Model Type: Feed Forward ANN, Solver: adam, Activation: relu, Alpha: 0.01, Learning Rate: 0.0001

Test Loss: 1438.5330810546875, Test Accuracy: 0.9461895823478699

Model Type: Shallow ANN, Solver: adam, Activation: relu, Alpha: 0.0001, Learning Rate: 0.0001

Test Loss: 351.3888244628906, Test Accuracy: 0.953904926776886

Model Type: Deep ANN, Solver: adam, Activation: tanh, Alpha: 0.0001, Learning Rate: 0.0001

Test Loss: 0.2164868414402008, Test Accuracy: 0.920325517654419

Model Type: Hybrid ANN, Solver: sgd, Activation: sigmoid, Alpha: 0.01, Learning Rate: 0.01

Test Loss: 1.213391900062561, Test Accuracy: 0.8312811851501465

Model Type: Feed Forward ANN, Solver: adam, Activation: relu, Alpha: 0.01, Learning Rate: 0.0001

Test Loss: 4817.4814453125, Test Accuracy: 0.9450021982192993

Model Type: Shallow ANN, Solver: adam, Activation: relu, Alpha: 0.0001, Learning Rate: 0.001

Test Loss: 294.1300354003906, Test Accuracy: 0.9623293280601501

Model Type: Deep ANN, Solver: adam, Activation: sigmoid, Alpha: 0.0001, Learning Rate: 0.0001

Test Loss: 0.23533883690834045, Test Accuracy: 0.9301398992538452

Model Type: Hybrid ANN, Solver: adam, Activation: relu, Alpha: 0.001, Learning Rate: 0.0001

Test Loss: 0.24203117191791534, Test Accuracy: 0.934371829032898

Lack of comprehensive studies comparing the performance of different ANN architectures for NIDS on IoT edge devices.

* Absence of benchmarking frameworks to systematically evaluate and compare the efficacy of these architectures under varying conditions and attack scenarios.
* Limited research addressing the unique challenges of deploying NIDS with ANNs on IoT edge devices with limited computational resources and memory.
* Insufficient exploration of techniques to optimize ANN models for efficient execution on resource-constrained IoT edge devices without compromising detection accuracy.
* Inadequate investigation into how different ANN architectures influence NIDS performance, resource utilization, and scalability in IoT edge environments.
* Lack of understanding regarding which ANN architectures are most suitable for specific types of attacks and network conditions encountered in IoT edge deployments.

|  |  |  |
| --- | --- | --- |
| Paper | Key Findings | Focus |
| TSP\_CMC\_18708.pdf | - Proposes PCA-CNN for intrusion detection in IoT. - Achieves high accuracy in binary and multiclass classification. | Deep Learning Intrusion Detection |
| Injection-attack-detection-using-machine-learning-for-s\_2022\_Physical-Commun.pdf | - Machine learning for intrusion detection in IoT with high accuracy (99%) for injection attacks. - Random Forest classifier outperforms others. | Machine Learning for Intrusion Detection |
| IJCDS-110117-1570719367.pdf | - Hybrid deep learning (CNN-LSTM) for intrusion detection in IoT networks. - Achieves 99.32% accuracy. | Deep Learning Intrusion Detection |
| electronics-13-01053.pdf | - Challenges of deploying IDSs in resource-constrained IoT edge environments. - Lightweight IDS with machine learning for anomaly-based intrusion detection. | Intrusion Detection Systems (IDS) for IoT |
| 1645511771\_12362-English.pdf | - Emphasizes anomaly-based IDS techniques using machine learning for IoT. - Need for efficient and scalable IDS for resource-constrained IoT devices. | Intrusion Detection Systems (IDS) for IoT |
| 2012.01174.pdf | - Explores Multi-Access Edge Computing (MEC) for overcoming limitations of resource-constrained IoT devices in IDS. - Importance of real-time threat detection and response. | Intrusion Detection Systems (IDS) for IoT using MEC |
| 1-s2.0-S0045790623001519-main.pdf | - Deep learning for network intrusion prevention in IoT with edge intelligence. - Distributed IDS architecture with local and global deep learning models. | Deep Learning Intrusion Detection for IoT |
| sensors-22-03744-v2.pdf | - Reviews NIDS design approaches for resource-constrained IoT devices. - Explores MEC for sophisticated IoT security systems. - Analyzes Machine Learning for anomaly-based intrusion detection in IoT. - Compares datasets and metrics for NIDS development in IoT. - Proposes a security framework for IoT using MEC. | Network Intrusion Detection Systems (NIDS) for IoT using MEC and Machine Learning |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Paper | | Key findings | | | Focus | | | |
| TSP\_CMC\_18708.pdf | | - Proposes PCA-CNN for intrusion detection in IoT. - Achieves high accuracy in binary and multiclass classification. | | | Deep Learning Intrusion Detection | | | |
| Injection-attack-detection-using-machine-learning-for-s\_2022\_Physical-Commun.pdf | | - Machine learning for intrusion detection in IoT with high accuracy (99%) for injection attacks. - Random Forest classifier outperforms others. | | | Machine Learning for Intrusion Detection for injection attack | | | |
| IJCDS-110117-1570719367.pdf | - Hybrid deep learning (CNN-LSTM) for intrusion detection in IoT networks. - Achieves 99.32% accuracy. | | | | | Deep Learning Intrusion Detection | | |
| electronics-13-01053.pdf | - Challenges of deploying IDSs in resource-constrained IoT edge environments. - Lightweight IDS with machine learning for anomaly-based intrusion detection. | | | | | Intrusion Detection Systems (IDS) for IoT | | |
|  |  | | | | |  | | |
| 1645511771\_12362-English.pdf | - Emphasizes anomaly-based IDS techniques using machine learning for IoT. - Need for efficient and scalable IDS for resource-constrained IoT devices. | | | | | Intrusion Detection Systems (IDS) for IoT | | |
| 2012.01174.pdf | - Explores Multi-Access Edge Computing (MEC) for overcoming limitations of resource-constrained IoT devices in IDS. - Importance of real-time threat detection and response. | | | | | Intrusion Detection Systems (IDS) for IoT using MEC | | |
|  | | |  | | | | |  |
| 1-s2.0-S0045790623001519-main.pdf | | | - Deep learning for network intrusion prevention in IoT with edge intelligence. - Distributed IDS architecture with local and global deep learning models. | | | | | Deep Learning Intrusion Detection for IoT |
| sensors-22-03744-v2.pdf | | | - Reviews NIDS design approaches for resource-constrained IoT devices. - Explores MEC for sophisticated IoT security systems. - Analyzes Machine Learning for anomaly-based intrusion detection in IoT. - Compares datasets and metrics for NIDS development in IoT. - Proposes a security framework for IoT using MEC. | | | | | Network Intrusion Detection Systems (NIDS) for IoT using MEC and Machine Learning |
|  | | | |  | | |  | |
|  | | | |  | | |  | |

[1] [2] [3] [4] [5] [6] [7] [8]

|  |  |
| --- | --- |
| [1] | M. A. R. K. a. T. A.-H. Mohd Anul Haq, "Development of PCCNN-Based Network Intrusion Detection System for EDGE Computing," *Computers, Materials & Continua,* vol. 71, p. 20, 2021. |
| [2] | b. ,. A. E.-G. c. ,. A. E. H. Tarek Gaber a, "Injection attack detection using machine learning for smart IoT applications," *Elsevier,* vol. 52, p. 14, 2022. |
| [3] | M. A. a. O. M. Idriss Idrissi1, "A Lightweight Optimized Deep Learning-based Host-Intrusion Detection System Deployed on the Edge for IoT," *International Journal of Computing and Digital Systems,* vol. 11, p. 8, 2022. |
| [4] | S. Y. a. M. Dener, "IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm," *Electronics,* p. 28, 2024. |
| [5] | R. K. b. ,. G. R. c. ,. K. S. S. d. ,. S. S. e. ,. S. K. Dhanke Jyoti Atul a, "A machine learning based IoT for providing an intrusion detection system for security," *Elsevier,* p. 10, 2021. |
| [6] | P. S. a. F. Cuomo1, "INTRUSION DETECTION SYSTEMS FOR IOT: OPPORTUNITIES AND CHALLENGES OFFERED BY EDGE COMPUTING AND MACHINE LEARNING," p. 25, 2012. |
| [7] | M. R. I. b. ,. S. M. c. ,. A. S. A. d. Mansura Habiba a, "Edge intelligence for network intrusion prevention in IoT ecosystem✩," *Elsevier,* p. 15, 2023. |
| [8] | E. G. ∗. a. A. Jurcut, "Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets," *Sensors,* vol. 22, p. 33, 2022. |