International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 9, Issue 9, pp 49-53 September-2025
https://doi.org/10.47001/IRJIET/2025.909008

A Comprehensive Review on Energy Efficient Intrusion Detection System Based on Machine Learning and Deep Learning Technique

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

[1]M. Tech. Scholar, CSE, NIIST, India. E-mail: rdsenthiya@gmail.com
[2]AP, CSE, NIIST, India. E-mail: 9.nitesh@gmail.com

***Abstract* - With the rapid expansion of network-based applications, intrusion detection systems (IDS) have become essential for safeguarding sensitive data and ensuring system reliability. However, traditional IDS models often face challenges related to high computational cost and energy consumption, especially in resource-constrained environments. This paper presents a comprehensive review of energy-efficient IDS approaches based on machine learning and deep learning techniques. It covers various methods, including CNN, LSTM, auto encoders, optimization algorithms, and hybrid models, highlighting how they improve detection accuracy while reducing computational overhead. The review also analyzes datasets, performance metrics, and energy optimization strategies such as pruning, quantization, and knowledge distillation. By categorizing existing research and identifying gaps, this work aims to provide insights into designing scalable, low-latency, and energy-aware IDS solutions for modern networks. The findings serve as a foundation for future advancements in sustainable and intelligent cyber security systems.**

Keywords: Intrusion Detection System, Classification, Deep Learning, Pre-processing, Feature Selection, Deep learning models, Energy efficiency, Cyber security.

I. INTRODUCTION

With the widespread adoption of internet-based services, cloud computing, IoT, and mobile networks, cyber security threats have become increasingly sophisticated and frequent. Intrusion Detection Systems (IDS) play a critical role in protecting networks from unauthorized access, malware, and other malicious activities. Traditional IDS models, while effective in detecting known threats, often rely on signature-based methods that struggle with evolving attacks and unknown patterns. To overcome these limitations, researchers have increasingly turned to machine learning (ML) and deep learning (DL) techniques, which enable systems to learn from data and adapt to new threats. However, the deployment of ML/DL-based IDS in real-world scenarios faces significant challenges. These models are computationally intensive, leading to high energy consumption and longer processing times, especially in edge devices and resource-constrained environments. As networks scale and data volumes grow, energy efficiency becomes a major concern alongside detection accuracy. The growing demand for real-time threat detection in industries such as healthcare, finance, and smart cities further emphasizes the need for efficient IDS solutions. Energy-efficient models not only reduce operational costs but also extend the lifespan of devices in distributed networks. This review consolidates recent advancements and offers practical insights to enhance IDS designs, ensuring robust security while minimizing energy consumption. Efficient intrusion detection is crucial for maintaining network reliability without overburdening system resources.

This paper presents a comprehensive review of energy-efficient IDS solutions that leverage machine learning and deep learning approaches. It systematically analyzes various architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), autoencoders, and hybrid frameworks, along with optimization methods like pruning, quantization, and knowledge distillation. The review also highlights the datasets used, evaluation metrics, and tools that aid in achieving an optimal balance between accuracy and energy efficiency. By identifying research gaps, common challenges, and best practices, this review aims to guide future work in developing lightweight, scalable, and energy-aware IDS frameworks. The findings are intended to support researchers and practitioners in designing advanced cyber security solutions that are both intelligent and sustainable for modern network infrastructures.

II. INTRUSION DETECTION SYSTEM (IDS)

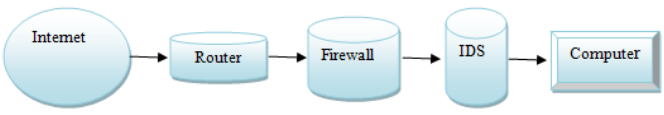

Figure 1: Intrusion Detection Systems

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 9, pp 49-53 September-2025

https://doi.org/10.47001/IRJIET/2025.909008

III. 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, DL-based 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

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 9, pp 49-53 September-2025

https://doi.org/10.47001/IRJIET/2025.909008

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.

IV. FINDING OF THE REVIEW

The review of recent studies on energy-efficient intrusion detection systems (IDS) reveals significant advancements in applying machine learning and deep learning techniques to enhance cybersecurity while minimizing resource usage. Several authors have focused on improving accuracy and energy efficiency by integrating optimization strategies such as pruning, quantization, and feature selection. For instance, authors [1] and [3] successfully demonstrated hybrid models combining CNN, LSTM, and biological inspirations to achieve high accuracy, low latency, and adaptability in real-time scenarios.

The analysis also shows that datasets like CICIDS2017, NSL-KDD, and UNSW-NB15 are widely used, providing a robust foundation for training and validating IDS models. Authors [2] and [5] highlighted the importance of addressing challenges such as redundant features, inefficient pre-processing, and over fitting, especially in high-dimensional IoT data streams. Additionally, models like XGBoost-LSTM author [8] and anomaly detection techniques using variation mode decomposition author [7] have shown promising results in optimizing feature space and reducing detection delays. While conventional machine learning algorithms like KNN, NB, and SVM [6] offer reasonable accuracy, deep learning models significantly outperform them in handling complex patterns, nonlinear relationships, and novel attacks. However, challenges remain in balancing computational efficiency, robustness against adversarial attacks, and scalability. Authors [4] and [9] emphasized the need for further research into real-time processing, parameter tuning, and hybrid frameworks to strengthen IDS performance in practical settings.

Overall, this review confirms that energy-efficient IDS based on deep learning is a growing field with substantial potential, but continued innovation is needed to enhance adaptability, reduce computational overhead, and ensure reliability across diverse cyber environments. Main points of review are:

Hybrid deep learning models, such as CNN-LSTM with pruning, quantization, and knowledge distillation, provide high accuracy and energy efficiency for real-time intrusion detection.

Feature selection and optimization techniques like XGBoost, adaptive sampling, and variation mode decomposition reduce computational overhead and improve detection performance.

Deep learning approaches outperform traditional machine learning models (like KNN, SVM) in handling high-dimensional, nonlinear, and novel attack patterns, especially in IoT environments.

Widely used datasets like CICIDS2017, NSL-KDD, and UNSW-NB15 support the evaluation of IDS models, but redundant data and noise remain key challenges.

Future research directions include improving adversarial robustness, scalability, and computational efficiency through hybrid architectures and advanced optimization methods to meet the demands of modern network security.

V. CONCLUSION

This review highlights the growing importance of energy-efficient intrusion detection systems based on machine learning and deep learning techniques. Hybrid models, especially those combining CNN and LSTM with optimization strategies like pruning, quantization, and feature selection, have shown significant improvements in accuracy, speed, and energy consumption. Deep learning approaches outperform traditional methods in handling large, complex datasets and detecting new forms of attacks. However, challenges such as redundant data, high-dimensional inputs, and adversarial threats still need to be addressed. Future research should focus on developing scalable, robust, and lightweight IDS solutions that ensure real-time performance while minimizing computational and energy costs. These advancements will be crucial in securing modern networks and IoT infrastructures against evolving cyber threats.

ISSN (online): 2581-3048
Volume 9, Issue 9, pp 49-53 September-2025
https://doi.org/10.47001/IRJIET/2025.909008

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, Second quarter 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).

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 9, pp 49-53 September-2025

https://doi.org/10.47001/IRJIET/2025.909008

Citation of this Article:

Rahul Senthiya, & Prof. Nitesh Gupta. (2025). A Comprehensive Review on Energy Efficient Intrusion Detection System Based on Machine Learning and Deep Learning Technique. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(9), 49-53. Article DOI https://doi.org/10.47001/IRJIET/2025.909008

