Explainable Anomaly Detection in Linux System Call Sequences

Dalia Elnagar, Sampo Sovio

The Problem

- Novel attacks can evade signature-based IDS
  - **Solution:** Anomaly Detectors
- Syscall sequences encode behaviour at kernel level
  - Making them strong intrusion signals.
- Existing DL-based detectors are black boxes + may generate FPs
  - SOC analysts can't triage or trust them

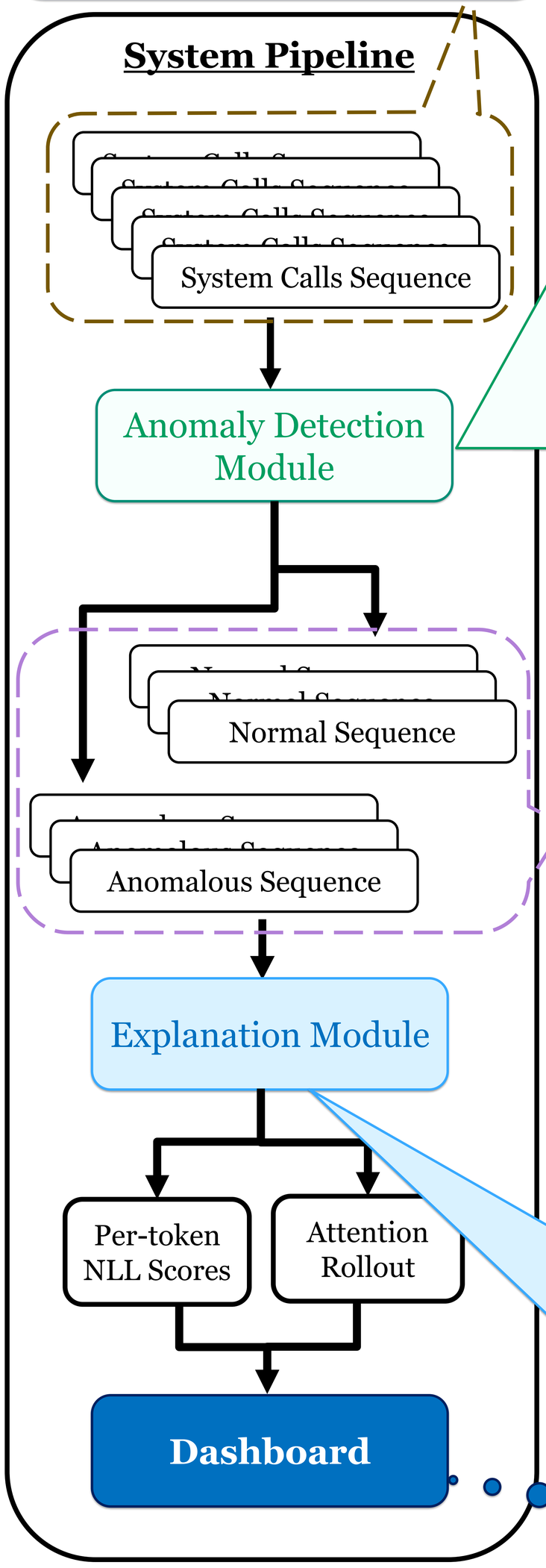
The Goals

- Train self-supervised decoder-only Transformer-based anomaly detector
- Produce token-level explanations
  - NLL scores + attention rollout
- Visualize results through a SOC analyst dashboard
- Test feasibility on resource-constraint devices

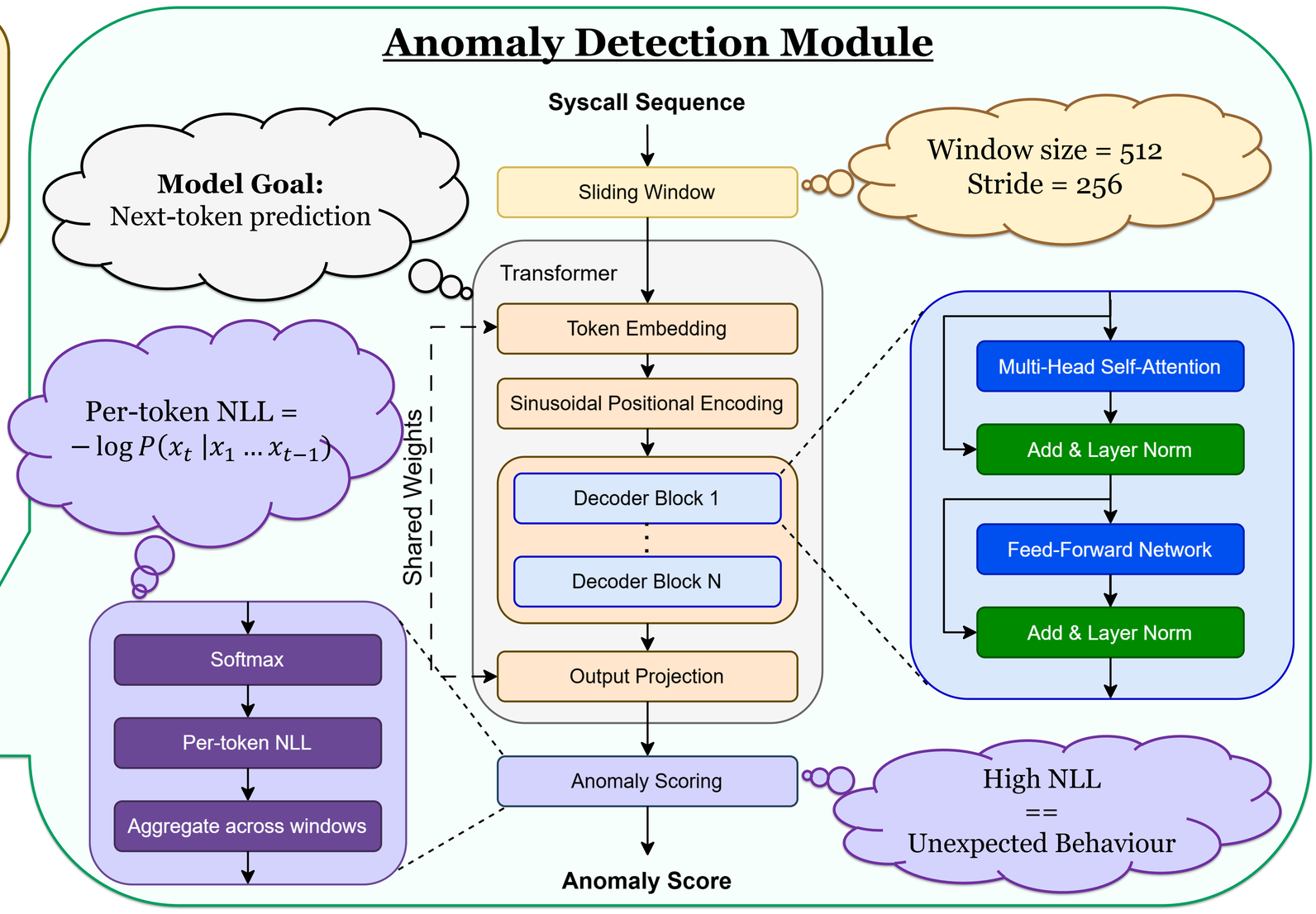
Training Data

- DongTing Dataset
- Train & Val: Normal seq. only
- Normal dataset ratio
  80% train : 10% val : 10% test

System Pipeline



Anomaly Detection Module



Results

AUC	Dataset	DongTing	ADFA-LD	PLAID
	Ours	**0.979**	**0.425**	**0.878**
	Baseline	0.972	0.292	0.750

Test dataset ratio
50% benign : 50% atk

Baseline: LSTM
(2 layers, 400 cells)

Edge Deployment	Method	AUC	Size (MB)	Inference Avg (ms)	
				Raspberry Pi	Jetson Board
	ONNX	**0.979**	3.66	**149.66**	33.65
	TFLite	0.880	**0.88**	179.66	114.29
	TensorRT	**0.979**	4.23	NA	**21.94**

Explanation Module

Goals	Method
1- Which syscalls drove the score	→ Per-token NLL scores
2- Why were they unexpected *(which prior syscalls was the model looking at when predicting)*	→ Attention Rollout: • Propagates attention weights backwards layer-by-layer *(how input tokens influence each output prediction)*

NB: Overlapping windows averaged

Check the demo!

Helsinki System Security Lab (HSSL)

HSSL drives renewal and mastery in the field of platform and device related security technologies, especially for Huawei consumer devices such as mobile phones, laptops, televisions and automotive. We do research in topics such as hardware-assisted isolation and integrity, as well as in operating system protection (hypervisor, TEE, secure enclaves and kernel hardening). We also carry expertise in cryptography and systems security functionality such as device key management (PKI), device attestation and key-store solutions.

HUAWEI