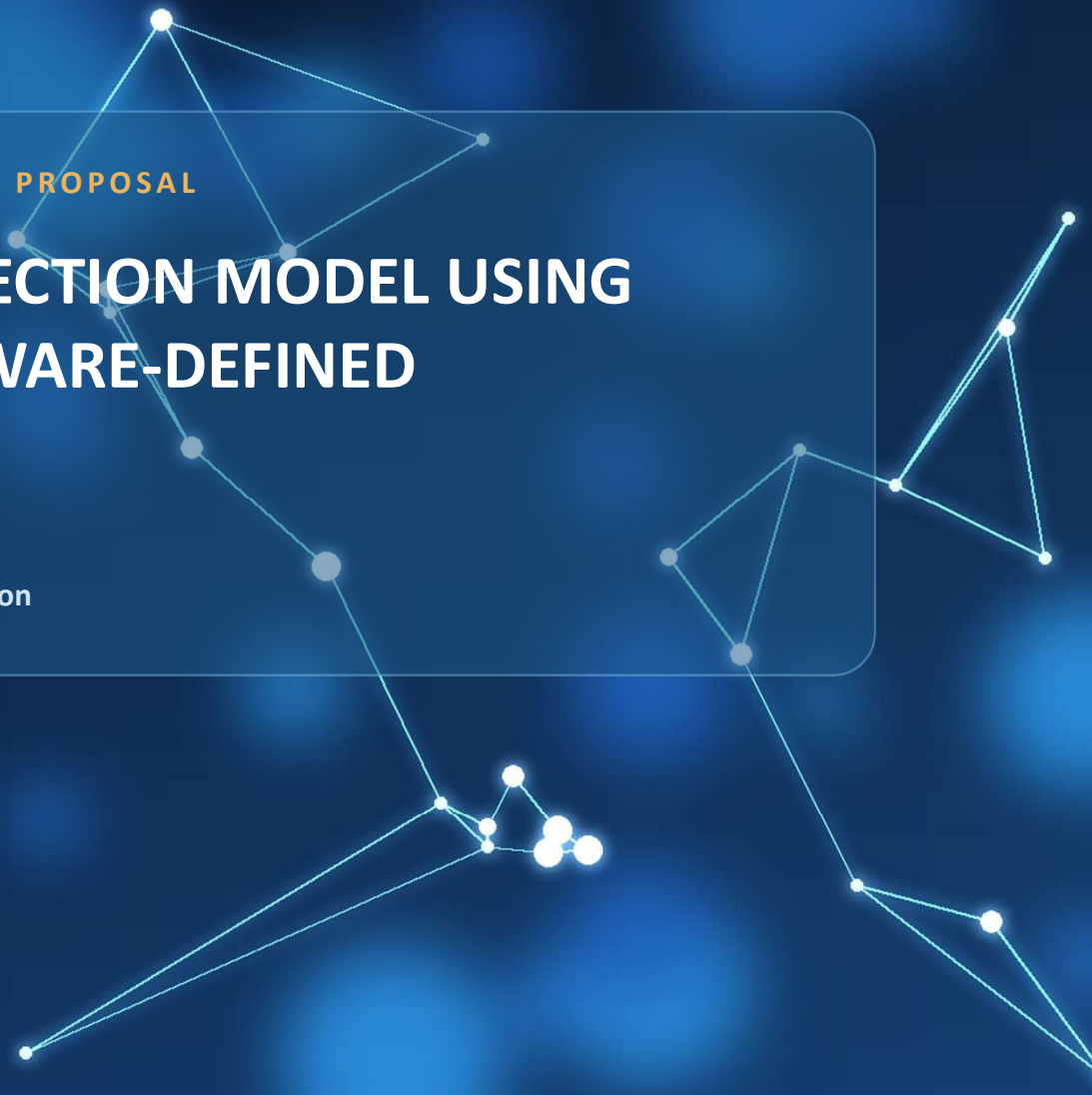
GENERAL SESSIONS · RESEARCH COLLABORATION PROPOSAL

CROSS-COUNTRY THREAT DETECTION MODEL USING MACHINE-LEARNING IN SOFTWARE-DEFINED NETWORKING

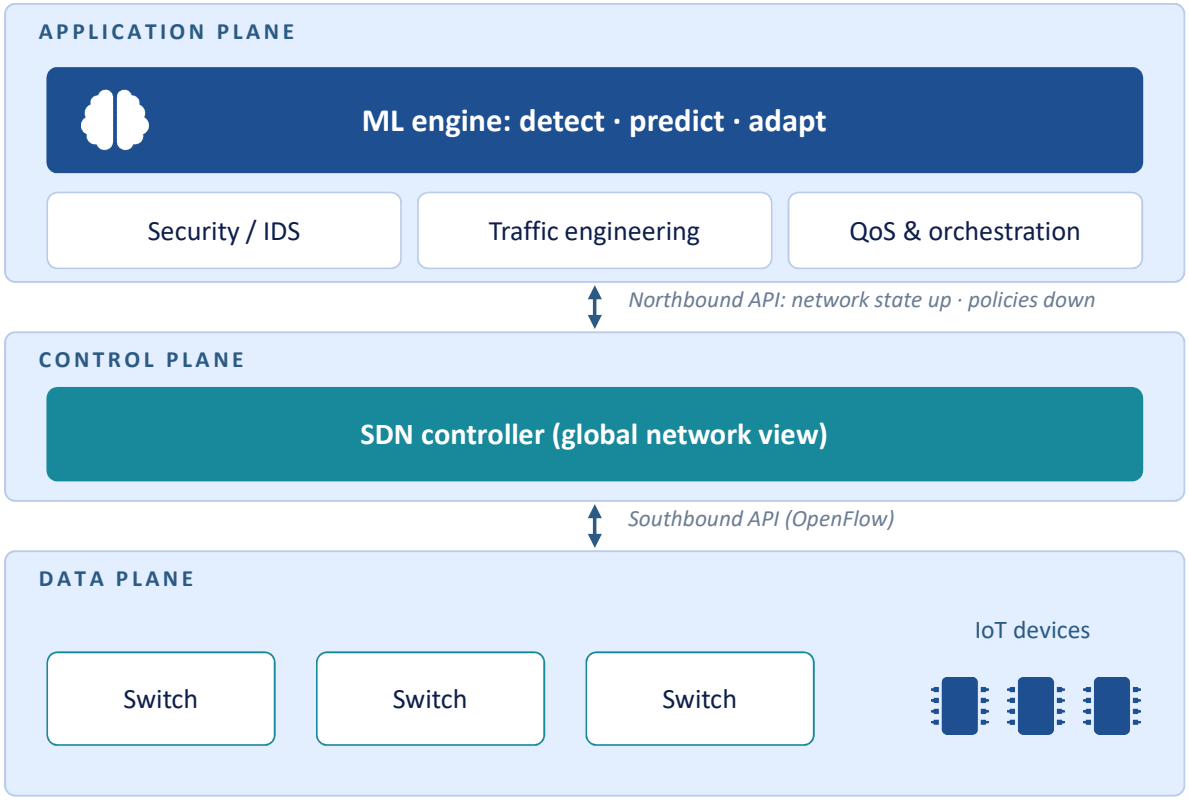
Invitation to collaborate: federated learning · model generalisation

Abdullah Kamaruddin, Tan Saw Chin

Multimedia University (MMU), Malaysia



SDN + ML: powerful, but fragile



WHAT BREAKS WHEN ML MEETS REAL NETWORKS

Distribution shift

Accuracy drops when traffic differs from the training data

Resource & real-time limits

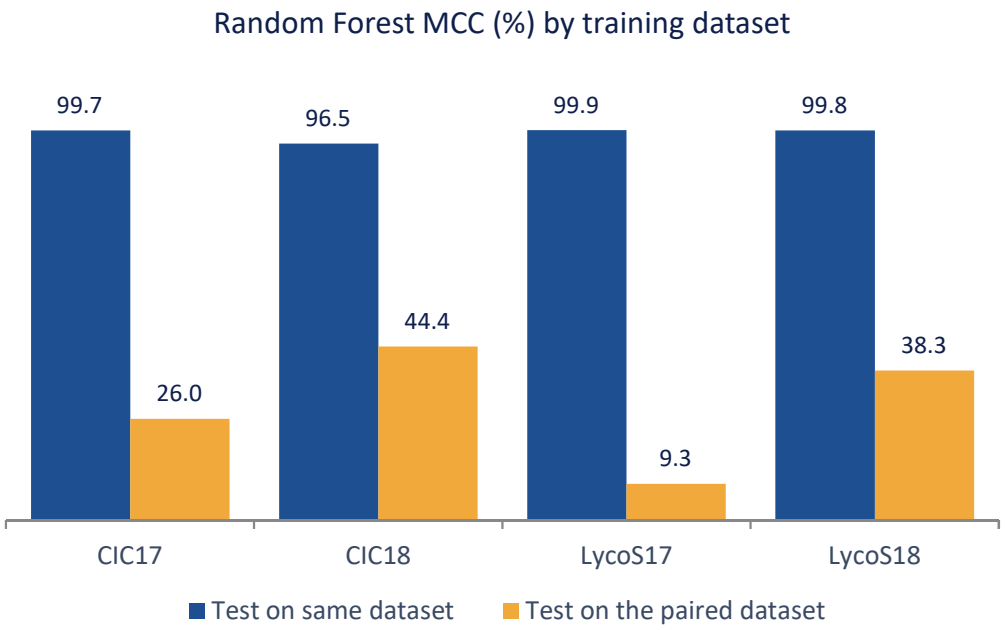
Edge devices, tight latency budgets

Data availability & privacy

Raw traffic is hard to collect and share

Sources: SDN planes after Kreutz et al. [1]; ML-in-SDN challenges after project brief and [2].

ML detectors fail across borders



TARGET 1

Cross-country threat detection

Federated learning: train across countries, keep data private

TARGET 2

Transfer & adaptation

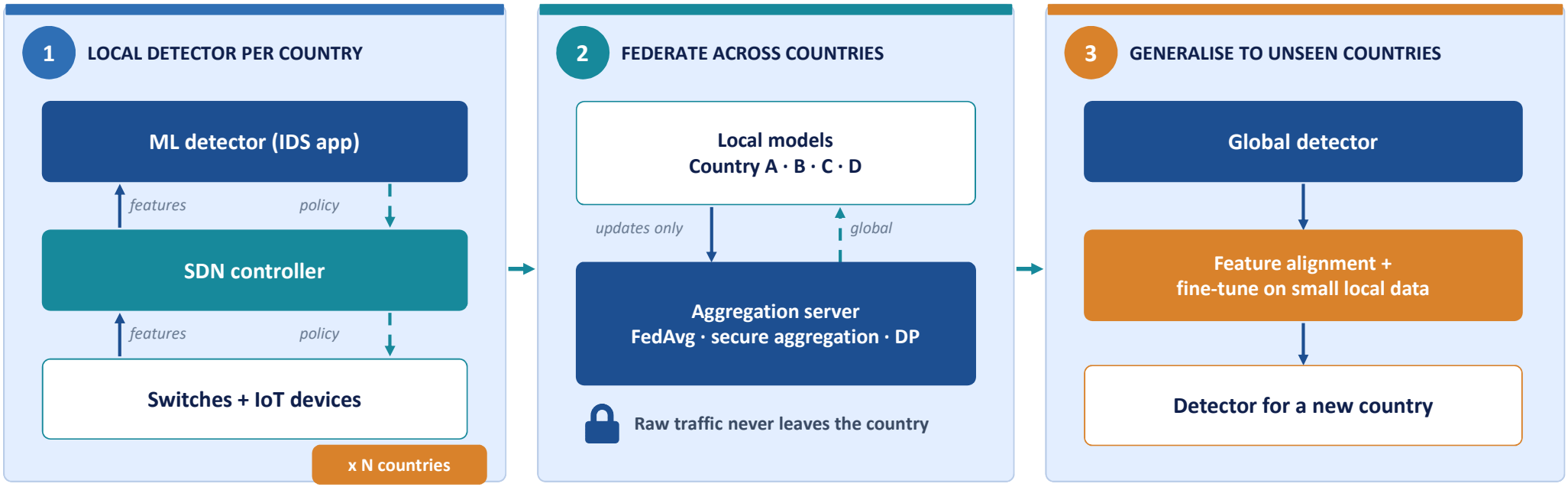
Model generalisation: train in one country, work in others

WHY COUNTRIES DIFFER

- Laws & rules
- Time zones & routines
- Economy & activity
- Traffic patterns

Source: [2] Cantone et al., IEEE Access 2024 (MCC; pairs CIC17-CIC18 and LycoS17-LycoS18; four public datasets). Targets from project brief.

Our proposal: train together, detect anywhere



4 EVALUATE

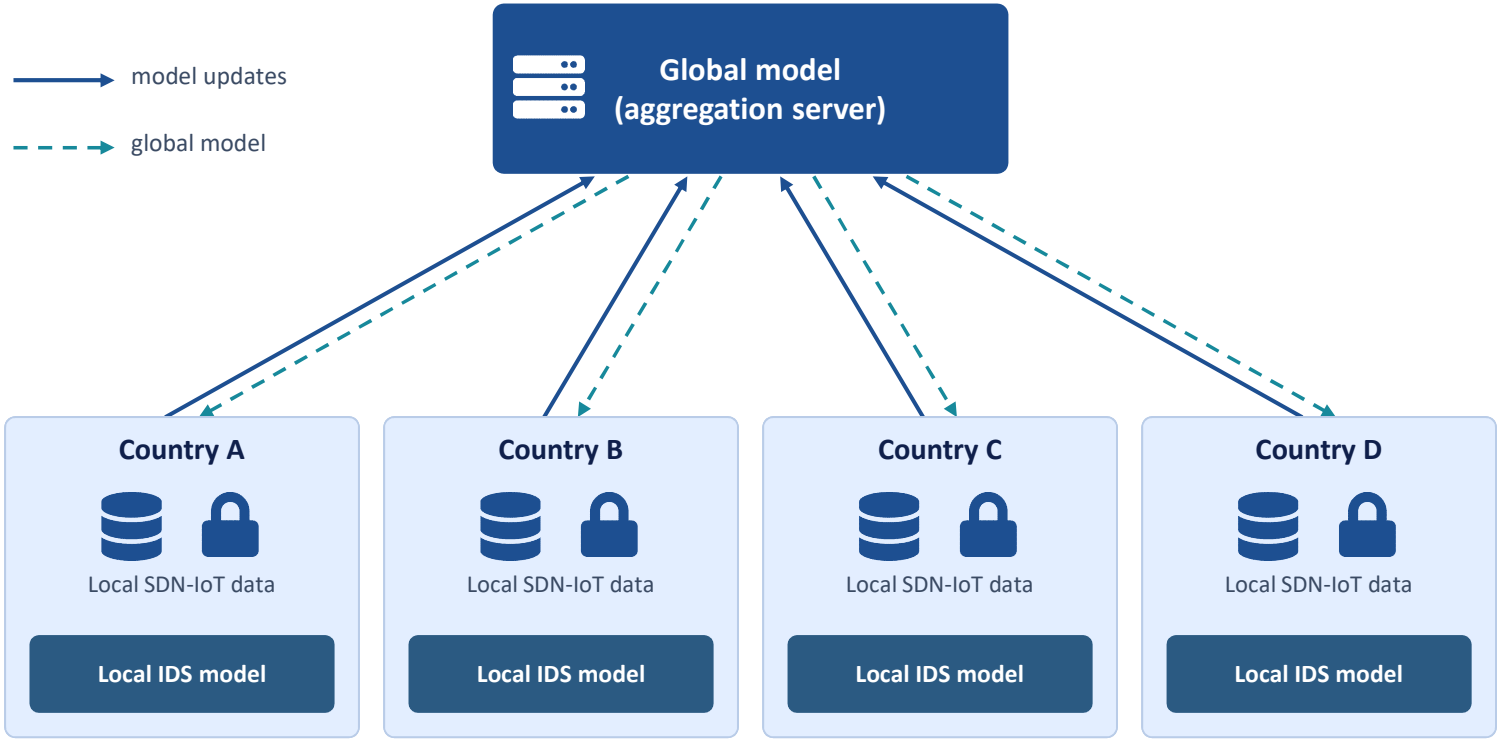
Cross-country test grid · generalisation gap · stability of selected features (Kuncheva, Nogueira)

5 SHARE

Open framework · anonymised multi-country dataset · guidelines for standards bodies

Proposed framework (authors' design). ML as an SDN application [1]; federated learning [3][4][5][6]; transfer and adaptation [10]; evaluation [2][50]; anonymisation [34].

Federated learning: train together, share no raw data

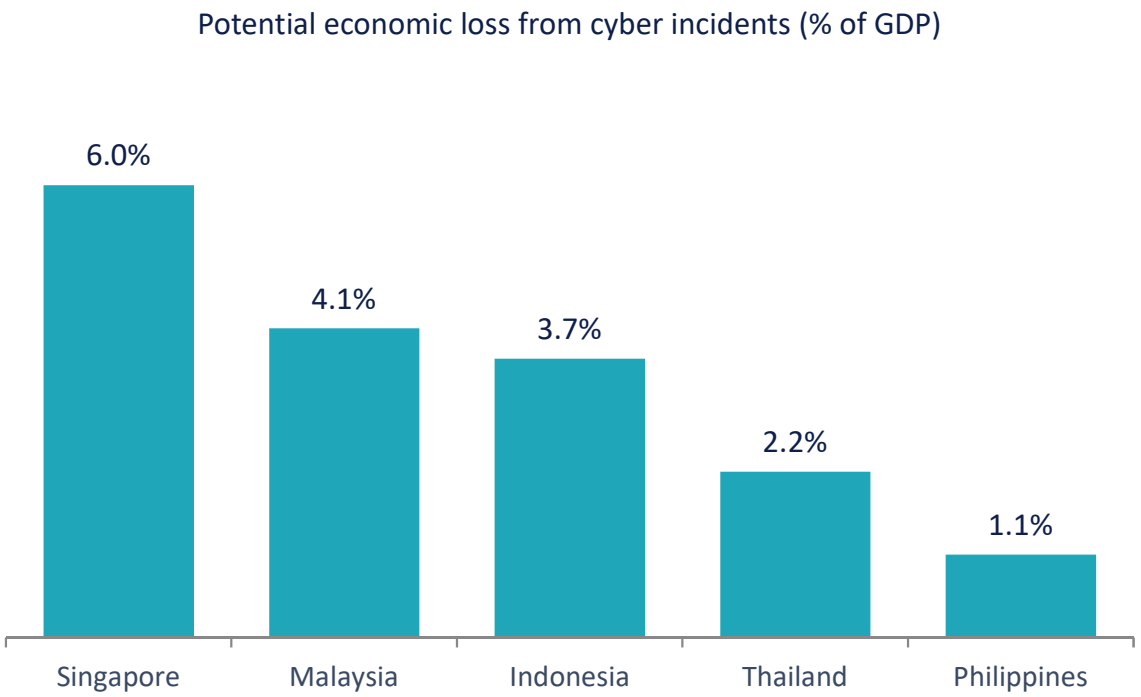


1. **Train locally**
2. **Send updates only**
3. **Aggregate (FedAvg)**
4. **Return global model**

Raw data never leaves the country | **Secure aggregation** | **Differential privacy**

Sources: FL principle [3][4]; FedAvg [5]; privacy mechanisms [3]; FL + DNN inside SDN for IoT [6]. Countries are illustrative.

Attack losses differ by country



135,000+ ransomware attacks recorded in Asia & South Pacific, 2024

+92% rise in DDoS attacks in Asia & South Pacific, 2024 vs 2023

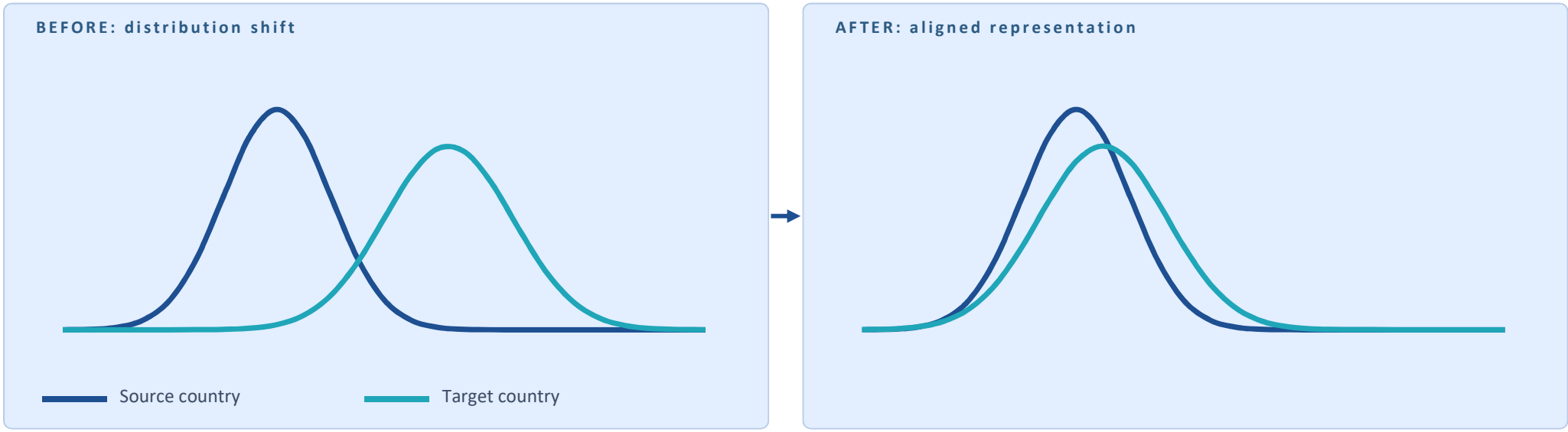
6.5 B cyber threats detected and mitigated in the region, 2024

Asia-Pacific total: potential loss above 7% of regional GDP (US$1.745 trillion) · modelled estimates, not audited losses

Sources: potential loss, % of GDP, Frost & Sullivan for Microsoft, 2018 (SG, MY, ID, TH) [7]; Philippines [8]; regional figures INTERPOL [9]. Malaysia reported as 'more than 4%'.

Generalisation: carry knowledge across countries





Curves are illustrative. Sources: transfer learning to narrow distribution gaps [10]; cross-dataset generalisation gap [2][11].

Different traffic, lower detection accuracy

ASEAN IN CLOUDFLARE'S GLOBAL TOP 10, Q4 2025



Rank 1 = most attacked location / largest source of DDoS traffic. Indonesia stays #3 source in H1 2026 [13].

Other ASEAN states are not shown where the sources do not list them.

94.6% → 29.4%

average MCC, same dataset vs a different dataset [2]

–30.45%

average AUROC drop for unsupervised models tested on another dataset [14]

Benign ≠ attack

benign traffic partly transfers; DoS, DDoS and backdoor classes barely do [11]

Sources: rankings [12][13] (Cloudflare network data); detection loss [2][11][14]. Rankings reflect where botnet nodes sit, not the location of attackers.

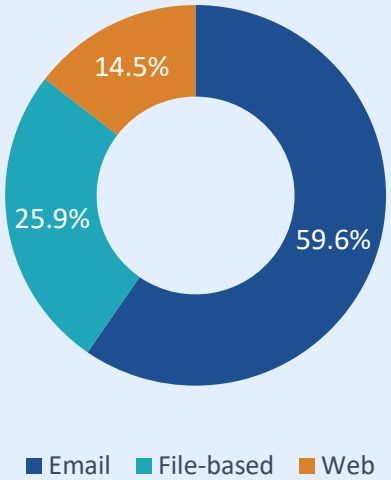
Implementation & experiments

SDN-IoT traffic per country → Pre-process & align features → Local training (DNN) → FL aggregation (FedAvg) → **Cross-country evaluation**

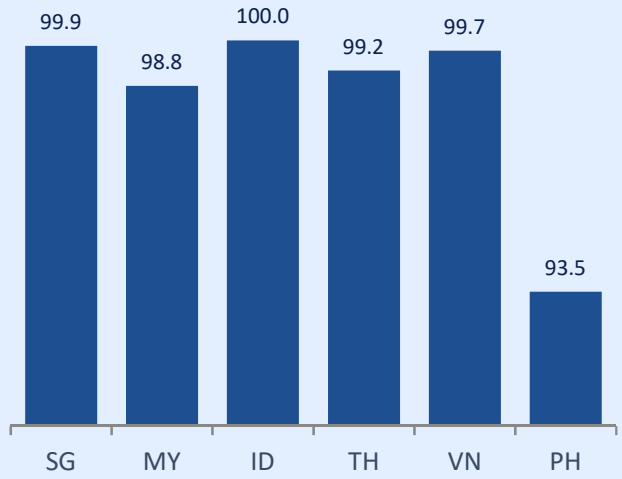
DATA SOURCES

- **Public benchmarks: UNSW-NB15 · TON_IoT · CIC-IDS**
- **Partner-country SDN-IoT traffic**
- **INTERPOL threat statistics**
- **ITU cyber-maturity index**

THREAT TRAFFIC BY VECTOR, ASIA & SOUTH PACIFIC 2024



ITU GLOBAL CYBERSECURITY INDEX 2024 (AXIS FROM 90)



Sources: threat mix [9] (Trend Micro data via INTERPOL); GCI scores [15] (Philippines Tier 2, others Tier 1); benchmark datasets [2][11]; SDN-specific datasets needed [16].

Generalisation evaluation: metrics and protocol

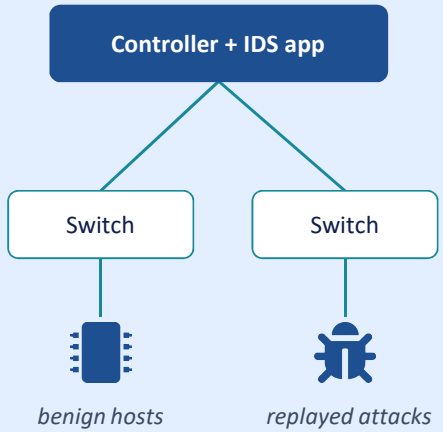
CROSS-COUNTRY TEST GRID

Train on \ Test on	A	B	C	D
A	in	cross	cross	cross
B	cross	in	cross	cross
C	cross	cross	in	cross
D	cross	cross	cross	in

Dark = in-country baseline · light = unseen country

Detection	Accuracy · Precision · Recall · F1
Imbalance-robust	MCC · AUROC
Operational	False-alarm rate · Latency
Federated	Comm. rounds & bytes · Privacy budget (ε)
Stability	Kuncheva index · Nogueira stability (next slide)

FIELD TEST: SDN TESTBED



GENERALISATION GAP

$$\Delta M = M_{in} - M_{cross}$$

RELATIVE DROP

$$\Delta M / M_{in} \times 100\%$$

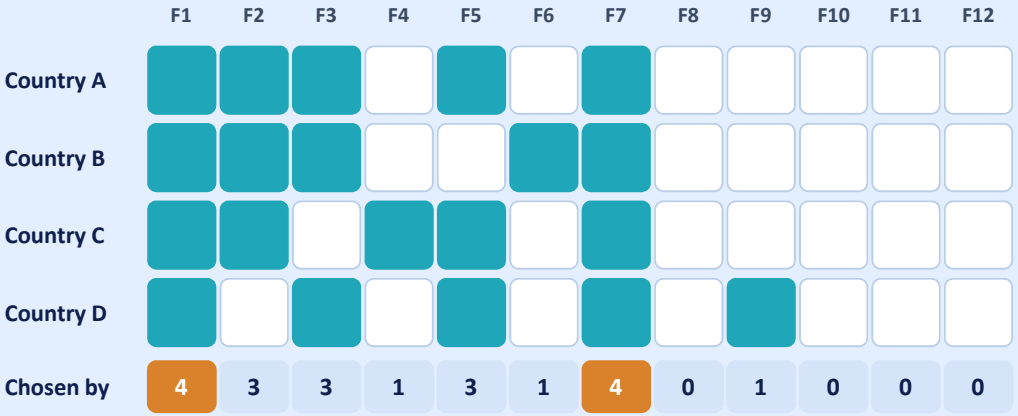
WORKED EXAMPLE [2]

94.6 → 29.4 MCC = −65.3 pts (−69%)

Metrics: MCC, F1, AUROC as in [2]; precision, recall, false-positive rate as in [11]; classification-performance assessment per ISO/IEC TS 4213 [17]. Countries A-D are placeholders.

Stability: do countries select the same features?

ILLUSTRATIVE FEATURE CHOICES PER COUNTRY (5 OF 12 FEATURES)



Kuncheva index = 0.49

Nogueira stability = 0.49

KUNCHEVA INDEX

$$KI(A,B) = (r \cdot d - k^2) / (k(d - k))$$

r = features shared by two subsets of size k out of d. Averaged over all pairs. 1 = identical, about 0 = chance.

NOGUEIRA STABILITY

$$\Phi = 1 - \text{mean}(s_f^2) / [\ (k/d)(1 - k/d)\ ]$$

s_f^2 = how much feature f flips between selections. Corrects for chance and allows different subset sizes. 1 = always the same.

REPORTING TEMPLATE (RESULTS TO COME)

Per classifier, across countries	RF	LR	DT
Kuncheva index	*to be measured*	*to be measured*	*to be measured*
Nogueira stability	*to be measured*	*to be measured*	*to be measured*
MCC on unseen countries (mean ± SD)	*to be measured*	*to be measured*	*to be measured*

Kuncheva index and Nogueira measure as defined and compared in [50]; stability scores used for IDS feature selection in [51]. Feature choices shown are illustrative.

Impact: scientific & technological

Siloed national data	Collaborative learning without sharing data
Dataset-specific models	Generalisable detection in unseen networks
Centralised IDS, single point of failure	Distributed, privacy-preserving IDS

BENCHMARK EVIDENCE: THE GAP WE TARGET

94.6%

to 29.4%

Average MCC of ML detectors tested on the same vs a different public dataset [2]. Benchmark data, not operator field data.

Telecoms, service providers & carriers were the most-attacked industry of 2025 [12]

Sources: gap [2] (reported averages, public benchmark datasets); most-attacked industry [12]; centralised-IDS limits and FL benefits [3][18][19].

Impact: privacy-compliant protection across ASEAN

ASEAN data-protection laws arrived at different times, with different transfer rules



Different rules

Cross-border data transfer is restricted or conditional

Federated: data stays local

Only model updates cross borders

Shared protection

One detector benefits every partner

10 ASEAN member states, one shared threat landscape

Sources: law years: MY [23], SG [24], TH [25], ID [26], VN [52]; transfer-rule divergence [20][21][22]; regional coordination: INTERPOL [27][28].

Policy & standards landscape

Layer	Policy and standard instruments	What it means for our design
Global	UN Convention against Cybercrime (adopted 2024) [29] · UNESCO Recommendation on the Ethics of AI (2021) [30] · OECD AI Principles (2019, updated 2024) [31] · ISO/IEC 42001:2023 [32] · ISO/IEC TS 4213:2022 [17]	**Cross-border cyber cooperation; robust, transparent AI; a standard way to assess ML classifiers**
ASEAN	ASEAN Guide on AI Governance & Ethics (2024; GenAI 2025) [33] · Guide on Data Anonymisation (2025) [34] · Model Contractual Clauses (voluntary) [35] · DEFA: negotiations concluded May 2026, signing due Nov 2026 [35][36]	**Anonymised shared data; trusted cross-border data flows; one regional rulebook**
Europe	GDPR, Regulation (EU) 2016/679 [37] · EU AI Act, Regulation (EU) 2024/1689 [38] · NIS2 Directive (EU) 2022/2555 [39]	**Data minimisation by design; partners in France and Spain**
National	MY: PDPA 2010 [23], Cyber Security Act 2024 (Act 854) [40] · SG: PDPA 2012 [24] · TH: PDPA 2019 [25] · ID: Law No. 27/2022 [26] · VN: PDP Law 91/2025 [52]	**Raw traffic stays inside each country**

Sources: [29]-[40] and [52] as listed. DEFA status as reported in mid-2026 [36]: check whether it has been signed before presenting.

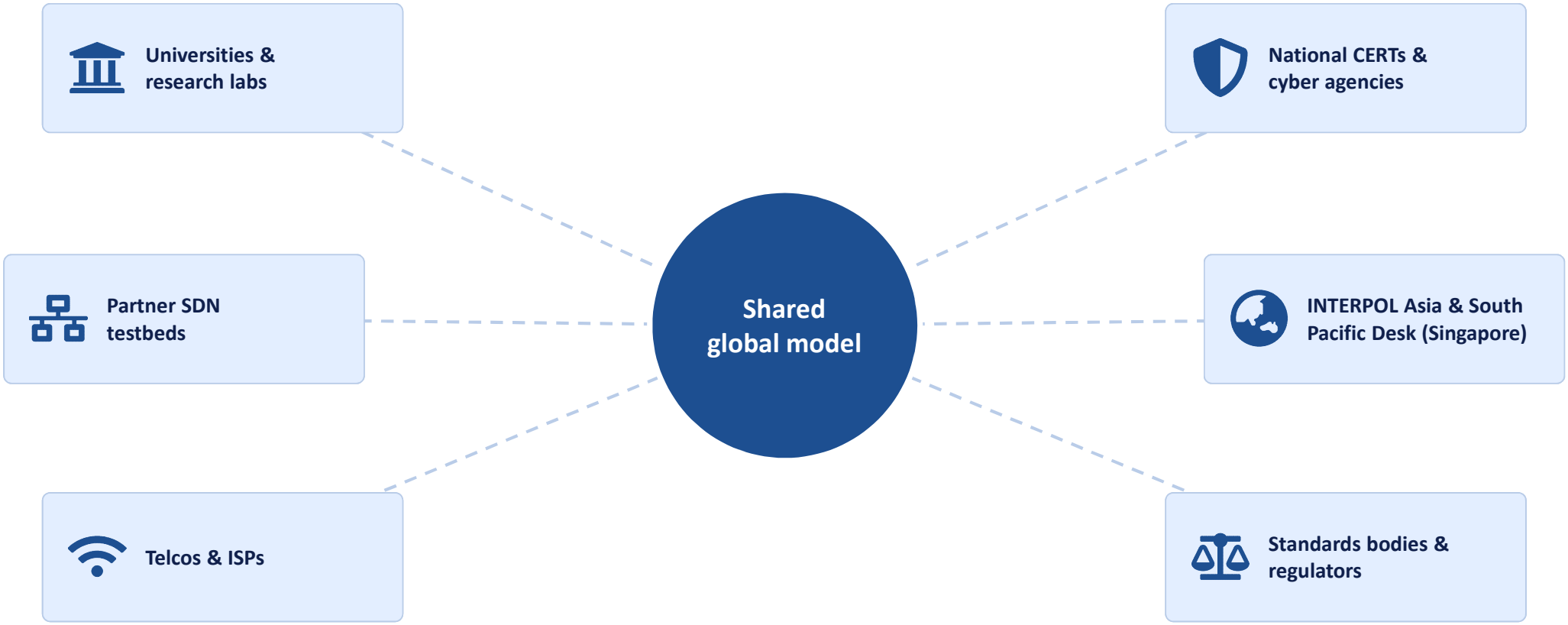
Our design vs policy principles

	Privacy & data protection GDPR [37] · ASEAN anonymisation [34]	**Transparency & accountability** OECD [31] · UNESCO [30]	**Robustness & security** OECD [31] · ISO/IEC 42001 [32]	**Cross-border cooperation** UN Convention [29] · DEFA [36]	**Inclusive participation** UNESCO [30] · ASEAN AI Guide [33]
Raw traffic stays in each country	●	○	○	●	○
Secure aggregation + differential privacy	●	○	●	○	○
Anonymised public benchmark dataset	●	●	○	●	●
Open evaluation protocol & metrics	○	●	●	○	●
Multi-country partner network	○	●	○	●	●

Teal dot = principle addressed by the design choice (authors' mapping)

Mapping is the authors' own reading of [29]-[39]; it is an alignment argument, not a compliance claim or legal advice.

Impact: one network, many partners



Partner types are proposed. INTERPOL Asia & South Pacific Desk (Singapore) coordinates regional cyber operations [9].

Outputs: science and society

SCIENTIFIC

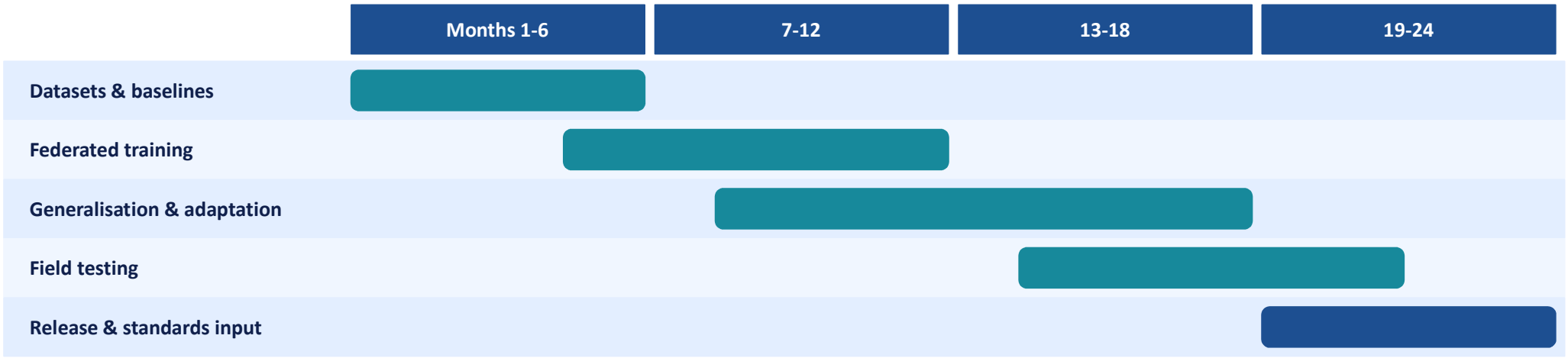
- **Open FL-based IDS framework for SDN**
- **Cross-country generalisation method**
- **Publications & benchmark results**

SOCIETAL

- **Public multi-country SDN-IoT dataset**
  anonymised, following ASEAN guidance [34]
- **Guideline documents for standards bodies**
- **Technology transfer to telcos & CERTs**

Proposed outputs. Need for realistic SDN-specific datasets and privacy-preserving collaboration: [16]. Anonymisation guidance: [34].

Outcomes: roadmap and partner network



PROPOSED PARTNER NETWORK

ASEAN

Malaysia (lead)

MMU

CyberSecurity Malaysia (MyCERT)

Indonesia

UMN (Universitas Multimedia Nusantara)

Vietnam

Danang University

Cambodia

Telecommunication Regulator of Cambodia (TRC)

EUROPE

France

Conservatoire national des arts et métiers (Cnam)

CEDRIC Laboratory

Spain

INCIBE-CERT

University of Extremadura

Partners are proposals to approach; no agreements implied. Bodies: [41]-[47]; FL-IDS groups: IMT Atlantique [48], University of Murcia [49]. Regional channel: INTERPOL [9]. Timeline illustrative.

Summary

TARGETS

- Detect threats across countries
- Keep each country's data private
- Generalise to unseen networks

METHOD

- Federated learning across borders
- Transfer learning & adaptation
- Validated on SDN-IoT testbeds

IMPACT

- Science: generalisable, private IDS
- Society: ASEAN-wide protection
- Collaboration: shared partners & data

Train together · share nothing raw · detect anywhere

THANK YOU

Questions & discussion

Abdullah Kamaruddin · Tan Saw Chin

Multimedia University (MMU), Malaysia

Invitation: partners in ASEAN and Europe for federated and transferable threat detection



References

[1] Kreutz, D., Ramos, F. M., Verissimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14-76.

[2] Cantone, M., Marrocco, C., & Bria, A. (2024). Machine learning in network intrusion detection: A cross-dataset generalization study. IEEE Access, 12. https://doi.org/10.1109/ACCESS.2024.3472907

[3] Matthew, K., & John-Dewole, T. (2025). Federated learning-driven intrusion detection in cloud-IoT settings: A security-centric survey. Lead City University Postgraduate Multidisciplinary Serials, 2025(1), 603-618.

[4] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2022). Federated learning for intrusion detection system: Concepts, challenges and future directions. Computer Communications, 195, 346-361.

[5] McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. Artificial Intelligence and Statistics (PMLR 54), 1273-1282.

[6] Dawood, R. N. (2026). Federated deep learning for intrusion detection in Internet of Things networks using software-defined networking. Ingénierie des Systèmes d'Information, 31(2), 625.

[7] Frost & Sullivan for Microsoft (2018). Understanding the cybersecurity threat landscape in Asia Pacific. Microsoft News Center country releases, May-Jul 2018 (SG, ID, TH, MY). news.microsoft.com

[8] The Asia Foundation (2022). Cybersecurity in the Philippines: Global context and local challenges (cites the 2018 Frost & Sullivan estimate of 1.1% of GDP).

[9] INTERPOL (2025/2026). Asia and South Pacific Cyber Threat Assessment Report 2025/2026. INTERPOL Asia and South Pacific Desk (ASPJOC), Singapore.

[10] Kheddar, H., Himeur, Y., & Awad, A. I. (2023). Deep transfer learning for intrusion detection in industrial control networks: A comprehensive review. Journal of Network and Computer Applications, 220, 103760.

[11] Iwanowski, M., Olszewski, D., Graniszewski, W., Krupski, J., & Pelc, F. (2025). The choice of training data and the generalizability of machine learning models for network intrusion detection systems. Applied Sciences, 15(15), 8466. https://doi.org/10.3390/app15158466

[12] Cloudflare (2026, 5 Feb). DDoS threat report for 2025 Q4. Cloudflare Blog / Radar. blog.cloudflare.com/ddos-threat-report-2025-q4

[13] Cloudflare (2026, 11 Aug). Cloudflare DDoS threat report H1 2026. Cloudflare Blog. blog.cloudflare.com/ddos-threat-report-2026-h1

[14] Verkerken, M., D'hooge, L., Wauters, T., Volckaert, B., & De Turck, F. (2022). Towards model generalization for intrusion detection: Unsupervised machine learning techniques. Journal of Network and Systems Management, 30.

[15] International Telecommunication Union (2024). Global Cybersecurity Index 2024 (5th ed.). Geneva: ITU.

[16] Batool, S., Aslam, M., Akpokodje, E., & Jilani, S. F. (2025). A comprehensive review of DDoS detection and mitigation in SDN environments: Machine learning, deep learning, and federated learning perspectives. Electronics, 14(21), 4222.

[17] ISO/IEC TS 4213:2022. Information technology - Artificial intelligence - Assessment of machine learning classification performance. Geneva: ISO/IEC.

[18] Rezaei, H., Taheri, R., Nowroozi, E., Hajizadeh, M., Shiaeles, S., & Bauschert, T. (2025). A survey on security and privacy in federated learning-based intrusion detection systems for 5G and beyond networks. IEEE Open Journal of the Communications Society, 7, 253-300.

[19] Hamad, N. A., Bakar, K. A. A., Qamar, F., Jubair, A. M., Mohamed, R. R., & Mohamed, M. A. (2025). Systematic analysis of federated learning approaches for intrusion detection in the Internet of Things environment. IEEE Access, 13, 95410-95444.

[20] Hoang Le, M. (2026). From fragmentation to interoperability: How the GDPR shapes ASEAN data privacy and cross-border data flows. Journal of Data Protection & Privacy, 8(3), 236-253.

[21] Hanyu, M., Yusoff, Z. B. M., & Romli, F. (2026). Data protection regulations in ASEAN: Current landscape and prospects for regional collaboration. UUMILC 2025, 633-648. Atlantis Press.

[22] Data governance landscape in major ASEAN countries (supplementary table, data to June 2025). Politics and Governance, Cogitatio Press.

[23] Malaysia. Personal Data Protection Act 2010 (Act 709).

[24] Singapore. Personal Data Protection Act 2012.

[25] Thailand. Personal Data Protection Act B.E. 2562 (2019).

[26] Indonesia. Law No. 27 of 2022 on Personal Data Protection.

[27] INTERPOL (2021, 22 Jan). INTERPOL report charts top cyberthreats in Southeast Asia. interpol.int/en/News-and-Events/News/2021/

[28] Lexology. lexology.com/library/detail.aspx?g=4a45c2f9-6e35-4de9-849b-4228fd174f96

[29] United Nations (2024). United Nations Convention against Cybercrime. Adopted 24 Dec 2024; open for signature in Hanoi, 25 Oct 2025. UNODC. unodc.org/unodc/en/cybercrime/convention/home.html

[30] UNESCO (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO.

[31] OECD (2019, updated 2024). Recommendation of the Council on Artificial Intelligence (OECD AI Principles). Paris: OECD.

[32] ISO/IEC 42001:2023. Information technology - Artificial intelligence - Management system. Geneva: ISO/IEC.

[33] ASEAN (2024, 2 Feb; 2025, 17 Jan). ASEAN Guide on AI Governance and Ethics; Expanded Guide - Generative AI. Via IMDA, ASEAN Working Group on AI Governance. imda.gov.sg

[34] Rajah & Tann Asia (2025). ASEAN data protection and generative AI guides issued at Digital Ministers Meeting (ASEAN Guide on Data Anonymisation). rajahtannasia.com

[35] ASEAN Briefing (2026). ASEAN's Digital Economy Framework Agreement (DEFA): What foreign businesses should know. aseanbriefing.com

[36] Rajah & Tann Asia (2026, 2 Jul). ASEAN DEFA negotiations concluded, targeted for signing in November 2026. rajahtannasia.com

[37] European Union (2016). Regulation (EU) 2016/679 (General Data Protection Regulation).

[38] European Union (2024). Regulation (EU) 2024/1689 (Artificial Intelligence Act).

[39] European Union (2022). Directive (EU) 2022/2555 (NIS2 Directive).

[40] Malaysia. Cyber Security Act 2024 (Act 854).

[41] CyberSecurity Malaysia. MyCERT (Malaysia Computer Emergency Response Team).

[42] Cyber Security Agency of Singapore (CSA). SingCERT.

[43] Electronic Transactions Development Agency (ETDA), Thailand. ThaiCERT.

[44] Badan Siber dan Sandi Negara (BSSN), Indonesia. ID-SIRTII/CC.

[45] Vietnam Computer Emergency Response Team Coordination Center (VNCERT/CC).

[46] Agence nationale de la sécurité des systèmes d'information (ANSSI), France. CERT-FR.

[47] Instituto Nacional de Ciberseguridad (INCIBE), Spain. INCIBE-CERT.

[48] IRISA SOTERN team, IMT Atlantique (2024, 7 Oct). PhD defense of L. Lavaur: Improving intrusion detection in distributed systems with federated learning. www-sotern.irisa.fr

[49] Mármol Campos, E., Fernández Saura, P., González-Vidal, A., Hernández-Ramos, J. L., Bernal Bernabé, J., Baldini, G., & Skarmeta, A. (2022). Evaluating federated learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks, 203, 108661.

[50] Nogueira, S., Sechidis, K., & Brown, G. (2018). On the stability of feature selection algorithms (defines and compares the Kuncheva index and Nogueira's measure). Journal of Machine Learning Research, 18(174), 1-54.

[51] Bouke, M. A., Abdullah, A., Cengiz, K., & Akleylek, S. (2024). Application of BukaGini algorithm for enhanced feature interaction analysis in intrusion detection systems. PeerJ Computer Science, 10, e2043. https://doi.org/10.7717/peerj-cs.2043

[52] Vietnam. Law on Personal Data Protection No. 91/2025/QH15 (passed 26 June 2025; effective 1 January 2026).