FUTURAE

Future-proof, user-centric Authentication

www.futurae.com

ANASTASIA SYNTYCHAKI, DATA SCIENTIST

Blitz:
Detecting "Fake Support" attacks that circumvent 2FA

March 28, 2022

The leading provider of Authentication

Futurae offers a specialized platform for authentication and transaction confirmation catered to banks and financial institutions, elevating both **security** and **usability**.

Proven track record in **minimizing operational** and **helpdesk costs**.

100+ customers

40+ countries of customers

25M+ authentications a month

CyberTech 100 2019-2021

2020 Efma Capgemini winner of Retail and Commercial Banking

2018 **Gartner Cool Vendor** in Identity and Access Management

Build trust, not inconvenience

FOR SKILLS ON SMART HOME DEVICES

FOR MOBILE APPLICATIONS

FOR TABLETS

FOR WEB APPLICATIONS

The Futurae Platform authenticates your users. However you want it. Wherever they are.

Agenda

- Blitz scope
- Data & initial challenges
- Underlying models
- Results

Intro: Why Blitz

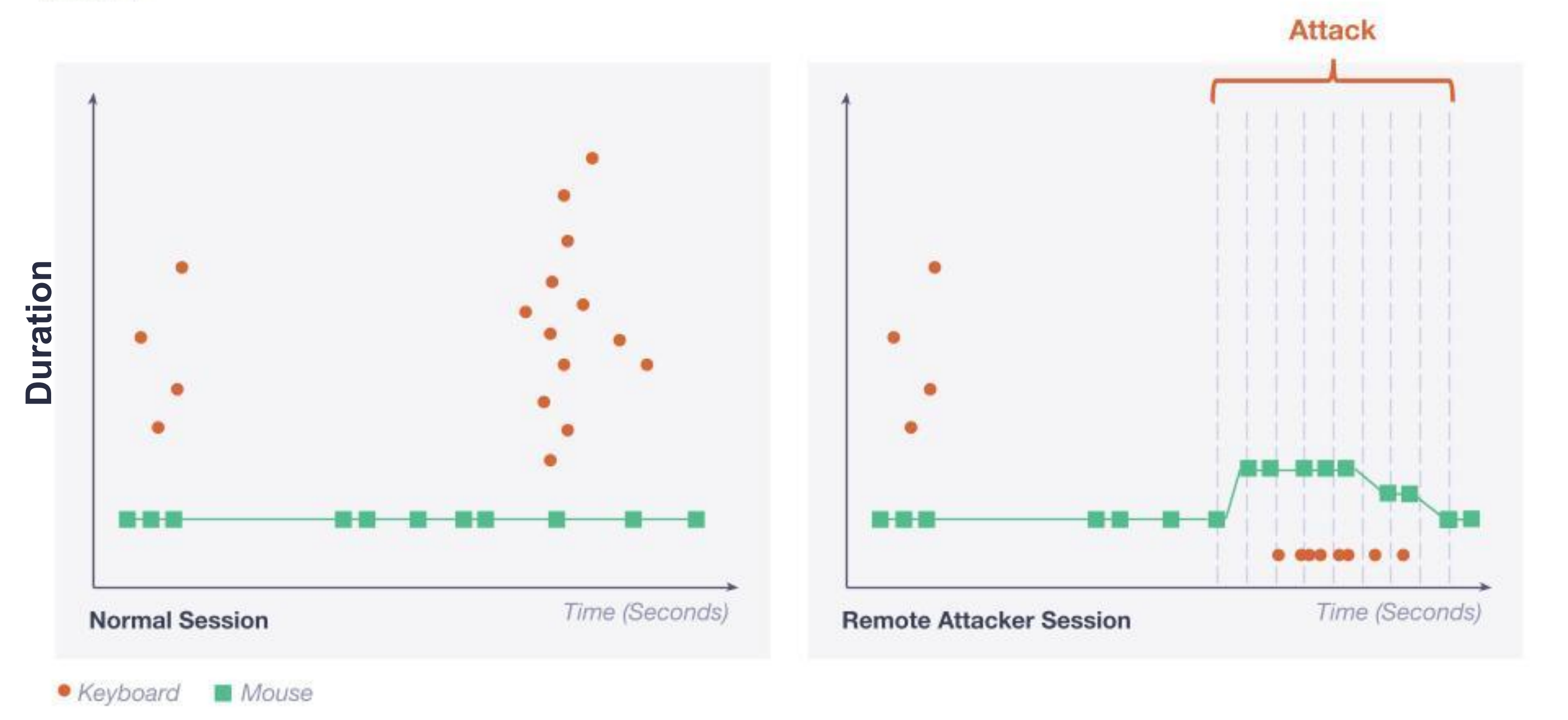
Protection against so-called “fake technical support” attacks with web banking:

- User installs remote desktop tools (e.g., TeamViewer) and grants access to attacker
- Victim follows instructions, proceeds with login & strong customer authentication
- Then performs a transaction to “whitelist” an attacker’s controlled IBAN
- Attacker “takes over” the session and performs a larger transaction as from the victim

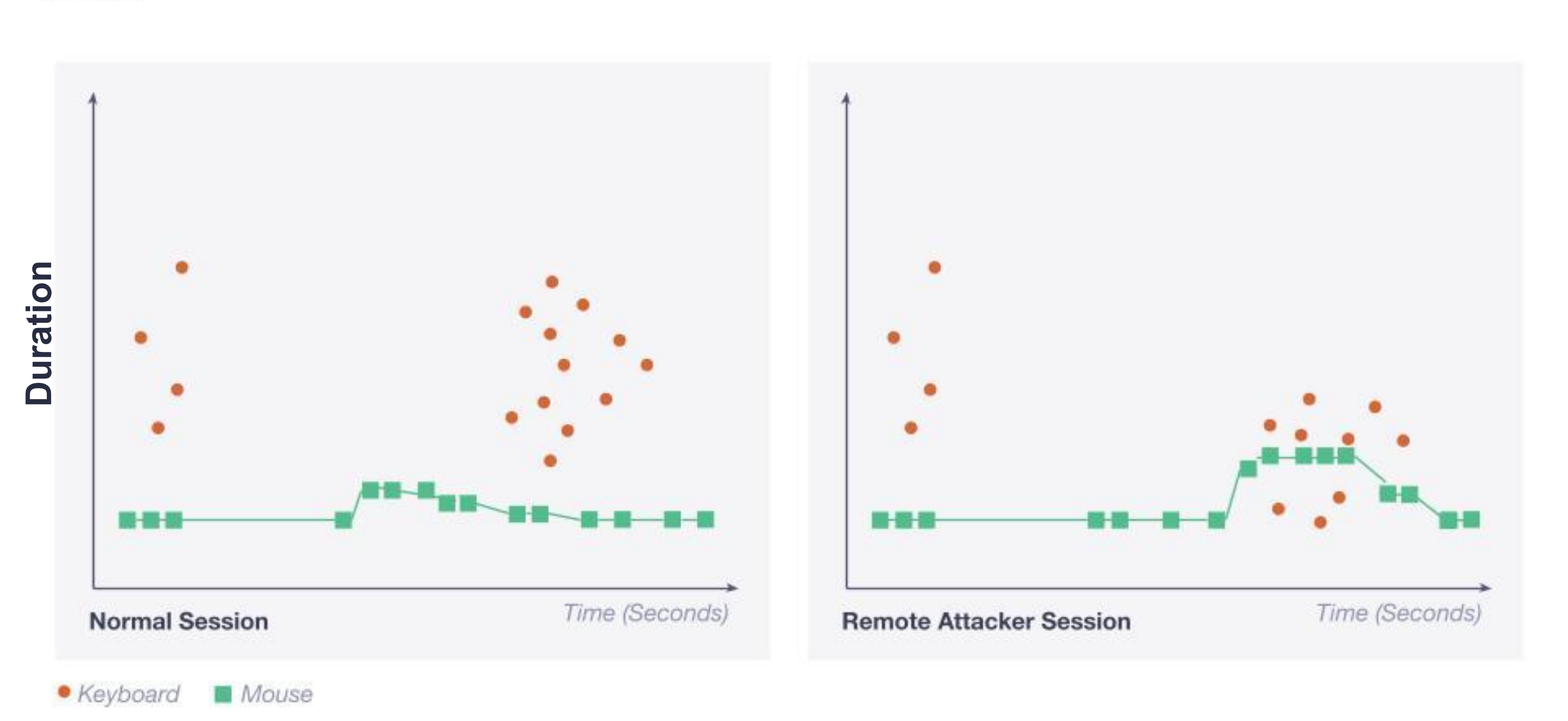
Detection:

- Blitz.js records “misbehaviours” from the user’s side based on keyboard and mouse interactions (recorded in JS in the browser), building a ML model in the backend

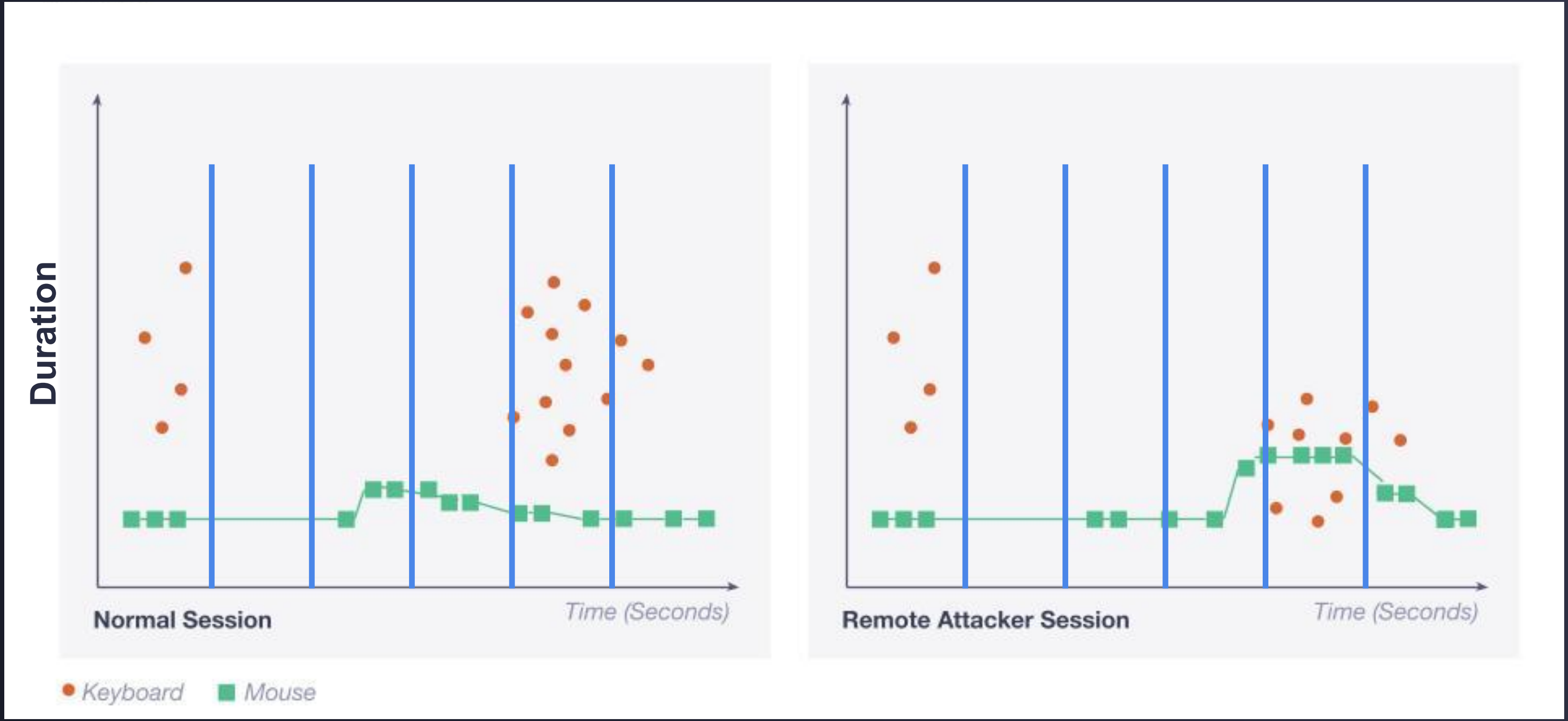
The data


Attack
Duration
Time (Seconds)
Normal Session
Time (Seconds)
Remote Attacker Session
● Keyboard
■ Mouse

The data


Duration
Normal Session
Time (Seconds)
Remote Attacker Session
Time (Seconds)
● Keyboard
🟩 Mouse

The data


Duration
Normal Session
Time (Seconds)
Remote Attacker Session
Time (Seconds)
● Keyboard
■ Mouse

Initial approach & challenges

XGBoost model had 30-50% Recall and 5% False Positive Rate

Goal:

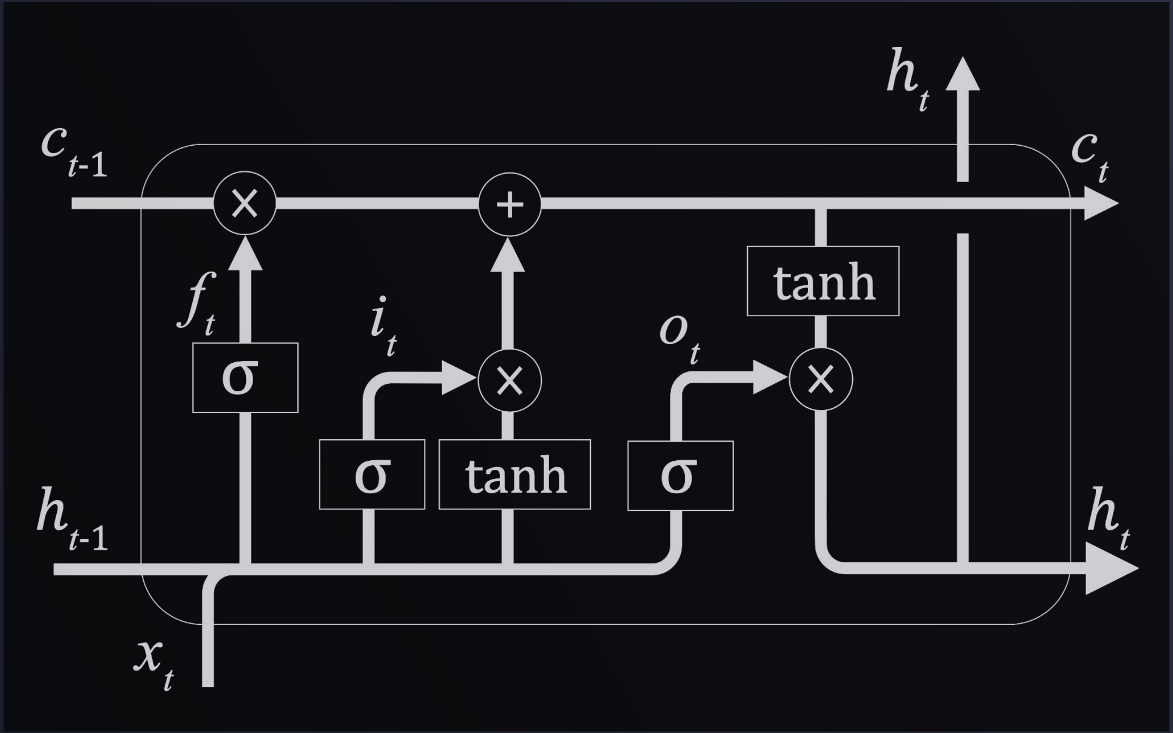
- High Recall → We want to reduce the FNs
- Low FPR → We want to reduce the FPs

Initial approach & challenges

XGBoost model had 30-50% Recall and 5% False Positive Rate

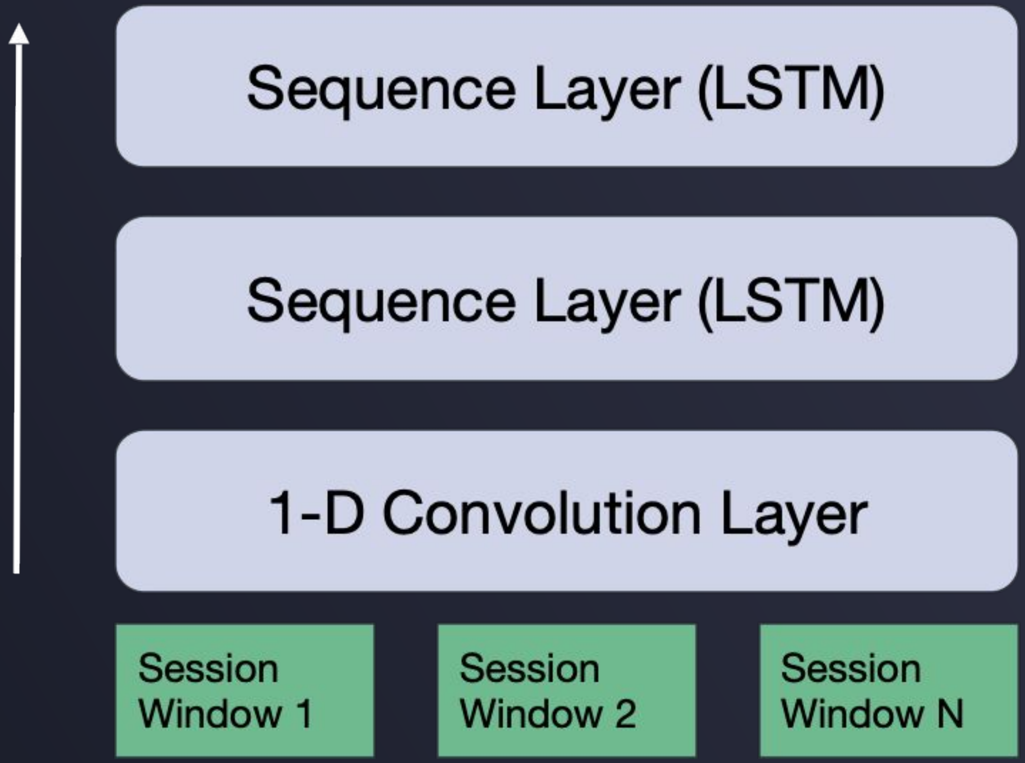
- Extremely imbalanced datasets
- ~25% of reported attacks are without key presses
  ~50% of sessions are without key presses
- Sessions vary highly in terms of events

New model deployment - LSTM

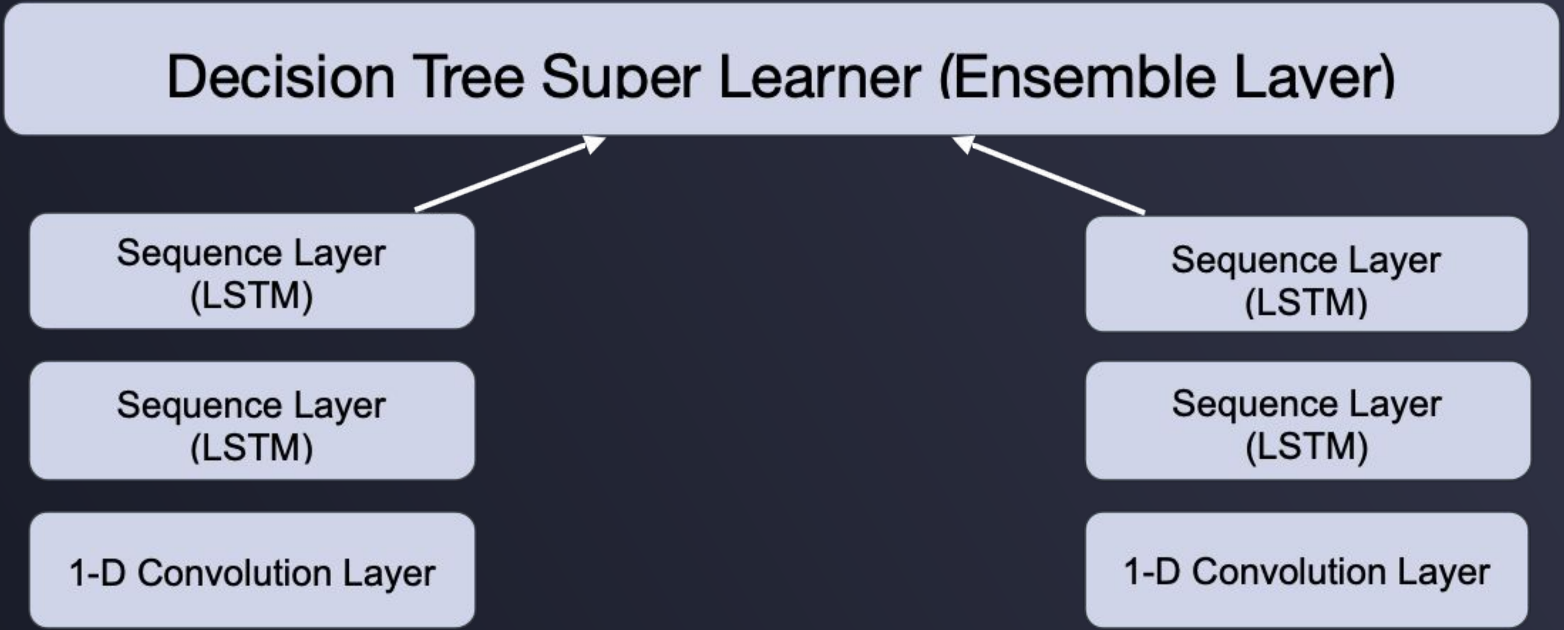


Beltran-Hernandez *et al.*,
doi: 10.3934/mbe.2020293

CNN-LSTM Architecture



CNN-LSTM Ensemble



Decision Tree Super Learner (Ensemble Layer)

Sequence Layer (LSTM)

Sequence Layer (LSTM)

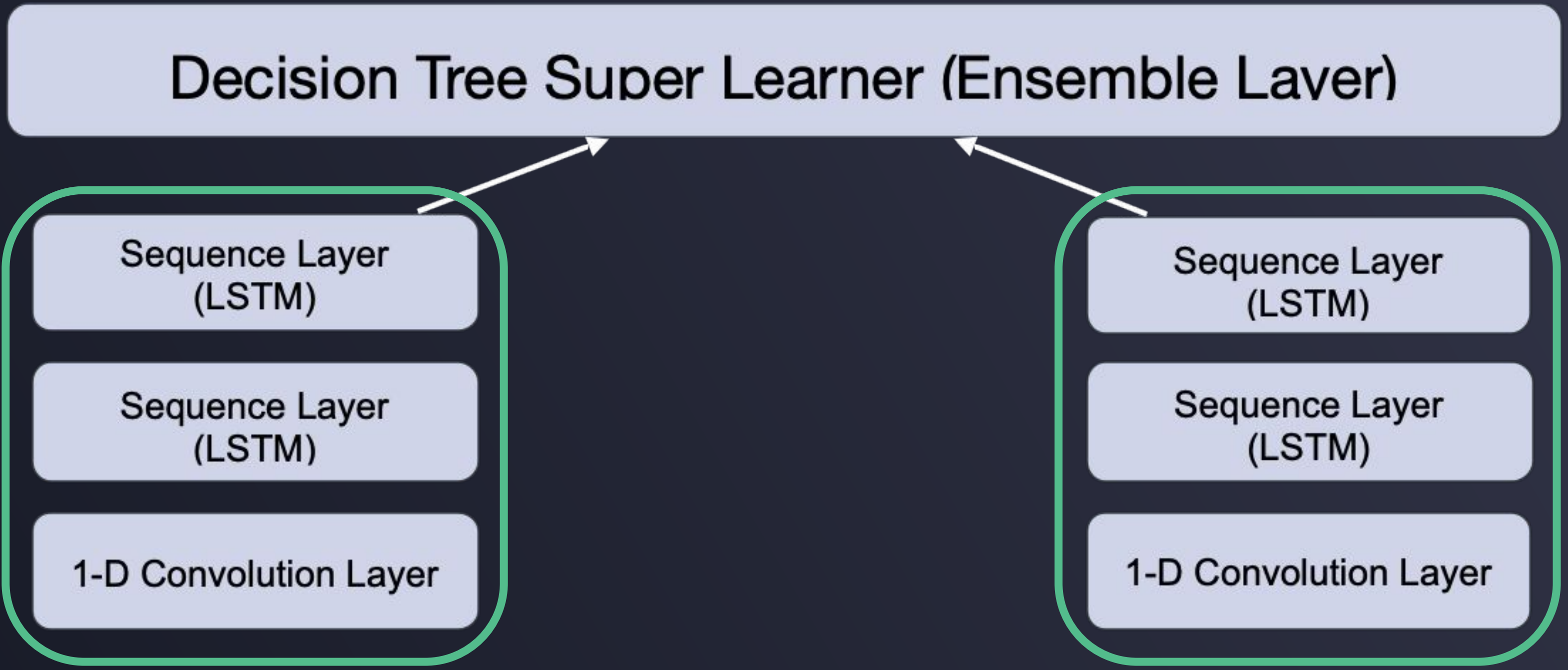
1-D Convolution Layer

Sequence Layer (LSTM)

Sequence Layer (LSTM)

1-D Convolution Layer

CNN-LSTM Ensemble



Decision Tree Super Learner (Ensemble Layer)

Sequence Layer (LSTM)

Sequence Layer (LSTM)

1-D Convolution Layer

Sequence Layer (LSTM)

Sequence Layer (LSTM)

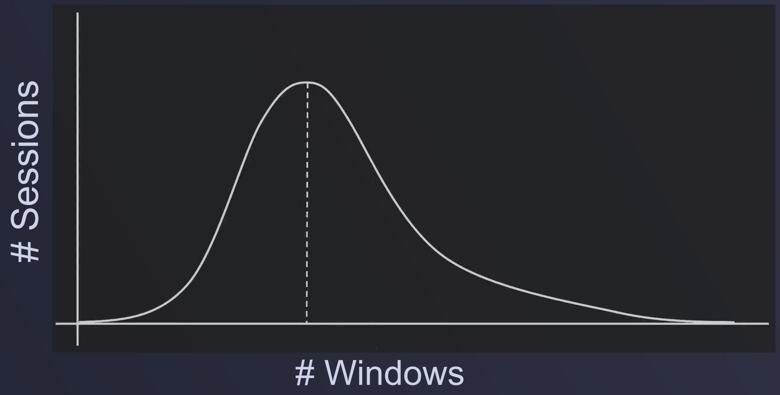
1-D Convolution Layer

Normal Sessions: Day 1 + All Attacks

Normal Sessions: Day N + All Attacks

Data processing enhancement

Built synthetic data



- **Augmentation:**

  Padded all short sessions

  by duplicating existing windows.

- **Boosting with bootstrapping:**

  Resampled existing attacks to generate new ones.

CNN-LSTM Results Summary

	JUN			JUL			AUG			
	Total att.	Found	**Recall**	Total att.	Found	**Recall**	Total att.	Found	**Recall**	**FPR**
MMs	21	14	**0.66**	31	22	**0.70**	4	3	**0.75**	**0.023**
KPs + MMs	12	11	**0.92**	17	13	**0.76**	4	3	**0.75**	**0.027**

- Recall in range of 75-95%
- FPR at 2-3%

THANK YOU

Zürich
Schweiz

FUTURAE

Future-proof, user-centric authentication

www.futurae.com

Anastasia@futurae.com

Find us on Twitter: **@_futurae** and via **@_futurae,** LinkedIN and Facebook

Gartner
Cool Vendors
Identity Access
management