Julius-Maximilians-UNIVERSITÄT WÜRZBURG

TECHNISCHE UNIVERSITÄT DARMSTADT

KOBIL

AuthentiSense:

A Scalable Behavioural Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms

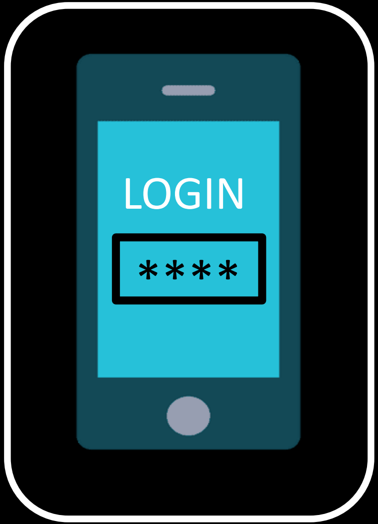
Hossein Fereidooni, Jan Koenig, Phillip Rieger, Marco Chilese, Bora Goekbakan, Moritz Finke, Alexandra Dmitrienko, and Ahmad-Reza Sadeghi

NDSS 01.03 2023

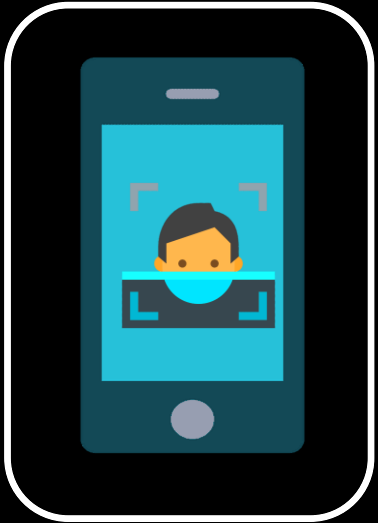
System Security Lab

Mobile Services
Fast-growing

Traditional Authentication



Passwords



Physiological
Biometrics

Multi-factor methods

One-time methods

Behavioural Authentication

Behavioural Biometrics:

- Motion Patterns
- Typing
- Touch Gestures
- Navigation
- etc .

Challenges:

- Large amount of training data
- Scalability
- User-spesific Models
- Long Interaction Time

Contributions

Fast and efficient, not requiring hand-crafted features for model training

Scalable to authenticate millions of users

User-agnostic, no model re-training when users dynamically changing (i.e., joining or leaving)

Fast and efficient, not requiring hand-crafted features for model training

Contributions

Fast and efficient, not requiring hand-crafted features for model training

Scalable to authenticate millions of users

User-agnostic, no model re-training when users dynamically changing (i.e., joining or leaving)

Scalable to authenticate millions of users

Contributions

Fast and efficient, not requiring hand-crafted features for model training

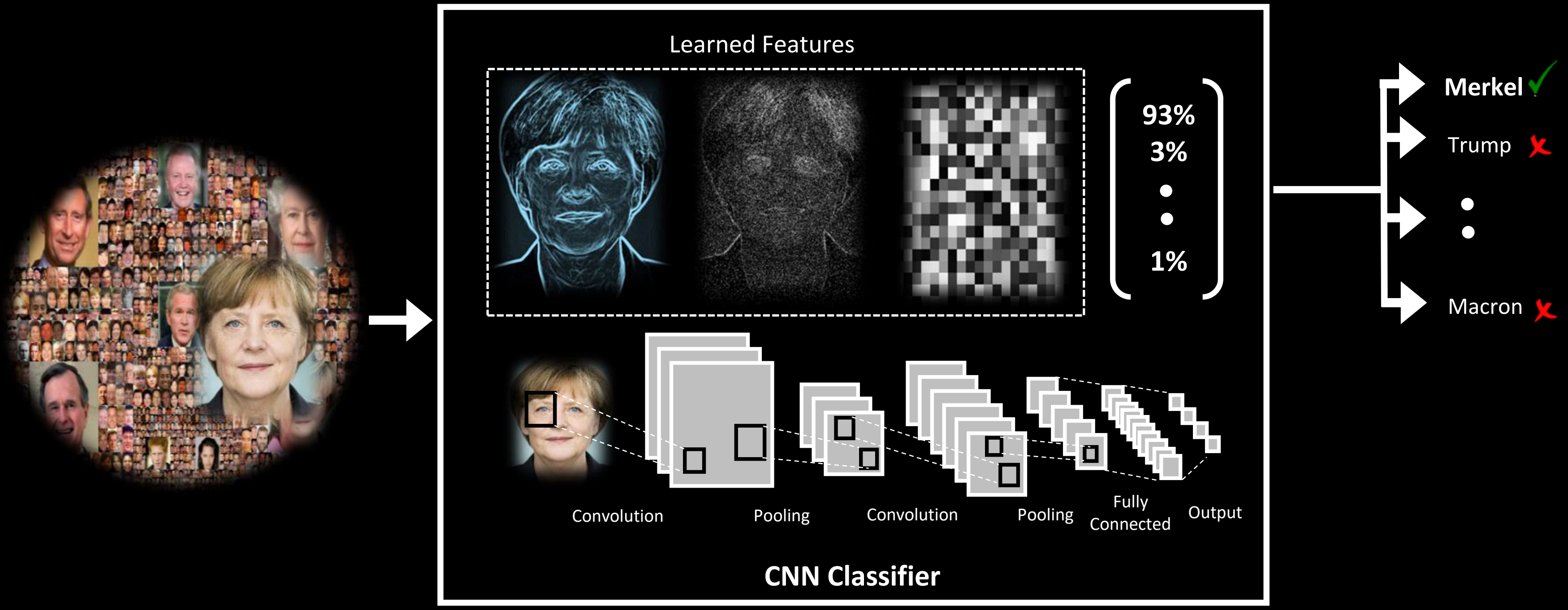
Scalable to authenticate millions of users

User-agnostic, no model re-training when users dynamically changing (i.e., joining or leaving)

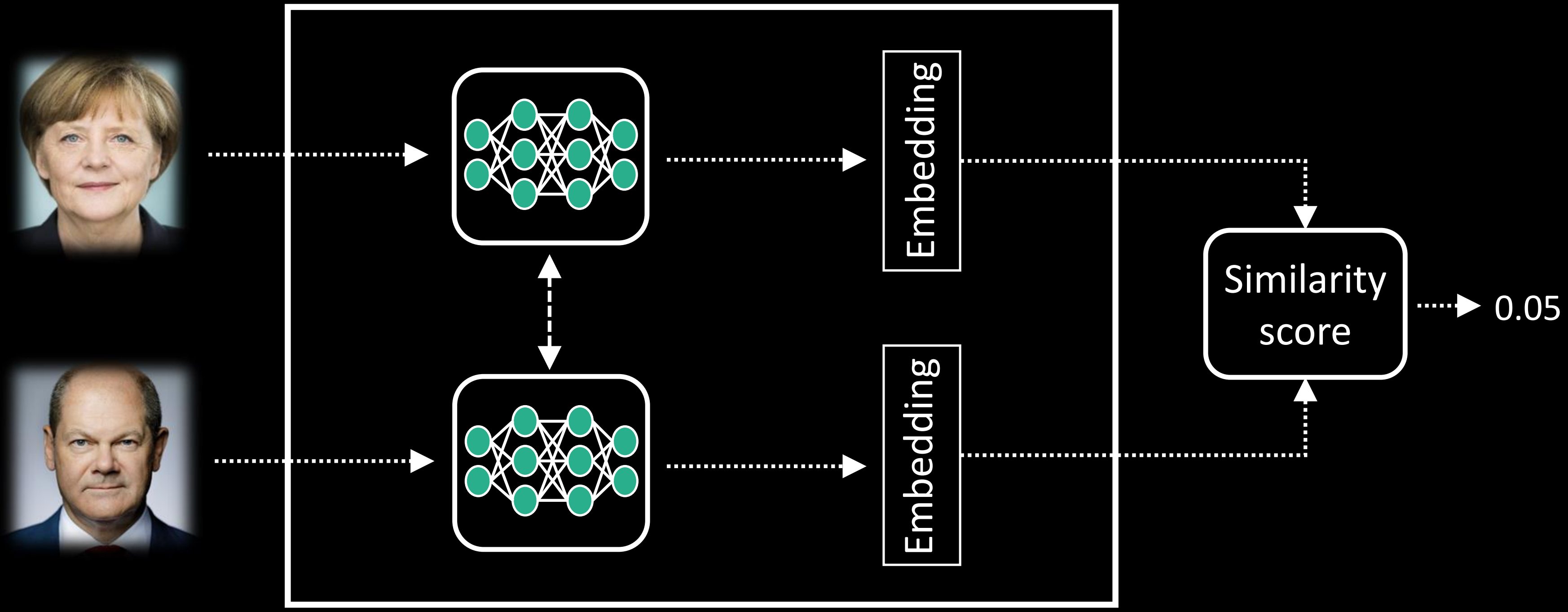
User-agnostic, no model re-training when users dynamically changing (i.e., joining or leaving)

Few-Shot Learning (FSL)
vs.
Standard Supervised Learning (SSL)

SSL for Classification



Few-Shot Learning (FSL)



Embedding

Embedding

Similarity score

0.05

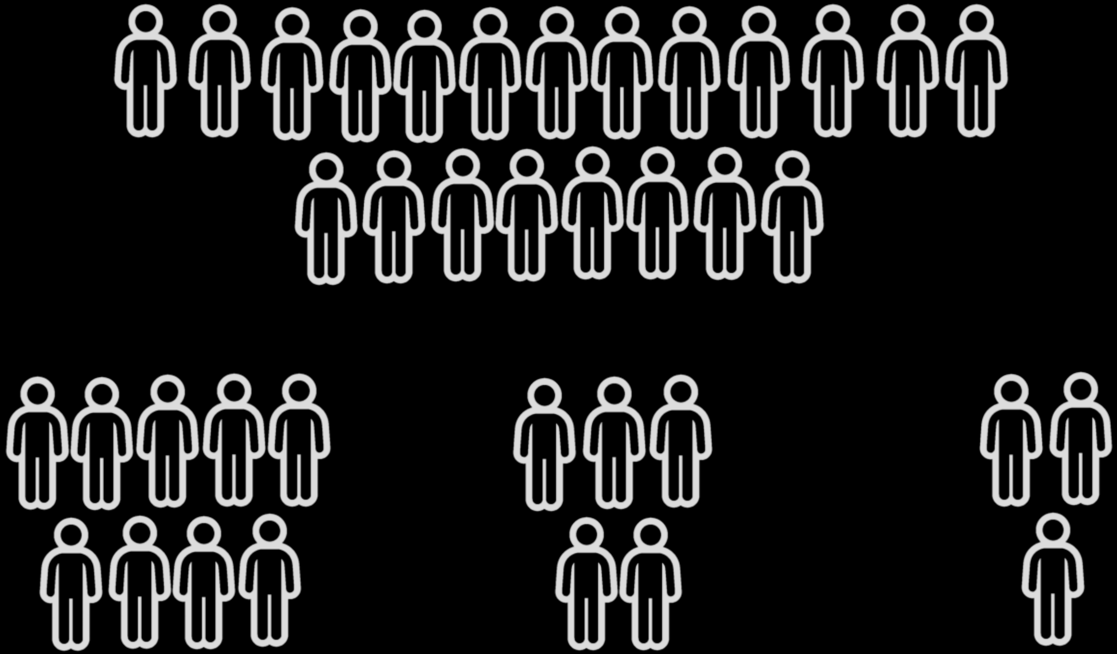
Dataset[1]

The dataset contains 45 Users

- 15 sessions per User
- Each session 90 seconds in length

The dataset contains different

- Genders
- Ages
- Occupations



35 Users
Training

7 Users
Testing

3 Users
Validation

---

[1] [Incel et. al DAKOTA IEEE Access 2021]

Dataset (Cont.)

Frequently used Functions in mobile banking

Transactions
T1: Account and credit card balance
T2: Account search
T3: Money transfer
T4: Foreign exchange buy operation
T5: Credit card debt payment
Postures
P1: Phone in hand and sitting
P2: Phone in hand and standing
P3: Phone on the table and sitting

Data captured through three sensors

Accelerometer

Gyroscope

Magnetometer

Dataset (Cont.)

Frequently used Functions in mobile banking

Transactions
T1: Account and credit card balance **T2**: Account search **T3**: Money transfer **T4**: Foreign exchange buy operation **T5**: Credit card debt payment
Postures
P1: Phone in hand and sitting **P2**: Phone in hand and standing **P3**: Phone on the table and sitting

Data captured through three sensors

Accelerometer

Gyroscope

Magnetometer

Accelerometer

Dataset (Cont.)

Frequently used Functions in mobile banking

Transactions
T1: Account and credit card balance **T2**: Account search **T3**: Money transfer **T4**: Foreign exchange buy operation **T5**: Credit card debt payment
Postures
P1: Phone in hand and sitting **P2**: Phone in hand and standing **P3**: Phone on the table and sitting

Data captured through three sensors

Accelerometer

Gyroscope

Magnetometer

Gyroscope

Dataset (Cont.)

Frequently used Functions in mobile banking

Transactions
T1: Account and credit card balance
T2: Account search
T3: Money transfer
T4: Foreign exchange buy operation
T5: Credit card debt payment
Postures
P1: Phone in hand and sitting
P2: Phone in hand and standing
P3: Phone on the table and sitting

Data captured through three sensors

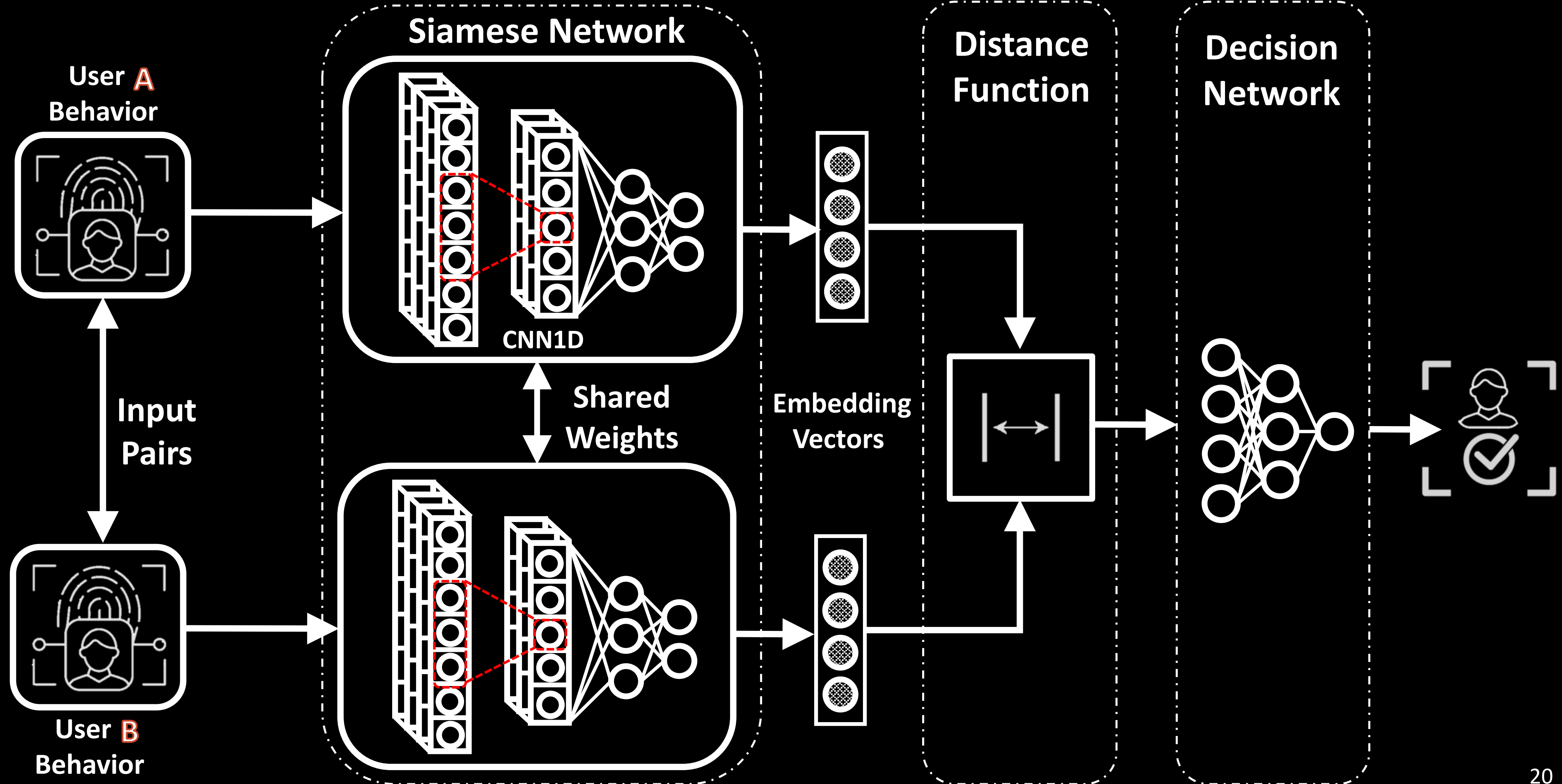
Accelerometer

Gyroscope

Magnetometer

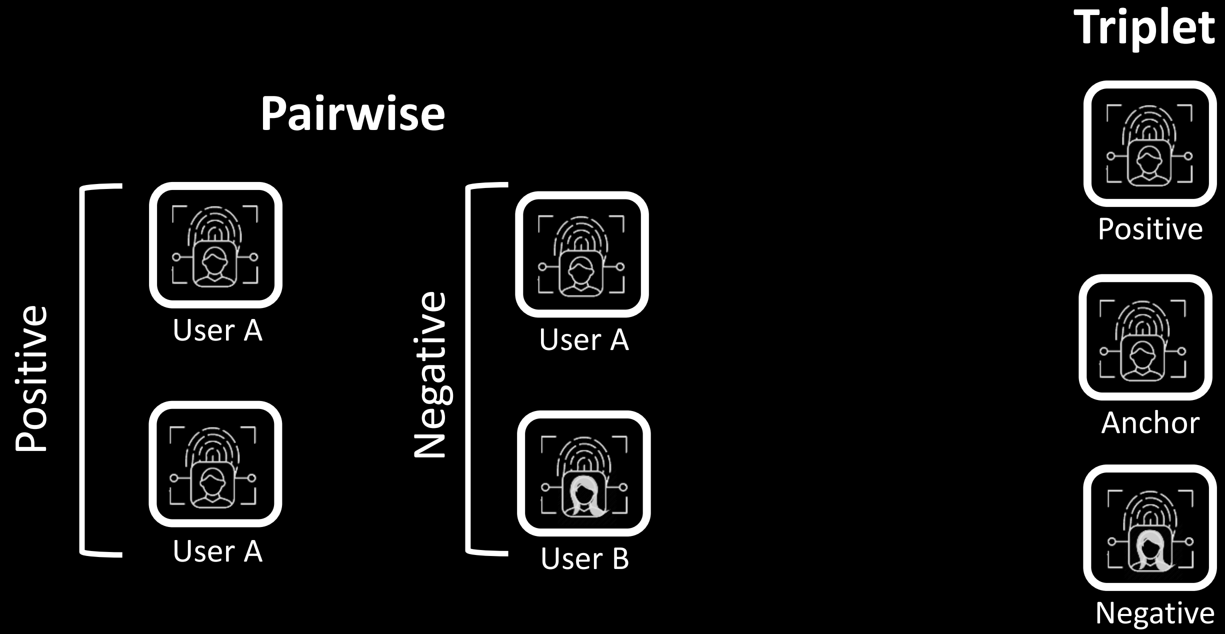
Magnetometer

AuthentiSense at High-Level


Siamese Network
User A Behavior
Input Pairs
User B Behavior
CNN1D
Shared Weights
Embedding Vectors
Distance Function
Decision Network

Network Training

- Sample Generation Strategy



Pairwise

Positive

User A

User A

Negative

User A

User B

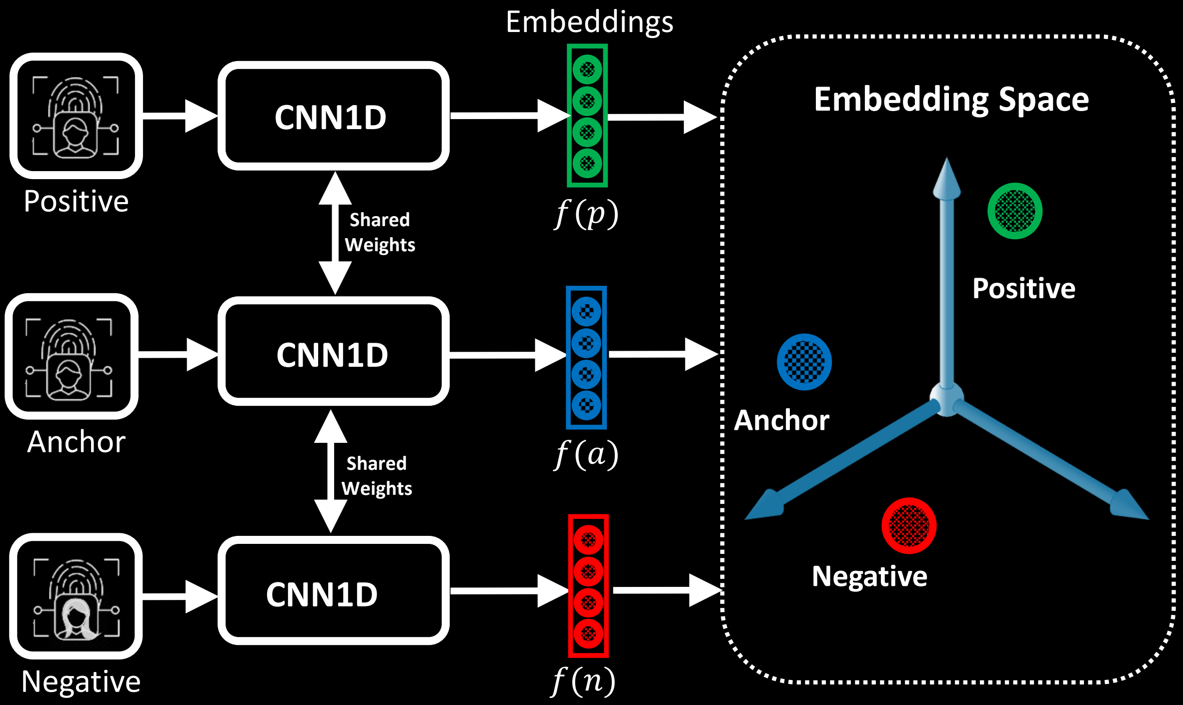
Triplet

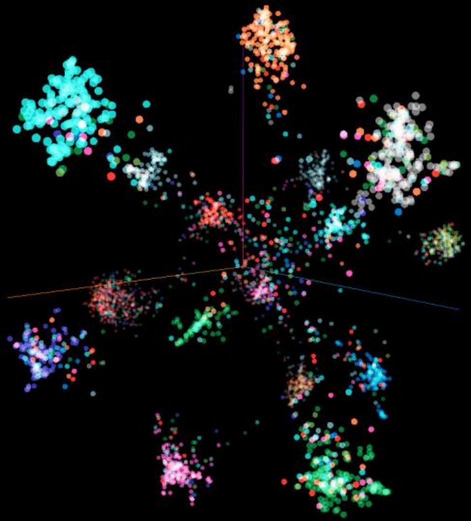
Positive

Anchor

Negative

Triplet Training

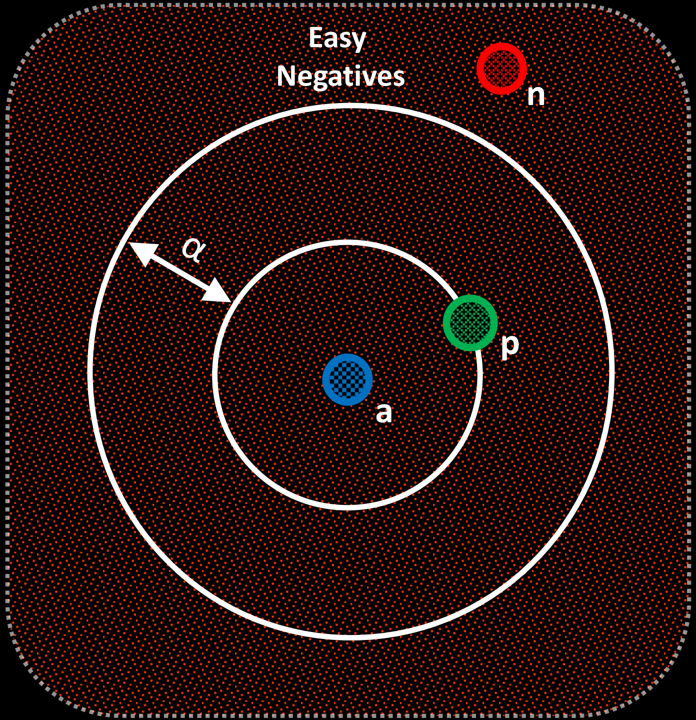




$$L(a,p,n) = \max(\|f(a)-f(p)\|^2 - \|f(a)-f(n)\|^2 + \alpha, 0)$$

Triplet Training (Cont.)

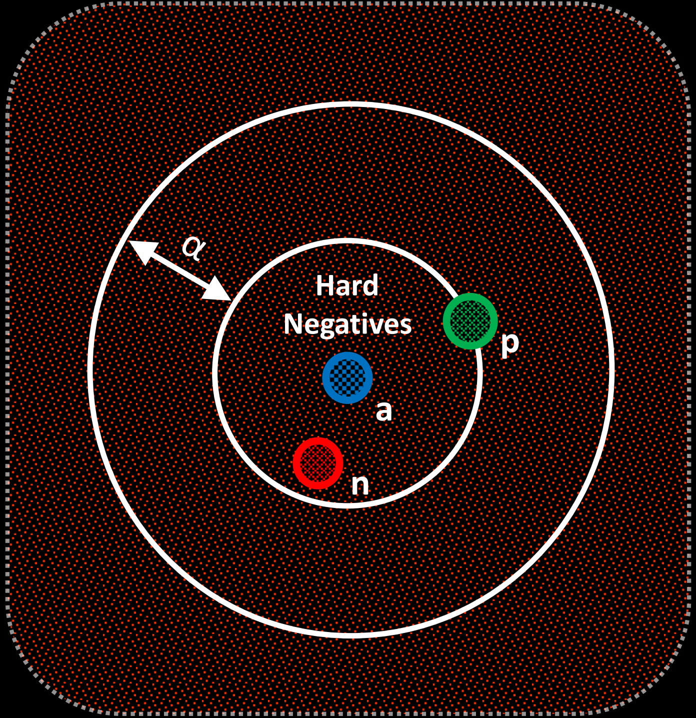
- Easy Negative:
  $\|f(a) - f(p)\| + \alpha \leq \|f(a) - f(n)\|$



Triplet Training (Cont.)

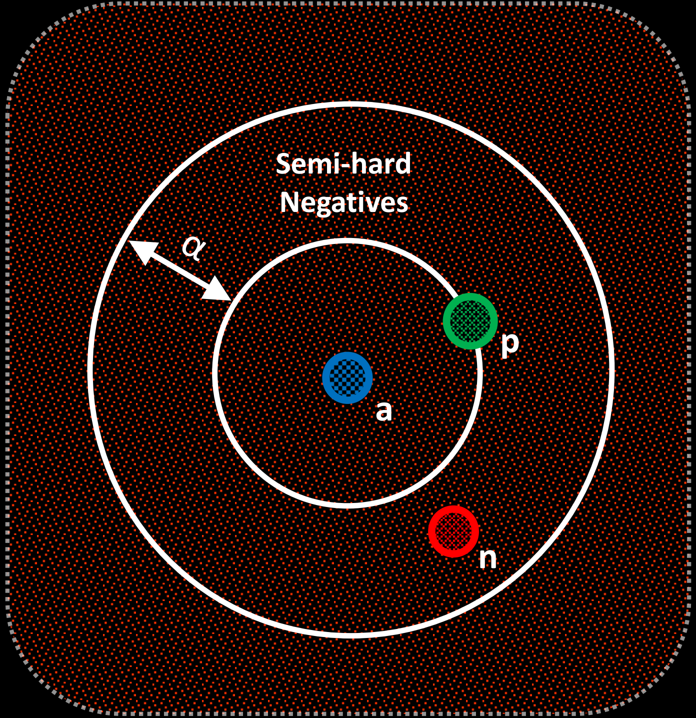
- Easy Negative:
  $||f(a) - f(p)|| + \alpha \leq ||f(a) - f(n)||$

- Hard Negative:
  $||f(a) - f(n)|| \leq ||f(a) - f(p)||$

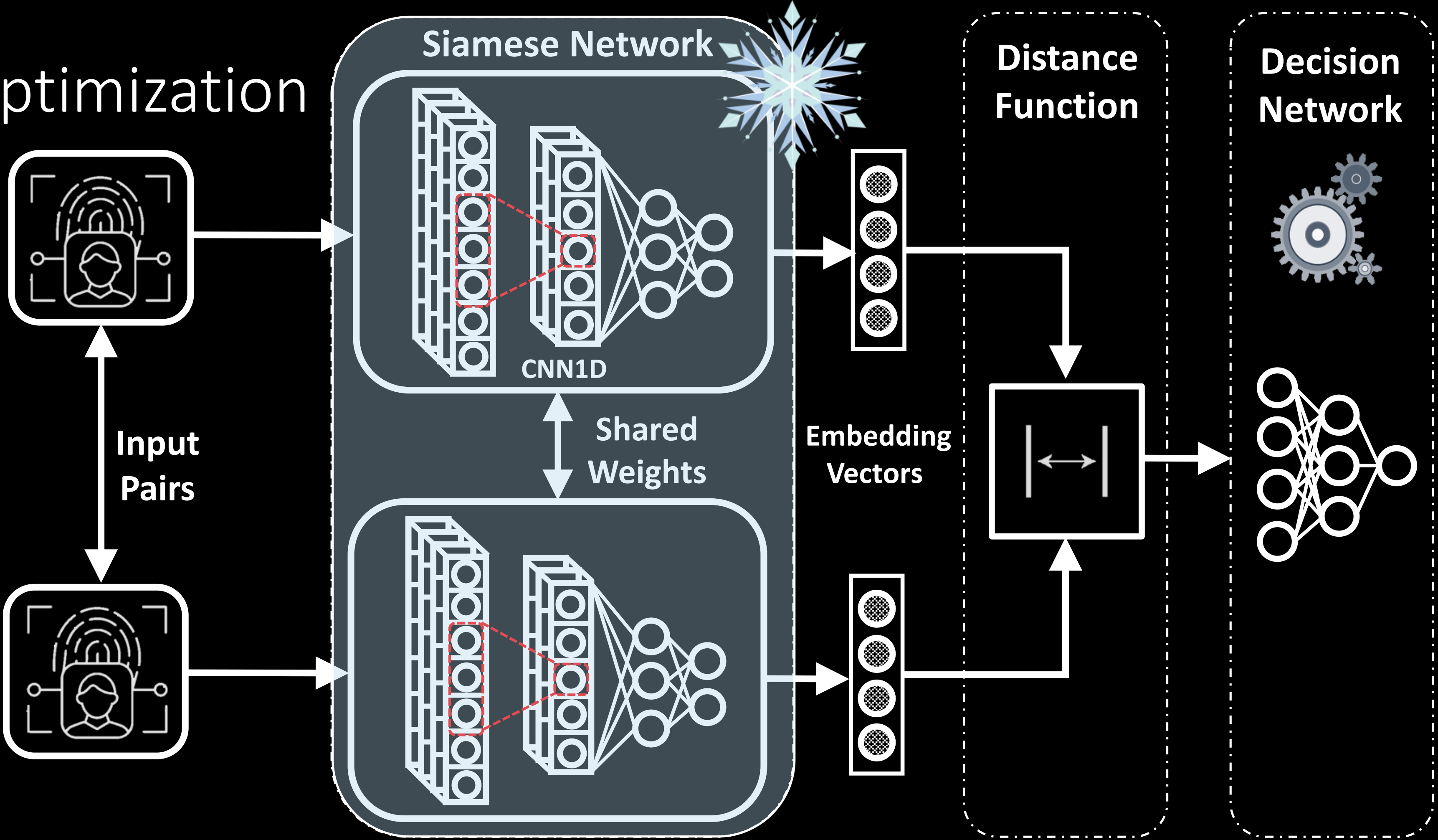


Triplet Training (Cont.)

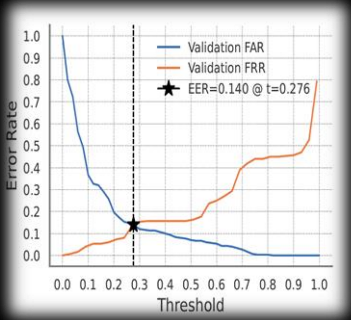
- Easy Negative:
  $\|f(a) - f(p)\| + \alpha \leq \|f(a) - f(n)\|$
- Hard Negative:
  $\|f(a) - f(n)\| \leq \|f(a) - f(p)\|$
- Semi-hard Negative:
  $\|f(a) - f(p)\| \leq \|f(a) - f(n)\| \leq \|f(a) - f(p)\| + \alpha$



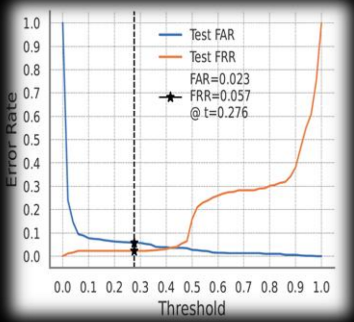
E2E Optimization



Evaluation



Calculation of Equal Error Rate (ERR)

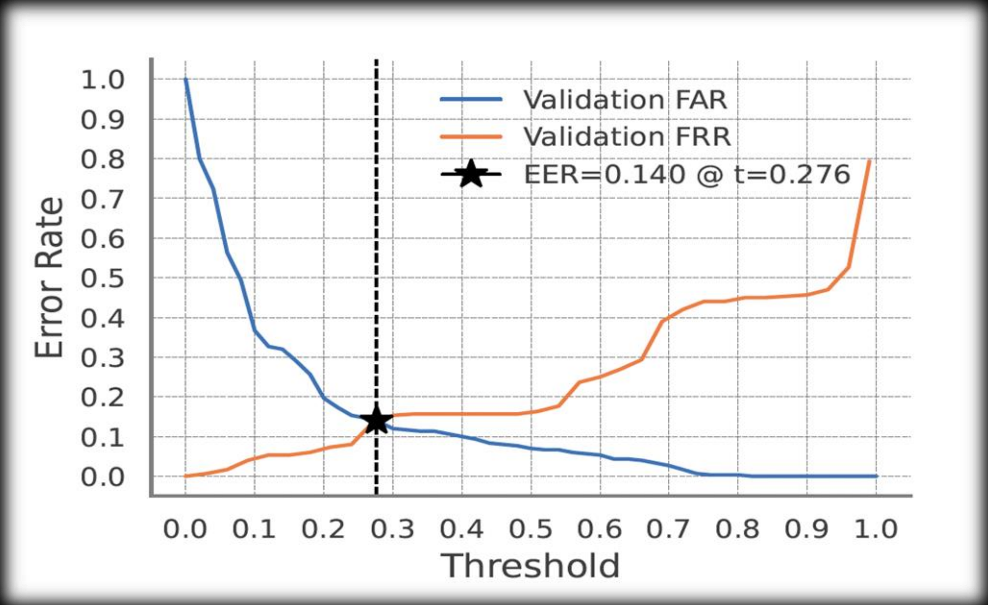


Calculation of FAR and FRR on test set

$TP - true\ positive$
$FP - false\ positive$
$FN - false\ negative$
$TN - true\ negative$

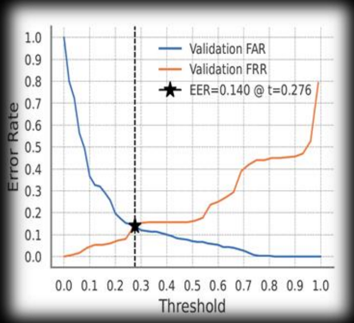
$$FAR = \frac{FP}{FP + TN}$$

$$FRR = \frac{FN}{FN + TP}$$

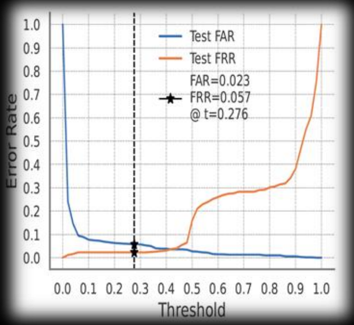


Calculation of Equal Error Rate (ERR)

Evaluation



Calculation of Equal Error Rate (ERR)

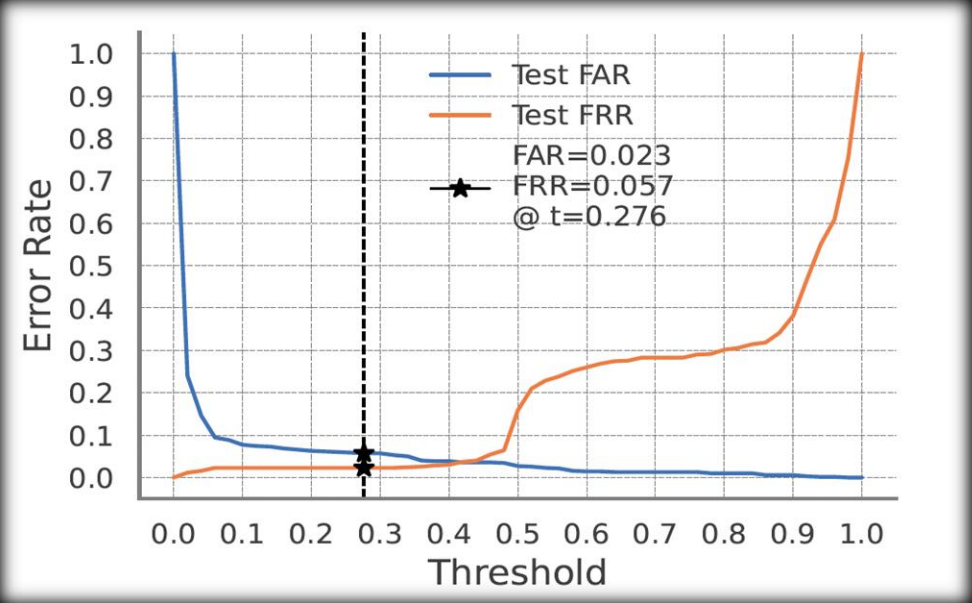


Calculation of FAR and FRR on test set

$TP - true\ positive$
$FP - false\ positive$
$FN - false\ negative$
$TN - true\ negative$

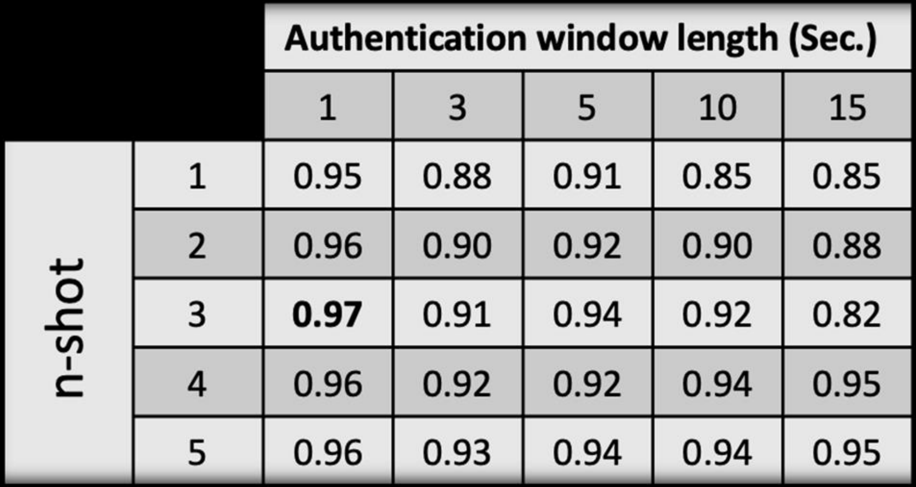
$$FAR = \frac{FP}{FP + TN}$$

$$FRR = \frac{FN}{FN + TP}$$



Calculation of FAR and FRR on test set

Evaluation(Cont.)



		Authentication window length (Sec.)				
		1	3	5	10	15
n-shot	1	0.95	0.88	0.91	0.85	0.85
	2	0.96	0.90	0.92	0.90	0.88
	3	**0.97**	0.91	0.94	0.92	0.82
	4	0.96	0.92	0.92	0.94	0.95
	5	0.96	0.93	0.94	0.94	0.95

F1-Score for triplet training on test set

$TP - true\ positive$
$FP - false\ positive$
$FN - false\ negative$

$$Precision = \frac{TP}{TP + FP} \qquad Recall = \frac{TP}{TP + FN} \qquad F1\_Score = 2 \times \frac{Precision\ \times\ Recall}{Precision + Recall}$$

n-shot: # enrolment samples to compare with test sample

Conclusion

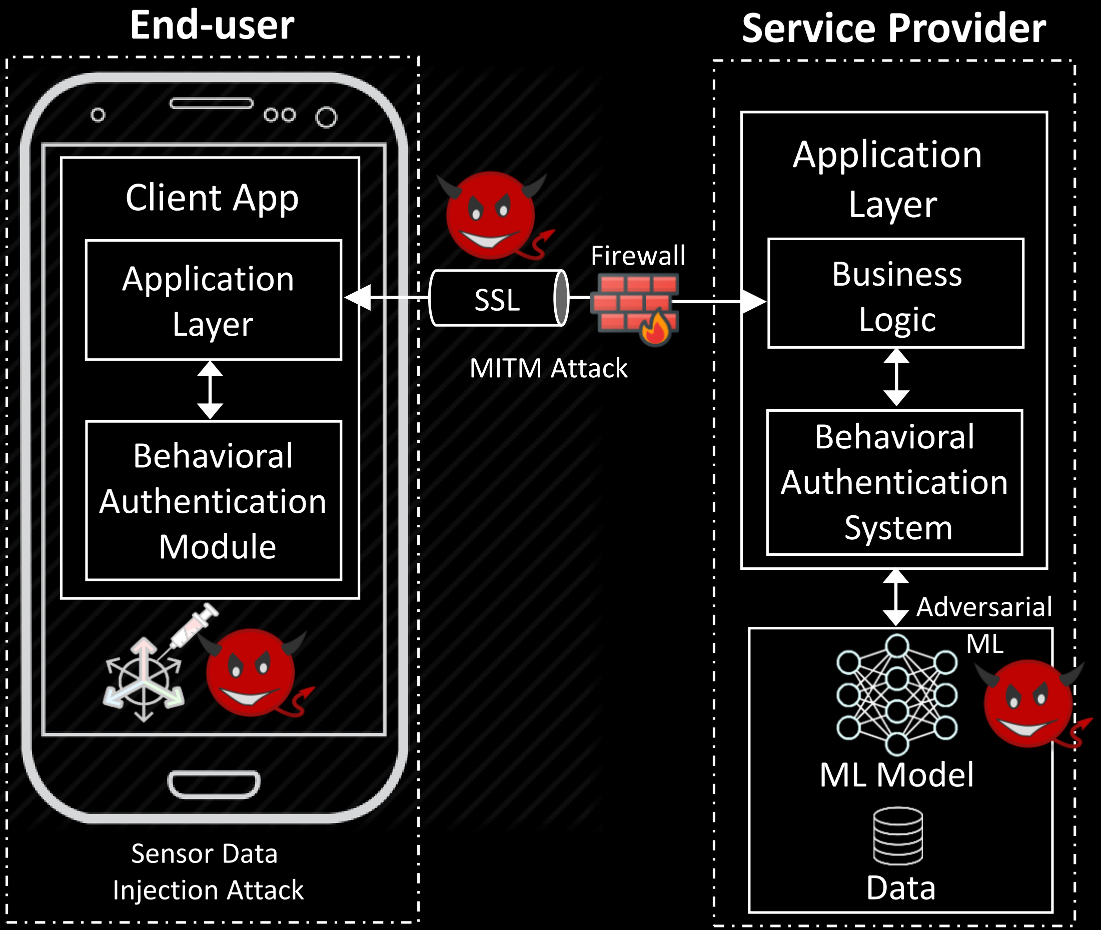
- AuthentiSense tackles challenges of existing user authentication methods and:

1. is efficient, not requiring hand-crafted features
2. is scalable, can authenticate millions of users
3. is user-agnostic, not requiring model retraining
4. can achieve accuracy in terms of F1-Score up to *97%* and FAR and FRR of *0.023* and *0.057* respectively
5. can authenticate users only after 1 Sec. of user interaction

Q&A ?

Backup Slides

Threat Model


End-user
Service Provider
Client App
Application Layer
Behavioral Authentication Module
Sensor Data Injection Attack
SSL
Firewall
MITM Attack
Application Layer
Business Logic
Behavioral Authentication System
Adversarial ML
ML Model
Data