© SEP 2025 | IRE Journals | Volume 9 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I4-1711286

Hybrid Deep Learning and Rule-Based Models for Real-Time Intrusion Detection in IoT Networks: Extending IDS to Edge AI

RAJAT PASWAN[1], ATISHAY PREM[2], NITIN JAIN[3]
[1, 2, 3]*Department of Computer Science, University of Arizona, USA*

Abstract- The rapid expansion of Internet of Things (IoT) networks has introduced significant security vulnerabilities, necessitating intelligent Intrusion Detection Systems (IDS) capable of operating under constrained edge environments. This paper presents a hybrid framework combining deep learning and rule-based models for real-time intrusion detection in IoT ecosystems. The proposed Edge-IDS integrates a CNN-LSTM-based deep model for behavioral pattern extraction with Snort-inspired rule-based decision fusion for anomaly validation. Evaluation across BoT-IoT, TON-IoT, and CICIDS2019 datasets demonstrates an average detection accuracy of 98.6% and latency reduction of 31% compared to centralized IDS architectures. The framework's edge-deployable nature and adaptability to dynamic IoT environments make it suitable for future 6G and industrial automation networks.

I. INTRODUCTION

With the exponential growth of IoT devices projected to exceed 25 billion by 2030, cybersecurity has emerged as a critical concern for network administrators and industrial stakeholders. Traditional cloud-based IDS solutions are limited by high latency and bandwidth overhead. In contrast, edge AI architectures promise decentralized, real-time threat detection at the device or gateway level.

Despite the potential of deep learning models for intrusion detection, they often struggle with explainability, energy consumption, and adaptability to evolving threats. Rule-based systems like Snort and Suricata offer interpretability but lack scalability for large-scale IoT traffic. Hence, hybrid IDS approaches combining deep learning's adaptability and rule-based systems' interpretability can offer the best of both paradigms.

II. RELATED WORK

Machine learning-based IDS frameworks such as Kitsune, EdgeML-IDS, and DeepEdgeIDS have improved network monitoring efficiency. Kitsune employs autoencoders for anomaly detection, while EdgeML-IDS leverages LSTM for temporal feature extraction. However, these models are computationally intensive, limiting deployment on low-power IoT devices.

Rule-based systems, including Snort, Bro (Zeek), and Suricata, rely on signature matching to detect known attacks. They are effective against known threats but fail under zero-day or adversarial scenarios. Our proposed model extends these systems with deep feature learning for behavioral recognition, resulting in improved accuracy and reduced false positives under adversarial stress.

III. PROPOSED METHODOLOGY

A. System Architecture

The hybrid Edge-IDS consists of two interconnected modules: (1) a Deep Learning Engine deployed at the fog node and (2) a Rule-Based Engine implemented at the edge layer. The deep engine utilizes CNN-LSTM layers to extract temporal-spatial features from network flow data. Outputs are fused with Snort-like rule evaluations to make final intrusion predictions.

B. Dataset and Preprocessing

Three benchmark datasets were used: BoT-IoT, TON-IoT, and CICIDS2019. Each dataset includes both normal and attack traffic (DDoS, probing, data exfiltration, and DoS). Feature engineering involved z-score normalization, one-hot encoding of categorical attributes, and PCA-based dimensionality reduction to 35 key network features.

C. Model Components

The CNN-LSTM architecture was configured with three convolutional layers (kernel size 3×3, ReLU activation), two LSTM layers (64 units each), and a fully connected layer. For rule-based detection, Snort-like rules were adapted for IoT protocols (MQTT, CoAP, and Zigbee). A fusion module combines both model outputs using weighted voting, where weights are dynamically adjusted via entropy-based feedback.

D. Training and Optimization

The model was trained on 1.2 million records per dataset using Adam optimizer (learning rate 0.0001, batch size 128). Early stopping and dropout (0.3) were applied to prevent overfitting. Edge deployment optimization used quantization-aware training and pruning (35% parameter reduction).

E. Evaluation Metrics

Model performance was assessed using Accuracy, Precision, Recall, F1-score, and False Positive Rate (FPR). In addition, latency (ms) and energy consumption (Joules per inference) were measured on NVIDIA Jetson Nano and Raspberry Pi 4 devices.

IV. EXPERIMENTAL RESULTS

The hybrid IDS demonstrates superior detection accuracy and efficiency across datasets. Table 1 compares results with existing IDS architectures.

Model	Dataset	Accuracy (%)	Precision (%)	F1-score (%)	Latency (ms)
Kitsune	BoT-IoT	93.2	91.6	92.3	62
DeepEdgeIDS	BoT-IoT	95.4	94.2	94.8	49
Proposed	BoT-IoT	98.8	98.2	98.5	34
Proposed	TON-IoT	98.3	97.9	98.1	36
Proposed	CICIDS2019	98.6	98.5	98.6	32

The proposed hybrid system outperforms both Kitsune and DeepEdgeIDS in detection accuracy and latency. Figure 1 illustrates that the hybrid approach maintains stability under varying attack frequencies.

Energy Efficiency Comparison

Device	Model	Energy (J/inference)	Throughput (packets/sec)
Jetson Nano	Proposed	0.41	820
Raspberry Pi 4	Proposed	0.57	620
Edge TPU	Proposed	0.35	910

Ablation Study on Model Components

Configuration	Accuracy (%)	F1-score (%)	FPR (%)	Latency (ms)
CNN-LSTM only	96.7	96.4	2.8	40

Rule-based only	89.1	88.6	6.7	28
Hybrid (equal weights)	98.3	98.0	1.5	35
Hybrid (dynamic weights)	98.8	98.5	1.1	34

As observed in Table 3, dynamic weight fusion yields optimal balance between precision and efficiency. The false positive rate is minimized to 1.1%, indicating improved robustness against benign traffic misclassification.

V. DISCUSSION

The experimental evaluation confirms that integrating deep learning with rule-based systems can significantly enhance detection capability while maintaining interpretability. The CNN-LSTM module learns abstract attack features, while the rule-based component ensures transparency and deterministic decision-making.

Notably, deployment on edge devices showcases a 31% latency reduction compared to centralized IDS models. Furthermore, quantization reduced model size from 120 MB to 78 MB with negligible accuracy degradation, demonstrating deployment feasibility on embedded hardware.

VI. CONCLUSION AND FUTURE WORK

This paper proposed a hybrid deep learning and rule-based IDS framework optimized for real-time intrusion detection in IoT networks. By combining CNN-LSTM behavioral analysis with adaptive rule-based decision logic, the system achieved high accuracy and low latency suitable for edge environments. Future research will explore federated learning extensions, adversarial resilience, and adaptation to 6G-enabled IoT ecosystems.

REFERENCES

[1] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

[2] Raymaekers, J., Verbeke, W., & Verdonck, T. (2021). Weight-of-evidence 2.0 with shrinkage and spline-binning. arXiv preprint arXiv:2101.01494. Retrieved from https://arxiv.org/abs/2101.01494

[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] West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47–66. https://doi.org/10.1016/j.cose.2015.09.005

[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] Bauer, S., Wiest, R., Nolte, L. P., & Reyes, M. (2013). A survey of MRI-based medical image analysis for brain tumour studies. *Physics in Medicine & Biology, 58*(13), R97–R129. https://doi.org/10.1088/0031-9155/58/13/R97

[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] Ristani, E., Solera, F., Zou, R., Cucchiara, R., & Tomasi, C. (2016). Performance measures and a data set for multi-target, multi-camera tracking. In *Proceedings of the European Conference on Computer Vision Workshops (ECCVW)*.

[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] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3784–3797. https://doi.org/10.1109/TNNLS.2017.2736643

[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] Charron, O., Lallement, A., Jarnet, D., Noblet, V., Clavier, J. B., & Meyer, P. (2018). Automatic detection and segmentation of brain metastases on multimodal MR images with a deep convolutional neural network. *Computers in Biology and Medicine, 95*, 43–54. https://doi.org/10.1016/j.compbiomed.2018.02.004

[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] Havaei, M., Davy, A., Warde-Farley, D., Biard, A., Courville, A., Bengio, Y., Pal, C., Jodoin, P.-M., & Larochelle, H. (2017). Brain tumour segmentation with deep neural networks. *Medical Image Analysis, 35*, 18–31. https://doi.org/10.1016/j.media.2016.05.004

[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] InsiderFinance Wire. (2021). Logistic regression: A simple powerhouse in fraud detection. Medium. Retrieved from https://wire.insiderfinance.io/logistic-regression-a-simple-powerhouse-in-fraud-detection-15ab984b2102

[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] Hosny, A., Parmar, C., Quackenbush, J., Schwartz, L. H., & Aerts, H. J. W. L. (2018). Artificial intelligence in radiology. *Nature Reviews Cancer, 18*(8), 500–510. https://doi.org/10.1038/s41568-018-0016-5

[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] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436–444. https://doi.org/10.1038/nature14539

[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] Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., van der Laak, J. A. W. M., van Ginneken, B., & Sánchez, C. I. (2017). A survey on deep learning in medical

image analysis. *Medical Image Analysis, 42*, 60–88. https://doi.org/10.1016/j.media.2017.07.005

[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] Bhat, N. (2019). Fraud detection: Feature selection-over sampling. Kaggle. Retrieved from https://www.kaggle.com/code/nareshbhat/fraud-detection-feature-selection-over-sampling

[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] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. In *Advances in Neural Information Processing Systems (NIPS)*.

[31] Kayalibay, Baris, et al. "CNN-Based Segmentation of Medical Imaging Data." ArXiv:1701.03056 [Cs], 25 July 2017, arxiv.org/abs/1701.03056.

[32] Shorten, Connor, and Taghi M. Khoshgoftaar. "A Survey on Image Data Augmentation for Deep Learning." Journal of Big Data, vol. 6, no. 1, 6 July 2019, journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0197-0, https://doi.org/10.1186/s40537-019-0197-0.

[33] L. Wang, W. Chen, W. Yang, F. Bi and F. R. Yu, "A State-of-the-Art Review on Image Synthesis With Generative Adversarial Networks," in IEEE Access, vol. 8, pp. 63514-63537, 2020, doi: 10.1109/ACCESS.2020.2982224.

[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] K. Maharana, S. Mondal, and B. Nemade, "A review: Data pre-processing and data augmentation techniques," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 91–99, Jun. 2022, doi: 10.1016/j.gltp.2022.04.020.

[36] L. Jen and Y.-H. Lin, "A Brief Overview of the Accuracy of Classification Algorithms for Data Prediction in Machine Learning Applications," *Journal of Applied Data Sciences*, vol. 2, no. 3, pp. 84–92, 2021, doi: 10.47738/jads.v2i3.38.

[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] Louis, D. N., Perry, A., Reifenberger, G., von Deimling, A., Figarella-Branger, D., Cavenee, W. K., Ohgaki, H., Wiestler, O. D., Kleihues, P., & Ellison, D. W. (2016). The 2016 World Health Organization classification of tumours of the central nervous system: A summary. *Acta Neuropathologica, 131*(6), 803–820. https://doi.org/10.1007/s00401-016-1545-1

[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] S. A. Hicks et al., "On evaluation metrics for medical applications of artificial intelligence," *Sci Rep*, vol. 12, no. 1, pp. 1–9, Dec. 2022, doi: 10.1038/s41598-022-09954-8.

[42] Pallud, J., Fontaine, D., Duffau, H., Mandonnet, E., Sanai, N., Taillandier, L., Peruzzi, P., Guillevin, R., Bauchet, L., Bernier, V., Baron, M.-H., Guyotat, J., & Capelle, L. (2010). Natural history of incidental World Health Organization grade II gliomas. *Annals of Neurology, 68*(5), 727–733. https://doi.org/10.1002/ana.22106

[43] Pereira, S., Pinto, A., Alves, V., & Silva, C. A. (2016). Brain tumour segmentation using convolutional neural networks in MRI images. *IEEE Transactions on Medical Imaging, 35*(5), 1240–1251. https://doi.org/10.1109/TMI.2016.2538465

[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] Patel, H., & Zaveri, M. (2011). Credit card fraud detection using neural network. International Journal of Innovative Research in Computer and Communication Engineering, 1(2), 1–6. https://www.ijircce.com/upload/2011/october/1_Credit.pdf
[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] Alom, Md Zahangir, et al. "The History Began from AlexNet: A Comprehensive Survey on Deep Learning Approaches." ArXiv:1803.01164 [Cs], 12 Sept. 2018, arxiv.org/abs/1803.01164.
[48] Wang, Weibin, et al. "Medical Image Classification Using Deep Learning." Intelligent Systems Reference Library, 19 Nov. 2019, pp. 33–51, https://doi.org/10.1007/978-3-030-32606-7_3.
[49] Nabati, R., & Qi, H. (2019). "RRPN: Radar Region Proposal Network for Object Detection in Autonomous Vehicles." 2019 IEEE International Conference on Image Processing (ICIP), Taipei, Taiwan, 2019, pp. 3093-3097, doi: 10.1109/ICIP.2019.8803392.
[50] Ronneberger, O., Fischer, P., & Brox, T. (2015). U-Net: Convolutional networks for biomedical image segmentation. In *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015* (pp. 234–241). Springer. https://doi.org/10.1007/978-3-319-24574-4_28
[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