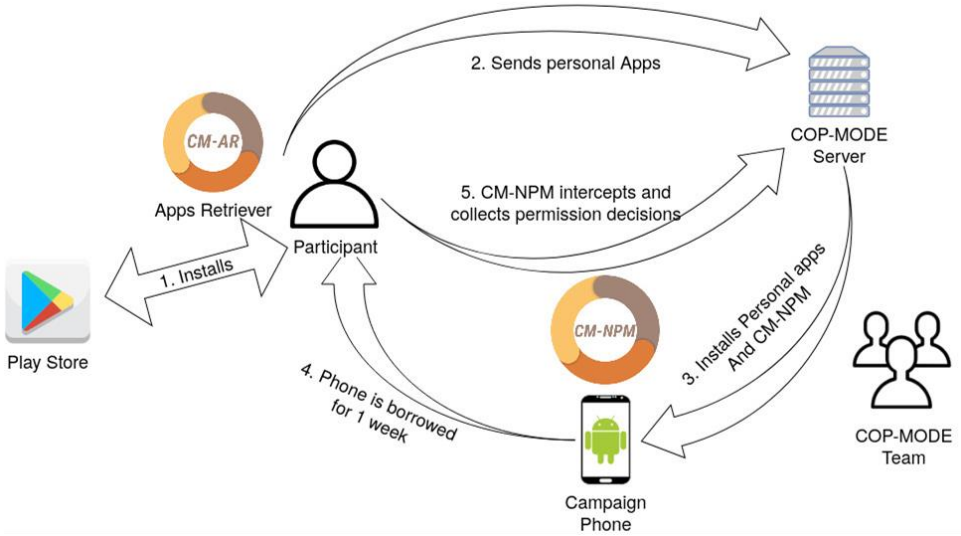
- Prediction of Grant Decisions (Allow / Deny)
- According to Users' Preferences

For this, we need data!

8

22

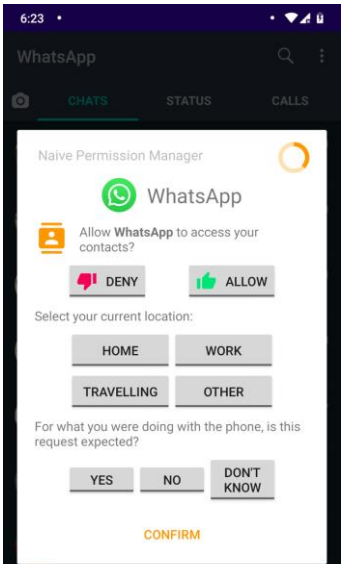
COP-MODE: Data Gathering Campaigns



9

23

COP-MODE: Data Gathering Campaigns (2)



https://cop-mode.dei.uc.pt/cm-npm

Collected data (summarized):

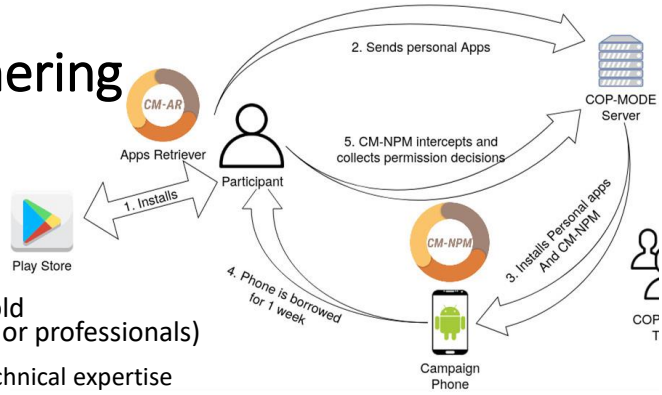
- **Requesting application:** name and play store category
- **Permission:** name, group and grant result (allow/deny)
- **Phone state:** geolocation, network connection, plug, dock, call and screen state, and apps running in the foreground/background
- **User context:** time, semantic location and if the user is in an event, according to their calendar.
- **Expectancy:** answer to “For what you were doing with the phone, is this request expected?”

https://cop-mode.dei.uc.pt/dataset

10

24

COP-MODE: Data Gathering



93 participants

- 64.5% were students
- 71% were between 18 and 24 years old
- 57% with an IT background (studying or professionals)

→ Biased data towards young adults with technical expertise

Using our smartphones for 1 week+

Collected answers to 2M+ permission requests

65K+ manually answered requests

(~837/day, ~35/hour)

https://cop-mode.dei.uc.pt/campaigns

11

25

COP-MODE Data: Main Findings

65K+ manually answered permission requests:

- Avg 836 requests/day/user, nearly 35/hour
- **Nearly 50% requests unexpected to users**
- **15% privacy violations**

To catch 15% privacy violations ► answer 35 requests/hour

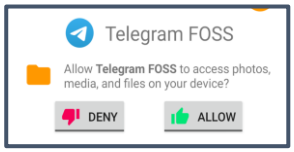
[Mendes et al., "Effect of User Expectation on Mobile App Privacy: A Field Study", PerCom'22]

12

29

Solution: Automated Privacy Decisions

- Several devices with local info on:
  - Requesting Application
  - Permission
  - Grant Decision



- Goal: Prediction of Grant Decisions (Allow / Deny)
- According to Users' Preferences

Which features are relevant for prediction of grant decisions?

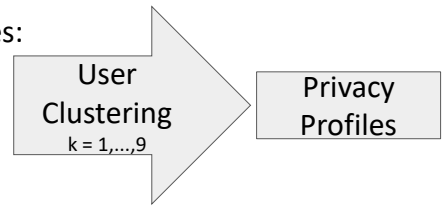
13

36

Automated Privacy Decisions: Methodology

Contextual Features:

- [C]ategory
- [P]ermission
- [E]xpectation
- [V]isibility
- [L]ocation
- [N]etwork status
- …

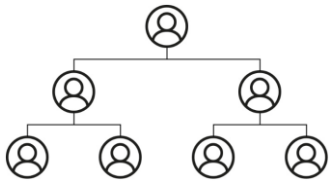


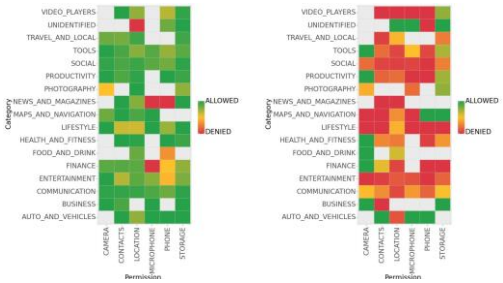
14

37

Generation of Privacy Profiles

- Clustering of users into privacy profiles
  - (app category, permission, avg_grant_result)
- Profiles represent users' beliefs and expectations
- 2 approaches:
  - Hierarchical clustering
  - K-means clustering





Permissive User **Restrictive User**

15

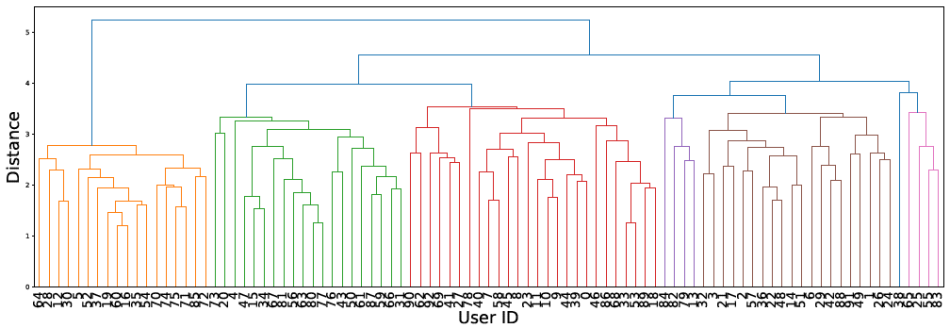
38

Hierarchical Clustering

- Per user (Category, Permission, Grant result):

App category: / Requested permission:	EVENTS CALENDAR	EVENTS CAMERA	...	AUTO_AND_VEHICLES PHONE	AUTO_AND_VEHICLES CONTACTS
Grant result:	0.9	0	...	0	0
	0.2	0.1	...	0.35	0.4

- Hierarchical clustering to divide users into profiles by creating a dendogram of distances and make a cut were appropriate

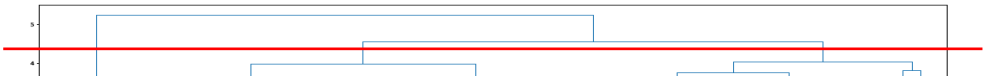


16

39

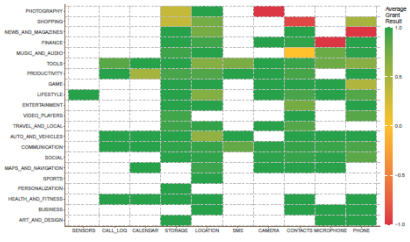
Hierarchical Clustering

- Making a cut at distance 4.3

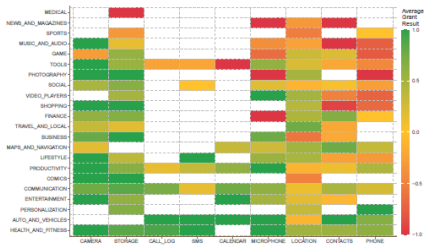


- Would result in 3 profiles as follows

(a) Profile 1 - the privacy conscious user.



(b) Profile 2 - permissive user.

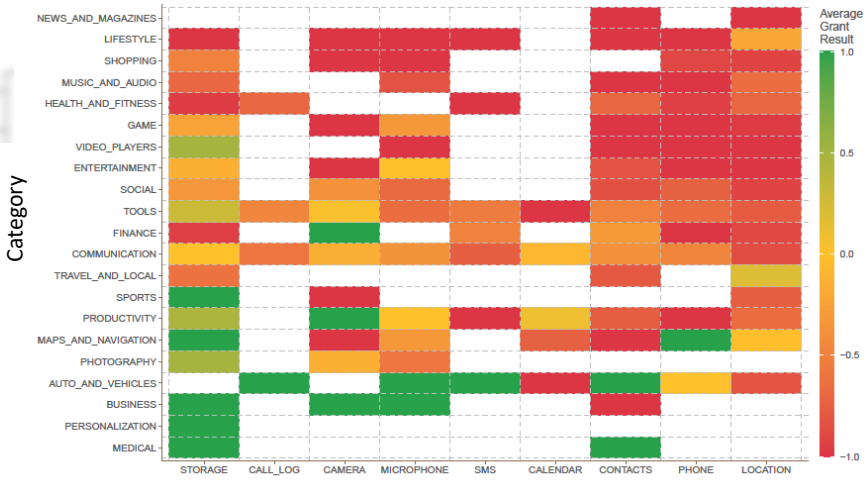


(c) Profile 3 - the middle ground user.

17

40

Hierarchical Clustering



(a) Profile 1 - the privacy conscious user.

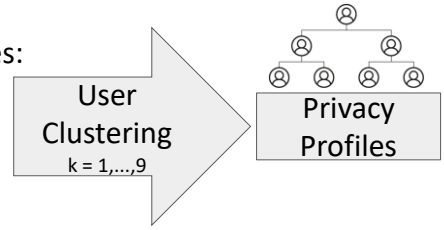
18

41

Automated Privacy Decisions: Methodology

Contextual Features:

- [C]ategory
- [P]ermission
- [E]xpectation
- [V]isibility
- [L]ocation
- [N]etwork status
- …



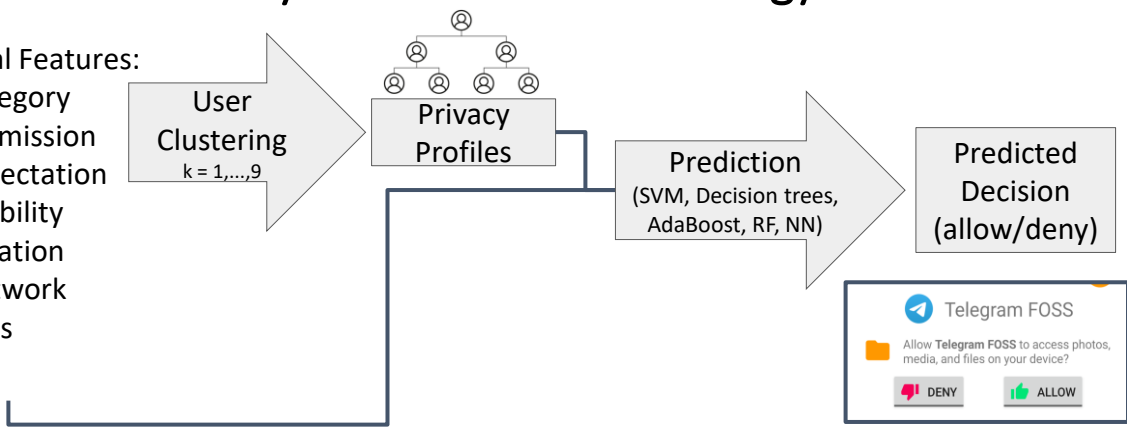
19

45

Automated Privacy Decisions: Methodology

Contextual Features:

- [C]ategory
- [P]ermission
- [E]xpectation
- [V]isibility
- [L]ocation
- [N]etwork status
- …



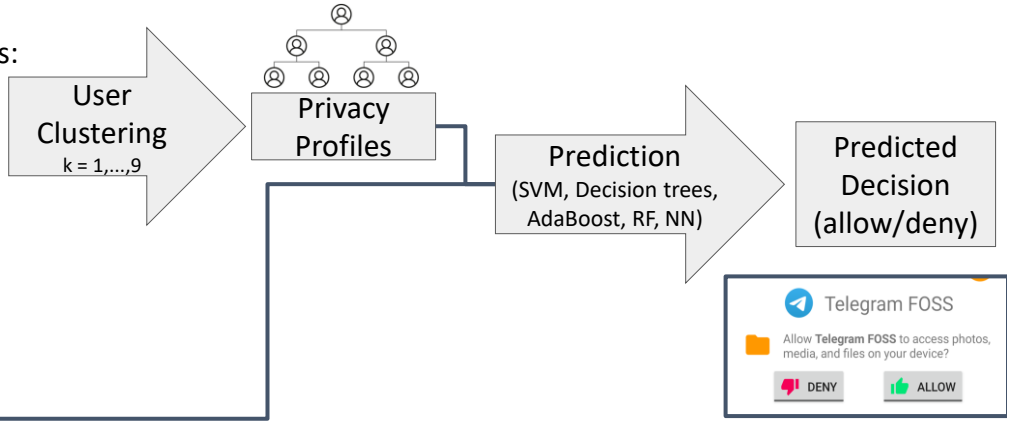
20

46

Automated Privacy Decisions: Methodology

Contextual Features:

- [C]ategory
- [P]ermission
- [E]xpectation
- [V]isibility
- [L]ocation
- [N]etwork status
- …



Prediction of Grant Result - Summarized Procedure:

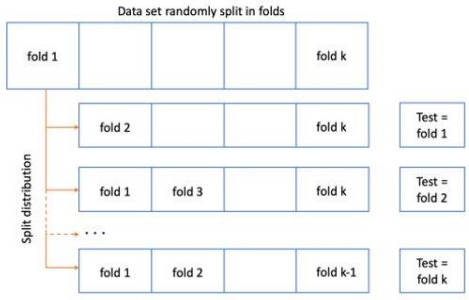
1. One-hot encoding of categorial features (eg app category)
2. Selection of best predictor model through grid search on several parameters
3. Area Under the Receiving Operation Curve (ROC AUC) as performance indicator
4. Prediction with and without profiles (baseline) for several category sets

21

47

Prediction of Permission Requests - more detail

- **Labels:** deny encoded by 0, grant encoded by 1
- **Metrics:** ROC AUC, F1, accuracy, recall and precision
- **Features:** category, permission, expectation, visibility, location, network status, ...
- One-hot-encode categorical features
- Stratified train test split
- **Grid-search** over several combinations of hyperparameters
- **Evaluation methodology:** 5-fold cross validation
- **Models:** decision tree, adaboost, NN, ...



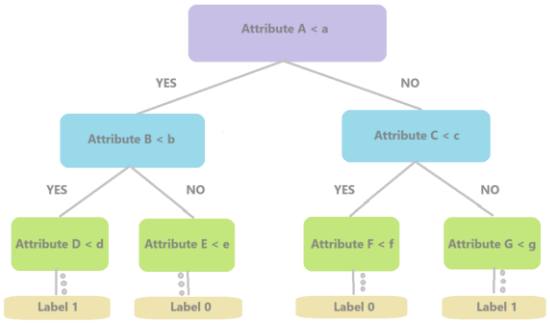
22

48

Learning as search

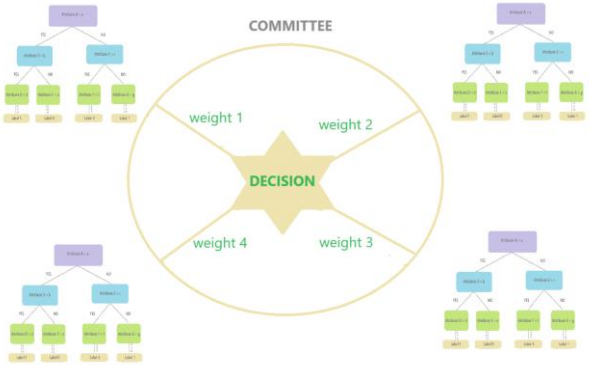
Decision Tree:

- Recursively divide into subregions until some stopping criteria is met



Tree Ensembles – Adaboost:

- Weight decision according to performance
- Iteratively focus on harder examples



23

49

Decision Tree – COP-MODE

- Set of requests is mostly described by binary features
- **Divide set of requests** into 2 sets according to their value with respect to a certain feature
- Choose **feature to split** wisely - feature that **best distinguishes** denied requests from granted ones in that set of uses
- **Repeat process** until a further split does not compensate complexity increase (or until a maximum number of splits is reached)
- Single model to classify users' response may not be enough (small changes in the training set may cause significantly different view over the set of users)
- **Solution:** try **ensembles** of decision trees or more **complex** models

24

50

AdaBoost – COP-MODE

- Build many decicion trees based on different training sets
- How different are subsequent training sets? Model(i) will be trained on **difficult to classify requests** (based on misclassification rate from i-1 models before)
- Given a request, each decicion tree will have a prediction
- How to weight each decision tree prediction to the final decision? The **weight is proportional to its performance**
- Final prediction will be the weighted sum of each decision tree prediction

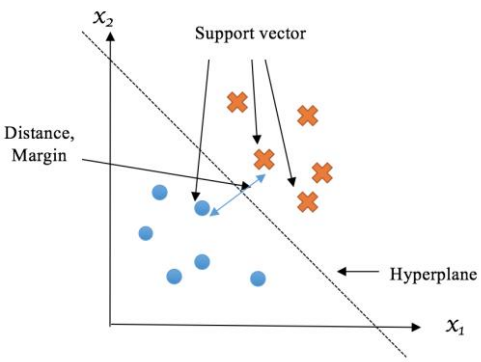
25

51

Support Vector Machines

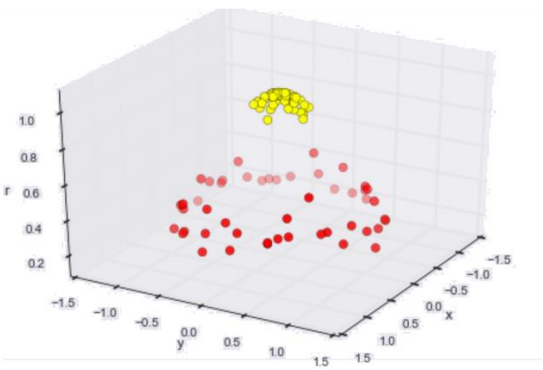
Linearly separable case:

- Find decision boundary with the safest margin by finding most problematic points - **support vectors**



Non-linearly separable case:

- Find new dimmension where classes are linearly separable

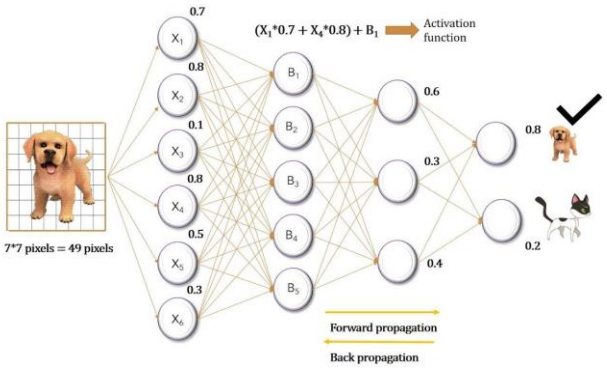


26

52

Neural Networks

- Most **successful** ML model - highly **flexible** model that can approximate many types of functions
- **Architecture:** input, hidden and output **layers** linked by **activation functions**



27

53

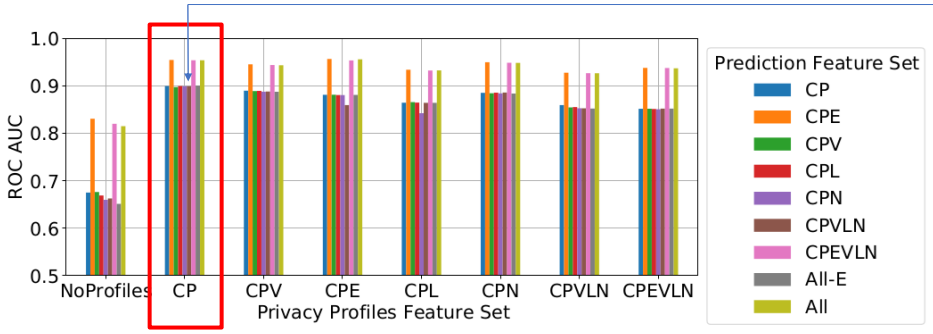
Neural Networks – COP-MODE

- **Goal:** Based on requests' features (that characterize context) **model grant probability**
- Each request is passed through the network
- Use gradient of the loss of a batch of requests to update model weights
- Final output is the probability of the request being granted
- For a **fixed threshold**, we predict a positive response if the grant probability is higher than the threshold (usually = 0.5)

28

54

Results



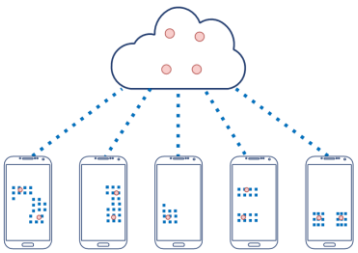
- Best results (Ada Boost) achieved when profiling with only **[C]ategory and [P]ermission**
- Best performance achieved when predicting with **CPE (orange bars)**
  - ~0.96 ROC AUC (F1 score 0.92)
- Without user expectation we achieve a ROC AUC 0.9 (F1 score 0.88) with **CPVLN**
  - Very similar to just using **CP**
- **CP** suffices for clustering users
- Prediction requires more features, particularly the **Expectation**

Contextual Features:
[C]ategory, [P]ermission, [E]xpectation, [V]isibility, [L]ocation, [N]etwork status

29

55

Solution: Automated Privacy Decisions



- Several devices with local info on:
  - Requesting Application
  - Permission
  - Grant Decision

- Prediction of Grant Decisions (Allow / Deny): ROC AUC of 0.9
- According to Users' Preferences

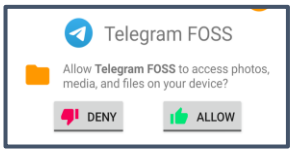
For this, we need data!

30

57

Solution: Automated Privacy Decisions

- Several devices with local info on:
  - Requesting Application
  - Permission
  - Grant Decision



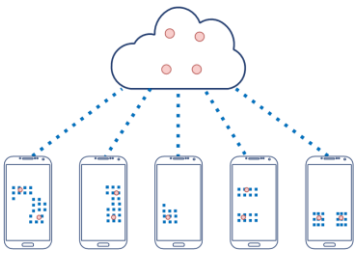
- Prediction of Grant Decisions (Allow / Deny)
- According to Users' Preferences

For this, we need data!

31

59

Solution: Automated Privacy Decisions



- Several devices with local info on:
  - Requesting Application
  - Permission
  - Grant Decision

- Prediction of Grant Decisions (Allow / Deny)
- According to Users' Preferences

WITHOUT ACCESS/SHARING OF USER DATA

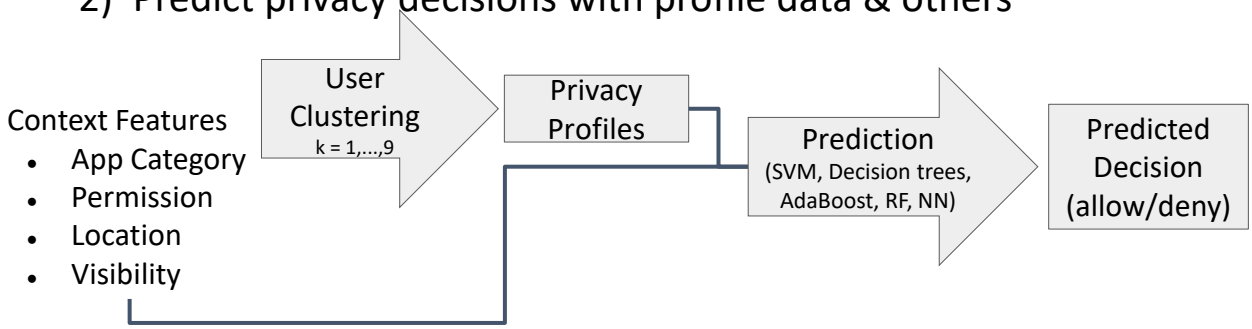
32

60

Prediction of Grant Decisions

A 2-stage approach:

1) Clustering users into profiles
2) Predict privacy decisions with profile data & others



33

63

Prediction of Grant Decisions with Privacy Guarantees

A 2-stage approach:

1) Clustering users into profiles
2) Predict privacy decisions with profile data & others

In a privacy-aware manner, i.e. without access to user data:

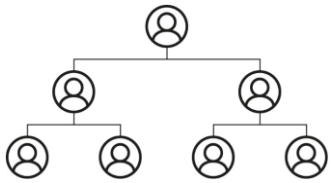
- Privacy-preserving clustering mechanisms
- Federated mechanisms for prediction of privacy decisions

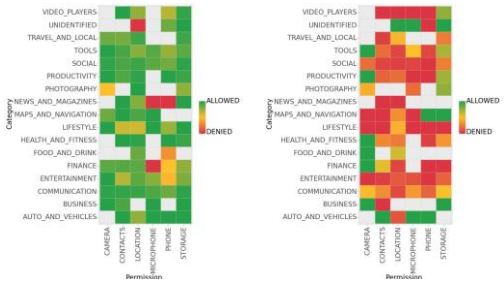
34

64

1) Secure Generation of Privacy Profiles

- Clustering of users into privacy profiles
  - (app category, permission, avg_grant_result)
- Profiles represent users' beliefs and expectations
- 2 approaches:
  - Distributed hierarchical clustering [Hamidi et al. PDP'18]
  - Private k-means clustering [Brandão et al. IDA'21]





Permissive User **Restrictive User**

35

65

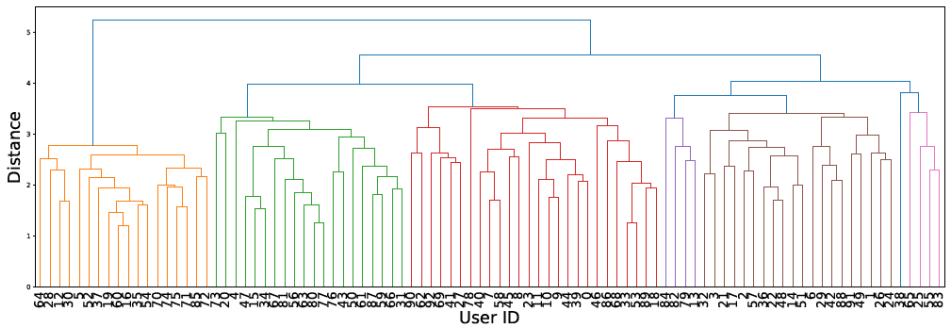
Distributed Hierarchical Clustering

[Hamidi et al. PDP'18]

- Per user (Category, Permission, Grant result):

App category: / Requested permission:	EVENTS CALENDAR	EVENTS CAMERA	...	AUTO_AND_VEHICLES PHONE	AUTO_AND_VEHICLES CONTACTS
Grant result:	0.9	0	...	0	0
	0.2	0.1	...	0.35	0.4

- Hierarchical clustering to divide users into profiles by creating a dendogram of distances and make a cut were appropriate



- **Privacy-preserving version based on secure scalar product**

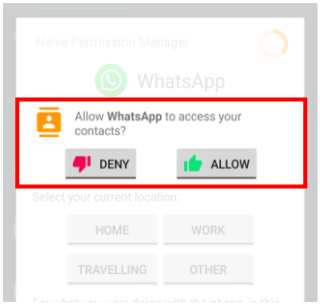
[Vaidya, Clifton' 02]

36

68

2) Grant Prediction with Federated Learning

- Features:
  - **Profile (previous slide)**
  - app_category
  - isForeground
  - checkedPermissionGroup
  - isTopAppRequestingApp
  - checkedPermission
  - screenIsInteractive
  - hour
  - networkStatus
  - weekday
  - profile



- Federated learning:
  1. Train neural network locally, on each smartphone, using only local data
  2. Share only the neural network weights (not the data) with a central server on each iteration

[Brandão et al., "Prediction of Mobile App Privacy Preferences with User Profiles via Federated Learning", CODASPY'22]

37

75

Grant Prediction with Federated Learning - Details

Neural network details

- Input size = 53
- **1 hidden layer** of size 128
- ReLU as activation function
- Sigmoid as output function
- **Simple network that achieves good results**
- Output (local and global): either deny or grant the request

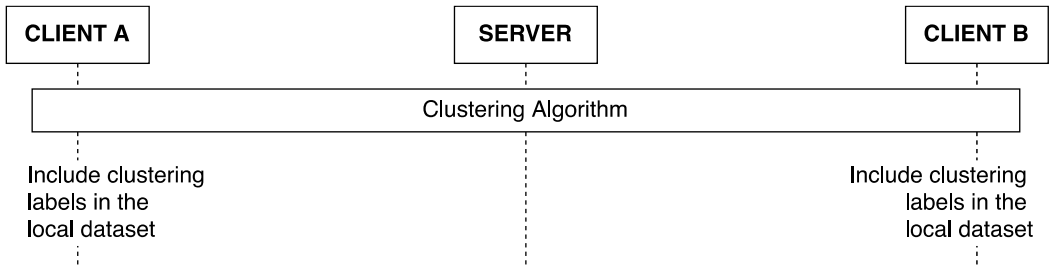
Learning protocol (FedAvg)

- **Same architecture** for local and global models
- Clients divided by userID
- Every client participates in each training round
- Each client reserves a part of its data for training and another for testing (75-25%)

38

77

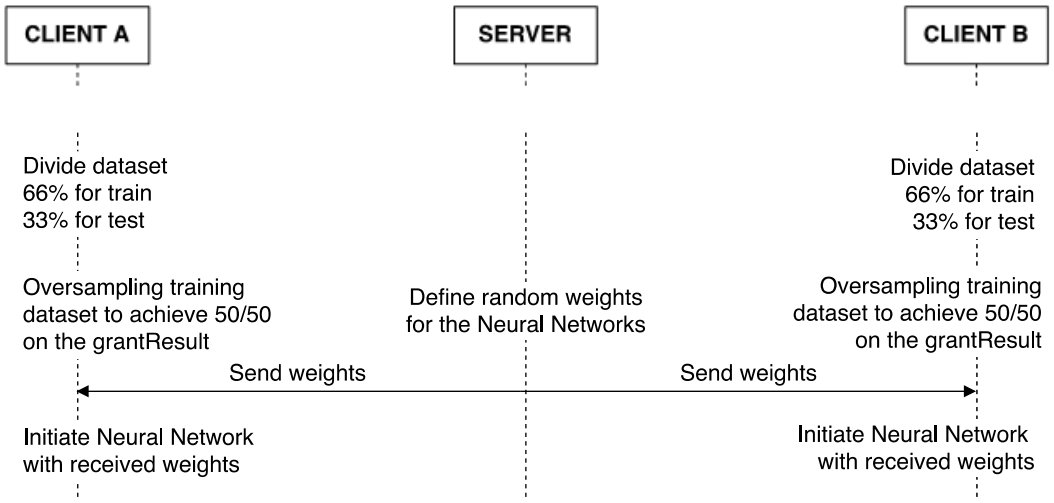
Federated Learning for Grant Prediction



39

80

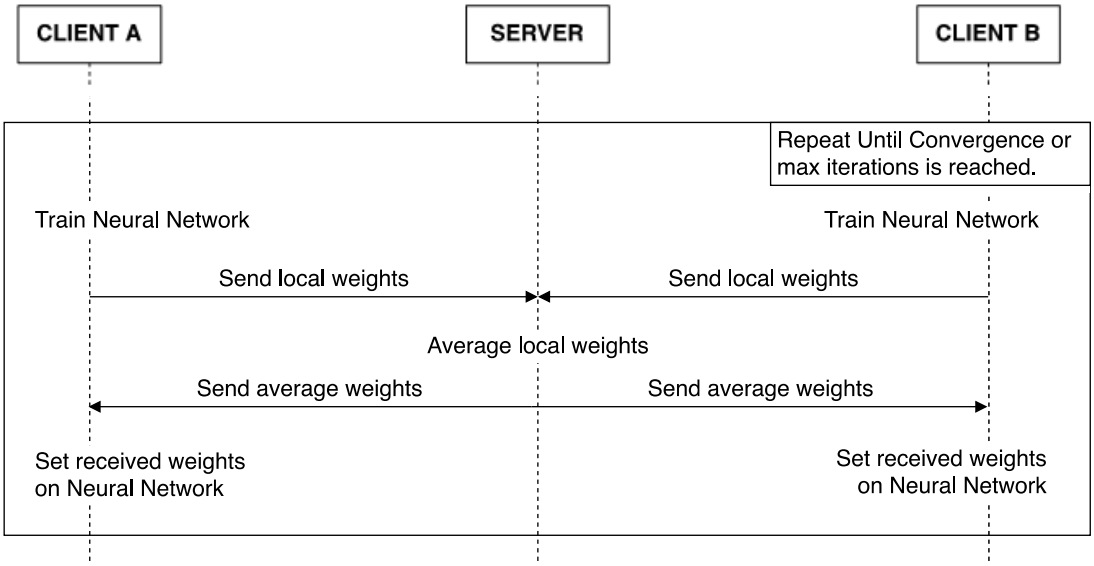
Federated Learning for Grant Prediction



40

81

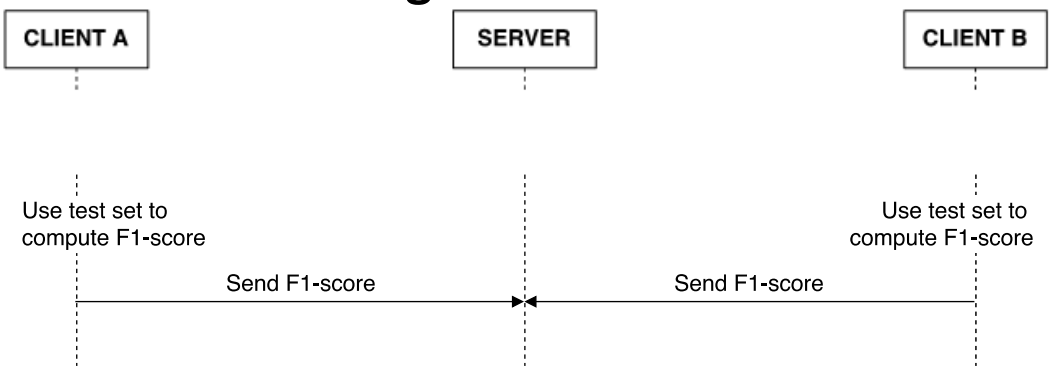
Federated Learning for Grant Prediction



41

82

Federated Learning for Grant Prediction



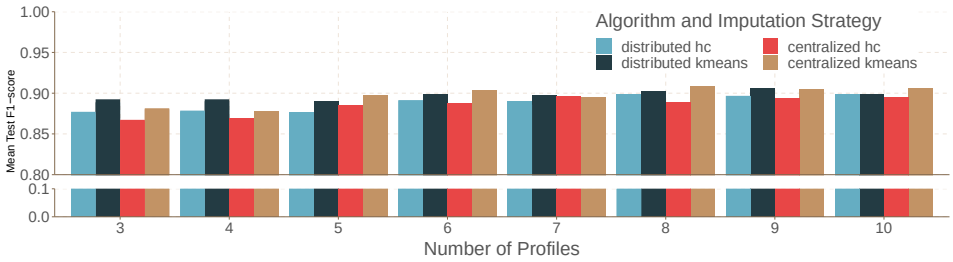
42

83

Evaluation

Applied to our dataset of ~65K grant decisions from 93 users [Mendes et al. PerCom' 22]
http://cop-mode.dei.uc.pt/dataset

- Validation:
  - Grid search on the following parameters:
    - Clustering Algorithm (k-means and hierarchical)
    - Approach (distributed and centralized)
    - Number of Clusters
  - 5-fold cross validation with 80% of the dataset



84

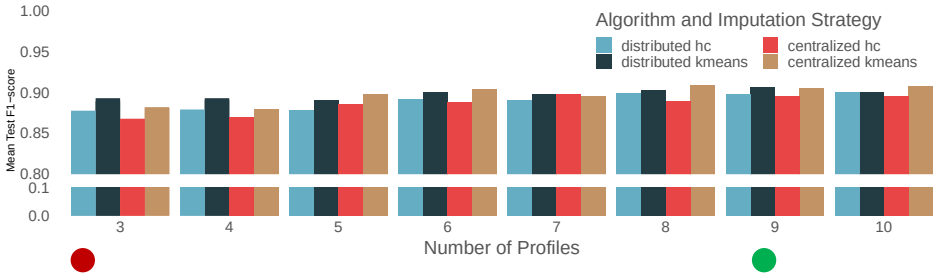
Evaluation

Applied to our dataset of ~65K grant decisions from 93 users [Mendes et al. PerCom' 22]
http://cop-mode.dei.uc.pt/dataset

- Validation:
  - Grid search on the following parameters:
    - Clustering Algorithm (k-means and hierarchical)
    - Approach (distributed and centralized)
    - Number of Clusters
  - 5-fold cross validation with 80% of the dataset

Best Mean F1-score of $\mathbf{0.91}$ with: Distributed k-Means ($k = 9$)

Worst Mean F1-score of $\mathbf{0.87}$ with: Distributed hc ($k = 3$)



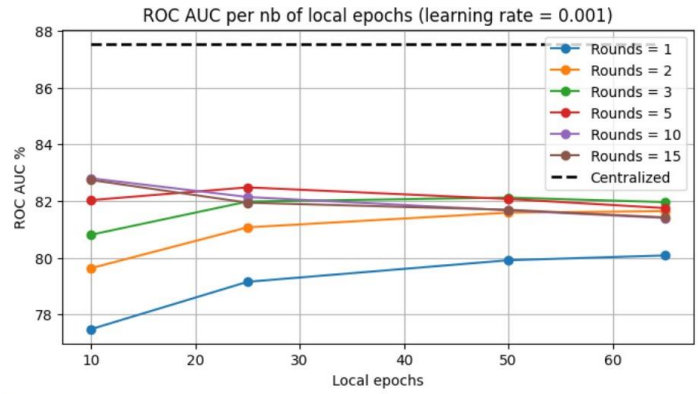
Global F1-score: 0.91

- **Comparable to the centralized version**
- **Prediction and clustering in a privacy-preserving manner**

85

Speed of Convergence - Analysis

- Tendency to **stabilize performance** as the number of **local epochs increases**
- For a small number of local epochs, results depend strongly on the number of rounds
- Long term evolution seems to be inde pendent of the number of rounds (>1)
- Hard to approximate centralized results without user profiles
- **Increasing the learning rate inverts evolution** – performance decreases as the number of local epochs increases



87

Conclusions and Future Work

- Privacy-preserving strategy to predict user's grant decisions
- Based on a 2-step approach:
  - Privacy-preserving clustering of users into profiles
  - Predict grant results through federated mechanisms
- Applied to a real world dataset of ~65K grant decisions from 93 users
- Maintain SoA prediction performance, **while preserving user privacy**
  - Reduces amount of privacy violations

- Future work:
  - Predicting user expectation
  - Effect of attacks over FL mechanisms
  - DL + FL to replace the two-step process by a single one

89

Main References

1. Mendes, Brandão, Vilela, Beresford, "Effect of User Expectation on Mobile App Privacy: A Field Study", International Conference on Pervasive Computing and Communications (PerCom), 2022
2. Mendes, Cunha, Vilela, Beresford, "Enhancing User Privacy in Mobile Devices Through Prediction of Privacy Preferences", European Symposium on Research in Computer Security (ESORICS), 2022
3. Brandão, Mendes, Vilela, "Prediction of Mobile App Privacy Preferences with User Profiles via Federated Learning", ACM Conference on Data and Application Security and Privacy (CODASPY), 2022
4. Brandão, Mendes, and Vilela, "Efficient privacy preserving distributed K-means for non-IID data". In Advances in Intelligent Data Analysis XIX, 2021
5. Hamidi, Sheikhalishahi, and Martinelli, "A Secure Distributed Framework for Agglomerative Hierarchical Clustering Construction". In Euromicro International Conference on Parallel, Distributed and Network based Processing, 2018