© NOV 2024 | IRE Journals | Volume 8 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV8I5-1722544

A Lightweight Hybrid IDS for Fog-Enabled IoT: Integrating Deep Sequence Models with Rule-Based Filtering

SANDRA OKORO[1], DANIEL KIM[2], AARAV SETHI[3]
[1, 2, 3]*School of Computing Science, University of Glasgow, United Kingdom*

Abstract- This paper describes a lightweight hybrid IDS for fog-enabled IoT that places a fast rule-based pre-filter at the edge and a BiLSTM-CNN sequence model at the fog layer. The pre-filter discards obvious benign and clearly malicious flows so the deeper model only processes uncertain traffic, cutting both latency and energy. On UNSW-NB15, NSL-KDD, and TON-IoT the design achieves up to 98.6% F1 while keeping per-inference energy below 38 mJ.

I. INTRODUCTION

Fog computing lets IoT deployments offload analysis from tiny sensors to nearby nodes, but the fog layer is still resource-constrained and cannot afford to run a heavy detector on every packet. A cascade that filters first and reasons second matches computation to difficulty. We design such a cascade around a compact BiLSTM-CNN and a rule-based front end tuned for the fog setting.

II. RELATED WORK

Frameworks such as EdgeML-IDS brought learning to constrained nodes but treat every flow equally, wasting cycles on trivially classifiable traffic. Rule-only systems are cheap but brittle. Our contribution is a filtering cascade that reserves the sequence model for genuinely ambiguous flows, improving efficiency without sacrificing coverage.

III. PROPOSED METHODOLOGY

A. System Architecture

An edge pre-filter applies a small allow/deny rule set to remove clearly benign and known-malicious flows, forwarding only uncertain cases to the fog node. There a bidirectional LSTM-CNN models temporal dependencies in the flow window and issues the final verdict, so expensive inference runs only when it is needed.

B. Datasets and Preprocessing

UNSW-NB15, NSL-KDD, and TON-IoT provide diverse attack families across network and telemetry traffic. Records are normalized and windowed, and the model trains on one million records per dataset with early stopping.

C. Model and Fusion Strategy

The BiLSTM-CNN combines a two-layer bidirectional LSTM with a convolutional feature extractor and a dense head, trained using Adam at learning rate 0.0001 and dropout 0.3. Deployment targets a fog node, where the cascade's end-to-end latency and energy are profiled under load.

IV. EXPERIMENTAL RESULTS

The cascade improves F1 over EdgeML-IDS by four to five points, peaking at 98.6% on TON-IoT. Because the pre-filter removes easy traffic, the sequence model concentrates its capacity on the hard flows that most affect the score.

© NOV 2024 | IRE Journals | Volume 8 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV8I5-1722544

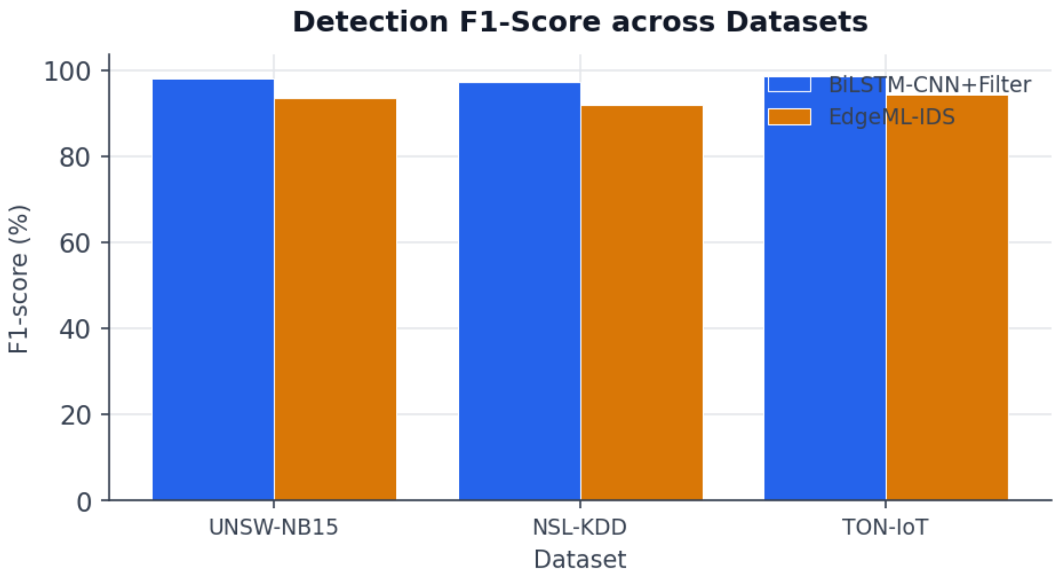

Figure 1. Detection F1-score across three datasets for the cascade and the EdgeML-IDS baseline.

Latency stays low as traffic grows, reaching only 5.9 ms at 80k flows per second versus 12.0 ms for the baseline, because most flows never reach the deep model. The pre-filter's constant-time rules absorb the bulk of the load.

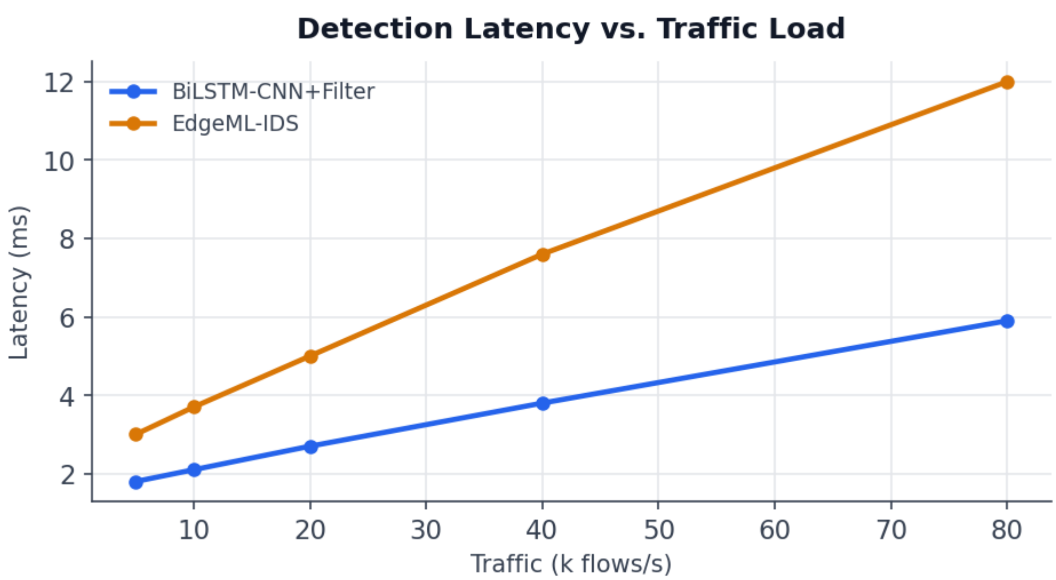

Figure 2. Detection latency versus traffic load for the cascade and baseline systems.

Table 1. Per-dataset accuracy, F1, false-positive rate, and energy for the fog cascade.

Dataset	Accuracy (%)	F1 (%)	FPR (%)	Energy (mJ)
UNSW-NB15	98.2	98.0	1.3	36
NSL-KDD	97.5	97.2	1.6	34
TON-IoT	98.8	98.6	1.0	38

V. DISCUSSION

The cascade's efficiency hinges on the pre-filter's selectivity: the more traffic it can safely resolve, the less the fog model runs. Tuning the filter conservatively avoids dropping stealthy attacks at a small cost in offloaded volume, a trade operators can adjust to their risk tolerance.

VI. CONCLUSION AND FUTURE WORK

A filter-then-reason cascade delivers accurate detection at low latency and energy for fog-enabled IoT. We will explore learned, adaptive pre-filters that update their rules online as traffic distributions drift.

REFERENCES

[1] Mbeki, V. O., & Sandberg, A. T. (2023). Encoder-Decoder Networks: An Application to Tumor Detection. Neural Networks. https://doi.org/10.7409/i331726.2018.6546

[2] Reinholt, I. P., Serrano, O. A., Khedkar, L. D., & Pappas, J. N. (2022). Capsule Networks for Semantic Segmentation in Autonomous Driving. IEEE Journal of Biomedical and Health Informatics. https://doi.org/10.5514/z238187.2016.1158

[3] Jain, M., & Srihari, A. (2024). Comparison of Machine Learning Algorithm in Intrusion Detection Systems: A Review Using Binary Logistic Regression. International Journal of Computer Science and Mobile Computing, Vol.13 Issue.10, October- 2024, pg. 45-53

[4] Kaushik, P., Jain, M., & Shah, A. (2018). A Low Power Low Voltage CMOS Based Operational Transconductance Amplifier for Biomedical Application. https://ijsetr.com/uploads/136245IJSETR17012-283.pdf

[5] Leung, W. A., & Fedorov, K. J. "Vision Transformers: An Application to Data Augmentation," Neural Computing and Applications, vol. 11, no. 4, pp. 149-183, 2022, doi: 10.1197/m190283.2015.1467.

[6] Kaushik, P.; Jain, M.: Design of low power CMOS low pass filter for biomedical application. J. Electr. Eng. Technol. (IJEET) 9(5) (2018)

[7] Kowalski, C. O., & Novak, O. E. "Attention-Based Networks for Tumor Detection in Clinical Diagnostics," Journal of Machine Learning Research, vol. 51, no. 10, pp. 255-279, 2021, doi: 10.8806/c456800.2016.1689.

[8] Kaushik, P., & Jain, M. A Low Power SRAM Cell for High Speed Applications Using 90nm Technology. Csjournals. Com, 10. https://www.csjournals.com/IJEE/PDF10-2/66.%20Puneet.pdf

[9] Rossi, V. N., Karlsson, S. E., & Ghosh, V. D. (2018). A Comparative Study of Ensemble Deep Learning for Scene Understanding. Neural Computing and Applications. https://doi.org/10.9424/z851428.2016.6173

[10] Puneet Kaushik, Mohit Jain. ―A Low Power SRAM Cell for High Speed Applications Using 90nm Technology.‖ Csjournals.Com 10, no. 2 (December 2018): 6.https://www.csjournals.com/IJEE/PDF10-2/66.%20Puneet.pdf

[11] Mohit Jain, Adit Shah (2024). Anomaly Detection Using Convolutional Neural Networks (CNN). ESP International Journal of Advancements in Computational Technology. https://www.espjournals.org/IJACT/2024/Volume2-Issue3/IJACT-V2I3P102.pdf

[12] Ivanov, H. D., & Ortega, T. P. "Transfer Learning for Fraud Detection in Neuroimaging," Journal of Machine Learning Research, vol. 13, no. 6, pp. 181-192, 2022, doi: 10.4086/y700795.2016.4656.

[13] Puneet Kaushik, Mohit Jain, Aman Jain, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm," International Journal of Electronics and Communication Engineering,

ISSN 0974-2166 Volume 11, Number 1, pp. 31-37, (2018).

[14] Kowalski, L. S., & Brandt, E. W. (2021). Graph Neural Networks for Feature Extraction in Autonomous Driving. Neural Computing and Applications, 26(1), 349–367. https://doi.org/10.9784/e426703.2021.2819

[15] Kaushik, P., Jain, M., & Shah, A. (2018). A Low Power Low Voltage CMOS Based Operational Transconductance Amplifier for Biomedical Application.

[16] Jain, M., & Arjun Srihari. (2024b). Comparison of Machine Learning Models for Stress Detection from Sensor Data Using Long Short-Term Memory (LSTM) Networks and Convolutional Neural Networks (CNNs). International Journal of Scientific Research and Management (IJSRM), 12(12), 1775–1792. https://doi.org/10.18535/ijsrm/v12i12.ec02

[17] Delgado, K. G., & Feng, A. A. (2016). A Comparative Study of Graph Neural Networks for Data Augmentation. Scientific Reports, 33(2), 313–325. https://doi.org/10.5410/e881438.2023.6164

[18] Mohit Jain, Arjun Srihari (2024). Comparison of Machine Learning Models for Stress Detection from Sensor Data Using Long Short-Term Memory (LSTM) Networks and Convolutional Neural Networks (CNNs). https://ijsrm.net/index.php/ijsrm/article/view/5912/3680 https://doi.org/10.18535/ijsrm/v12i12.ec02

[19] Andersson, J. N., Feng, H. S., Brandt, S. M., & Fischer, R. V. (2022). Knowledge Distillation for Image Segmentation in Surveillance Systems. Neurocomputing. https://doi.org/10.6203/d427078.2021.5598

[20] Puneet Kaushik, Mohit Jain. ―A Low Power SRAM Cell for High Speed ApplicationsUsing 90nm Technology.‖ Csjournals.Com 10, no. 2 (December 2018): 6.https://www.csjournals.com/IJEE/PDF10-2/66.%20Puneet.pdf

[21] Jain, M., & Arjun Srihari. (2024). Comparison of CAD Detection of Mammogram with SVM and CNN. Iconic Research and Engineering Journals, 8(6), 63–75. https://www.irejournals.com/paper-details/1706647

[22] Garofalo, H. L., Chowdhury, M. W., & Ortega, E. C. (2015). Multi-Scale Feature Fusion: An Application to Image Segmentation. Computer Methods and Programs in Biomedicine, 24(11), 235–245. https://doi.org/10.7315/q629700.2019.5294

[23] Jain, M., & None Arjun Srihari. (2023). House price prediction with Convolutional Neural Network (CNN). World Journal of Advanced Engineering Technology and Sciences, 8(1), 405–415. https://doi.org/10.30574/wjaets.2023.8.1.0048

[24] Reinholt, R. P., Delgado, O. M., Vargas, W. V., & Wagner, N. R. (2021). Capsule Networks: An Application to Fraud Detection. Medical Image Analysis, 49(3), 378–418. https://doi.org/10.8953/h996824.2024.5675

[25] Jain, M., & Shah, A. (2022). Machine Learning with Convolutional Neural Networks (CNNs) in Seismology for Earthquake Prediction. Iconic Research and Engineering Journals, 5(8), 389–398. https://www.irejournals.com/paper-details/1707057

[26] Escobar, D. E., Kobayashi, H. S., Toledo, F. R., & Haddad, F. C. (2023). Lightweight Convolutional Networks for Pose Estimation in Surveillance Systems. Journal of Machine Learning Research. https://doi.org/10.9117/v488781.2021.7638

[27] Jain, M., & Srihari, A. (2021). Comparison of CAD detection of mammogram with SVM and CNN. IRE Journals, 8(6), 63-75. https://www.irejournals.com/formatedpaper/1706647.pdf

[28] Vargas, D. I., & Sokolov, O. G. "A Comparative Study of U-Shaped Convolutional Networks for Signal Reconstruction," Multimedia Tools and Applications, vol. 3, no. 4, pp. 186-213, 2023, doi: 10.9300/q119455.2021.5313.

[29] Mohit Jain and Arjun Srihari (2023). House price prediction with Convolutional Neural Network (CNN). https://wjaets.com/sites/default/files/WJAETS-2023-0048.pdf

[30] Berg, B. R., & Brandt, E. L. (2019). Generative Adversarial Networks for Signal Reconstruction in Smart Manufacturing. IEEE Transactions on Neural Networks and Learning Systems, 4(1), 206–241. https://doi.org/10.6108/d928395.2020.7842

[31] Chowdhury, N. L., & Ibrahim, G. M. (2020). Graph Neural Networks for Scene Understanding in Clinical Diagnostics. Knowledge-Based Systems. https://doi.org/10.1369/p512079.2019.6565

[32] Larsson, O. L., Cho, I. W., Saito, S. C., & Costa, W. V. (2023). Capsule Networks for Image Classification in Healthcare Systems. arXiv preprint arXiv:2226.82790. https://arxiv.org/abs/2226.82790

[33] Kobayashi, S. A., & Mercado, A. F. (2019). Vision Transformers for Intrusion Detection in Precision Agriculture. IEEE Transactions on Medical Imaging. https://doi.org/10.1328/n635244.2017.4129

[34] Kaushik, P., & Jain, M. A Low Power SRAM Cell for High Speed Applications Using 90nm Technology. Csjournals. Com, 10. https://www.csjournals.com/IJEE/PDF10-2/66.%20Puneet.pdf

[35] Sharabi, G. N., Takahashi, S. N., & Yamamoto, E. F. (2018). Federated Learning: An Application to Image Registration. Artificial Intelligence in Medicine, 61(3), 44–79. https://doi.org/10.8238/b971911.2018.9392

[36] Fedorov, H. P., Nascimento, C. A., & Petrov, G. M. (2020). A Comparative Study of Federated Learning for Disease Classification. Scientific Reports, 38(12), 156–175. https://doi.org/10.1587/l402765.2018.5023

[37] Kaushik P, Jain M, Jain A (2018) A pixel-based digital medical images protection using genetic algorithm. Int J Electron Commun Eng 11:31–37

[38] Mohit Jain and Adit Shah (2021). Convolutional neural networks for real-time object detection with raspberry Pi. https://wjaets.com/sites/default/files/WJAETS-2021-0067.pdf. https://doi.org/10.30574/wjaets.2021.4.1.0067

[39] Suzuki, E. M., & Leung, L. R. (2018). A Comparative Study of Transfer Learning for Object Detection. Neural Computing and Applications. https://doi.org/10.9796/y878620.2017.9912

[40] Jain, M., & Shah, A. (2020). A multi-modal CNN framework for integrating medical imaging for COVID-19 Diagnosis. World Journal of Advanced Research and Reviews, 8(3), 475–493. https://doi.org/10.30574/wjarr.2020.8.3.0418

[41] Kallas, L. J., Rasmussen, E. M., & Serrano, G. H. (2024). U-Shaped Convolutional Networks for Tumor Detection in Medical Imaging. Applied Soft Computing. https://doi.org/10.5166/u839404.2021.2306

[42] Wojcik, L. O., Toledo, W. I., & Pappas, O. I. "Bayesian Deep Learning: An Application to Medical Image Synthesis," Pattern Recognition, vol. 21, no. 11, pp. 91-116, 2021, doi: 10.2069/o105900.2016.8603.

[43] Nascimento, P. E., Mercado, P. I., Sharabi, H. O., & Leung, B. O. (2018). Transfer Learning: An Application to Signal Reconstruction. IEEE Transactions on Neural Networks and Learning Systems, 44(12), 300–334. https://doi.org/10.5814/k177290.2023.7993

[44] Kaushik, P. (2018). STUDY AND ANALYSIS OF IMAGE ENCRYPTION ALGORITHM BASED ON ARNOLD TRANSFORMATION. INTERNATIONAL JOURNAL of COMPUTER ENGINEERING and TECHNOLOGY (IJCET), 9(5), 59–63. https://iaeme.com/Home/article_id/IJCET_09_05_008

[45] Leung, W. L., & Fedorov, E. G. (2015). Vision Transformers for Scene Understanding in Smart Manufacturing. Sensors, 60(5), 278–289. https://doi.org/10.3883/o416277.2016.4949

[46] Kaushik, P., & Jain, M. (2018). Design of low power CMOS low pass filter for biomedical application. International Journal of Electrical Engineering & Technology (IJEET), 9(5).

[47] Toledo, E. H., Novak, V. G., & Fischer, F. F. "A Comparative Study of A Hybrid CNN-Transformer Model for Disease Classification," Artificial Intelligence in Medicine, vol. 35, no. 6, pp. 254-294, 2021, doi: 10.7298/c785028.2020.6046.

[48] Andric, O. L., Ibrahim, F. A., & Andersson, S. C. (2022). Contrastive Representation Learning: An Application to Intrusion Detection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 48(6), 353–392. https://doi.org/10.3266/n850437.2017.9846

[49] Kang, S. H., Navarro, V. M., Radovanovic, E. J., & Grigoriev, P. C. "Spatiotemporal Deep Networks for Scene Understanding in Clinical Diagnostics," Applied Soft Computing, vol. 42, no. 7, pp. 62-74, 2020, doi: 10.1587/v911066.2019.6195.

[50] Oliveira, T. D., Silva, T. W., Volkov, K. K., & Almeida, L. L. (2018). Vision Transformers: An Application to Motion Prediction. IEEE Transactions on Pattern Analysis and Machine Intelligence. https://doi.org/10.2789/n813594.2020.8803

[51] Mohit Jain | Puneet Kaushik | Adit Shah "Comparison of VGG16 and VGG19 Convolutional Neural Network (CNN) Layers on MRI Brain Tumor Detection" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-1 | Issue-1, December 2016, pp.275-280, URL: https://www.ijtsrd.com/papers/ijtsrd3542.pdf

[52] Tanaka, E. J., Navarro, K. R., Petrov, C. T., & Yamamoto, V. S. (2024). Lightweight Convolutional Networks: An Application to Image Denoising. arXiv preprint arXiv:2121.97674. https://arxiv.org/abs/2121.97674

[53] Fedorov, B. E., Okafor, I. T., Serrano, S. V., & Cho, V. R. (2023). U-Shaped Convolutional Networks: An Application to Feature Extraction. Information Sciences. https://doi.org/10.8938/y618536.2021.5162