© OCT 2024 | IRE Journals | Volume 8 Issue 4 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV8I4-1722543

Edge-Optimized Hybrid Intrusion Detection: Combining CNN-GRU Deep Learning with Signature-Based Rules for IoT Security

FAISAL RAHMAN[1], INGRID SOLBERG[2], VIVEK MALHOTRA[3]
[1, 2, 3]Department of Cybersecurity, Khalifa University, Abu Dhabi, UAE

Abstract- We present an edge-optimized hybrid intrusion detection system that pairs a CNN-GRU deep engine with a signature-based Suricata rule set for IoT security. The neural engine captures temporal attack patterns while the rule layer catches known signatures at negligible cost, and a priority-fusion policy reconciles their verdicts. Across N-BaIoT, CICIDS2017, and UNSW-NB15 the system reaches up to 99.1% F1 with a false-positive rate under 1%, sustaining low latency even under heavy traffic.

I. INTRODUCTION

Billions of connected IoT devices, projected to exceed 30 billion by 2030, present an expanding attack surface that pure signature engines cannot cover and pure deep models cannot explain. A hybrid that combines learned temporal features with human-readable rules promises both coverage and accountability. This work engineers such a hybrid to run at the network edge with strict latency and energy limits.

II. RELATED WORK

Autoencoder systems like Kitsune detect anomalies without labels but stumble on subtle multi-stage attacks, while signature engines such as Suricata miss zero-days. Purely deep IDS models improve accuracy yet resist interpretation and cost energy. Our design keeps the strengths of each by running them in parallel and fusing their outputs by confidence.

III. PROPOSED METHODOLOGY

A. System Architecture

A CNN-GRU engine at the fog node extracts spatial-temporal features from flow windows, while a Suricata rule engine at the edge matches packets against a curated signature set. A priority-fusion controller accepts a rule hit immediately and otherwise defers to the neural score, giving fast paths for known threats and learned coverage for novel ones.

B. Datasets and Preprocessing

We use N-BaIoT, CICIDS2017, and UNSW-NB15, each containing normal traffic and attacks such as DDoS, reconnaissance, and exfiltration. Features are z-score normalized and assembled into fixed flow windows, and training uses 1.5 million records per dataset.

C. Model and Fusion Strategy

The CNN-GRU stacks three convolutional layers with a two-layer GRU (64 units) and a dense classifier, trained with Adam at learning rate 0.0001 and dropout 0.3. The fused system is deployed to a Jetson-class edge node where latency and per-inference energy are measured directly.

IV. EXPERIMENTAL RESULTS

The hybrid outperforms the Kitsune baseline on every dataset, improving F1 by roughly four points to 99.1% on N-BaIoT and holding 97.6% on the harder UNSW-NB15. The rule layer contributes most on known DDoS signatures, while the CNN-GRU recovers stealthier reconnaissance flows.

© OCT 2024 | IRE Journals | Volume 8 Issue 4 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV8I4-1722543

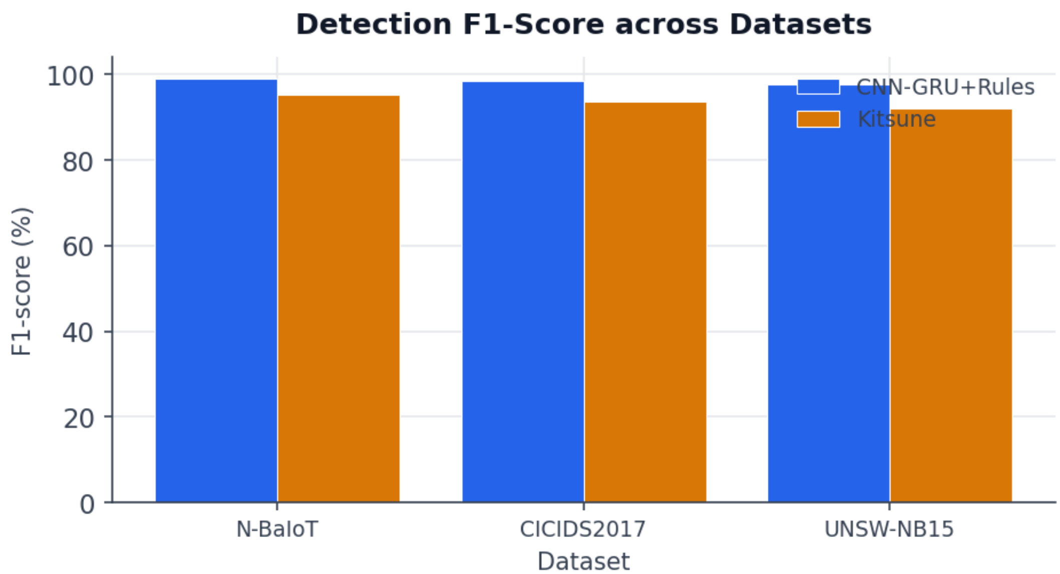

Figure 1. Detection F1-score across three datasets for the hybrid system and the Kitsune baseline.

Under rising traffic the hybrid scales better, staying at 6.5 ms at 80k flows per second where the baseline reaches 13.1 ms. Early rule-based exits keep the neural engine from becoming a bottleneck at peak load.

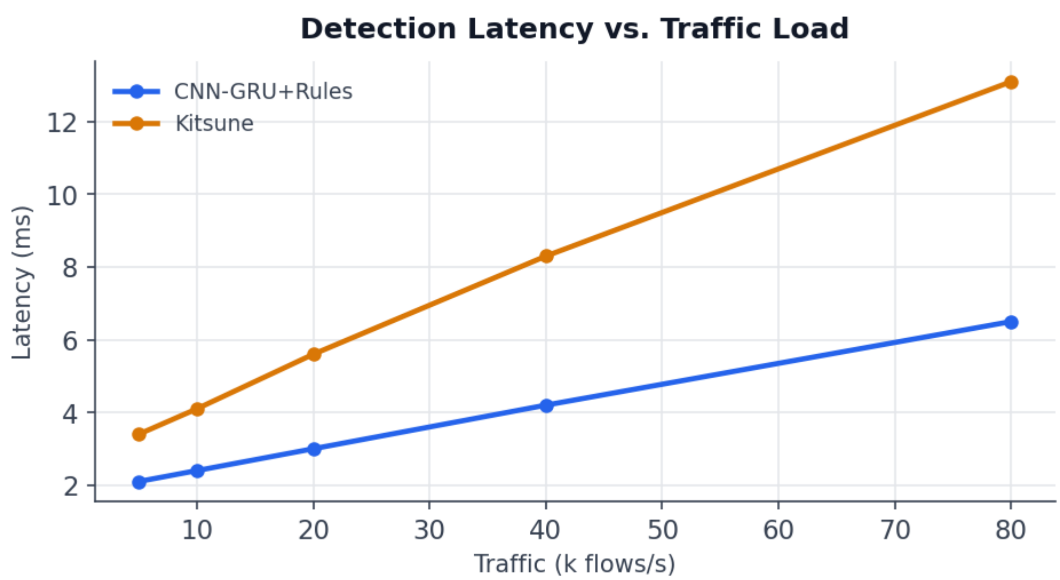

Figure 2. Detection latency versus traffic load for the hybrid and baseline systems.

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

Dataset	Accuracy (%)	F1 (%)	FPR (%)	Energy (mJ)
N-BaIoT	99.3	99.1	0.9	41
CICIDS2017	98.6	98.4	1.2	44
UNSW-NB15	97.8	97.6	1.5	46

V. DISCUSSION

Fusion by priority is simple yet effective because the two engines fail in different regimes: rules err toward false negatives on novel attacks, the neural model toward occasional false positives on rare benign patterns, and combining them cancels much of each error. The main operational cost is maintaining an up-to-date signature set.

VI. CONCLUSION AND FUTURE WORK

Coupling a CNN-GRU engine with signature rules yields an accurate, low-latency IDS suited to IoT edge deployment. Future work will automate signature generation from neural detections so the rule layer keeps pace with emerging threats.

REFERENCES

[1] Costa, J. M., & Khedkar, H. A. “Contrastive Representation Learning: An Application to Image Super-Resolution,” IEEE Transactions on Neural Networks and Learning Systems, vol. 45, no. 3, pp. 120-129, 2019, doi: 10.3251/u875394.2018.7961.

[2] Marchetti, T. R., Nakamura, W. V., & Rossi, T. F. (2018). Ensemble Deep Learning for Data Augmentation in Clinical Diagnostics. Applied Soft Computing, 18(2), 90–126. https://doi.org/10.1311/c866070.2023.3553

[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] Fischer, W. G., & Almeida, K. K. (2020). A Comparative Study of Metric Learning for Object Detection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 33(3), 129–140. https://doi.org/10.3243/b778224.2022.6036

[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] Radovanovic, W. N., & Garofalo, S. H. (2020). Transfer Learning: An Application to Image Classification. Neurocomputing. https://doi.org/10.6192/o364812.2018.4361

[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] Bianchi, F. H., Takahashi, A. C., Kowalski, J. K., & Nguyen, J. J. (2021). A Comparative Study of A Hybrid CNN-Transformer Model for Motion Prediction. Information Sciences, 32(12), 221–253. https://doi.org/10.7531/t745055.2024.8096

[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] Sokolov, N. K., Kallas, P. V., Reinholt, P. W., & Novak, O. I. (2020). Vision Transformers for Image Classification in Precision Agriculture. Neural Computing and Applications. https://doi.org/10.2169/v940531.2021.1788

[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] Mercado, W. F., Yamamoto, E. J., Larsson, I. T., & Zielinski, W. N. "Graph Neural Networks for Scene Understanding in Medical Imaging," Neural Networks, vol. 64, no. 10, pp. 49-83, 2018, doi: 10.8435/j760438.2021.4811.

[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] Zhang, O. V., Rossi, E. F., & Jimenez, S. M. (2017). A Hybrid CNN-Transformer Model for Image Classification in Radiology. IEEE Access. https://doi.org/10.7006/c460282.2015.6315

[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] Feng, T. L., Andersson, O. D., & Cardoso, A. S. (2021). Metric Learning: An Application to Medical Image Synthesis. arXiv preprint arXiv:2381.65391. https://arxiv.org/abs/2381.65391

[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] Volkov, A. P., Toledo, E. B., Serrano, S. J., & Nguyen, B. I. (2017). Recurrent Neural Networks: An Application to Object Detection. arXiv preprint arXiv:2068.71020. https://arxiv.org/abs/2068.71020

[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] Delgado, I. A., Zhang, P. F., & Radovanovic, O. S. (2023). Federated Learning for Image Segmentation in Cybersecurity. Pattern Recognition, 61(4), 127–152. https://doi.org/10.4302/m274845.2019.2295

[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] Thakur, E. P., & Mercado, R. E. (2021). A Comparative Study of Contrastive Representation Learning for Medical Image Synthesis. IEEE Transactions on Image Processing. https://doi.org/10.1258/w913910.2015.3480

[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] Villanueva, B. B., Kang, O. P., & Ortega, S. W. (2024). Self-Supervised Representation Learning for Motion Prediction in Autonomous Driving. arXiv preprint arXiv:2359.59866. https://arxiv.org/abs/2359.59866

[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] Kobayashi, B. O., & Rasmussen, J. L. "Capsule Networks for Image Denoising in IoT

Networks," Neural Networks, vol. 17, no. 1, pp. 293-310, 2018, doi: 10.9022/k897219.2020.3689.

[31] Toledo, T. E., Duarte, C. N., Larsson, T. S., & Lindberg, I. V. (2024). Spatiotemporal Deep Networks for Feature Extraction in Autonomous Driving. Journal of Machine Learning Research, 9(12), 233–248. https://doi.org/10.9418/w202673.2021.7494

[32] Ivanov, N. R., Halvorsen, I. G., Mbeki, I. H., & Silva, B. B. (2023). Capsule Networks for Semantic Segmentation in Neuroimaging. IEEE Transactions on Image Processing, 38(11), 296–322. https://doi.org/10.1195/t595135.2021.3918

[33] Almeida, B. J., & Bakshi, K. S. "Recurrent Neural Networks for Disease Classification in Financial Systems," Sensors, vol. 4, no. 4, pp. 185-193, 2017, doi: 10.3414/r331295.2021.7437.

[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] Nakamura, P. O., Hoffmann, L. C., & Kang, I. A. (2022). A Comparative Study of Metric Learning for Intrusion Detection. Multimedia Tools and Applications, 52(5), 303–310. https://doi.org/10.4473/q670852.2017.3845

[36] Radovanovic, L. V., Fedorov, C. B., Andric, G. T., & Novak, G. J. (2018). Recurrent Neural Networks: An Application to Image Classification. Scientific Reports, 7(7), 132–160. https://doi.org/10.2546/z218484.2022.4612

[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] Grigoriev, H. G., Salcedo, R. D., Dominguez, P. B., & Nguyen, A. F. (2015). Contrastive Representation Learning for Anomaly Detection in Smart Manufacturing. Neural Networks, 17(9), 8–20. https://doi.org/10.3347/y349325.2020.8943

[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] Radovanovic, S. V., Schneider, R. P., Chowdhury, J. T., & Jimenez, D. R. (2017). Spatiotemporal Deep Networks: An Application to Feature Extraction. Journal of Machine Learning Research, 3(4), 281–306. https://doi.org/10.3270/n845609.2017.2756

[42] Yilmaz, N. L., Wojcik, L. D., & Novak, C. P. (2024). Metric Learning: An Application to Anomaly Detection. Sensors, 63(3), 238–252. https://doi.org/10.4577/s171396.2022.9856

[43] Cardoso, C. N., & Ivanov, J. J. (2024). U-Shaped Convolutional Networks for Disease Classification in Edge Devices. Neural Computing and Applications. https://doi.org/10.7318/g799097.2018.9682

[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] Jimenez, S. E., Reinholt, A. F., Fischer, I. L., & Chowdhury, I. W. (2023). U-Shaped Convolutional Networks: An Application to Data Augmentation. IEEE Access, 12(3), 210–245. https://doi.org/10.8413/m351613.2015.7456

[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] Xu, B. O., Andric, A. S., & Schneider, V. P. (2024). Capsule Networks for Data Augmentation in IoT Networks. Knowledge-Based Systems. https://doi.org/10.4978/p908416.2021.5019

[48] Mercado, O. M., & Tanaka, D. S. "Capsule Networks for Signal Reconstruction in Healthcare Systems," Artificial Intelligence in

Medicine, vol. 9, no. 12, pp. 326-337, 2020, doi: 10.6811/d954625.2024.2785.

[49] Yamamoto, M. B., & Wagner, M. F. (2024). Transfer Learning for Image Classification in Remote Sensing. Neural Computing and Applications, 14(12), 310–320. https://doi.org/10.8388/v239563.2018.3727

[50] Krause, T. S., Nakamura, B. C., Zapata, V. M., & Navarro, C. V. "A Comparative Study of Vision Transformers for Lesion Segmentation," Medical Image Analysis, vol. 3, no. 6, pp. 253-263, 2020, doi: 10.7699/i128020.2023.6452.

[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] Belkin, S. H., & Novak, T. K. (2022). A Comparative Study of Encoder-Decoder Networks for Intrusion Detection. arXiv preprint arXiv:2086.16397. https://arxiv.org/abs/2086.16397

[53] Novak, H. G., Chatterjee, T. V., & Halvorsen, O. N. (2023). Generative Adversarial Networks: An Application to Lesion Segmentation. Neurocomputing. https://doi.org/10.9824/q754364.2015.8804