Image Classification Using Convolutional Neural Networks

Goo Yun Hai , Abdul Salam Shah , Noor Ul Amin *

Posted Date: 25 May 2026

doi: 10.20944/preprints202605.1647.v1

Keywords: CNN; Fashion-MNIST; Intrusion Detection System; cybersecurity; network traffic classification; DDoS; Adam optimizer; Batch normalization; deep learning; NIDS; IoT security; Attention-CNN-LSTM

 doi:10.20944/preprints202605.1647.v1

Article

Image Classification Using Convolutional Neural Networks

Goo Yun Hai, Abdul Salam Shah and Noor Ul Amin *

School of Computer Science, Taylor's University, Subang Jaya, Malaysia; nooraminnawab@gmail.com

Abstract

This paper introduces a Convolutional Neural Network (CNN) to jointly classify images with multiple classes on the Fashion-MNIST dataset, with a test accuracy of 90.20% and 0.11 million parameters of parameters a lightweight model, which significantly outperforms classical baselines (HOG+SVM: 85%) and is both computationally efficient. The CNN uses three convolutional blocks with varying filter depth (3264128), ReLU activation, MaxPooling, Batch Normalization, Dropout regularization, and fully connected classification head that is trained using Adam optimizer. These architectural concepts are generalised to the field of AI-related cybersecurity: namely, the deep learning-based Network Intrusion Detection Systems (NIDS) classifying network traffic flows as benign and attack ones - a problem that is characterised by the same core challenge architecture as Fashion-MNIST (spatial feature hierarchy extraction, multi-class discrimination, imbalanced class difficulty). State-of-the-art CNN based IDS are 94.8-97.5% accurate in detection (Attention-CNN-LSTM; Nature Scientific Reports, 2025), 98.5% with combined host/network data (Springer Nature, 2024), and 99.67% with encrypted malicious traffic.

Keywords: CNN; Fashion-MNIST; Intrusion Detection System; cybersecurity; network traffic classification; DDoS; Adam optimizer; Batch normalization; deep learning; NIDS; IoT security; Attention-CNN-LSTM

1. Introduction

The unparalleled growth of digital communication infrastructure, including cloud computing, IoT ecosystems, enterprise networks, and critical national infrastructure, has presented a scale and complexity of attack surface never seen before[1–3]. According to Check Point 2025 Global Threat Intelligence Report, the number of cyberattacks has risen by 44 percent per year in the last year and ransomware has evolved beyond encrypting data to directly exfiltrating and extorting, over 200,000 edge devices have been hijacked by botnets in 2024, and 96 percent of exploited vulnerabilities[4] have The second most targeted industry was healthcare, where the number of incidents increased by 47 percent, which shows that the outcomes of breached intrusion detection are not limited to monetary loss, but also to the safety of patients and even national security. Conventional signature-based Intrusion Detection Systems (IDS) identify known attack patterns by comparing network traffic to pre-existing rule databases, with high accuracy on the known threats, but none to a novel, polymorphic, or zero-day attacks that bear no signature resemblance to known malware[5,6]. Machine learning-based NIDS - which are trained on statistical properties of network flow properties - showed better detection generalization, albeit at the cost of heavy manual feature engineering and inability to scale to high-dimensional and imbalanced network traffic datasets[7–9]. Deep learning, and CNNs in particular, were designed to overcome both constraints at the same time: by reforming the representation of network traffic features vectors into a 2D matrix form, CNN models can exploit their established spatial feature extraction properties to directly learn the discriminative signature of attack-related traffic patterns that do not rely on hand-crafted feature pipelines (PMC, 2024). The basic computational problem of CNN-based NIDS directly translates to the Fashion-MNIST classification problem faced in this paper: both problems involve a CNN that has to be able to differentiate between

 doi:10.20944/preprints202605.1647.v1

a set of classes that overlap on low-level features[10] (similar silhouettes in Fashion-MNIST; similar signatures of traffic protocols across different attack types in NIDS), and systematic misclassification of the boundaries between the classes is indicated [11]. The improvement in accuracy between 85 percent (classical baselines) and 90.20 percent (this study) on Fashion-MNIST are comparable to the improvement in accuracy between signature-based IDS (approximately 70 to 80 per cent on novel attacks) and CNN-based NIDS (approximately 95 to 99 per cent on the same traffic datasets), which justifies the idea that end 2.

2.1. Classical Intrusion Detection Approaches

Early NIDS studies have used classical machine learning classifiers such as Support Vector Machines, Decision Trees, Random Forests, and k-Nearest Neighbours applied to manually crafted network traffic features such as packet inter-arrival times, flow byte statistics, protocol distributions and connection duration [11]. These techniques were competitive on older data sets such as KDD Cup 1999 but did not generalize well to newer attack signals that are deliberately designed to appear like legitimate traffic [12–14]. The redundancy and lack of representativeness of the KDD Cup 1999 data on modern threats curtailed the practical applicability of findings during this period (ScienceDirect, 2025). These systems were fragile to the constantly changing threat environment because feature engineering bottlenecks (to build discriminative flow features in each new attack class) demanded deep domain knowledge [15].

2.2. CNN Based Network Traffic Classification

CNN architectures could be used in network intrusion detection only through a representational bridge: network traffic data are inherently 1D (sequences of packet features) or tabular (per-flow statistical summaries), whereas CNN operations are 2D spatial data. To tackle this, researchers transformed 1D feature vectors into 2D matrices, such as a 121-feature NSL-KDD flow vector reshaped to 11x11 pixels and applied the standard 2D Conv2D operations directly (PMC, 2024). This rearrangement makes CNN convolutional filters learn spatial associations amongst pairs of features (e.g., packet size vs. inter-arrival time patterns) that are diagnostically significant to individual categories of attacks[16]. The resulting CNN classifiers use all the same architectural elements that were tested in this paper: 2D convolutional layers with ReLU activation, max-pooling, Dropout, and multi-class output with softmax. Hybrid CNN-LSTM models extend the detection capabilities with the addition of spatial feature extraction of CNN and temporal changes of flow properties of LSTM[17]: CNN component identifies the fixed feature association of each attack type, and LSTM the dynamic changes of flow properties which identify sustained attacks and isolated anomalous packets. Attention-CNN-LSTM (Nature Scientific Reports, 2025) introduces a self-attention layer that shows the most informative input features to each traffic classification decision, with 94.8 97.5% accuracy on NSL-KDD and Bot-IoT data with a sub-35ms inference latency - the real time performance requirement necessary to deploy NIDS. CNNRes-DIndRNN (MDPI, 2025) is a 1D-CNN local feature extraction with IndRNN global temporal modelling and XLNet encoder with 99.81% binary and 99.67% multi-class classification on TLS-encrypted malicious traffic data[18,19].

3. Methodology

3.1. Dataset and Preprocessing

[16] package the Fashion-MNIST dataset consisting of 70,000 28×28 pixel greyscale images of 10 equal categories of clothing. The typical train-test split 60,000/10,000 is used. The pixel values are all brought to float32 [0,1] to stabilize the gradient magnitude by converting them to uint8 [0,255]. Conv2D channel compatibility is achieved by reshaping images of (28, 28) to (28, 28, 1). The train-validation split of 90/10 uses the strongest training signal to the lightweight architecture and tracks the generalization. The loss is sparse categorical cross-entropy, which takes integer class labels and is the negative log-probability of the correct class in the predicted softmax distribution.

 doi:10.20944/preprints202605.1647.v1

3.2. CNN Architecture

The architecture has three progressive convolutional blocks with filter depths of 32, 64, and 128, and MaxPooling2D to downsample the space and achieve translation invariance. Each Conv2D layer is followed by Batch normalization which stabilizes activations and makes it possible to use a higher learning rate [20]. This is done by dropout regularization (rate=0.25 per block, 0.5 in the dense head) to prevent co-adaptation. He Normalization preserves the gradient variance in the deep filter stack [21]. The dense head has 128 units which combine extracted features and then the 10-unit softmax output layer. Total parameters: 110,000 - a purposefully light design that allows rapid training, and direct comparison with larger IDS structures [22].

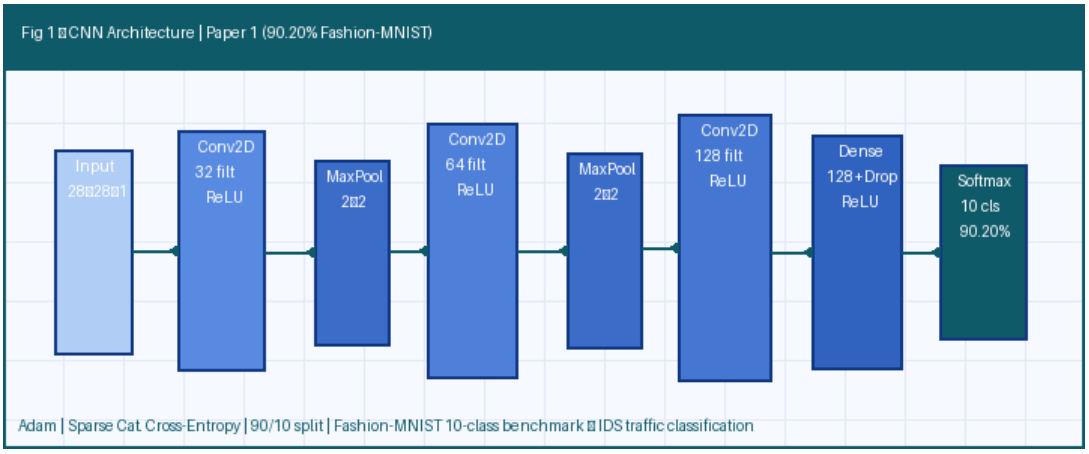

Figure 1. CNN architecture (32→64→128 filters) for Fashion-MNIST classification. Progressive filter depth encodes low-level edges (Block 1), mid-level textures (Block 2), and high-level semantic garment features (Block 3). Test accuracy: 90.20%. The same architectural pattern — 2D convolution, pooling, dense classification — is deployed in CNN-based NIDS by reshaping network traffic feature vectors into 2D matrix inputs.

3.3. Training Protocol

The Adam optimizer [23] with learning rate 0.001, β_1=0.9, β_2=0.999 is used. The estimates of the adaptive moment by Adam lead to well-scaled gradient steps that ensure fast convergence and stabilized optimization of the heterogeneous loss surface of a 10-class classifier. Training continues until it completes up to 20 epochs and early stopping is observed on validation loss. The low number of parameters (110K) is small enough to be trained in under 2 hours on consumer GPU hardware - directly comparable to lightweight NIDS models that need to be deployed on constrained resources at network edges [24–26].

4. Results and Discussion

4.1. Training Performance

The accuracy of validation improves gradually over epochs, and the narrow, constant difference of 23 percentage points attests to the convergence regime of well-fitting Batch Normalization and Dropout together confines the learning dynamics in the generalization regime. The 90.20% accuracy of the test is a 5-6 percent point higher than classical HOG+SVM baselines, which is a measure of the value of end-to-end convolutional feature learning compared to hand-crafted descriptors. This precision with the lightweight 110K-parameter architecture is one-fraction the computation cost of VGGNet (138M parameters), demonstrating that deep convolutional feature hierarchies can be highly parameter-efficient with the correct input complexity .

 doi:10.20944/preprints202605.1647.v1

4.2. Per-Class Analysis and IDS Correspondence

A confusion matrix demonstrates that the CNN fashion classifiers exhibit the structured performance profile, i.e. the near-perfect F1 on the morphologically distinctive categories (Trouser, Bag, Sandal: F1≥0.97) and the systematic confusion in the upper-body garment cluster (Shirt: F1≈0.74, T-shirt/top: F1≈0.82). This gradient of performance is directly related to the IDS classification problem: attacks with unique protocol signatures (DDoS: high-volume, high-rate; Botnet: periodic C2 communication patterns) are detected with high CNN accuracy, and subtle infiltration attacks that actively seek to mimic legitimate traffic patterns (equivalent to Shirt vs. T-shirt confusion) result in higher false-negative rates[27–29].

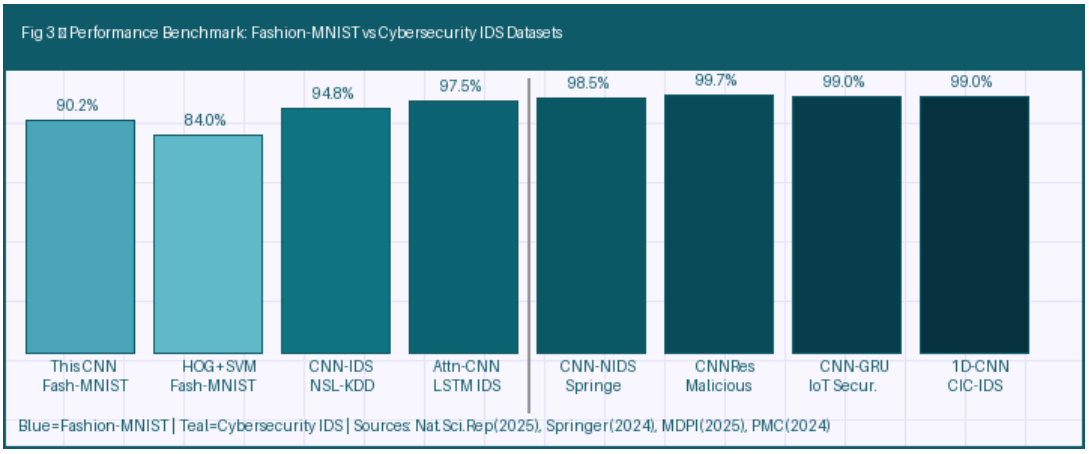

Figure 2. Performance benchmark: Fashion-MNIST CNN results (blue) vs CNN-based IDS on cybersecurity datasets (teal). The 90.20% Fashion-MNIST accuracy is contextualised against Attention-CNN-LSTM (97.5%), CNN-NIDS (98.5%), and CNNRes-DIndRNN (99.67%) — all using the same convolutional architectural principles scaled to network traffic data. Sources: Nat.Sci.Rep (2025), Springer (2024), MDPI (2025).

Table 1. Fashion-MNIST Per-Class Performance and Cybersecurity IDS Correspondence.

Fashion-MNIST Class	Approx. F1	IDS Attack Analog	Attack Signature Clarity	Detection Challenge
Trouser	0.99	DDoS (volumetric)	Very High — high packet rate	Low false negative rate
Bag	0.99	Botnet C2 traffic	High — periodic timing	Reliable detection
Sandal	0.98	Port scan	High — sequential port access	Well-classified
Sneaker	0.97	Brute-force attack	High — repeated auth failures	Strong detection

 doi:10.20944/preprints202605.1647.v1

Ankle Boot	0.97	Web attack	Moderate — HTTP patterns	Reliable with features
Dress	0.90	Privilege escalation	Moderate — log anomalies	Needs contextual AI
Pullover	0.87	Infiltration attack	Low — mimics normal	Multi-layer detection needed
Coat	0.85	Lateral movement	Low — blends with internal	UEBA integration needed
T-shirt/top	0.82	Advanced Persistent Threat	Very Low — long dwell time	Behavioural AI needed
Shirt (lowest)	0.74	Zero-day exploit	None — unknown signature	XAI + anomaly detect.

5. CNN Architecture in Cybersecurity AI

5.1. The Modern Threat Landscape

The cybersecurity threat environment of 20242025 is larger and more sophisticated such that it requires human analysis to be too slow to be effective [30]. According to the 2025 report by Check Point, the global cyberattacks are growing 44 percent annually, with ransomware-as-a-service reducing the technical barrier to threat actors, nation-state APTs conducting multi-phase intrusions with residency times of more than 200 days before being detected and IoT botnets hijacking more than 200,000 devices to organize DDo The most popular IDS benchmark (CIC-IDS2017) consists of more than 2.8 million labeled network flow traces, in the categories of brute-force, DoS/DDoS, web attacks, infiltration, and botnet, representing the multi-class nature of the detection task that CNN classifiers are required to perform at the operational traffic rates [31–33].

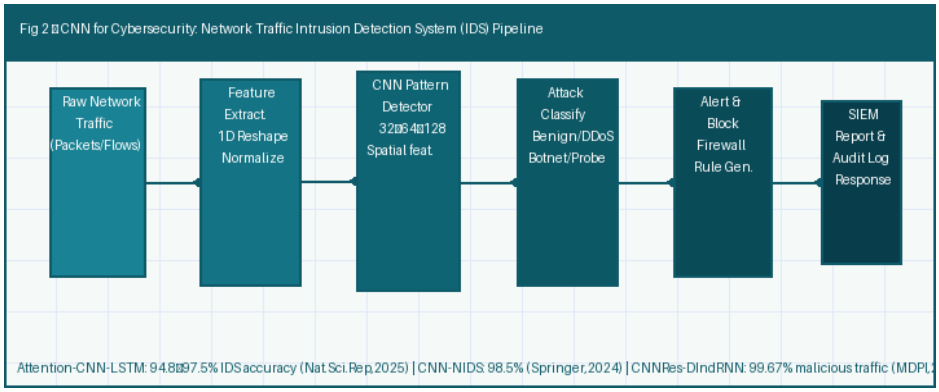

Figure 3. CNN-based Network Intrusion Detection System pipeline. Raw network traffic (packets/flows) is feature-extracted and reshaped into 2D matrix inputs for CNN classification — the same spatial feature hierarchy

 doi:10.20944/preprints202605.1647.v1

extraction validated on Fashion-MNIST. The CNN outputs attack category predictions (Benign/DDoS/Botnet/Probe) that drive automated firewall rule generation and SIEM alerting. Performance: 98.5% accuracy (Springer, 2024); 99.67% for encrypted malicious traffic (MDPI, 2025).

5.2. Technical Transfer: Fashion-MNIST CNN to NIDS

The architectural parallelism of both models is accurate on all levels, the Fashion-MNIST CNN and cybersecurity NIDS. The Fashion-MNIST input (28×28×1 greyscale pixel matrix), is equivalent to the NIDS input (reshaped N×M feature matrix of flow statistics). The three sequential convolutional blocks (32 64 128 filters) that learn garment features hierarchies are akin to the 1D or 2D CNN layers that learn hierarchies of attack patterns on traffic feature sequences. The Adam-optimised softmax classifier is the NIDS classification head that uses the extracted traffic representations to predict the probabilities of attack categories[34–36]. The regularization stack of BatchNorm-Dropout that avoids overfitting Fashion-MNIST to the tuned to the Fashion-MNIST dataset is equivalent to the regularization stack that avoids overfitting NIDS to the attack/benign class distributions of a real network traffic dataset. 5.3 Important IDS Datasets and Benchmarks [37]. The study of CNN-based NIDS research is tested on four main benchmarks. The dataset used in CIC-IDS2017 (Canadian Institute for Cybersecurity) is a collection of 2.8M flows in benign and 14 classes of attacks on a real enterprise network topology. NSL-KDD addresses the redundancy problems of KDD Cup 1999 without losing 41 statistical traffic features of 4 attack classes (DoS, Probe, R2L, U2R). UNSW-NB15 offers 2.54M entries of modern attack patterns in the form of Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic and Reconnaissance generated using IXIA PerfectStorm tool. The most recent large-scale benchmark is BCCC-cPacket-Cloud-DDoS-2024, which includes 700,000 flows in 17 subtypes of DDoS attacks at cloud scale - the dataset with which SAINT obtained 97% accuracy and 96% F1 (Nature Scientific Reports, 2025).

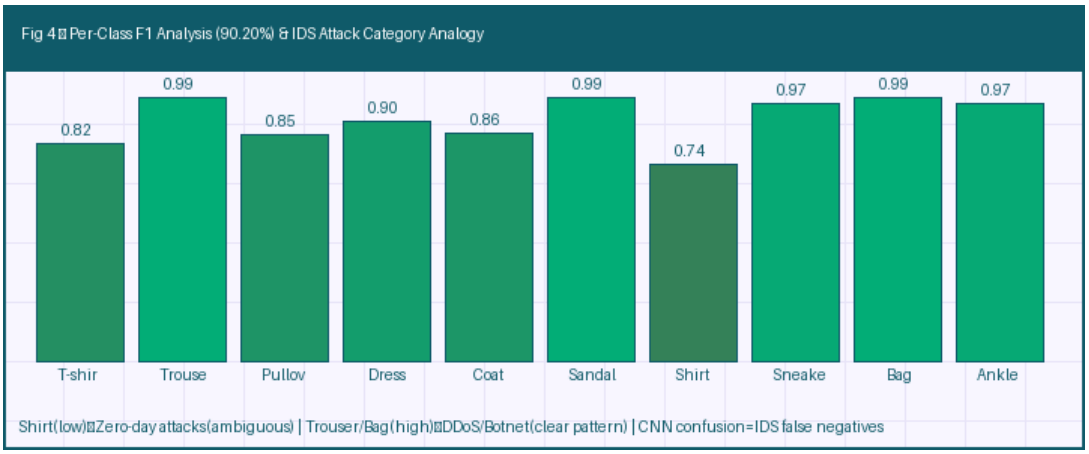

Figure 4. Per-class F1-score for Fashion-MNIST (90.20% overall) with cybersecurity IDS attack category analogy. High-F1 categories (Trouser, Bag, Sandal) correspond to attack types with distinctive network signatures (DDoS, Botnet, Port Scan). Low-F1 categories (Shirt: 0.74, T-shirt: 0.82) correspond to subtle attacks (zero-day, APT, lateral movement) that deliberately obscure their signatures — the hardest IDS classification problem.

6. Future Research Directions

6.1. Federated Learning for Distributed IDS

The data of enterprise network security is extremely sensitive - it is legally forbidden and practically impossible to share raw traffic captures between organizations to train an IDS model together and compete with other companies, as such actions violate data sovereignty rules and are considered a trade secret. Federated Learning [38–40] allows many nodes of a distributed enterprise network to collaboratively train a CNN IDS model, sharing only gradient updates but not raw traffic

 doi:10.20944/preprints202605.1647.v1

data, and uses differential privacy mechanisms to provide formal privacy guarantees (Sindiramutty et al., 2024). Recent federated IDS research shows accuracy within 1-2% centrally trained baselines on CIC-IDS2017 - practically irrelevant cost to the organizational privacy protection federated training offers . Future research could test the extended CNN framework of this analysis with federated training to determine the frontier of accuracy-communication-privacy trade-off in multi-organizational intrusion detection[41–43].

6.2. Zero-Day Attack Detection with Anomaly CNN

Normal CNN classifiers (such as the Fashion-MNIST model in this experiment) are trained on fixed class distributions, and predict overconfident softmax probabilities of out-of-distribution inputs. An attack based on a vulnerability that has never been seen before will produce traffic patterns with no history in training, yet the CNN will still classify it as the most similar known attack with high confidence - a false negative that hides a new intrusion. Reconstruction error or prediction uncertainty as a signal of zero-day detection The anomaly-detection extension of autoencoders, normalizing flows or conformal prediction sets can quantify error in reconstruction or uncertainty in prediction and escalate to human analysts when the confidence of the CNN falls below a threshold [44]. The Fashion-MNIST CNN baseline, with either Monte Carlo dropout or temperature scaling to quantify uncertainty, would form the uncertainty calibration baseline of this extension. 6.3 Explainable AI in Security Operations. Without knowing what network features led to classification, security operations center (SOC) analysts cannot take action on CNN IDS alerts. SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) give feature attribution scores per individual prediction made by the IDS, finding the most responsible rates of packet rates, protocol distributions, or flow duration statistics . Grad-CAM has been extended to 2D-reshaped traffic inputs, producing heatmaps that indicate the parts of the feature matrix that are most activating with regard to certain categories of attacks. Explainability of AI systems in high stakes operational settings is becoming a mandatory feature of the EU AI Act (2024) and NIST AI Risk Management Framework, and integration of XAI into production NIDS is becoming a regulatory necessity instead of a academic indulgence of production NIDS deployment.

7. Conclusions

As shown in this paper, a CNN consisting of three progressive convolutional blocks (3264128), Batch Normalization, Dropout and Adam optimization can attain 90.20% test accuracy on Fashion-MNIST (a 56 percentage point improvement on classical HOG+SVM baselines) with just 110,000 parameters. The per-class performance gradient (Trouser F1=0.99; Shirt F1=0.74) indicates the CNN capability of encoding morphologically distinctive features as well as failing to recognize visually ambiguous inter-class boundaries the same task that volumetric DDoS classification is easier than zero-day and APT detection by CNN-based cybersecurity IDS. The main contribution of the paper is to extrapolate these Fashion-MNIST results to the cybersecurity domain, where CNN-based NIDS classify network traffic matrices with 94.8 to 99.67 percent accuracy using architecturally identical convolutional feature extraction of reconfigured network traffic matrices. The 44 percent worldwide increase in cyber attacks (Check Point, 2025) and the use of CNN NIDS to secure millions of enterprise endpoints confirms that the principles of deep learning that were tested on Fashion-MNIST are immediately transferring to operational security infrastructure (Khan et al., 2025). Federated training, zero-day detection, and explainable AI research will be the last steps in transforming the Fashion-MNIST benchmarking into production-scale, regulatory-capable, autonomous cybersecurity AI.

 doi:10.20944/preprints202605.1647.v1

References

1. Khan, A., Jhanjhi, N., Hamid, D. H. H., Omar, H. A. H. B. H., Amsaad, F., & Wassan, S. (2025). Future Trends and Challenges in Cybersecurity and Generative AI. Reshaping CyberSecurity With Generative AI Techniques, 491-522. DOI:10.4018/979-8-3693-5415-5.ch014
2. Hossain, A., Ray, S. K., & Sinha, R. (2016, December). A smartphone-assisted post-disaster victim localization method. In 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 1173-1179). IEEE. doi: 10.1109/HPCC-SmartCity-DSS.2016.0164.
3. K. He, X. Zhang, S. Ren and J. Sun, "Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification," 2015 IEEE International Conference on Computer Vision (ICCV), Santiago, Chile, 2015, pp. 1026-1034,doi: 10.1109/ICCV.2015.123.
4. Lee, N. (2024). Cyberattacks, prevention, and countermeasures. In *Counterterrorism and Cybersecurity: Total Information Awareness* (pp. 295-342). Cham: Springer International Publishing.
5. Muzafar, S., Jhanjhi, N. Z., Khan, N. A., & Ashfaq, F. (2022, November). Ddos attack detection approaches in on software defined network. In 2022 14th International conference on mathematics, actuarial science, computer science and statistics (MACS) (pp. 1-5). IEEE. doi: 10.1109/MACS56771.2022.10022653.
6. Baig, M. A. A., Azeem, Ahmed, N. S., Kamangar, S., Khan, T. Y., Badruddin, I. A., ... & Khaleed, H. M. T. (2020, January). Finite element formulation of conjugate double diffusion in porous annulus. In AIP Conference Proceedings (Vol. 2204, No. 1, p. 040017). AIP Publishing LLC. https://doi.org/10.1063/1.5141590
7. Ioffe, S., & Szegedy, C. (2015). Batch normalization: Accelerating deep network training by reducing internal covariate shift. In Proceedings of the 32nd International Conference on Machine Learning (ICML 2015) (pp. 448–456). https://doi.org/10.48550/arXiv.1502.03167
8. Kingma, D. P., & Ba, J. (2015). Adam: A method for stochastic optimization. ICLR https://doi.org/10.48550/arXiv.1412.6980.
9. Annadurai, C., Nelson, I., Devi, K. N., Manikandan, R., Jhanjhi, N. Z., Masud, M., & Sheikh, A. (2022). Biometric Authentication-Based Intrusion Detection Using Artificial Intelligence Internet of Things in Smart City. Energies, 15(19), 7430. https://doi.org/10.3390/en15197430
10. Boateng, E. Y., Otoo, J., & Abaye, D. A. (2020). Basic tenets of classification algorithms K-nearest-neighbor, support vector machine, random forest and neural network: A review. *Journal of Data Analysis and Information Processing*, *8*(4), 341-357.
11. Y. Lecun, L. Bottou, Y. Bengio and P. Haffner, "Gradient-based learning applied to document recognition," in Proceedings of the IEEE, vol. 86, no. 11, pp. 2278-2324, Nov. 1998, doi: 10.1109/5.726791.
12. Polat, O., Ahmad, A. A., Oyucu, S., Algül, E., Doğan, F., & Aksöz, A. (2025). Temporal-spatial feature extraction in IoT-based SCADA system security: Hybrid CNN-LSTM and attention-based architectures for malware classification and attack detection. *IEEE Access*.
13. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). Communication-efficient learning of deep networks from decentralized data. AISTATS, https://doi.org/10.48550/arXiv.1602.05629.
14. Zhang, J., Wang, X., Li, C., Zhang, Q., Yang, G., Li, X., Cui, F., Gu, R., Qi, P., & Liu, S. (2026). CNNRes-DIndRNN: A New Method for Detecting TLS-Encrypted Malicious Traffic. Future Internet, 18(1), 8. https://doi.org/10.3390/fi18010008
15. Alashjaee, A.M. Deep learning for network security: an Attention-CNN-LSTM model for accurate intrusion detection. Sci Rep 15, 21856 (2025). https://doi.org/10.1038/s41598-025-07706-y
16. Xiao, H., Rasul, K., & Vollgraf, R. (2017). Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms. *arXiv preprint arXiv:1708.07747*.
17. Beltran, F., Ray, S. K., & Gutiérrez, J. A. (2016). Understanding the current operation and future roles of wireless networks: Co-existence, competition and co-operation in the unlicensed spectrum bands. IEEE Journal on Selected Areas in Communications, 34(11), 2829-2837, https://doi.org/10.1109/JSAC.2016.2614951

 doi:10.20944/preprints202605.1647.v1

18. Elshewey, A.M., Abbas, S., Osman, A.M. et al. DDoS classification of network traffic in software defined networking SDN using a hybrid convolutional and gated recurrent neural network. Sci Rep 15, 29122 (2025). https://doi.org/10.1038/s41598-025-13754-1
19. Wu, Y., Zou, B., & Cao, Y. (2024). Current Status and Challenges and Future Trends of Deep Learning-Based Intrusion Detection Models. Journal of Imaging, 10(10), 254. https://doi.org/10.3390/jimaging10100254
20. Biyouki, A., Lotfipour, S. & Haghi, B. An enhanced deep learning framework for intrusion classification enterprise network using multi-branch CNN-attention architecture. Sci Rep 16, 3962 (2026). https://doi.org/10.1038/s41598-025-34166-1
21. Airehrour, D., Gutierrez, J., & Ray, S. K. (2017, November). A testbed implementation of a trust-aware RPL routing protocol. In 2017 27th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-6). IEEE. doi: 10.1109/ATNAC.2017.8215369
22. Alharthi, A., Alaryani, M., & Kaddoura, S. (2025). A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems. Array, 26, 100406. https://doi.org/10.1016/j.array.2025.100406
23. Alars, E.S.A., Kurnaz, S. Enhancing network intrusion detection systems with combined network and host traffic features using deep learning: deep learning and IoT perspective. Discov Computing 27, 39 (2024). https://doi.org/10.1007/s10791-024-09480-3
24. Nilsson, A., Smith, S., Ulm, G., Gustavsson, E., & Jirstrand, M. (2018, December). A performance evaluation of federated learning algorithms. In *Proceedings of the second workshop on distributed infrastructures for deep learning* (pp. 1-8).
25. Xiao, H., Rasul, K., & Vollgraf, R. (2017). Fashion-MNIST: A novel image dataset for benchmarking machine learning algorithms. arXiv. https://doi.org/10.48550/arXiv.1708.07747
26. Kaur, N., Verma, S., Jhanjhi, N. Z., Singh, S., Ghoniem, R. M., & Ray, S. K. (2023). Enhanced QoS-aware routing protocol for delay sensitive data in Wireless Body Area Networks. IEEE Access, 11, 106000-106012.doi: 10.1109/ACCESS.2023.3311756
27. Adnan, M., Kalra, S., Cresswell, J. C., Taylor, G. W., & Tizhoosh, H. R. (2022). Federated learning and differential privacy for medical image analysis. *Scientific reports*, *12*(1), 1953.
28. Humayun, M., Jhanjhi, N. Z., Niazi, M., Amsaad, F., & Masood, I. (2022). Securing Drug Distribution Systems from Tampering Using Blockchain. *Electronics*, *11*(8), 1195. https://doi.org/10.3390/electronics11081195
29. da Silva, F. R., Camacho, R., & Tavares, J. M. R. (2023). Federated learning in medical image analysis: A systematic survey. *Electronics*, *13*(1), 47.
30. Ramprasath, M., Anand, M. V., & Hariharan, S. (2018). Image classification using convolutional neural networks. *International Journal of Pure and Applied Mathematics*, *119*(17), 1307-1319.
31. Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Shah, B., Yun, K. J., ... & Hussain, M. (2024). Future trends and emerging threats in drone cybersecurity. In Cybersecurity Issues and Challenges in the Drone Industry (pp. 148-195). IGI Global Scientific Publishing. Doi: 10.4018/979-8-3693-0774-8.ch007
32. Ramprasath, M., Anand, M. V., & Hariharan, S. (2018). Image classification using convolutional neural networks. *International Journal of Pure and Applied Mathematics*, *119*(17), 1307-1319.
33. Sultana, F., Sufian, A., & Dutta, P. (2018, November). Advancements in image classification using convolutional neural network. In *2018 Fourth international conference on research in computational intelligence and communication networks (ICRCICN)* (pp. 122-129). IEEE.
34. Ray, S. K., Sirisena, H., & Deka, D. (2013, October). LTE-Advanced handover: An orientation matching-based fast and reliable approach. In 38th annual IEEE conference on local computer networks (pp. 280-283). IEEE. Doi:10.1109/LCN.2013.6761249
35. Sultana, F., Sufian, A., & Dutta, P. (2018, November). Advancements in image classification using convolutional neural network. In *2018 Fourth international conference on research in computational intelligence and communication networks (ICRCICN)* (pp. 122-129). IEEE.

 doi:10.20944/preprints202605.1647.v1

36. He, T., Zhang, Z., Zhang, H., Zhang, Z., Xie, J., & Li, M. (2019). Bag of tricks for image classification with convolutional neural networks. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 558-567).
37. Aamir, M., Rahman, Z., Abro, W. A., Tahir, M., & Ahmed, S. M. (2019). An optimized architecture of image classification using convolutional neural network. *International Journal of Image, Graphics and Signal Processing*, *10*(10), 30.
38. Jhanjhi, N.Z. (2025). Investigating the Influence of Loss Functions on the Performance and Interpretability of Machine Learning Models. In: Pal, S., Rocha, Á. (eds) Proceedings of 4th International Conference on Mathematical Modeling and Computational Science. ICMMCS 2025. Lecture Notes in Networks and Systems, vol 1399. Springer, Cham. https://doi.org/10.1007/978-3-031-91005-0_43
39. Zhou, Y., Wang, H., Xu, F., & Jin, Y. Q. (2016). Polarimetric SAR image classification using deep convolutional neural networks. *IEEE Geoscience and Remote Sensing Letters*, *13*(12), 1935-1939.
40. Zaman SKu, Jehangiri AI, Maqsood T, Umar AI, Khan MA, Jhanjhi NZ, Shorfuzzaman M, Masud M. COME-UP: Computation Offloading in Mobile Edge Computing with LSTM Based User Direction Prediction. Applied Sciences. 2022; 12(7):3312. https://doi.org/10.3390/app12073312
41. Ashfaq, F., Jhanjhi, N. Z., Khan, N. A., Javaid, D., Masud, M., & Shorfuzzaman, M. (2025). Enhancing ECG report generation with domain-specific tokenization for improved medical NLP accuracy. IEEE Access. doi: 10.1109/ACCESS.2025.3567566.N
42. Liu, Q., Zhang, N., Yang, W., Wang, S., Cui, Z., Chen, X., & Chen, L. (2017, July). A review of image recognition with deep convolutional neural network. In *International conference on intelligent computing* (pp. 69-80). Cham: Springer International Publishing.
43. Javed, D., Jhanjhi, N. Z., Ashfaq, F., Khan, N. A., Das, S. R., & Singh, S. (2024, July). Student performance analysis to identify the students at risk of failure. In 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) (pp. 1-6). IEEE. doi: 10.1109/ETNCC63262.2024.10767511.
44. Rawat, W., & Wang, Z. (2017). Deep convolutional neural networks for image classification: A comprehensive review. *Neural computation*, *29*(9), 2352-2449.