Free Full Text from Publisher View Full Text on ProQuest

Export Add To Marked List

1 of 3

Cognitive Detection at Big-Data Scale: A CNN-LSTM-DQN Framework with Prioritized Experience Replay for Cross-Attack-Family Generalization and Multi-Seed Initialization Sensitivity Analysis

By

Are you this author?

Rushendra (Rushendra) [1] ; Ramli, K (Ramli, Kalamullah) [1] ; Purnamasari, PD (Purnamasari, Prima Dewi) [1] ; Gunawan, TS (Gunawan, Teddy Surya) [2] ; Salman, M (Salman, Muhammad) [1]

Source BIG DATA AND COGNITIVE COMPUTING

View Journal Impact

Volume: 10 Issue: 7

DOI: 10.3390/bdcc10070239

Article Number 239

Published JUL 16 2026

Indexed 2026-07-31

Document Type Article

Abstract

Real-world IoT network security generates traffic at big-data scale with extreme class imbalance, temporal non-stationarity, and continuously evolving attack strategies that overwhelm static supervised classifiers. This paper presents a cognitive computing framework for network intrusion detection: a CNN-LSTM-DQN architecture with Prioritized Experience Replay (PER) evaluated on a 5,000,000-flow naturalistic sample of the TON_IoT Processed_Network dataset (4,000,000 training/1,000,000 temporally held-out test flows; 94.5% attack ratio) under a strict temporal split. The cognitive agent optimizes detection decisions using an Alerts per Million Flows (ARMF)-aware reward function that encodes both alert-fatigue cost and missed-attack penalty. We conduct a cross-attack-family generalization study: the methodology-architecture template, reward design, and hyperparameter calibration-is inherited from a framework previously validated on CSE-CIC-IDS2018, re-instantiated and retrained on the structurally different TON_IoT environment, and compared against the previously published benchmark. Initialization sensitivity is characterized across five independent random seeds using paired Wilcoxon signed-rank and t-tests. Across the five seeds, the proposed X2 model attains recall 0.833 +/- 0.306 and F1 0.874 +/- 0.241 (mean +/- sample SD), versus the supervised X1 baseline at 0.858 +/- 0.178 and 0.912 +/- 0.116; the best-performing seed (42) achieves 97.52% accuracy, 98.02% attack recall, 99.46% precision, and 98.73% F1-score on 1,000,000 held-out XSS flows-an attack family entirely absent from training-with temporal stability variances of 4.63 × 10(-7) (recall) and 1.38 × 10(-7) (F1). The X2 advantage observed among the four stable seeds is not statistically demonstrated at n = 5 (statistical power approximate to 5.1%); the initialization-sensitivity finding itself, including one degenerate alert-suppression seed, is reported as a primary contribution. A formal, exactly additive ARMF decomposition distinguishes the detected-attack (structural) component (99.46%) from the model-induced false-positive component (0.54%), and we report a multi-seed, ARMF-aware cognitive IDS evaluation on naturalistic TON_IoT traffic under an unseen-attack-family test condition that, to the best of our knowledge, has not been reported in the surveyed RL-based NIDS literature.

Keywords

Author Keywords: big data security; cognitive computing; intrusion detection system; deep reinforcement learning; CNN-LSTM; prioritized experience replay; TON_IoT; cross-attack-family generalization; multi-seed sensitivity analysis; ARMF; IoT network security; class imbalance at scale

Author Information

Corresponding Address: Ramli, Kalamullah; Salman, Muhammad (corresponding author)

Univ Indonesia, Dept Elect Engn, Depok 16424, Jawa Barat, Indonesia

E-mail Addresses : kalamullah.ramli@ui.ac.id; muhammad.salman@ui.ac.id

Addresses :

[1] Univ Indonesia, Dept Elect Engn, Depok 16424, Jawa Barat, Indonesia

[2] Int Islamic Univ Malaysia, Dept Elect & Comp Engn, Kulliyyah Engn, Kuala Lumpur 50728, Malaysia

E-mail Addresses : rushendra91@ui.ac.id; kalamullah.ramli@ui.ac.id; prima.dp@ui.ac.id; tsgunawan@iium.edu.my; muhammad.salman@ui.ac.id

Data availability statement

The TON_IoT Processed_Network dataset used in this study is publicly available at https://research.unsw.edu.au/projects/toniot-datasets (accessed on 1 May 2026). All experimental result files generated in this study—including per-seed performance metrics, multi-seed combined results, statistical test outputs, DQN training curves, confusion matrices, FP/FN trade-off curves, temporal stability window metrics, and PCA projection data—will be deposited on Zenodo upon acceptance of this manuscript, with a permanent DOI assigned to ensure long-term accessibility. Model training scripts are available upon reasonable request to the corresponding author at kalamullah.ramli@ui.ac.id.

Conflict of interest statement

The authors declare no conflicts of interest.

Categories/ Classification

Research Areas: Computer Science

Web of Science Categories

Computer Science, Artificial Intelligence; Computer Science, Information Systems; Computer Science, Theory & Methods

Funding

View funding text

Funding agency	Grant number	Show All Details
Ministry of Research and Technology of the Republic of Indonesia (RISTEK)	PKS-291/UN2.RST/HKP.05.00/2025	Show details

+ See more data fields

Journal information

BIG DATA AND COGNITIVE COMPUTING

← View Journal Impact

eISSN	2504-2289
Current Publisher	MDPI, MDPI AG, Grosspeteranlage 5, CH-4052 BASEL, SWITZERLAND
Research Areas	Computer Science
Web of Science Categories	Computer Science, Artificial Intelligence; Computer Science, Information Systems; Computer Science, Theory & Methods

5.3
Journal Impact Factor ™ (2025)

0.91
Journal Citation Indicator ™ (2025)

Citation Network

In Web of Science Core Collection

0 Citations

Create citation alert

35
Cited References

→ View Related Records

How does this document's citation performance compare to peers?

Use in Web of Science

0
Last 180 Days

0
Since 2013

Learn more →

This record is from:

Web of Science Core Collection

- Emerging Sources Citation Index (ESCI)

Suggest a correction

If you would like to improve the quality

of the data in this record, please Suggest a correction

← Open comparison metrics panel

Data is from InCites Benchmarking & Analytics

35 Cited References

View as set of results

Showing 30 of 35 *(from Web of Science Core Collection)*

Clarivate

© 2026 Clarivate. All rights reserved.

Legal Center
Privacy Statement
Copyright Notice
Training Portal
Product Support
Newsletter
Cookie Policy
Manage cookie preferences
Data Correction
Accessibility Help
Terms of Use
Follow Us