INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 998-1002

www.ijprems.com
editor@ijprems.com

e-ISSN : 2583-1062
Impact Factor : 7.001

TOWARDS SUSTAINABLE CYBER SECURITY: ENERGY-AWARE INTRUSION DETECTION USING DEEP LEARNING

Rahul Senthiya[1], Prof. Nitesh Gupta[2]

[1]M.Tech Scholar, CSE, NIIST, India.

[*2]AP, CSE, NIIST, India.

rdsenthiya@gmail.com, nitesh@gmail.com

DOI: https://www.doi.org/10.58257/IJPREMS43903

ABSTRACT

The increasing sophistication of cyber threats in modern networks necessitates intelligent and resilient security solutions. Conventional intrusion detection systems (IDS) are often hindered by high computational requirements and limited scalability, making them less effective for real-time use in resource-constrained settings. To overcome these limitations, this research introduces energy-efficient IDS leveraging the CICIDS2017 dataset, which offers a diverse mix of benign and malicious traffic for robust training and evaluation. The proposed method employs a hybrid deep learning framework that combines Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks to extract both spatial and temporal characteristics from network flows. Pruning and quantization enhance energy efficiency without reducing accuracy. The model achieves strong performance while lowering energy use, making it fit for real-time, energy-sensitive environments.

Keywords: CNN, Intrusion Detection System, Classification, Deep Learning, Recurrent Neural Network (RNN), Pre-Processing, Feature Selection, Deep Learning Models, Energy Efficiency, Cyber Security.

1. INTRODUCTION

The exponential growth of digital communication and online services has dramatically increased the vulnerability of modern networks to cyberattacks. Malicious activities such as denial-of-service, brute force, botnet attacks, and infiltration not only compromise sensitive information but also threaten the overall reliability of critical infrastructures. As a result, the demand for effective intrusion detection systems (IDS) has become more urgent than ever. Traditional IDS approaches, which rely heavily on signature-based or shallow machine learning methods, often struggle to cope with the dynamic and evolving nature of network threats. Moreover, these conventional solutions typically demand high computational resources, making them unsuitable for real-time deployment in environments where energy efficiency and scalability are crucial. Deep learning has emerged as a promising solution due to its capability to automatically extract high-level features and adapt to complex attack patterns. In particular, hybrid models that combine Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are effective in capturing both spatial correlations and temporal dependencies in network traffic. However, while deep learning models provide high detection accuracy, their computational complexity often results in significant energy consumption, posing challenges for deployment in resource-constrained or real-time scenarios.

To address these challenges, this research focuses on developing an energy-efficient IDS based on deep learning techniques. The CICIDS2017 dataset, which offers a comprehensive collection of benign and malicious traffic flows, is employed for model training and evaluation. In addition to adopting CNN-LSTM hybrid architecture, the proposed system incorporates optimization strategies such as pruning and quantization to reduce computational overhead and memory footprint, thereby enhancing energy efficiency without compromising performance. The proposed IDS not only achieve high accuracy, precision, recall, and F1-score but also demonstrates significant reductions in energy consumption compared to traditional deep learning models. This balance between detection capability and energy efficiency makes the system a promising candidate for deployment in real-time, energy-sensitive environments.

2. INTRUSION DETECTION SYSTEM (IDS)

In the era of information culture, as network-based computer systems play main roles, they have become the target for intrusions by attackers and criminals. Intrusion prevention technique such as firewalls, user authentication, information protection and data encryption have failed to completely shield networks and systems behaviour from the growing and sophisticated attacks and malwares. To protect the information from various attacks and viruses the Intrusion Detection Systems (IDS) are designed. An Intrusion Detection Systems (IDS) is a device that monitors network or system behaviour for malicious activities and produces reports to a management station [2]. An Intrusion Detection System (IDS) is a cyber security tool designed to monitor network traffic or system activities for malicious activities or policy violations. It acts as a security watchdog, identifying suspicious behaviours or unauthorized access attempts in real-time. IDS can be classified into two main types: Network-based IDS (NIDS), which monitors entire network traffic, and Host-based IDS (HIDS), which focuses on activities on individual devices [3]. Detection techniques include signature-based detection, which identifies known attack patterns, and anomaly-based detection, which flags deviations from normal behavior. While IDS can alert administrators of potential threats, it doesn't actively block them, distinguishing it from Intrusion Prevention Systems (IPS). Modern IDS solutions often integrate with other security tools to enhance threat response. By providing early warnings, IDS helps organizations mitigate security risks, maintain data integrity, and comply with regulatory standards. Effective IDS deployment requires regular updates and tuning to address evolving threats [5].

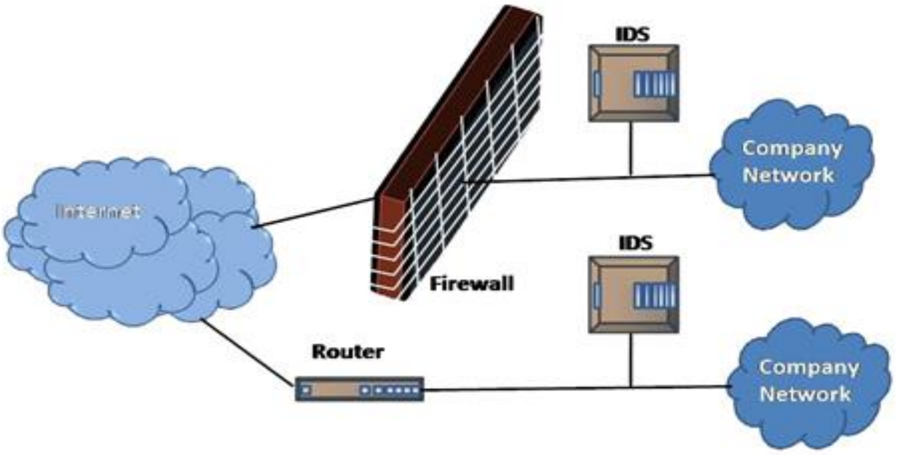

Figure: 1. Intrusion Detection Systems

3. LITERATURE SURVEY

There are several works related to intrusion detection system which is used deep neural network, convolution neural network, and recurrent neural network. Detailed review of the work is discussed in this chapter.

Authors [1] work introduces an energy-efficient IDS framework built on a modified Deep Neural Network incorporating Knowledge Distillation and Quantization (DNN-KDQ) to overcome existing challenges. The CICIDS2017 dataset was pre-processed to extract energy-focused features, while adaptive sampling and model compression techniques were employed to optimize system performance. The proposed DNN-KDQ model achieves a test accuracy of 99.43%, compresses model size from 196.77 KB to 20.18 KB, and delivers an inference time of just 0.07 ms per sample in real-time conditions. These outcomes confirm the practicality of deploying high-accuracy, low-latency IDS solutions on resource-constrained edge devices, paving the way for more scalable and energy-aware cyber security frameworks in modern network infrastructures.

Authors [2] review 50 papers on IoT intrusion detection, classifying methods into CNN, DNN, and optimization-based approaches. The analysis compares datasets, tools, performance metrics, and implementation aspects, highlighting key research gaps and the need for more efficient, scalable, and energy-aware IDS solutions.

Authors [3] work proposes an energy-efficient hybrid deep learning IDS inspired by biological systems, enabling intelligent decision-making for stronger security infrastructures. The model achieves high accuracy across metrics such as TPR, precision, and F-Measure, while showing resilience for long-term adaptation against evolving cyber threats despite minor variations in FPR and FNR.

Authors [4] propose an Intrusion Detection System that, leveraging on probabilistic data structures and Deep Learning techniques, is able to process in real time the traffic collected in a backbone network, offering excellent detection performance and low false alarm rate. Indeed, the extensive experimental tests, run to validate our system and compare different Deep Learning techniques, confirm that, with a proper parameter setting, we can achieve about 92% of detection rate, with an accuracy of 0.899.

Authors [5] paper reviews techniques related to intrusion detection, machine learning techniques and deep learning techniques, and focuses on deep learning-based IDSs. Traditional machine learning IDSs are able to deal with problems requiring a large number of rules and inefficient complex problems, however, they have several limitations, such as feature extraction and data pre-processing that are not optimised enough, leading to low detection accuracy; the presence of redundant or irrelevant data, leading to long training times and high risk of over fitting; and high noise interference and weak identification of novel attacks. These problems are particularly prominent when dealing with high-dimensional data generated by massive amounts of IoT sensors and devices. Compared to machine learning, DLbased IDS overcomes the ML slow training problem, is more suitable for handling large-scale, diverse and high-dimensional network traffic data, and can efficiently train non-linear models and detect new forms of attacks with high accuracy, making it a superior technique.

Authors [6] studies the supervised machine learning algorithms classifiers that is KNN, NB and SVM for identifying whether the data is normal or attack for binary classification. These algorithms tested using NSL KDD standard dataset. Effective classifiers identified by comparing the performance on the Accuracy, False Positive rate and True Positive Rate (Recall). We conclude that from the experiment KNN Classifier outperforms other classifiers using 27 features of NSL KDD dataset for both 10% and 20% NSL KDD standard Dataset. It has the accuracy of 99 percent.

Authors [7] proposed algorithms that apply variation mode decomposition technique to find and extract periodic components from the original data before using Long Short-Term Memory neural networks to detect anomalies in the remainder time series. Furthermore, Authors methods include advanced techniques to eliminate prediction errors and automatically tune operational parameters. Extensive numerical results show that the proposed algorithms achieve comparable performance in terms of Precision, Recall, F-score, and MCC metrics while outperforming most of the state-of-the-art anomaly detection approaches in terms of initialisation delay and detection delay, which is favourable for practical applications.

Authors [8] examined an XGBoost-based feature selection algorithm was implemented to reduce the feature space of each dataset. Following that process, 17 and 22 relevant attributes were picked from the UNSW-NB15 and NSL-KDD, respectively. The accuracy obtained through the test subsets was used as the main performance metric in conjunction with the F1-Score, the validation accuracy, and the training time (in seconds). The results showed that for the binary classification tasks using the NSL-KDD, the XGBoost-LSTM achieved the best performance with a test accuracy (TAC) of 88.13%, a validation accuracy (VAC) of 99.49% and a training time of 225.46 s. For the UNSW-NB15, the XGBoost-Simple-RNN was the most efficient model with a TAC of 87.07%. For the multiclass classification scheme, the XGBoost-LSTM achieved a TAC of 86.93% over the NSL-KDD and the XGBoost-GRU obtained a TAC of 78.40% over the UNSW-NB15 dataset. These results demonstrated that our proposed IDS framework performed optimally in comparison to existing methods.

Authors [9] study demonstrates the significant potential of AI-based anomaly detection systems in enhancing real-time cyber security. These systems offer high detection accuracy, real-time processing capabilities, adaptability, and a degree of resilience to adversarial attacks. However, challenges related to computational efficiency and adversarial robustness need to be addressed to ensure the broader adoption and effectiveness of these systems in diverse cyber security environments. Future research should continue to explore hybrid models, advanced defense mechanisms, and efficient algorithms to overcome these challenges and further enhance the capabilities of AI-driven cyber security solutions.AI-based anomaly detection systems represent a transformative advancement in real-time cyber security.

4. PROPOSED METHODOLOGY

The proposed methodology introduces an energy-efficient intrusion detection system (IDS) that leverages a hybrid deep learning framework to ensure both high detection accuracy and reduced computational overhead. The approach is designed around three core stages: data pre-processing, model development, and optimization for energy efficiency. In the first stage, the CICIDS2017 dataset is selected due to its comprehensive mix of benign and malicious traffic flows, including various attack categories. Data pre-processing involves normalization, feature extraction, and dimensionality reduction to eliminate redundancy and highlight critical traffic attributes. Energy-centric features are emphasized to align the system with real-time, resource-constrained environments. The second stage focuses on model development using a hybrid Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) architecture. The CNN layers extract spatial correlations among features, while the LSTM layers capture sequential and temporal dependencies within network traffic. This combination allows the model to effectively distinguish between normal and malicious activities with improved generalization. The final stage integrates optimization techniques to achieve energy efficiency. Pruning is applied to remove redundant connections, reducing model complexity, while quantization compresses model parameters to minimize memory and computational requirements. In addition, knowledge distillation is employed to transfer learning from a larger, accurate teacher model to a lightweight student model, further reducing resource consumption without compromising accuracy. The optimized IDS is evaluated using performance metrics such as accuracy, precision, recall, F1-score, and energy consumption per inference. This methodology ensures scalable, accurate, and energy-aware IDS suitable for deployment in real-time, resource-limited network environments.

5. RESULT ANALYSIS

The comparative evaluation of the proposed hybrid IDS model against baseline CNN and LSTM models highlights its superior performance in both accuracy and efficiency. The CNN-based IDS achieved an accuracy of 98.1% with precision and recall values of 97.1% and 96.8%, respectively, while the LSTM model slightly improved performance with 98.54% accuracy, 97.7% precision, and 97.3% recall. Although both baselines demonstrated strong detection capability, they required larger model sizes (210.3 KB and 185.4 KB) and higher inference times (0.32 ms and 0.25 ms per sample), resulting in limited suitability for resource-constrained environments. In contrast, the proposed hybrid CNN-LSTM model significantly outperformed both baselines by achieving 99.1% accuracy, 98.64% precision, 98.54% recall, and 98.4% F1-score. Most notably, it achieved this performance with a drastically reduced model size of only 20.12 KB and an inference time of 0.07 ms per sample. These improvements are attributed to the integration of pruning, quantization, and knowledge distillation, which enhanced both computational and energy efficiency. The results demonstrate that the proposed IDS not only provides higher detection accuracy but also ensures scalability and low-latency performance, making it highly effective for deployment in real-time and energy-sensitive network security applications.

Table 5.1 Performace Comparison of Proposed Model vs Baseline Models

Model	Accuracy	Precision	Recall	F1-Score	Model Size	Inference Time	Energy Efficiency
CNN Based IDS	98.1	97.1	96.8	97	210.3	0.32	Low
LSTM Model	98.54	97.7	97.3	97.6	185.4	0.25	Moderate
Proposed Hybrid (CNN+LSTM)	99.1	98.64	98.54	98.4	20.12	0.07	High

6. CONCLUSION

This research presented an energy-efficient Intrusion Detection System (IDS) utilizing a hybrid deep learning framework that combines CNN and LSTM architectures. By leveraging the CICIDS2017 dataset, the proposed model demonstrated its ability to effectively capture both spatial and temporal dependencies in network traffic, ensuring high detection accuracy across multiple attack scenarios. Optimization techniques such as pruning, quantization, and knowledge distillation further enhanced the model’s efficiency, reducing its size and inference time while maintaining superior detection performance. The comparative analysis with baseline CNN and LSTM models validated the effectiveness of the proposed IDS. While traditional deep learning-based models provided strong accuracy, they exhibited higher computational overhead and energy demands, limiting their applicability in real-time, resource-constrained environments. In contrast, the proposed hybrid model not only achieved the highest accuracy (99.1%) and F1-score (98.4%) but also significantly minimized model size and inference latency. Overall, the findings highlight the potential of deploying lightweight, energy-efficient IDS solutions in modern network infrastructures. The proposed framework ensures scalability, low-latency detection, and sustainable energy usage, making it a promising approach for addressing the ever-evolving cyber security challenges in real-time environments.

7. REFERENCES

[1] Hafiz Gulfam Ahmad Umar, et. al. “Energy-efficient deep learning-based intrusion detection system for edge computing: a novel DNN-KDQ model” Journal of Cloud Computing (2025), https://doi.org/10.1186/s13677-025-00762-9, Springer

[2] Selvam Ravindran and Velliangiri Sarveshwaran “Deep Learning Towards Intrusion Detection System (IDS): Applications, Challenges and Opportunities” Journal of Mobile Multimedia, Vol. 19 5, 1299–1330. : 10.13052/jmm1550-4646.195, 8 2023 River Publishers

[3] Dr. Sandeep Kumar Hegde et. al. “ Energy Efficient Intrusion Detection System (IDS) and Feature Selection for IoT using DNN Model” International Journal of Intelligent Systems and Applications in Engineering IJISAE, 2024, 12(16s), 306–319

[4] Christian Callegari et. al. “A Real Time Deep Learning Approach for Based Detecting Network Attacks” https://doi.org/10.1016/j.bdr.2024.100446, Elsevier, 2024

[5] Yutong Wei, et. Al. “A review of deep learning based intrusion detection systems” Highlights in Science, Engineering and Technology AICT 2023 Volume 56 (2023)

[6] Surafel Mehari Atnafu, et. Al. “Comparative Analysis of Intrusion Detection Attack Based on Machine Learning Classifiers” Indian Journal of Artificial Intelligence and Neural Networking (IJAINN) ISSN: 2582-7626 (Online), Volume-1 Issue-2, April 2021

[7] Dániel László Vajda1 et al “ Machine learning-based real-time anomaly detection using data pre-processing in the telemetry of server farms” https://doi.org/10.1038/s41598-024-72982-z

[8] Sydney Mambwe Kasongo “A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework” https://doi.org/10.1016/j.comcom.2022.12.010 Elsevier, 2022

[9] Maloy Jyoti Goswami “AI-Based Anomaly Detection for Real-Time Cyber security” https://ijrrt.com, 2024

[10] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, F. Ahmad, Network intrusion detection system: A systematic study of machine learning and deep learning approaches, Trans. Emerg. Telecommun. Technol. 32 (1) (2021)

[11] R. Vinayakumar, M. Alazab, K.P. Soman, P. Poornachandran, A. Al-Nemrat, S. Venkatraman, Deep learning approach for intelligent intrusion detection system, IEEE Access 7 (2019) 41525–41550.

[12] Z. Chkirbene, A. Erbad, R. Hamila, A. Mohamed, M. Guizani, M. Hamdi, TIDCS: A dynamic intrusion detection and classification system based feature selection, IEEE Access 8 (2020).

[13] E. Alpaydin, Introduction to Machine Learning, MIT Press, 2020.

[14] M. Botvinick, S. Ritter, J.X. Wang, Z. Kurth-Nelson, C. Blundell, D. Hassabis, Reinforcement learning, fast and slow, Trends Cogn. Sci. 23 (5) (2019) 408–422.

[15] S. Raschka, V. Mirjalili, Python Machine Learning, Packt Publishing Ltd, 2017.

[16] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (7553) (2015) 436–444.

[17] Y. Wang, W. Liao, Y. Chang, Gated recurrent unit network-based short-term photovoltaic forecasting, Energies 11 (8) (2018) 2163.

[18] T. Chen, C. Guestrin, XGBoost: A scalable tree boosting system, in: Proceedings of the 22nd ACM Sigkdd Int Conf. on KDD, 2016, pp. 785–794.

[19] G. Meena, R.R. Choudhary, A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA, in: Int. Conf. on Comput. Commun. Electron., IEEE, 2017, pp. 553–558.

[20] A. F.. Jahwar and S.. Y. Ameen, "A Review on Cybersecurity based on Machine Learning and Deep Learning Algorithms", jscdm, vol. 2, no. 2, pp. 14 -25, Oct. 2021.

[21] A. L. Buczak and E. Guven, "A Survey of datas Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & amp; Tutorials, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016, doi: 10.1109/COMST.2015.2494502.

[22] http://nsl.cs.unb.ca/NSL-KDD/, November 2014.

[23] Samdanis, K. & Taleb, T. The road beyond 5G: A vision and insight of the key technologies. IEEE Network 34, 135–141. https://doi.org/10.1109/MNET.001.1900228 (2020).