Metadata Filtering for User-friendly Central Biometric Authentication

CHRISTIAN GEHRMANN, MARCUS RODAN AND
NIKLAS JÖNSSON

This presentation contains material from the following publication (to appear):

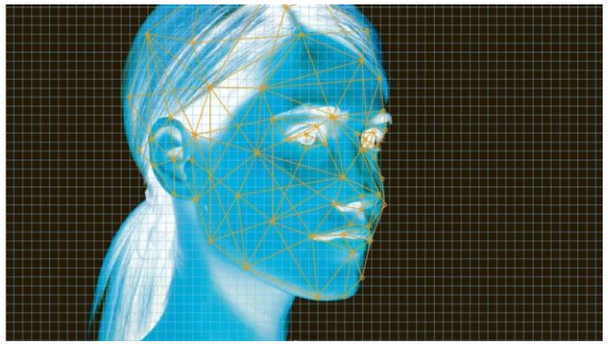
C. Gehrmann, M. Rodan and N. Jönsson, ” Metadata Filtering for User-Friendly Centralized Biometric Authentication”, EURASIP Journal on Information Security, 2019.

Outline

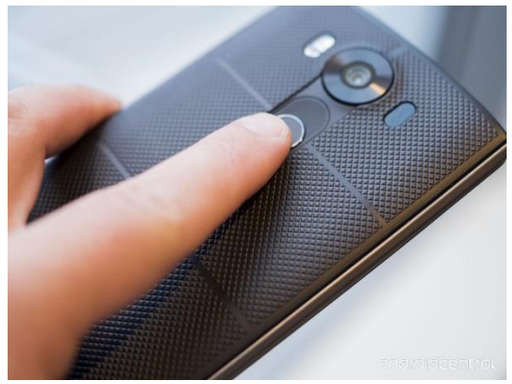
- Background to biometric authentication solutions
- Central authentication and identities
- Metadata filtering approach
- Different meta data filters
- Performance results from a simulation framework and simulation based on Swedish statistics
- Security analysis of the proposed approach
- Conclusions

LUND UNIVERSITY

Background (I)



- Biometrics widely used for convenient user authentication
- Main use case:
  - **Local unlock of a device, mobile, PC etc.**:
- Other use cases:
  - **Gym access**
  - **Indian Aadhaar ID system**

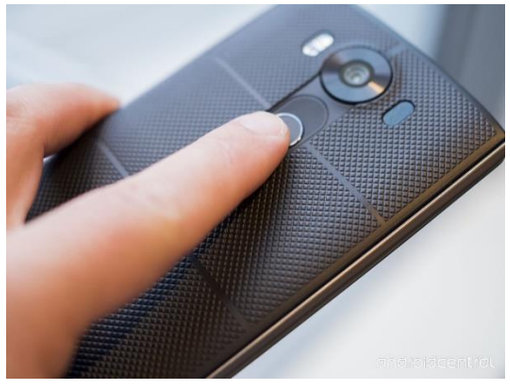


AADHAAR

सत्यमेव जयते
Unique Identification Authority of India

LUND UNIVERSITY

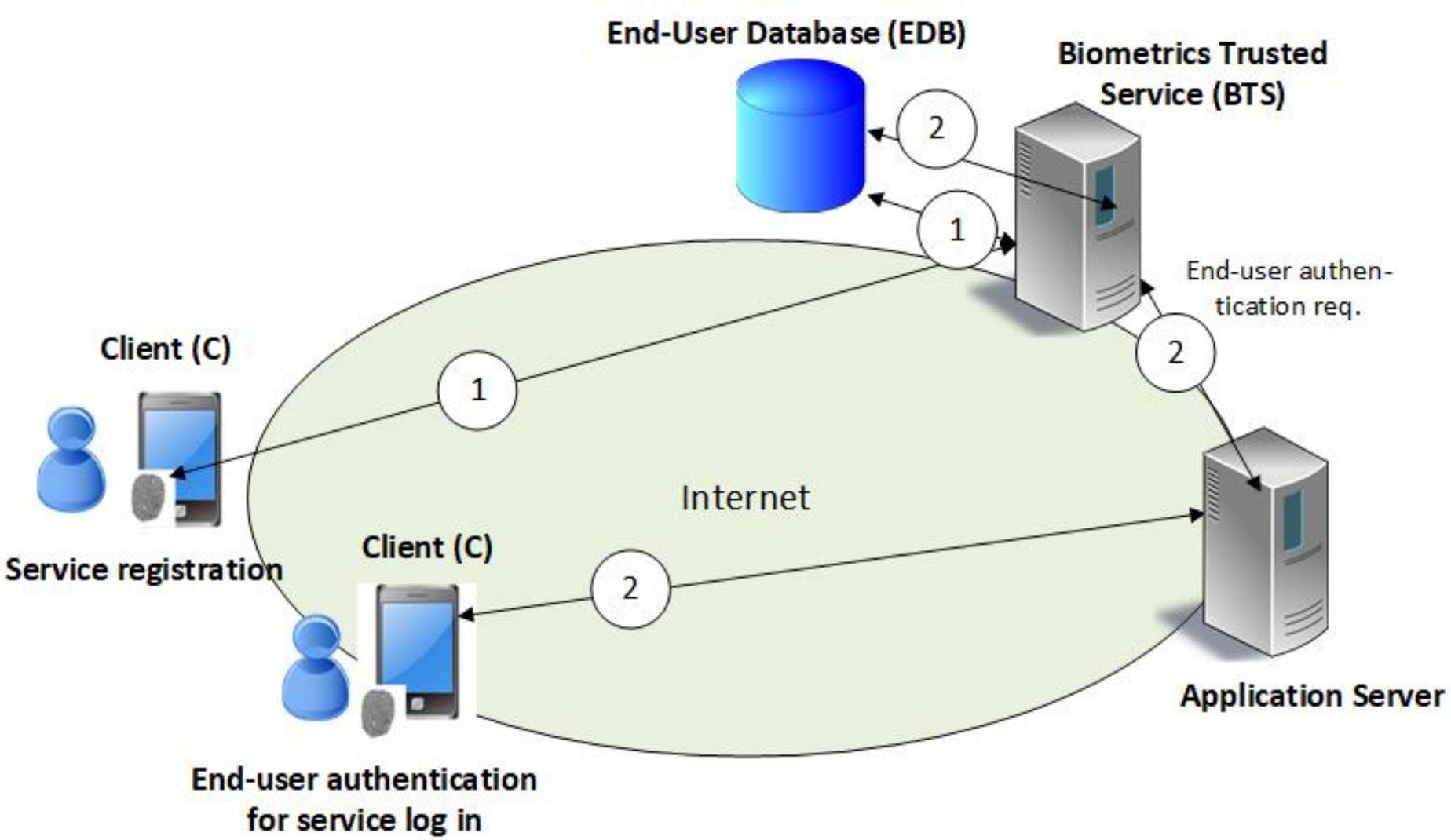
Background (II)



- The local unlock use case has the following main security advantages
  - Biometrics templates never exposed outside the local device
  - Strong keys and cryptography can be used for end-user authentication. The authentication functions are then just “unlocked” with the end-user biometrics
- The local unlock use case is limited in the following aspects:
  - The user cannot utilize the full freedom of not remembering passwords as when the user moves to a previously unused or new device, it must again be “customized”
  - The biometrics data, i.e. templates, must be protected locally all the time and is never allowed to leave the device.

LUND UNIVERSITY

Biometric central authentication - scenario



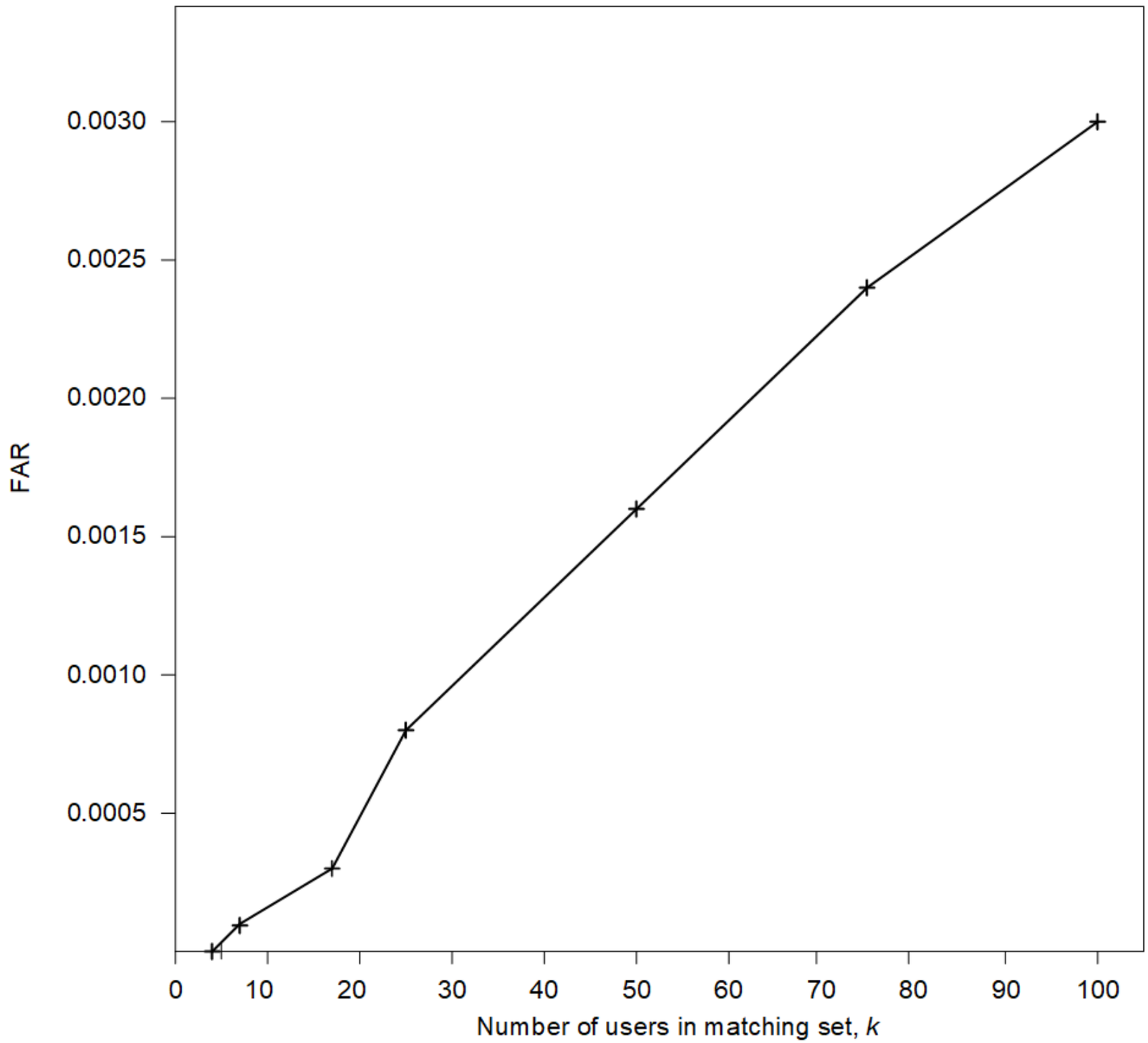
LUND UNIVERSITY

Biometric central authentication – some issues

- Biometrics templates are exposed centrally = > easy to hack
  - Can be handle by using biometrics transforms, i.e. not representing the template in its original form but in a non-invertible transformed representation which can be exchanged (cancellable biometrics)
- Different biometrics readers have different template representations, i.e. non-compatible systems
- **Small sensors, like the ones used in current mobile phone have a too large False Acceptance Rate (FAR),~1/100.000 to work for direct matching against large user populations**
  - Require the end-user to enter a unique user ID prior to perform the matching operation => not the most user-friendly solutions
  - **Use a filtering mechanism to reduce the matching set prior to perform the matching, the approach we have investigated!**

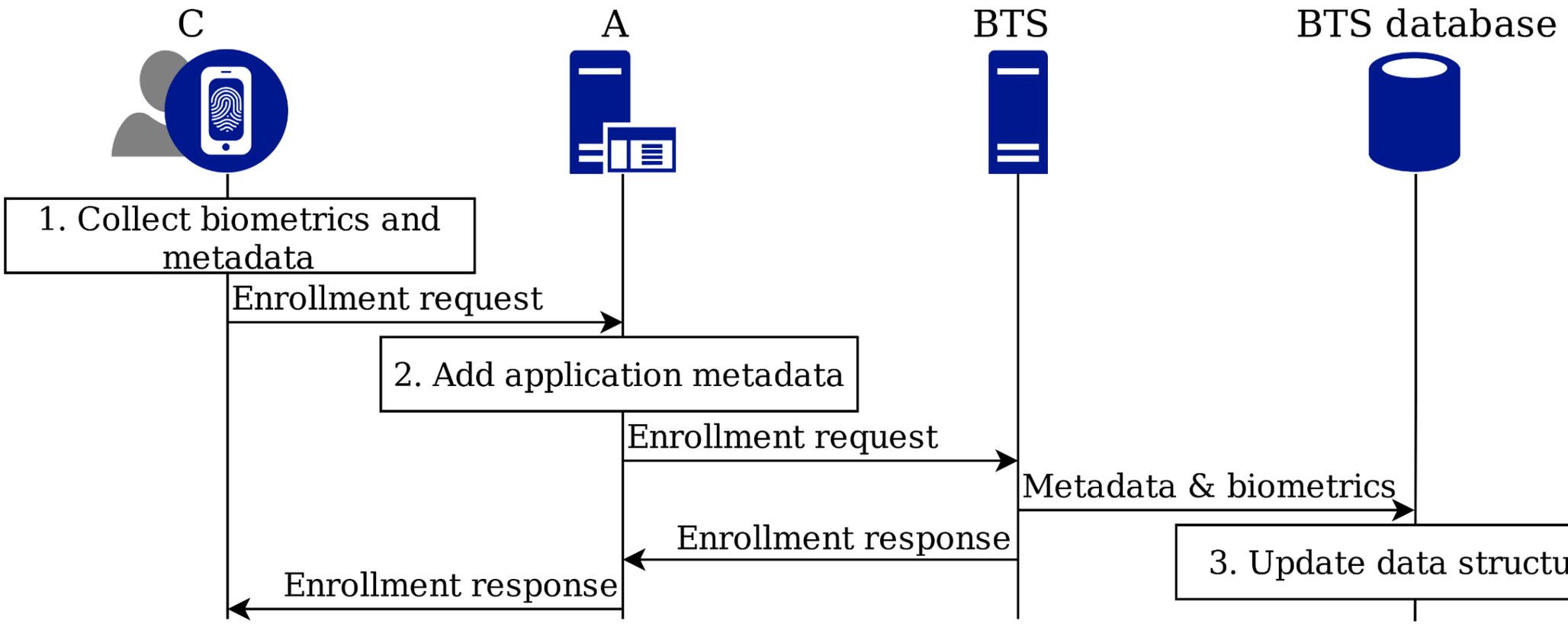
LUND UNIVERSITY

FAR in relation to population size (FVC2006 + sourceAFIS)



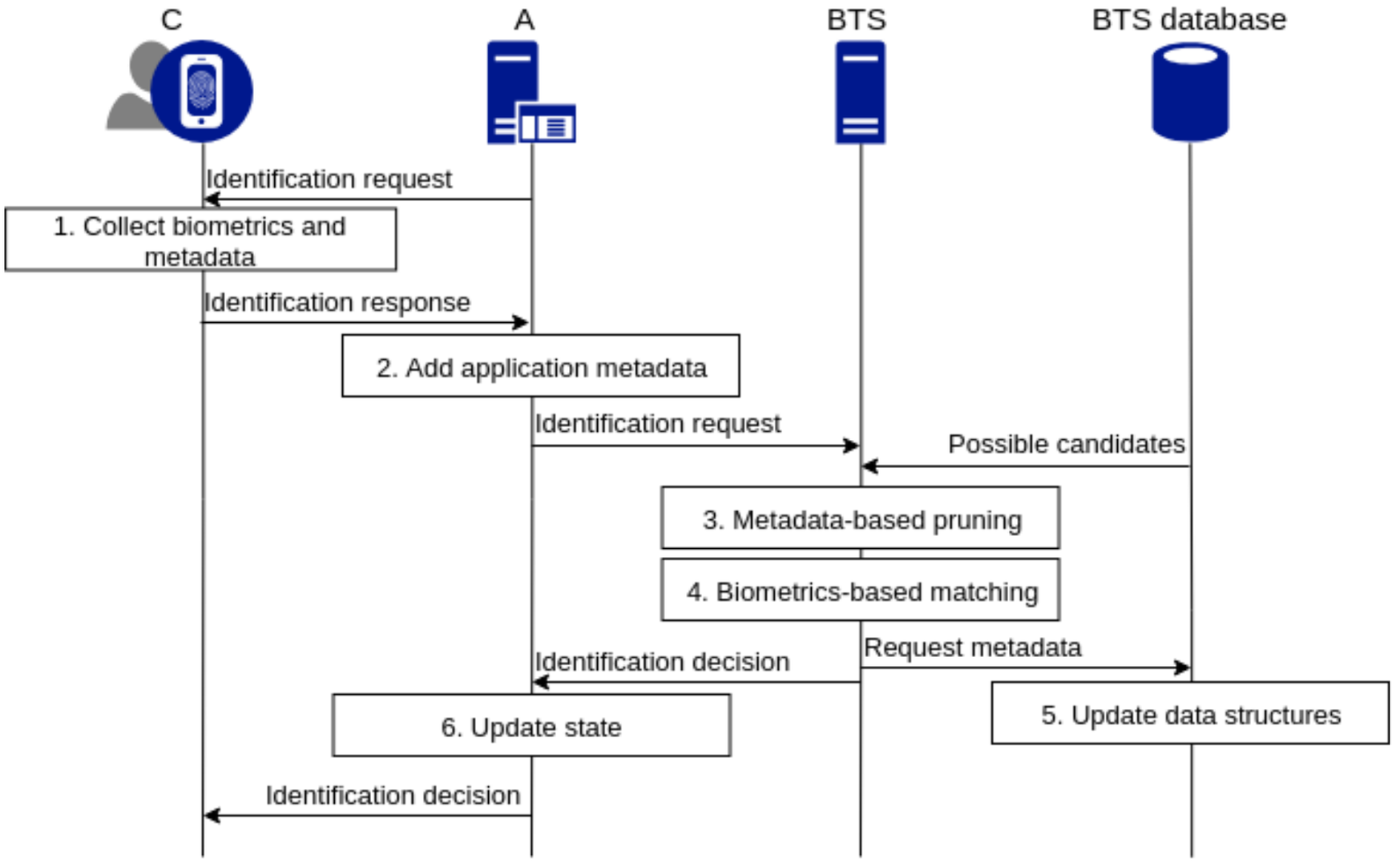
LUND UNIVERSITY

BTS with metadata filtering - enrollment



LUND UNIVERSITY

BTS with metadata filtering – identification with auth.



LUND UNIVERSITY

Metadata selection?

- Jain et. al (2004) identified the following wanted metadata properties
  - **Universality**: The selected metadata types should have high availability, implying that most users possess and can supply the metadata type.
  - **Distinctiveness**: Metadata types of higher entropy are more desirable than metadata types of lower entropy.
  - **Permanence**: The selected metadata types should be relatively stable over time.
  - **Collectability**: The metadata types should be as effortless as possible to collect to ensure a high level of user-friendliness. Automatically collectible metadata types are superior from a user-friendliness perspective.
  - **Acceptability**: The privacy concerns associated with meta collection varies between types where less sensitive metadata types are preferred.

LUND UNIVERSITY

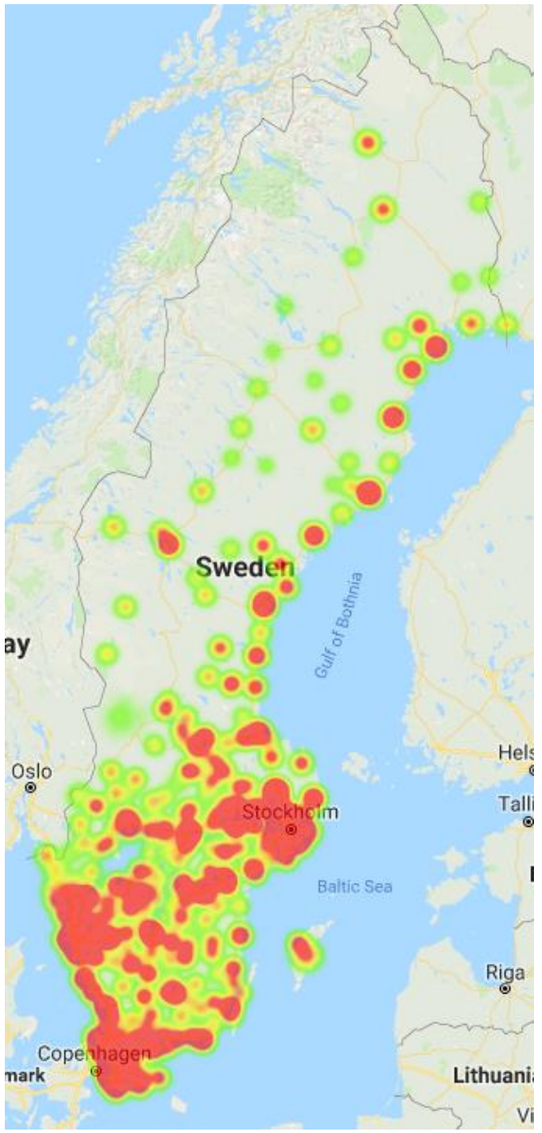
Investigated metadata types

- Device ID
  - During enrollment and/or after successfully authentication, the device ID is recorded.
- Location
  - Location information (GPS based) is uploaded during enrollment and after successful identification.
- Age and Name
  - Age and name are requested during enrollment and *might be* requested during an identification session.
  - Name and age must not be 100% correct during an authentication session but “close” to the true age or name.

LUND UNIVERSITY

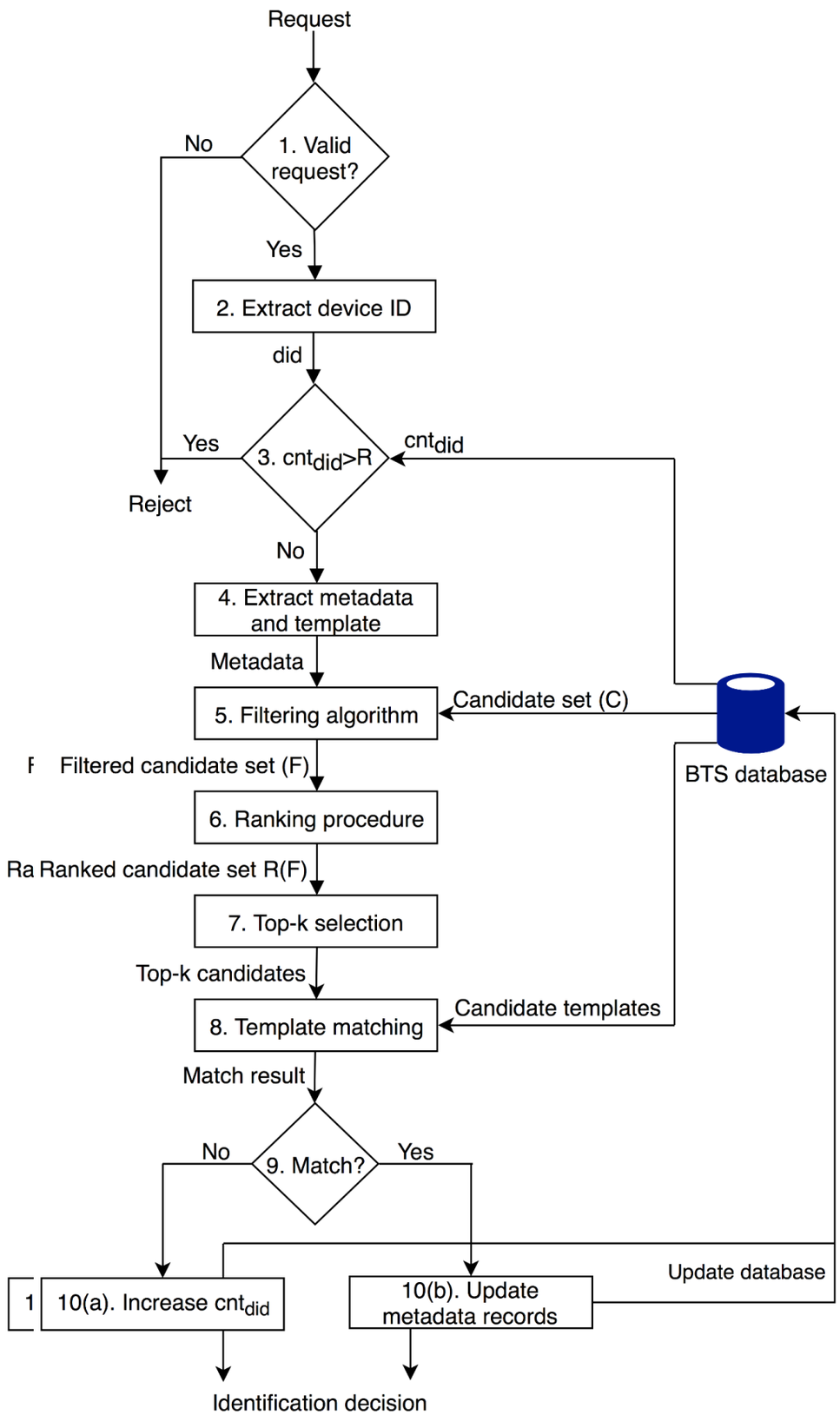
Evaluation using simulations

- Name and age distribution
  - The age and name of an enrolling user is generated using name and age distributions extracted from SCB. The SCB is governmental service providing highly reliable statistics for the Swedish population.
- Location
  - Location information is also extracted from SCB. We then associate each enrolling user which a given number of significant locations, with support from previous studies (The BTS does only now the enrollment location when the simulation starts):
  - Isaacman, S., Becker, R., C´aceres, R., Kobourov, S., Martonosi, M., Rowland, J., Var-shavsky, A.,"Identifying important places in people's lives from cellular network data", Pervasive Computing, Pervasive'11, pp.133–151, 2011.
  - Zhou, C., Bhatnagar, N., Shekhar, S., Terveen, L., "Mining personally important places from GPS tracks". In: 2007 IEEE 23rd International Conference on Data Engineering Workshop. IEEE, 2007.

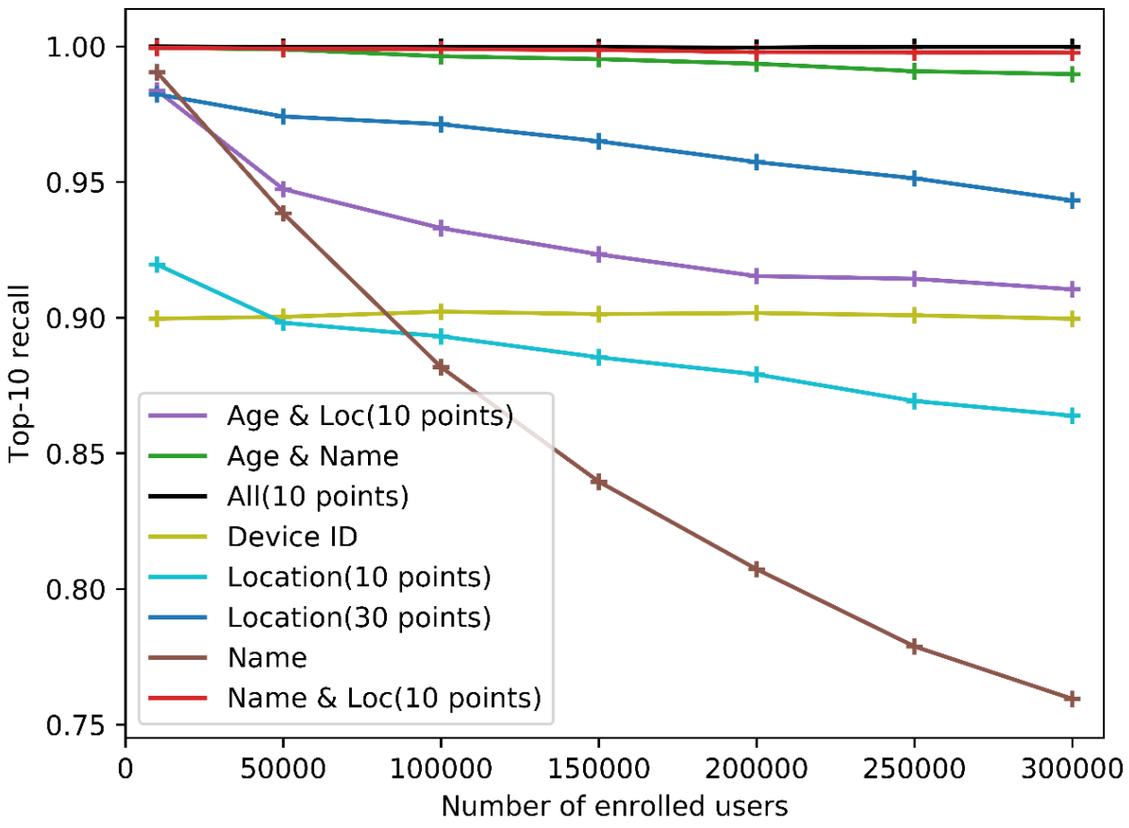


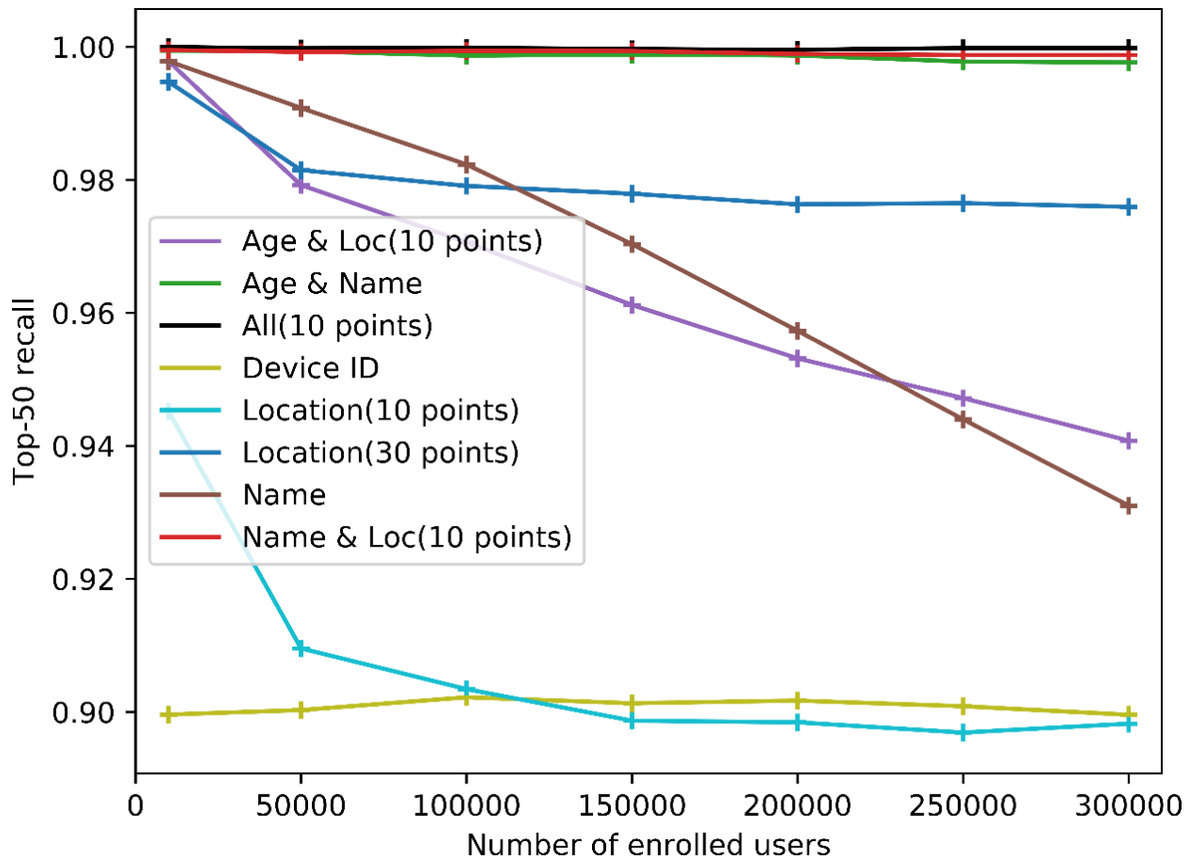
LUND UNIVERSITY

General filter procedure



Filtering results





LUND UNIVERSITY

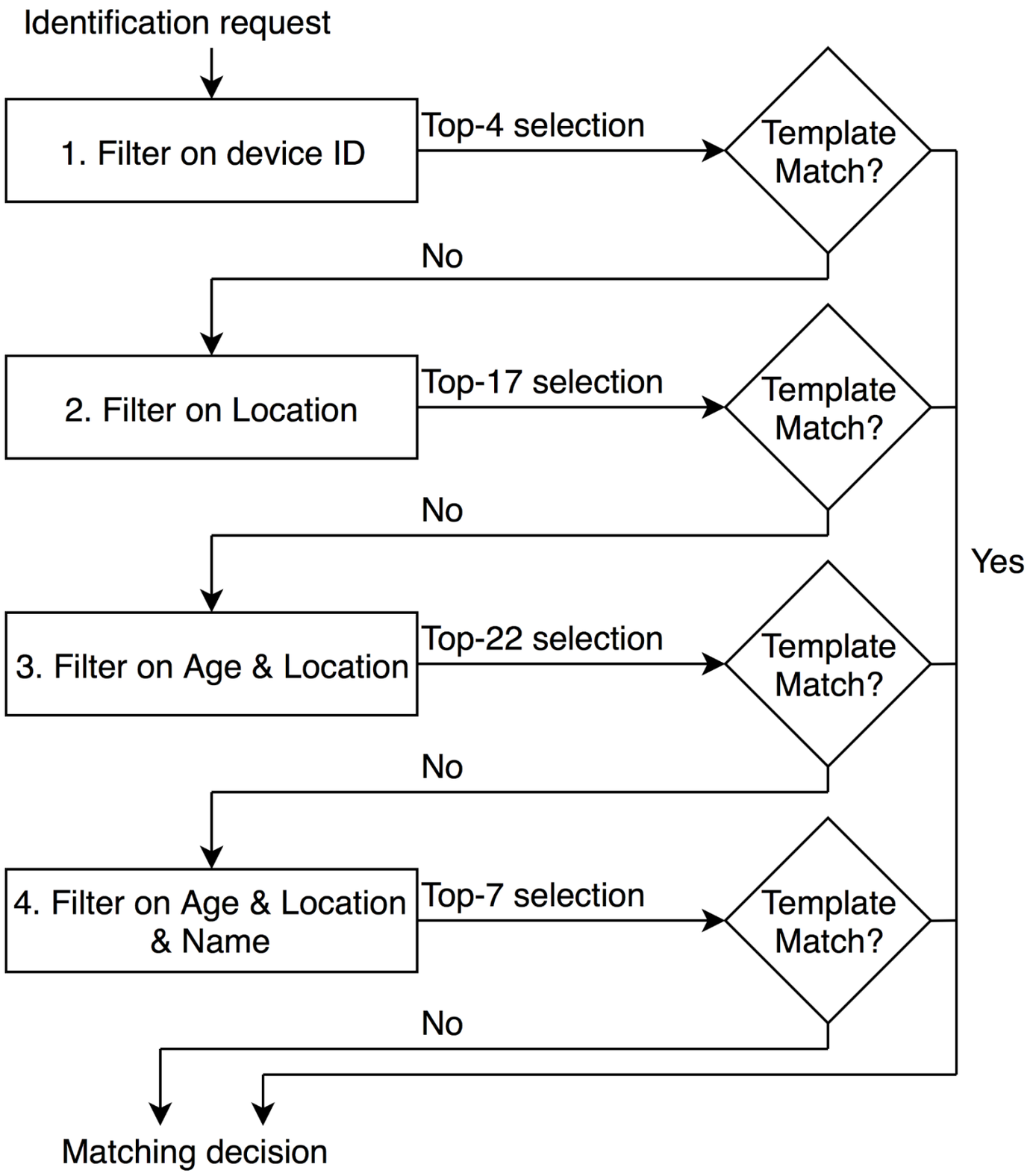
Full match False Rejection Rate (FRR)

Matching results using the FVC2006 fingerprint DB and the sourceAFIS matching algorithm at FAR = 0.00164 and with top 50 candidates:

	100.000 users			200.000 users		
	Name	**Location (30 p.)**	**Combined**	**Name**	**Location (30 p.)**	**Combined**
1-Recall	0.018	0.022	0.00025	0.0042	0.024	0.00031
FRR	0.022	0.028	0.004	0.046	0.026	0.004

LUND UNIVERSITY

Incremental procedure



LUND UNIVERSITY

Recall rates for inc. procedure

Number of users	Recall	Location collec-tion rate	Age collection rate	Name collection rate
10000	0.9999	1.000	0.0609	0.0076
100000	0.9994	1.000	0.0980	0.0430
200000	0.9986	1.000	0.1076	0.0663
300000	0.9974	1.000	0.1157	0.0809

Security

- False enrollment
  - Provide false metadata together with genuine biometric data-> will not give any benefits as the attacker still must bypass the biometric matcher.
  - Provide false biometric data together with genuine metadata-> will not give any benefits for later matching attempts.
- Trying to authenticate as a random users
  - We assume a rate limit, R, on the number of acceptable false authentication trials per device. Then attacker would need in the worst case (*k* new candidates retrieved at each trial) D number of devices to succeed with prob. close to 1 within T years:

$$D = \left\lfloor \frac{\frac{1}{FAR}}{R * T * k} \right\rfloor$$

- Trying to authenticate as specific user (with access to D device). This will then give the following success rate:

$$P = 1 - (1 - FAR)^{D*R*T}$$

LUND UNIVERSITY

Location privacy

- Location information is privacy sensitive
- The issue can be mitigate using techniques like:
  - Adding noise to the submitted location inf.
  - Use the biometrics as source for location transformation
- Pure addition of noise to location information gives considerable worse identification performance
- Use of location transform with biometric and a fuzzy extractor is a more viable solutions which we partly tried out.
  - The main limitation is that current mobile fingerprint sensors only capture a small part of a finger, i.e. many sub templates, which makes it impossible to extract a single stable value from one user fingerprint.

LUND UNIVERSITY

Conclusions

- Metadata filtering in combination with biometric based authentication such as fingerprint scanner is a most user-friendly approach (single touch!) for user authentication in application with *moderate* security requirements.
- Our simulations shows that using general available information such as device ID, location inf. as well as requesting the user to *occasionally* also enter age and/or name (sloppy) gives a high reliability.
- Further work is needed to provide a fully working solution that allows transformed location information to be submitted instead of the real location.

LUND UNIVERSITY

рахмат
danke
謝謝
ngiyabonga
Баярлалаа
spas
teşekkür ederim
mersi
kia ora
barka
welalin
tack
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
mahalo
tapadh leat
kiitos
dankie
nanni
nandri
dhanyavad
thank you
gracias
хвала
asante
manana
bedankt
bayarlalaa
gràcie
hvala
maururu
köszönöm
akun
dankon
aciú
obrigada
murakoze
tenki
enkosi
djiere dieuf
tau
mochchakkeram
дякую
mamnun
dziękuję
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
chokrane
sobodi
dėkuji
sagolun
sukriya
kop khun krap
taiku
obrigado
mèsi
didi madloba
ありがとう
arigatô
takk
dakujem
trugarez
najis tuke
terima kasih
tanemirt
grazie
rahmet
kam sah hamnida
rahmat
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercé
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci