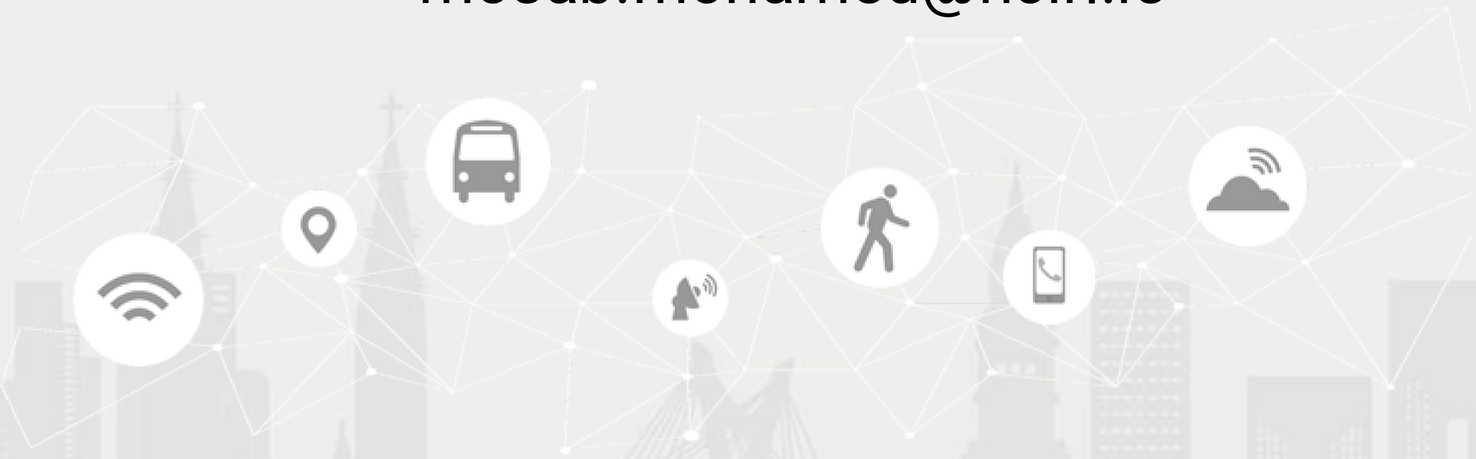
Explainable AI for Efficient & Transparent Network Traffic Classification

Dr. Mosab Hamdan

mosab.mohamed@ncirl.ie



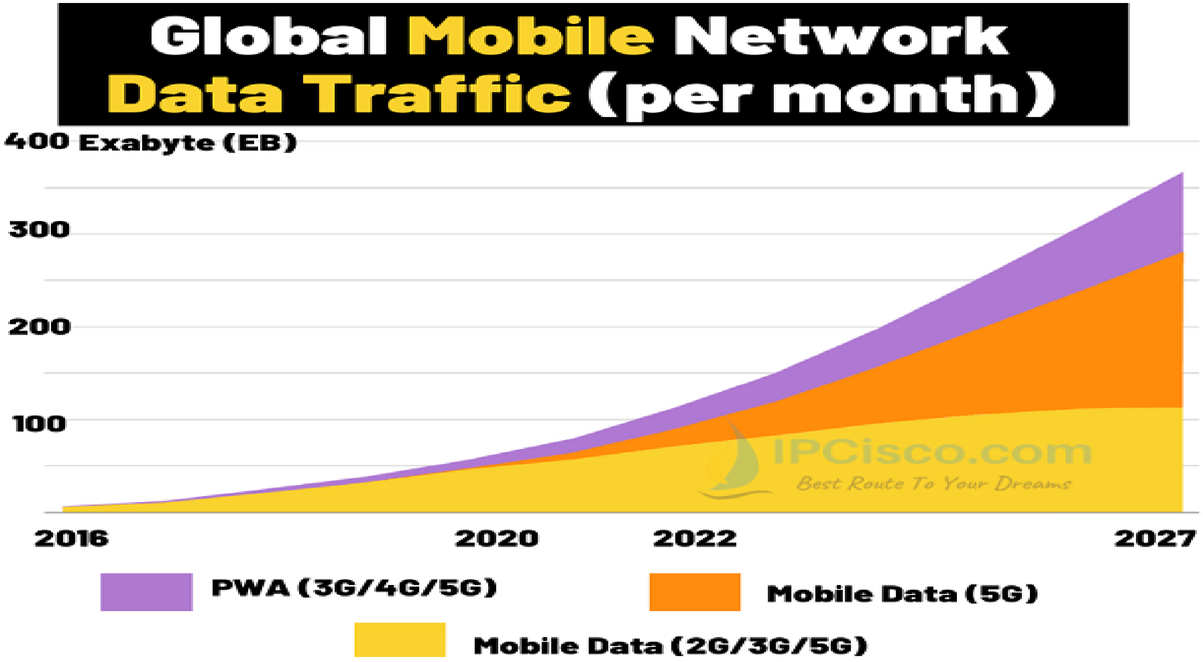
School of Computing, National College of Ireland, Ireland

Outlines

- Motivation for Network Traffic Classification (NTC)
- Toward Next-Gen AI Traffic Classifiers
- SDN-based Traffic Classification (TC)
- Stream-TC in SDN
- IDS based on TC
- XAI Integration with Lightweight TC

Motivation for Network Traffic Classification

- 27 billion IoT/IIoT devices by 2025 → ≈ 400 EB of traffic every month
- 90% of flows now encrypted → traditional DPI fails
- SDN/IoT/Edge introduce concept drift, tiny CPUs, and strict latency.
- Diverse protocols, constant drift
- Attacks move to the edge (smart homes, factories, cities)
- Need for millisecond decisions
- Traffic classification critical for QoS management, intrusion detection & anomaly monitoring
- Black-box ML ≠ regulatory trust



Ericsson Global Mobile Data Traffic 2027 Report

Toward Next-Gen Efficient & Transparent AI Traffic Classifiers

Pain-Points in Today’s AI-TC

Black-Box Decisions ⚠

- Ops team cannot see *why* a flow is blocked
- Hard to tune policies or satisfy auditors

Heavy, GPU-Hungry Training ⚠

- Full retrain whenever a new app / protocol appears
- Long downtimes, high cloud cost

Bulky Models at the Edge ⚠

- 10 MB-plus binaries, >1 GFLOPS per flow
- Unfit for Pi-level gateways or switches

Next-Gen Traffic Classification

Trustworthy & Explainable AI ✓

- Built-in LIME / SHAP snippets for every alert
- Human-readable logic → audit & compliance ready

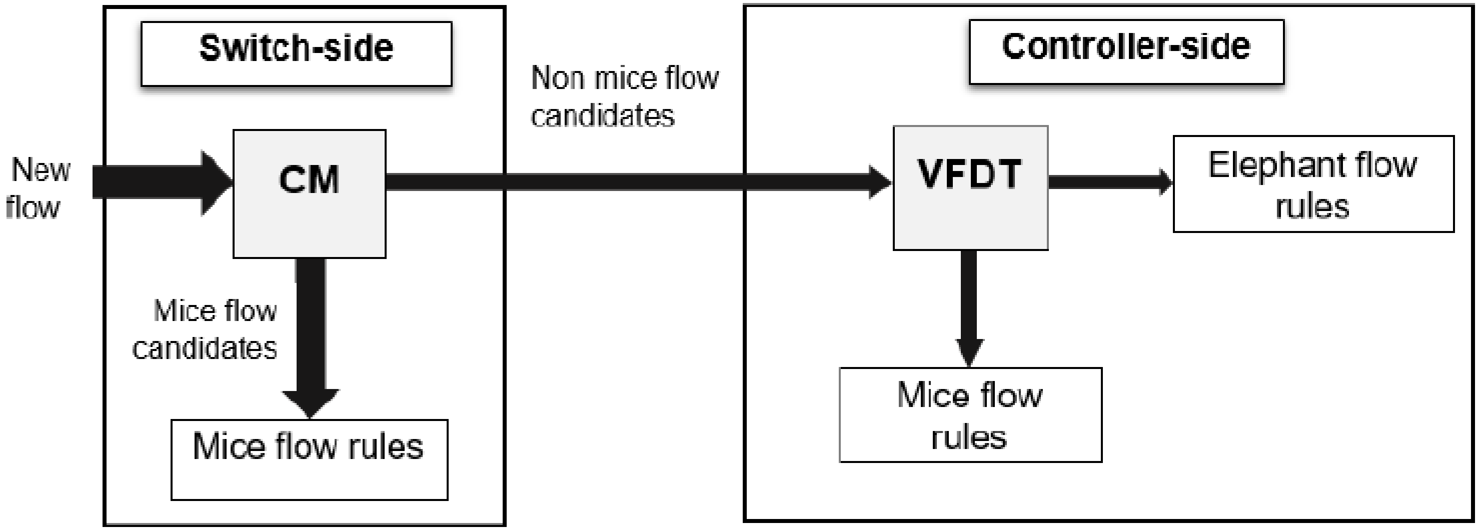
Class-Incremental Learning ✓

- Add new traffic classes on-the-fly—no “train-from-scratch” • Edge-friendly updates in seconds

Lightweight Architectures ✓

- Depthwise-Separable CNN / sketch trees <0.7 MFLOPS
- <40 k parameters—runs in < 2 ms on ARM SoC

Flow-Aware Elephant Flow Detection for Software-Defined Networks

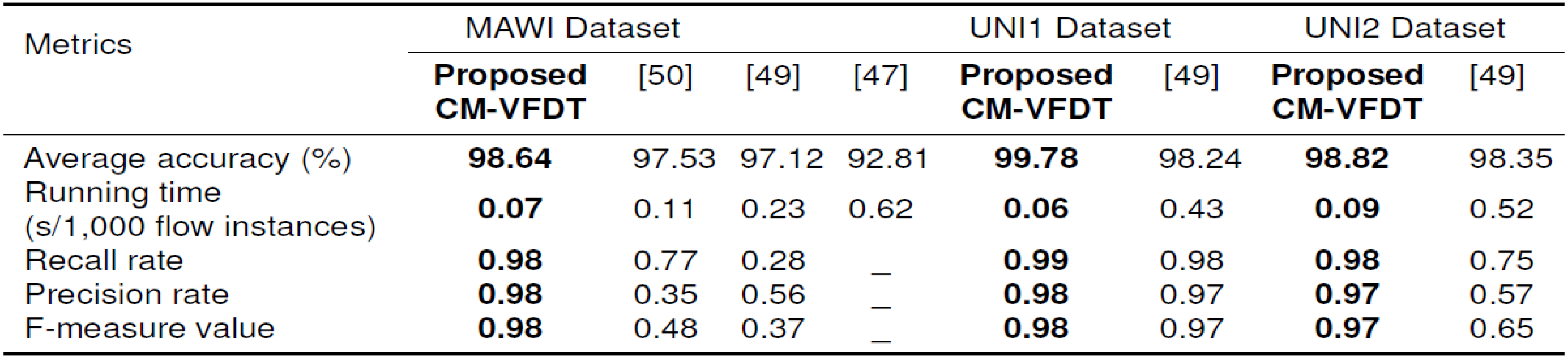


- Any traffic that exceeds a certain threshold per unit time (e.g., 10 Mbps) is often considered also as Efs.
- The switch-side classifier pre-filters MFs based on the CM sketch algorithm.
- The candidate non MFs are forwarded by the switch to the controller to performs the controller-side of the process, by using the VFDT classifier.

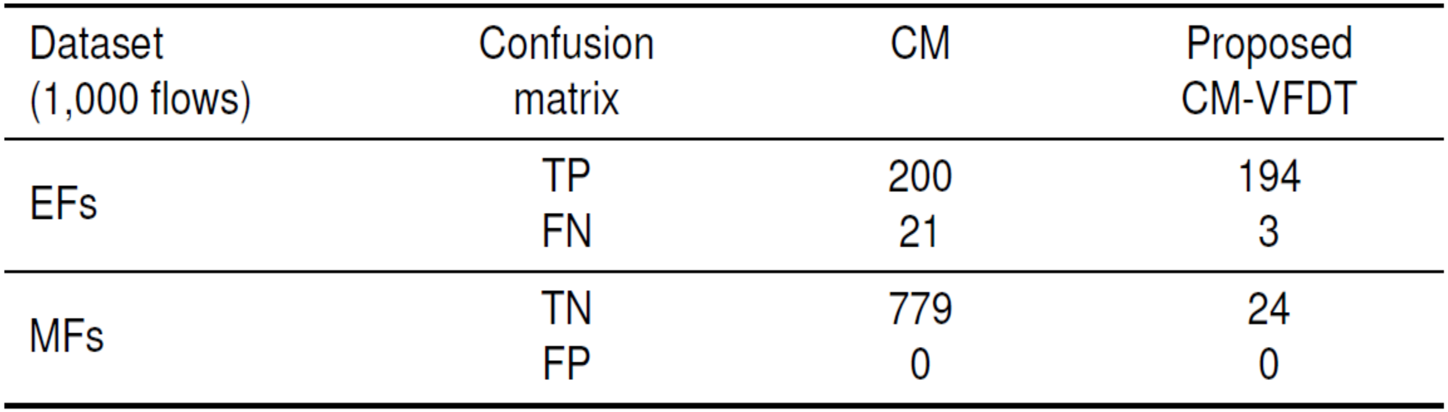
Hamdan et al., Flow-aware elephant flows in software-defined networks, *IEEE Access, 2020.*

Summary of Experiment Results

Switch-Controller Performance Comparison with Other Methods:



Metrics	MAWI Dataset				UNI1 Dataset		UNI2 Dataset	
	Proposed CM-VFDT	[50]	[49]	[47]	**Proposed CM-VFDT**	[49]	**Proposed CM-VFDT**	[49]
Average accuracy (%)	**98.64**	97.53	97.12	92.81	**99.78**	98.24	**98.82**	98.35
Running time (s/1,000 flow instances)	**0.07**	0.11	0.23	0.62	**0.06**	0.43	**0.09**	0.52
Recall rate	**0.98**	0.77	0.28	_	**0.99**	0.98	**0.98**	0.75
Precision rate	**0.98**	0.35	0.56	_	**0.98**	0.97	**0.97**	0.57
F-measure value	**0.98**	0.48	0.37	_	**0.98**	0.97	**0.97**	0.65

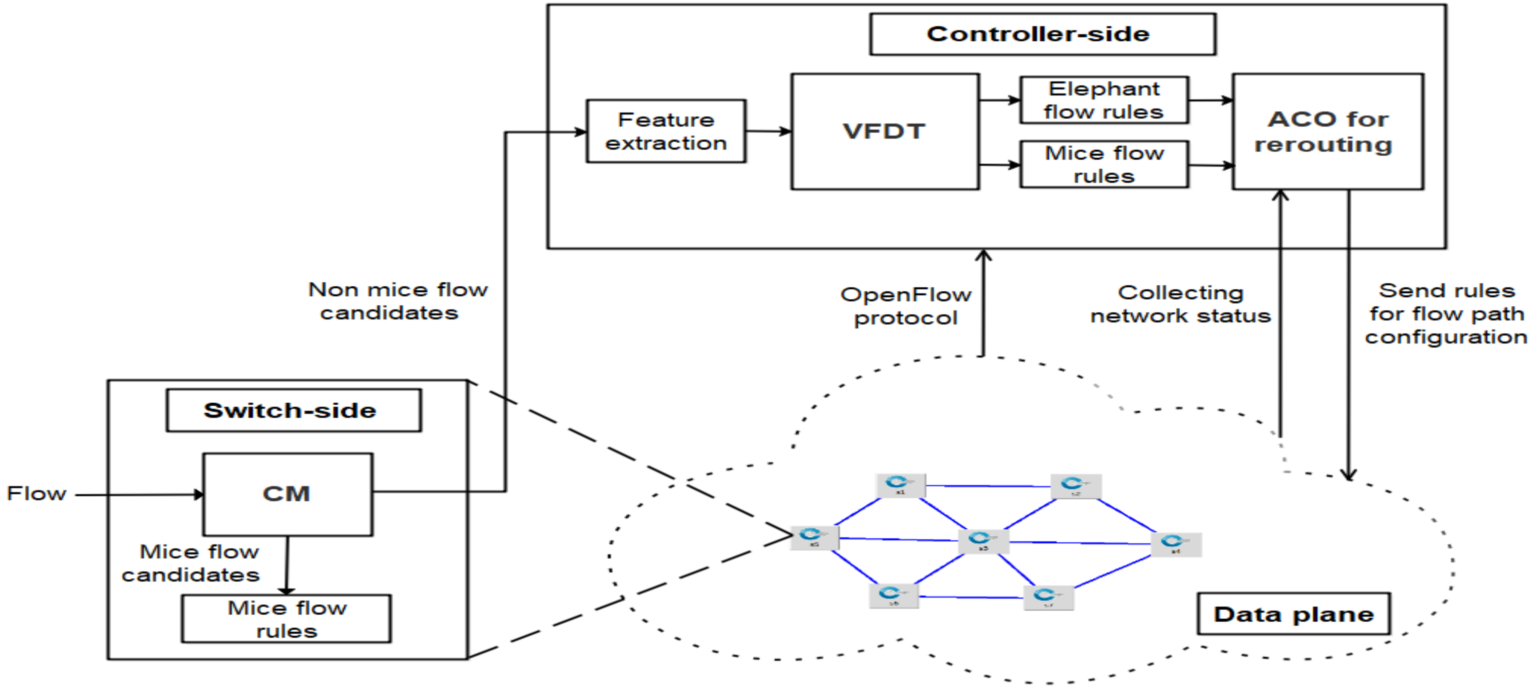


Dataset (1,000 flows)	Confusion matrix	CM	Proposed CM-VFDT
EFs	TP	200	194
	FN	21	3
MFs	TN	779	24
	FP	0	0

- The CM sketch classifier filters most MFs in the SDN switch, which can reduce the overhead switch-controller signalling on the controller close to 80%.

Hamdan et al., Flow-aware elephant flows in software-defined networks, *IEEE Access, 2020.*

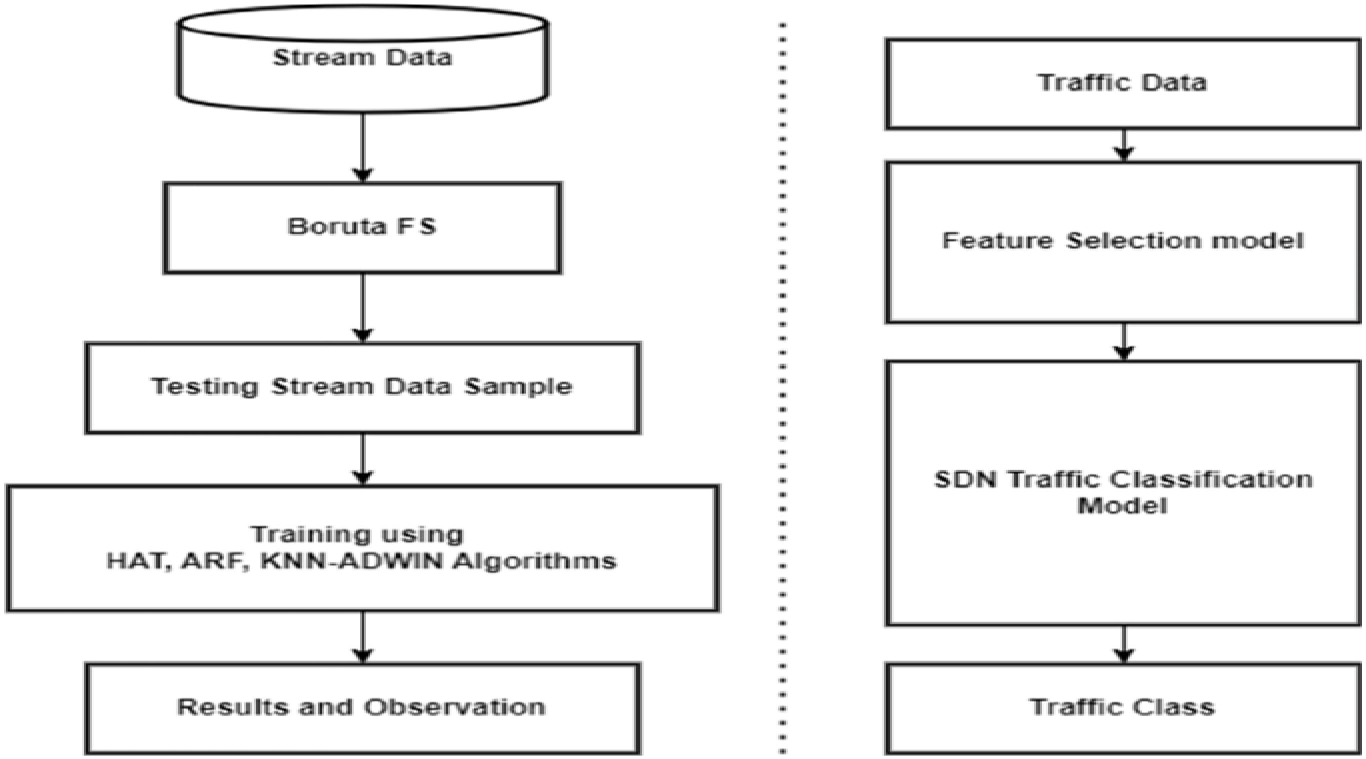
Load Balancing based TC in Software-Defined Networks



- Detecting EF using a joint switch/controller EF detection.
- Rerouting EF using ACO based on available link bandwidth.
- Forwarding the MFs without considering the available bandwidth.

Hamdan et al., *DPLBAnt:* Improved load balancing technique based on detection and rerouting of elephant flows in software-defined networks, *Computer Communications, 2021.*

Improved Feature Selection and Stream Traffic Classification Based on Machine Learning in Software-Defined Networks

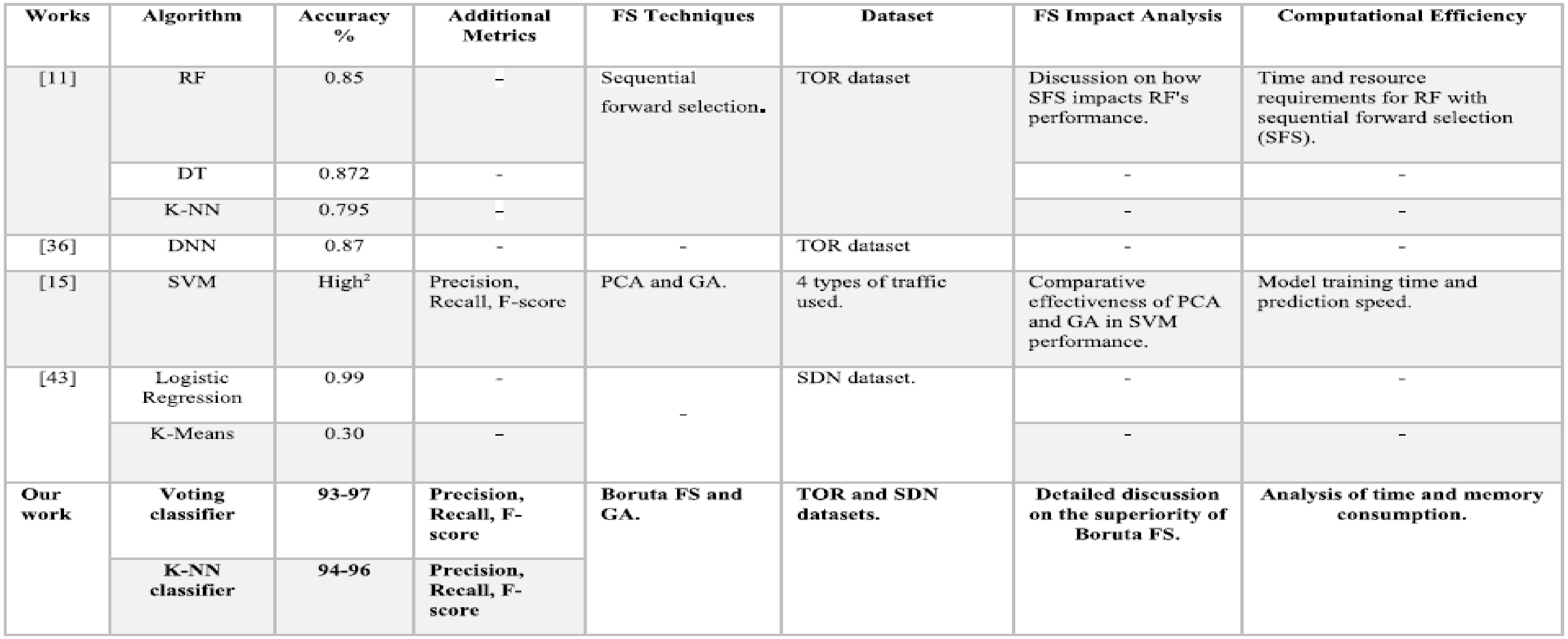


- This research aims to improve the overall performance of TC using the SL technique to select relevant FS to alleviate load from the SDN control plane by doing the following. First, an FS mechanism called Boruta is proposed. Second, we propose three streaming-based TC methods for SDN: Hoeffding adaptive trees (HAT), adaptive random forest (ARF), and k-nearest neighbour with adaptive sliding window detector (KNN-ADWIN).
- These techniques can dynamically handle the concept drift and solve the problem of memory and time consumption, lowering the overhead of the SDN controller.

Arwa M. ELDHAI , ***M. Hamdan et al.***, *Improved Feature Selection and Stream Traffic Classification Based on Machine Learning in Software-Defined Networks. IEEE Access, 2022.*

Results and Analysis

Classifier	Acc	Kappa	Time(s)	Memory(KB)
HAT	0.74	0.67	**15**	**105**
ARF	**0.87**	**0.87**	59	431
KNN-ADWIN	0.80	0.78	65	1154

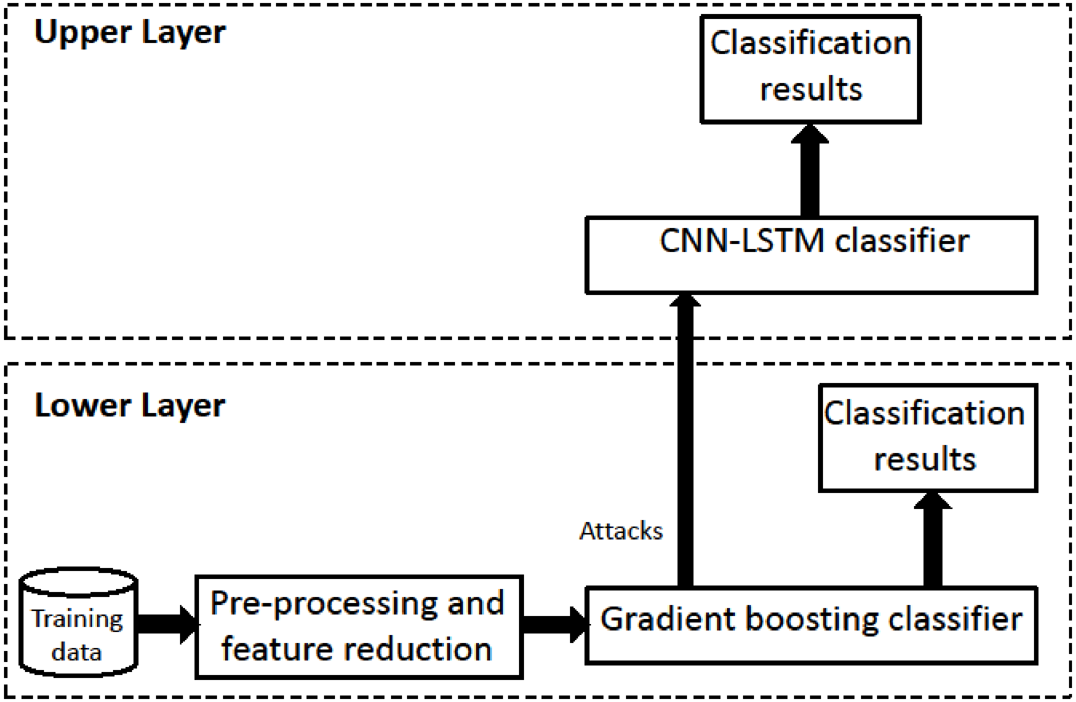


Works	Algorithm	Accuracy %	Additional Metrics	FS Techniques	Dataset	FS Impact Analysis	Computational Efficiency
[11]	RF	0.85	-	Sequential forward selection.	TOR dataset	Discussion on how SFS impacts RF's performance.	Time and resource requirements for RF with sequential forward selection (SFS).
	DT	0.872	-			-	-
	K-NN	0.795	-			-	-
[36]	DNN	0.87	-	-	TOR dataset	-	-
[15]	SVM	$High^2$	Precision, Recall, F-score	PCA and GA.	4 types of traffic used.	Comparative effectiveness of PCA and GA in SVM performance.	Model training time and prediction speed.
[43]	Logistic Regression	0.99	-	-	SDN dataset.	-	-
	K-Means	0.30	-			-	-
Our work	**Voting classifier**	**93-97**	**Precision, Recall, F-score**	**Boruta FS and GA.**	**TOR and SDN datasets.**	**Detailed discussion on the superiority of Boruta FS.**	**Analysis of time and memory consumption.**
	K-NN classifier	**94-96**	**Precision, Recall, F-score**				

- Dataset: TOR (1.18 M flows) & synthetic Mininet.
- HAT is ideal when every millisecond & KB matter; ARF wins if accuracy rules.

Arwa M. ELDHAI , ***M. Hamdan et al.****, Improved Feature Selection and Stream Traffic Classification Based on Machine Learning in Software-Defined Networks. IEEE Access, 2024.*

A Two-Tier Anomaly-based Intrusion Detection Approach for IoT-Enabled Smart Cities



❖ **Accurate IDS based on joint two-tier classifiers technique by:**

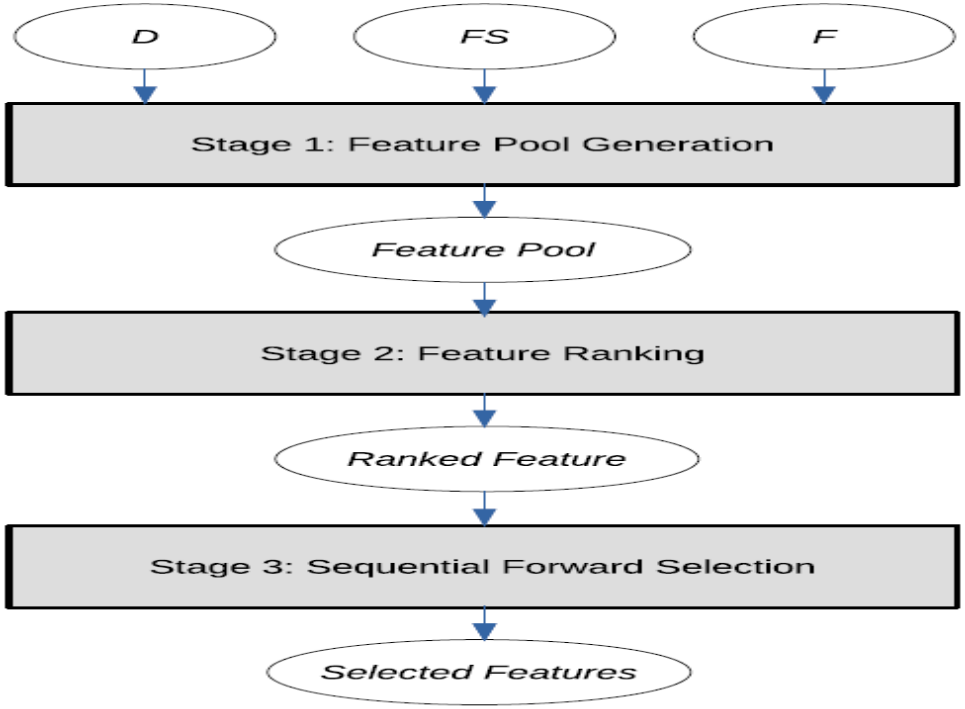
➢ Proposal of an enhanced Boruta feature selection technique.

➢ Proposal an enhanced IDS architecture for edge and fog architectures to be deployed in smart cities.

➢ Enhancing the detection effectiveness of an IDS for the IoT-based smart cities to detect multi-class attacks.

Mosab Hamdan et al. “A Two-Tier Anomaly-based Intrusion Detection Approach for IoT-Enabled Smart Cities” accepted in The 2023 IEEE International Conference on Computer Communications (INFOCOM), IEEE, 2023. USA.

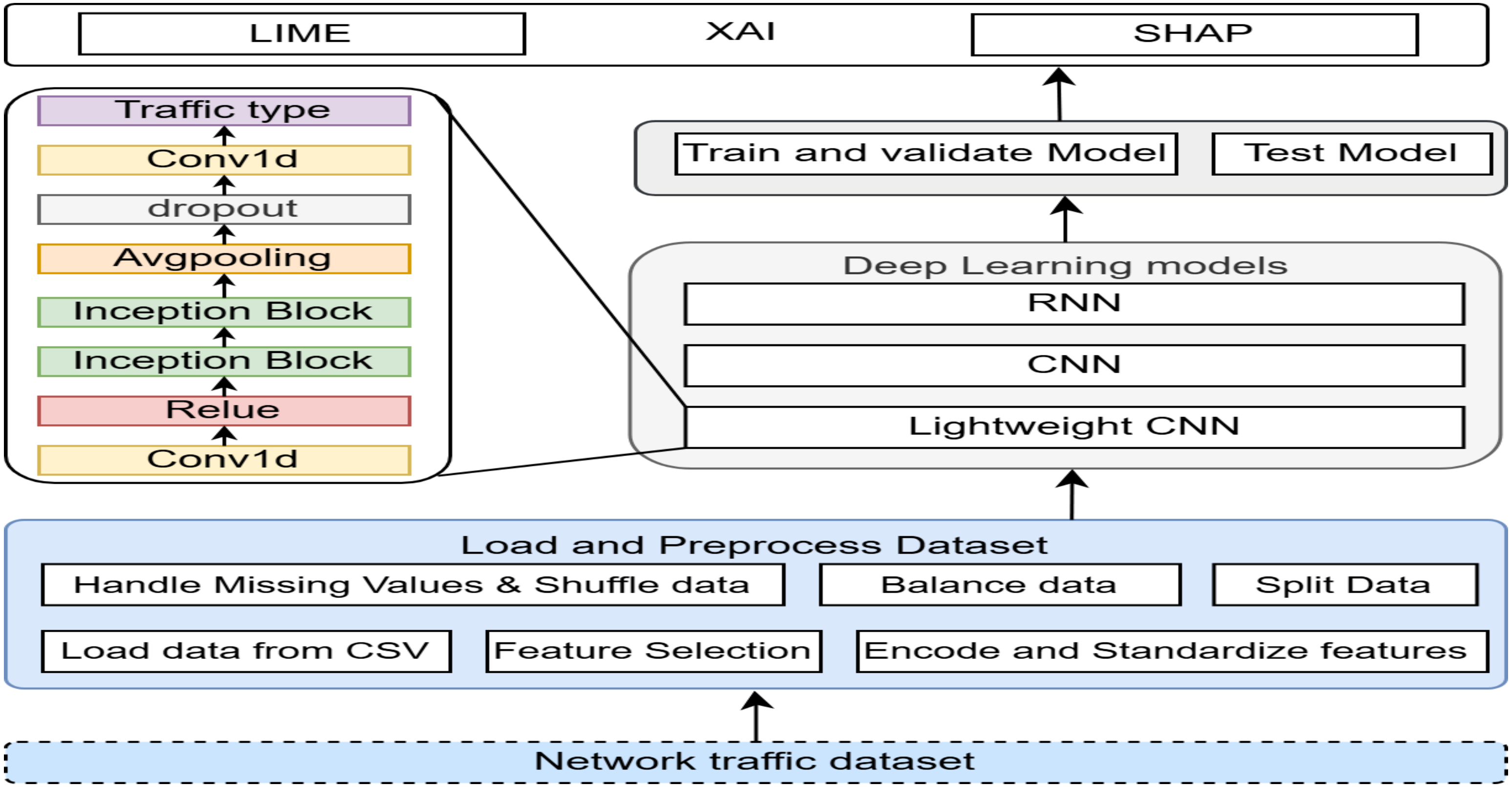
Feature Selection for Edge-IoT Network Traffic Classification



- Proposes a feature selection mechanism called Ensemble Weight Approach (EWA) for selecting significant features for Internet traffic classification based on multi-criterion ranking and selection mechanisms.
- EWA-selected features improve the mean accuracy up to 1.3% and reduce RMSE using fewer features than other feature selection methods. The smaller number of features directly contributes to shorter classification time.

*B Mohamed, **M. Hamdan et al.**, Edge Computing Intelligence Using Robust Feature Selection for Network Traffic Classification in Internet-of-Things. IEEE Access, 2020.*

XAI for Lightweight Network Traffic Classification using CNN



•**Depthwise-Separable CNN (DSC)**

•Replaces heavy 2-D kernels with **depthwise + 1×1 pointwise** ops

•Two *Inception* blocks (kernels 11/19/27) + GroupNorm → **30 k parameters**

•**Width-multiplier scaling**

•Dynamically shrinks channel counts (e.g., 32→24) for extreme compactness

•Cuts **85–95 %** of multiply-adds vs. standard conv nets

•**Prediction / Explanation decoupled**

•Core model runs **millisecond-latency** at the edge

•On-demand XAI path → *LIME* (local) & *SHAP* (global) reason about each flow

*M. Ghaleb, **M. Hamdan et al.**, Explainable AI for Lightweight Network Traffic Classification using Depthwise-Separable Convolutions. IEEE OJ CS, 2025.*

Results and Discussion

Datasets:

- **Unicauca flows**: 3.6 M records, 15 balanced classes
- **UT MobileNetTraffic'21**: 14 mobile apps, encrypted

Model	Params	FLOPS	Accuracy	CPU Inf.
CNN-baseline	2.8 M	9.94 M	99.90 %	1.3 s
RNN	4.1 M	2.55 M	98.53 %	25 s
DSC-Light (ours)	**30.6 k**	**0.63 M**	**99.96 %**	**1.5 s**

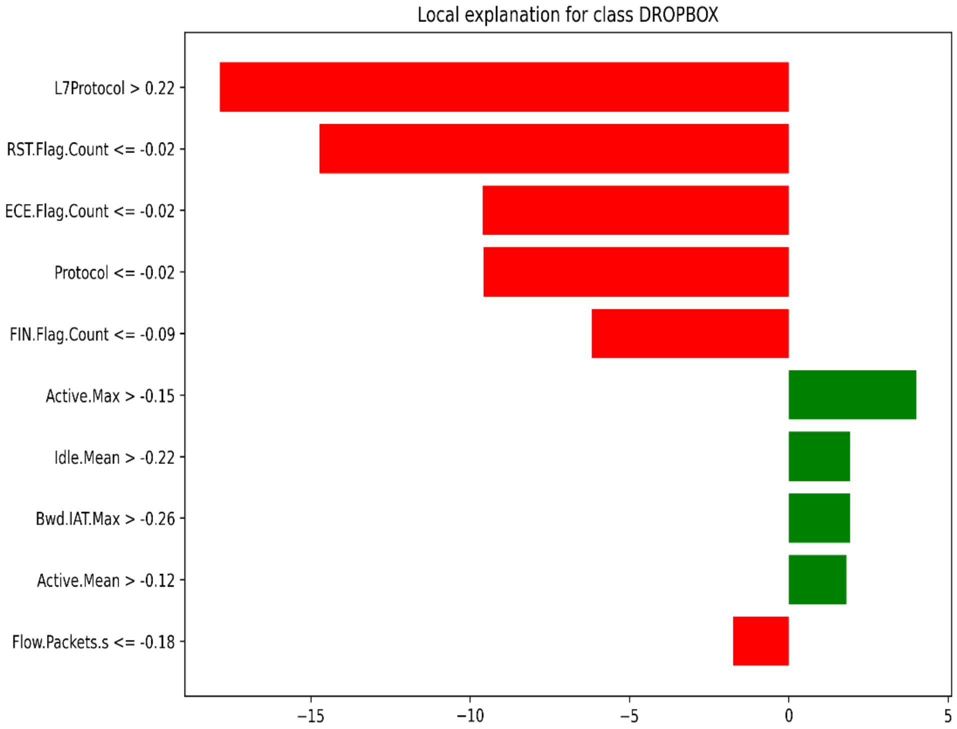
Highlights:

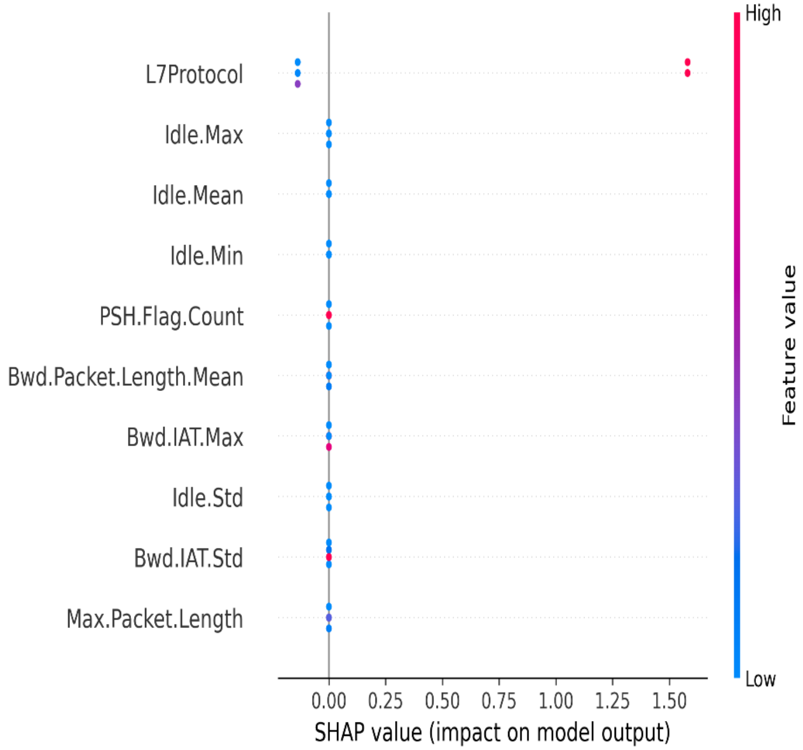
- ≈ **16×** fewer FLOPS & **91×** smaller than CNN, while matching Ulfar-grade accuracy
- Max per-class error ≤ 0.13 % (see confusion matrix)
- 70.6 % accuracy on small UT-MobileNet set after SMOTE
- XAI top drivers: *L7 Protocol*, *Idle.Time* stats, TCP-flag counts

*M. Ghaleb, **M. Hamdan et al.**, Explainable AI for Lightweight Network Traffic Classification using Depthwise-Separable Convolutions. IEEE OJ CS, 2025.*

Results and Discussion-2

Explainability: LIME & SHAP Insights:





•**Local view (LIME):** for a "Dropbox" flow, negative weight from *L7Protocol* & TCP flag counts explains rejection; *Idle* stats raise confidence.
•**Global view (SHAP):** top drivers across all classes → *L7Protocol*, *Idle.Max/Mean/Min*, *Bwd.IAT.Max*.
•Confirms model's focus on protocol semantics & burst-idle timing rather than packet size alone.
•**No runtime hit:** explanations computed offline; core DSC-CNN latency unchanged.

*M. Ghaleb, **M. Hamdan et al.**, Explainable AI for Lightweight Network Traffic Classification using Depthwise-Separable Convolutions. IEEE OJ CS, 2025.*

Challenges & Future Work

What still needs work?

Runtime overhead→ Ultra-light, hardware-aware explainers that stay within µ-seconds on gateways

Domain-specific XAI→ Protocol-aware, multi-view explanations that make sense to net-ops teams

Standardization gap→ Community metrics & open benchmarking suites for NTA-XAI

Where we're headed / Why it matters

Foundation models for NTA Self-supervised pre-training on raw packet sequences to boost zero-shot accuracy

Continual XAI Explanations that adapt online to drift & streaming updates

Unified SDN + Edge + XAI framework (our work) Proves efficiency + accuracy + transparency can coexist & paves the way for domain-tailored, always-on explainability

Thank you!

mosab.mohamed@ncirl.ie