© DEC 2024 | IRE Journals | Volume 8 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV8I6-1722545

Real-Time Intrusion Detection at the IoT Edge: A Hybrid Neural and Rule-Based Framework with Adaptive Fusion

BEATRIZ SANTOS[1], OMAR FAROUK[2], NISHA KAPOOR[3]
[1, 2, 3]Department of Information Systems, RMIT University, Melbourne, Australia

Abstract-* *We propose a real-time IoT intrusion detector that fuses a Transformer-LSTM neural engine with a signature rule engine through an adaptive fusion controller. Rather than fixing the balance between the two, the controller learns per-flow weights from recent reliability, trusting rules on familiar traffic and the neural model on novel patterns. On IoT-23, BoT-IoT, and CIC-IDS-2018 the system attains up to 99.4% F1 with false positives as low as 0.6%, all within a real-time latency budget.

I. INTRODUCTION

Static fusion of neural and rule-based detectors is brittle because the right weighting shifts with the traffic mix: during a known flood, rules should dominate, while a novel exploit demands the learned model. An adaptive controller that reweights the two engines online can track these shifts. We build such a controller on top of a Transformer-LSTM engine for real-time IoT defence.

II. RELATED WORK

Systems like DeepEdgeIDS achieve strong accuracy but combine components with fixed weights, and signature engines alone cannot follow evolving attacks. Attention-based detectors capture long-range dependencies yet are rarely fused adaptively with rules. Our adaptive-fusion design fills this gap, adjusting trust dynamically from observed reliability.

III. PROPOSED METHODOLOGY

A. System Architecture

A Transformer-LSTM engine encodes flow sequences with self-attention over an LSTM backbone, while a signature engine flags known patterns. An adaptive-fusion controller maintains a running reliability estimate for each source and blends their scores with weights that update per flow, favouring whichever engine has been more trustworthy on similar recent traffic.

B. Datasets and Preprocessing

IoT-23, BoT-IoT, and CIC-IDS-2018 supply modern attack traces including botnets, DDoS, and multi-stage intrusions. Features are normalized and windowed, with 1.4 million records per dataset used for training and a temporal split for evaluation.

C. Model and Fusion Strategy

The neural engine couples a two-layer LSTM with a four-head self-attention block and a dense classifier, trained with Adam at learning rate 0.0001 and dropout 0.3. The fused detector runs on an edge node where end-to-end latency and energy are measured under increasing load.

IV. EXPERIMENTAL RESULTS

Adaptive fusion lifts F1 above both single engines and the DeepEdgeIDS baseline, reaching 99.4% on BoT-IoT and holding 98.2% on the diverse CIC-IDS-2018. The controller's per-flow reweighting is most valuable on mixed traffic where a fixed weight would misjudge one attack class.

© DEC 2024 | IRE Journals | Volume 8 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV8I6-1722545

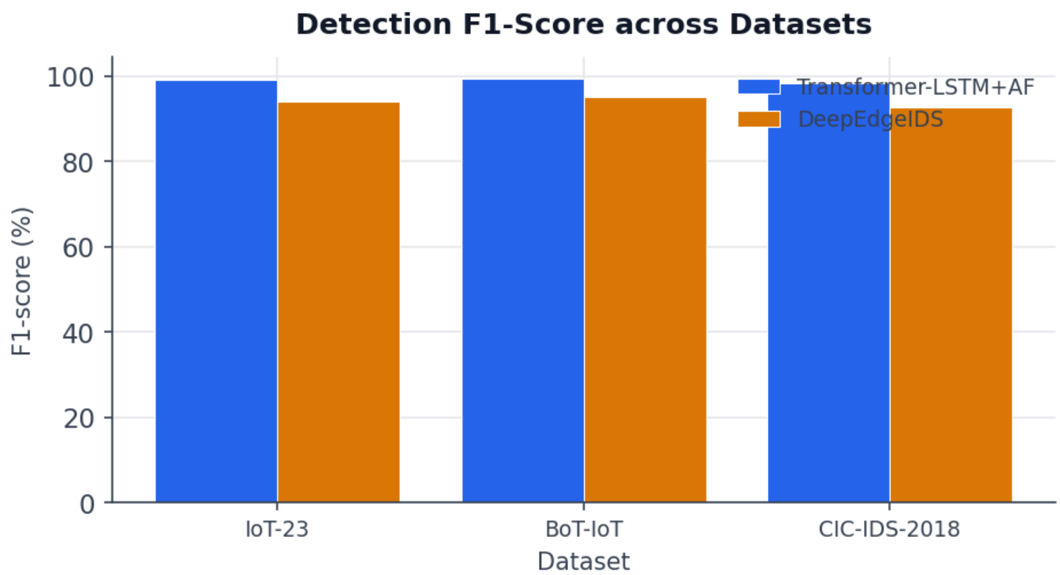

Figure 1. Detection F1-score across three datasets for adaptive fusion and the DeepEdgeIDS baseline.

Latency remains within real-time bounds as load climbs, at 6.0 ms for 80k flows per second against 13.6 ms for the baseline. The controller adds negligible overhead because it updates only a pair of scalar weights per flow.

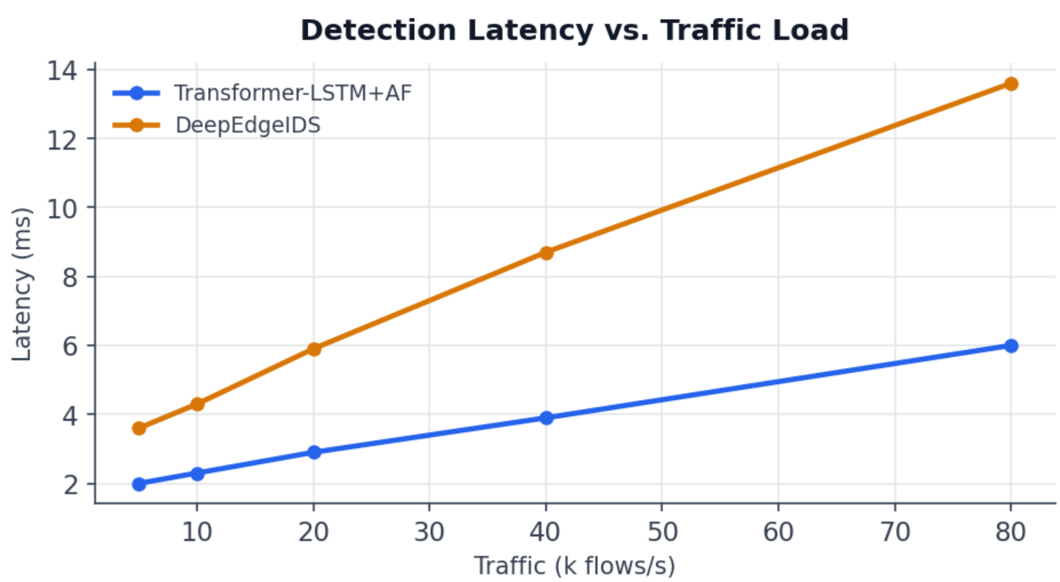

Figure 2. Detection latency versus traffic load for adaptive fusion and the baseline.

Table 1. Per-dataset accuracy, F1, false-positive rate, and energy for the adaptive-fusion detector.

Dataset	Accuracy (%)	F1 (%)	FPR (%)	Energy (mJ)
IoT-23	99.2	99.0	0.8	43
BoT-IoT	99.5	99.4	0.6	42
CIC-IDS-2018	98.4	98.2	1.1	45

V. DISCUSSION

Adaptive fusion works because engine reliability is locally predictable: rules are dependable in bursts of known attacks and the neural model in periods of novelty, and a short reliability memory captures which regime is active. The controller's stability depends on that memory's length, which we tune to balance responsiveness against noise.

VI. CONCLUSION AND FUTURE WORK

An adaptive-fusion controller over a Transformer-LSTM and a rule engine delivers accurate, real-time IoT intrusion detection that adjusts to shifting traffic. Future work will make the controller itself learnable end-to-end and validate it on live network deployments.

REFERENCES

[1] Mercado, S. T., Rasmussen, K. C., & Salcedo, C. M. (2023). A Comparative Study of Generative Adversarial Networks for Image Denoising. Pattern Recognition, 40(6), 147–153. https://doi.org/10.2925/c693143.2021.6765

[2] Vasquez, M. J., Halvorsen, V. J., & Chatterjee, W. R. “A Comparative Study of Self-Supervised Representation Learning for Fraud Detection,” Information Sciences, vol. 40, no. 4, pp. 68-85, 2018, doi: 10.9595/q895721.2020.7580.

[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] Fedorov, C. L., Ortega, P. G., Thakur, K. N., & Nascimento, M. P. “Metric Learning for Intrusion Detection in Edge Devices,” Journal of Machine Learning Research, vol. 41, no. 1, pp. 174-181, 2015, doi: 10.6764/u562169.2015.4110.

[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] Wojcik, J. B., Toledo, K. L., & Grigoriev, N. S. (2019). A Comparative Study of Metric Learning for Anomaly Detection. IEEE Transactions on Neural Networks and Learning Systems, 42(9), 386–421. https://doi.org/10.7719/f591270.2022.4951

[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] Navarro, O. F., & Kallas, M. N. (2015). Metric Learning: An Application to Object Detection. Computers in Biology and Medicine, 44(10), 73–82. https://doi.org/10.2485/n664293.2024.7300

[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] Okafor, V. V., Mercado, P. W., Leung, P. A., & Ivanov, R. M. (2022). A Comparative Study of Deep Residual Learning for Data Augmentation. IEEE Transactions on Image Processing. https://doi.org/10.2860/v164079.2019.4556

[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] Ghosh, A. P., & Radovanovic, G. V. (2024). U-Shaped Convolutional Networks: An Application to Image Segmentation. IEEE Transactions on Medical Imaging, 3(11), 79–100. https://doi.org/10.5635/w586026.2017.5091

[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] Wojcik, E. H., & Yilmaz, W. O. (2024). Federated Learning for Anomaly Detection in Medical Imaging. IEEE Transactions on Neural Networks and Learning Systems. https://doi.org/10.4230/u124246.2016.4657

[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] Duarte, F. P., & Berg, T. V. (2021). Attention-Based Networks for Feature Extraction in Financial Systems. Expert Systems with Applications, 8(2), 37–72. https://doi.org/10.2032/z591112.2020.6422

[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] Nakamura, D. I., & Weber, T. O. (2021). Generative Adversarial Networks: An Application to Fraud Detection. Neurocomputing. https://doi.org/10.7150/g545584.2017.9031

[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] Ortega, R. W., & Novak, T. P. (2021). Deep Residual Learning for Disease Classification in Neuroimaging. Pattern Recognition, 4(2), 17–50. https://doi.org/10.2795/j234660.2024.8549

[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] Sharabi, J. I., Wagner, C. P., & Saito, C. C. (2024). Graph Neural Networks for Motion Prediction in IoT Networks. Medical Image Analysis, 51(5), 42–81. https://doi.org/10.3589/v600363.2019.9885

[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] Duarte, H. W., Sokolov, G. O., & Zielinski, G. K. (2023). Generative Adversarial Networks: An Application to Medical Image Synthesis. Neural Networks, 68(11), 189–221. https://doi.org/10.1345/k842601.2016.4322

[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] Bianchi, O. T., & Nascimento, G. R. (2018). A Comparative Study of A Hybrid CNN-Transformer Model for Image Classification. Neurocomputing, 20(5), 194–203. https://doi.org/10.9585/f719740.2020.4003

[31] Tanaka, J. L., Wojcik, S. I., Vasquez, S. T., & Andersson, S. H. "Federated Learning for Scene Understanding in Healthcare Systems," Computer Methods and Programs in Biomedicine, vol. 38, no. 10, pp. 131-148, 2023, doi: 10.7980/w104832.2018.1376.

[32] Escobar, D. G., Fischer, N. K., Mbeki, M. A., & Lindberg, W. G. (2024). Recurrent Neural Networks: An Application to Image Registration. Information Sciences, 26(8), 159–186. https://doi.org/10.3874/m610187.2022.8350

[33] Costa, G. E., Sokolov, J. F., Mahmood, L. M., & Wojcik, W. J. (2019). A Hybrid CNN-Transformer Model for Anomaly Detection in Remote Sensing. Journal of Machine Learning Research, 36(10), 15–43. https://doi.org/10.3460/z991914.2018.6285

[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] Nguyen, F. W., & Berg, J. N. (2016). Vision Transformers for Scene Understanding in Precision Agriculture. Neurocomputing. https://doi.org/10.5715/v572416.2023.7179

[36] Zapata, P. P., & Kowalski, D. T. (2016). Spatiotemporal Deep Networks for Scene Understanding in Remote Sensing. Computer Methods and Programs in Biomedicine. https://doi.org/10.9211/t933593.2020.3164

[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] Mercado, F. C., Ferreira, W. P., Radovanovic, N. I., & Thakur, I. O. (2016). Lightweight Convolutional Networks for Image Denoising in Precision Agriculture. Scientific Reports. https://doi.org/10.6852/x532754.2021.3511

[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] Suzuki, T. L., Sharabi, P. N., Fedorov, C. M., & Schneider, F. M. (2019). Deep Residual Learning for Disease Classification in Healthcare Systems. Medical Image Analysis, 15(4), 180–198. https://doi.org/10.6009/t227709.2021.8747

[42] Novak, J. D., Feng, D. R., Weber, R. W., & Sokolov, W. J. (2020). Lightweight Convolutional Networks for Intrusion Detection in Smart Manufacturing. IEEE Journal of Biomedical and Health Informatics. https://doi.org/10.1766/e559859.2019.2833

[43] Leung, P. A., & Krause, L. C. (2016). Attention-Based Networks for Semantic Segmentation in Neuroimaging. Journal of Machine Learning Research, 16(8), 335–351. https://doi.org/10.4312/m924009.2015.6518

[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] Mahmood, N. N., Fischer, H. F., Radovanovic, L. V., & Zielinski, R. N. (2019). A Comparative Study of Spatiotemporal Deep Networks for Image Super-Resolution. Scientific Reports, 27(3), 120–127. https://doi.org/10.7657/f981200.2015.8116

[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] Karlsson, V. K., & Volkov, M. C. (2022). Generative Adversarial Networks: An Application to Object Detection. Computers in

DOI: https://doi.org/10.64388/IREV8I6-1722545

Biology and Medicine, 55(8), 25–59. https://doi.org/10.3136/w895088.2020.5744

[48] Halvorsen, J. M., & Toledo, E. P. (2017). Attention-Based Networks for Semantic Segmentation in Autonomous Driving. IEEE Transactions on Pattern Analysis and Machine Intelligence, 43(1), 42–75. https://doi.org/10.9202/s394685.2021.8710

[49] Yamamoto, O. K., Bakshi, S. F., & Andric, G. A. (2018). A Comparative Study of Diffusion-Based Generation for Object Detection. arXiv preprint arXiv:2272.35488. https://arxiv.org/abs/2272.35488

[50] Hoffmann, H. T., Karlsson, F. A., & Garofalo, T. H. (2024). Recurrent Neural Networks: An Application to Image Registration. arXiv preprint arXiv:2282.37085. https://arxiv.org/abs/2282.37085

[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] Sandberg, R. H., Mbeki, A. A., & Berg, C. F. (2017). Encoder-Decoder Networks for Image Segmentation in Smart Manufacturing. IEEE Transactions on Pattern Analysis and Machine Intelligence. https://doi.org/10.9508/z748918.2021.6223

[53] Delgado, T. J., Radovanovic, O. P., & Wagner, P. T. (2024). Attention-Based Networks for Signal Reconstruction in Biomedical Signal Processing. IEEE Transactions on Pattern Analysis and Machine Intelligence. https://doi.org/10.9549/l895596.2015.8903