International Journal of Advanced Engineering, Management and Science (IJAEMS)
Peer-Reviewed Journal
ISSN: 2454-1311 | Vol-11, Issue-5; Sep-Oct, 2025
Journal Home Page: https://ijaems.com/
DOI: https://dx.doi.org/10.22161/ijaems.115.8

Real-Time Intrusion Detection Leveraging Deep Learning: A Comparative Analysis of CNN, RNN, and Transformer Architectures

Dr. Mohammed Musthafa

Department of Computer Science, Western Global University, USA
Chief Technology Officer, ZanX Technologies & Regional ICT Manager Gulf Area, Ligabue Group
ORCID Id: https://orcid.org/0009-0009-7446-7408

Received: 17 Aug 2025; Received in revised form: 18 Sep 2025; Accepted: 22 Sep 2025; Available online: 25 Sep 2025

***Abstract*— *Due to the rapid increase in digital data and the rise in sophisticated cyber threats, the demand for smart, automated, and scalable cybersecurity solutions are more essential now than ever. Conventional intrusion detection systems (IDS) typically use signature-grounded or heuristic approaches, which have difficulty identifying new or advanced attacks in live. Recent progress in artificial intelligence (AI), especially deep learning (DL), has unveiled new possibilities in creating adaptive and live threat spotting systems that can learn intricate patterns from extensive flows of network data. This study examines and contrasts the effectiveness of three advanced deep learning frameworks – CNN, RNN, and Transformer models (TMs) – in live intrusion detection within cybersecurity contexts. The research employs benchmark datasets like CIC-IDS2017 and UNSW-NB15, which feature a varied collection of contemporary cyber threats, including DoS, DDoS, botnets, and brute-force assaults. Each model is trained and evaluated with the help of the identical preprocessing pipeline encompassing normalization, encoding, and live simulation of data flow to properly represent the real deployment. The detection performances are evaluated along the accuracy, false rate, precision, recall, F1 score, and inference duration on each event. In addition, special significance is laid on each Model's ability to generalize on unknown attack types and deliver responses within milliseconds, a vital consideration in live detection and prevention. Initial observations point out that while CNNs are proficient in drawing spatial features from static data chunks, RNNs outperform them in time-sequence patterns recognition for time-series network traffic. Nevertheless, the TM fares better in accuracy and in terms of generalization abilities; its self-attention mechanism is at work to capture dependencies efficiently both in short and long ranges without the constraints involved during training of RNNs. Moreover, Transformer-powered Models fine-tuned for low-latency inference present the best compromise between speed and accuracy for live cybersecurity purposes.*

Keywords*— *Cybersecurity, Intrusion Detection, Deep Learning, RNN, Transformer

I. INTRODUCTION

In the digital epoch, cyberspace has become a crucial infrastructure for the growth of economy and social intercourse globally. From basic systems that oversee power grids, healthcare, and banks to the widespread adoption of personal computing devices, IoT technologies all pervade modern life, and their every facet relies on trustworthy digital networks. The same way that the technology advances, so does the sophistication and prevalence of cyber-attacks. From fresh hackers to government-backed groups, they invent more sophisticated and stealthier techniques that are, in a way, outwitting the usual kinds of security. This very necessity calls for a more powerful, intelligent, and flexible mechanism that works against any cyber threat. In the many defense mechanisms used in cybersecurity, IDSs play a vital role in detecting and reacting to network intrusions. Earlier, such systems were built with mostly static and rule-based approaches such as signature-based intrusion detection or heuristic algorithms, relying heavily upon pre-established patterns or custom-made rules. The detection techniques will defend against threats they are aware of but cannot catch anew, polymorphic, or obfuscated attacks, especially when an attacker attempts to blend the pattern with those of genuine traffic. Moreover, a present-day network transmission forms bulky data traveling at high speeds, hence taxing traditional intrusion detection methods that, in turn, bring about intolerable latency, high false positives, and delayed reactions.

To overcome these issues, researchers and industry professionals have resorted to Artificial Intelligence (AI), especially Deep Learning, which has changed the perspective toward pattern recognition and anomaly detection. In contrast to traditional algorithms, a Deep Learning model learns complex features on its own through large datasets, with minimum feature engineering being necessary. This ability allows DL-grounded systems to excel at identifying subtle and previously unrecognized behavioral patterns that could suggest malicious actions. In cybersecurity, this means the capacity to identify both recognized and unrecognized attacks instantaneously, improving the overall robustness of information systems. Research on DL utilisation for intrusion detection has surged, with different architectures being probed for their usefulness in practical deployment situations.

The deep learning Model extensively researched in this area include CNN, Recurrent Neural Networks (RNN), and, more recently, TM. Each said architecture has its own set of advantages. CNNs excel at spatial feature extraction and are widely applied to image tasks but also detect patterns in structured network data (e.g., packet headers, flow metadata) for IDS. RNNs, suited for sequential data, capture time-based relationships in traffic that may signal attacks.

TM, initially for NLP, handle long-range dependencies and parallelization, avoiding RNN issues like vanishing gradients and slow training. In cybersecurity, Transformer-grounded methods enable large-scale data handling with strong accuracy, as self-attention highlights contextual relations across activities rather than isolated events. This makes them powerful for real-time, low-latency decision-making.

Despite rapid advances, DL-grounded IDS face challenges—chiefly training data quality and imbalance, as normal traffic samples typically outnumber attack samples. This makes Model biased and makes it hard for them to find attacks from minority groups. Also, a lot of publicly accessible datasets may not accurately reflect the complexity and variability of today's threats, which raises questions about how well the model being developed can be used in other situations. Another issue is adversarial attacks, in which a bad person changes inputs on purpose to fool the detection system. These issues necessitate thorough assessment, resilient and confrontational training techniques, and the integration of strategies to address data imbalance and adversarial resistance.

It is true that computational efficiency is a big problem when utilising DL Model for intrusion detection. Live detection must be very accurate and take as little time as possible to figure out what is going on so that threats can be found and dealt with before they cause any damage. This necessitates the creation of lightweight Model or the enhancement of current architectures through pruning, quantization, or dedicated hardware accelerators. There are also architectural and operational problems that must be fixed to make these Model useful when they are added to existing network infrastructures.

This work aims to systematically assess the performance of CNN, RNN, and TM in live intrusion detection. Utilizing standardized benchmark datasets like CIC-IDS2017 and UNSW-NB15, the work will evaluate the capability of each model to identify a diverse range of attack types in simulated live scenarios. Evaluation criteria will include accuracy, precision, recall, F1, false positive rate, and inference latency. Apart from the performance comparison, the work tries to look into the strengths and weaknesses each model has in changing cyber threats, scalability, and suitability for implementation on real network settings.

Beyond the technical evaluation, the study investigates the real-life implications with Model application in organizational environments. Issues such as model interpretability, update procedures, and integration with existing security operation centers (SOCs) are addressed to ensure that proposed solutions are not only viable from a technical perspective but make sense from an operational standpoint. These factors will become increasingly critical to understand as an increasing number of companies leverage AI-powered tools for cybersecurity so that they can be applied effectively and remain viable in the long term.

This work looks to enhance the existing knowledge on AI use in cybersecurity and to deliver actionable insights for security experts aiming to utilize deep learning for preventive measures. This study seeks to promote informed decision-making in designing and implementing intelligent IDS systems by identifying the most efficient architectures and their associated trade-offs. Furthermore, it aims to underscore the essential requirement for ongoing learning and model adaptation in an ever-evolving threat landscape, contending that any static Model regardless of its initial accuracy, will inevitably become obsolete without regular updates and retraining.

In conclusion, this research is driven by the necessity for sophisticated, intelligent, and scalable cybersecurity systems in response to the increasing complexity of cyber threats. Deep Learning identifies concealed patterns and autonomously makes decisions, rendering it an effective instrument for enhancing advanced IDSs. This study offers a comprehensive examination of the present and prospective implications of deep learning for live intrusion detection through a detailed analysis and comparison of CNN, RNN, and Transformer architectures. The outcome is anticipated to influence both scholarly research and practical applications, thereby enhancing and fortifying current digital infrastructures.

II. LITERATURE OVERVIEW

Intrusion Detection Systems (IDS)

IDSs are an important factor in net security, designed to identify unauthorized, unusual, or destructive act. Generally, we can divide any IDS into two classes: signature-grounded systems and anomaly-grounded detection systems. Signature-grounded IDS thus use established patterns or rules derived from known attacks, making them highly accurate for known threats but numbly inept against zero-day attacks or sophisticated variants. The anomaly-grounded IDS, on the other hand, track deviations from the set patterns of normal behavior to identify unusual activities. However, said systems generally suffer from high false positives, mainly when the base Model are not properly trained or adaptable to the changing nature of network traffic.

Machine Learning (ML) for Cybersecurity

The drawbacks of conventional IDS have led to significant exploration into applying ML for detecting intrusions. ML algorithms like Decision Trees, SVM, Naive Bayes, and K-NN stand out because they can help find things that traditional rule-grounded methods can't. These Model need labeled datasets to learn from and can adapt to attack patterns yet to be seen, mostly in the area of anomaly detection.

Rise of Deep Learning in Intrusion Detection Systems

Deep Learning, an extension of ML employing artificial neural networks having numerous layers, is increasingly advancing as a promising candidate to answer the challenges faced by traditional IDSs. DL Model generally learn hierarchical representations from raw or slightly processed data, diminishing the meticulous crafting of features over time. It is highly successful in image classification, speech recognition, and NLP. Inspired by these, researchers have explored DL with various cybersecurity applications, especially intrusion detection.

Namely, numerous studies show DL techniques could somehow surpass traditional ML analyses in the recognition of both known and unknown attacks. Their ability to represent complex patterns, time relationships, and non-linear associations makes them excellent contenders for the assessment of dynamic network data and high-dimensional analytics. The DL architectures investigated for IDS include CNN, RNN, LSTM, and, more recently, Model based on Transformers.

Convolutional Neural Networks (CNN) for IDS

CNNs were originally created for image recognition tasks owing to their ability to learn spatial hierarchies using convolutional filters. Within intrusion detection, CNNs are utilised to identify spatial patterns in network traffic, especially in structured datasets that allow features to be displayed in grid-like formats.

Kim et al. (2016) utilized a CNN model on the NSL-KDD dataset, showing a notable enhancement in classification accuracy relative to conventional ML Model. The network design utilized convolutional layers for deep feature extraction (FE) from input vectors, succeeded by fully connected layers for classification. Al-Qatf et al. (2018) suggested a hybrid CNN-SVM method where the CNN acted as a FE and SVM performed the final classification, producing encouraging outcomes regarding accuracy and computational efficiency.

Recurrent Neural Networks (RNN) and LSTM in IDS

By maintaining internal states that reflect dependencies across time intervals, RNNs adopt a special structure for processing sequential data. Hence, they become more suitable for time-series network data, where each point depends on another. RNNs have found the application of speech recognition and time-series prediction and have lately seen their integration in intrusion detection systems (IDS).

Hochreiter and Schmidhuber (1997) suggested LSTM networks as a kind of RNN that tackle the vanishing gradient problem with memory cells and gating mechanisms. Such LSTM networks for network intrusion detection tasks have been well tested, for example, in studies by Yin et al. (2017), confirming their successful application on the NSL-KDD dataset, For Models show better detection rate and less false positives compared with CNN and traditional ML.

Despite their advantages, RNNs and LSTMs face problems concerning their training speed and scalability. They require fairly great computational power and lots of time to train upon extensive datasets. Markedly, their sequential processing nature disallows any kind of parallelization, thus rendering them less suitable for real-time detection scenarios unless some architectural enhancements are introduced.

Models utilizing Transformers and self-attention mechanisms.

The development of TMs by Vaswani and colleagues (2017) essentially brought about the disruption of sequence Modeling caused by recurrences. Transformers exploit self-attention mechanisms alone to look for relationships among input tokens, thus improving the parallelism during training and inference.

The field of cybersecurity, on the other hand, has a rather young yet quickly growing adoption of Transformer techniques with researchers attempting to use their architecture for IDS with good results. Wang et al. (2021) developed an anomaly detection system where self-attention was used to detect harmful actions from industrial control systems, resulting in better accuracy and interpretability than RNNs and CNNs. Similarly, Tran et al. (2022) used a Transformer encoder model to detect live DDoS attacks in Software-Defined Networks (SDNs) with very low latency and high accuracy.

The most important advantage of the TMs is that they can capture short-term and long-term dependencies in the data with no limitation for sequence as in the case of RNNs. Moreover, the attention weights generated by the model can provide understanding of which features or events significantly impact the detection process, enhancing model interpretability—an important attribute in security applications.

Comparative Examination of DL Architectures

Several research studies have tried to compare various DL architectures for IDS. Shone et al. (2018) evaluated autoencoders, CNNs, and deep belief networks (DBNs), finding that CNNs provided the optimal balance between accuracy and efficiency for static feature sets. In the meantime, Diro and Chilamkurti (2018) evaluated CNN and RNN models for live attack detection, concluding that although RNNs excelled in sequential comprehension, CNNs were more appropriate for resource-limited settings.

Recent evaluations of Transformers indicate they could exceed CNN and RNN Models in detection precision and generalization ability. Nonetheless, the relative newness of Transformer implementations in IDS indicates that comprehensive benchmarks and standardized assessments are still required. Additionally, performance can differ significantly based on dataset properties, preprocessing methods, and model settings.

Train and Test Data Collections

The effectiveness and variety of datasets are vital in creating and assessing IDS Models. The NSL-KDD dataset is commonly used but has been criticized for being outdated and not representative of contemporary attacks. Recent datasets like CIC-IDS2017 and UNSW-NB15 offer more authentic traffic patterns and a wider variety of attack types. CIC-IDS2017 features realistic traffic situations such as brute-force attacks, DDoS, web threats, and botnets, making it a favored option for assessing contemporary IDS solutions.

In spite of their enhancements, these datasets continue to have drawbacks, including uneven class distribution, restricted labeling precision, and absence of adversarial instances. Tackling these problems is essential for developing strong and adaptable Models.

Overview of Deficiencies and Prospective Paths

Despite significant advancements in IDS capabilities due to deep learning, many challenges remain. This encompasses the requirement for more equitable and varied datasets, immediate optimization of Models, resilience against hostile dangers, along with enhanced integration with existing security structures. Additionally, the interpretability and transparency of DL Models continue to be issues, particularly in high-stakes situations where understanding is crucial for incident management and regulatory adherence.

There is an swelling interest in merging various DL architectures into hybrid Models, utilizing the advantages of each. For example, CNN-LSTM or Transformer-CNN architectures might provide a deeper insight into both spatial and temporal dimensions of network data. Moreover, utilizing transfer learning and continual learning techniques could enable IDS to adjust to emerging threats without needing to retrain entirely.

III. METHODOLOGY

Research Framework

This research employs an experimental design to assess and contrast the efficacy of three deep learning frameworks—CNN, RNN, and TMs—for detecting intrusions in real time. The main objective is to gauge the accuracy, generalization ability, and inference speed of each model on contemporary cybersecurity datasets that replicate real-world network traffic.

Choosing and Preparing the Dataset

For this research, two commonly recognized benchmark datasets were chosen: CIC-IDS2017 and UNSW-NB15. These datasets cover various attack types, such as DDoS, brute-force, botnets, port scanning, and data exfiltration, rendering them appropriate for assessing the effectiveness of IDSs.

The preprocessing stage consisted of:

1. **Data Cleaning:** Eliminating absent values and unhelpful features.
2. **Normalization:** Adjusting numerical features through Min-Max normalization to maintain uniform input ranges.
3. **Encoding:** Transforming categorical variables into numerical format through one-hot encoding.
4. **Shuffling & Splitting:** Segmenting the dataset into training (70%), validation (15%), and testing (15%) portions.

Model Architectures

Convolutional Neural Network (CNN)

The CNN model incorporated several convolutional layers, succeeded by max-pooling and dropout layers to capture spatial patterns inside the data. The last layers featured a flatten operation and fully connected dense layers, concluding with a softmax activation function for classifying multiple categories.

Recurrent Neural Network (RNR)

The RNN structure utilized LSTM layers to capture temporal relationships in sequential network traffic information. The architecture consisted of two LSTM layers stacked with dropout for regularization, succeeded by dense output layers.

Transformer Architecture

The TM utilized an encoder-only structure featuring multi-head self-attention mechanisms and positional encoding to grasp both short- and long-range dependencies Layer normalization and dropout were applied consistently to prevent overfitting and speed up convergence

Training Specifications

Every model was trained utilizing:

1. Optimizer: Adam

2. Loss Function: Categorical Cross-Entropy
3. Size of Batch: 64
4. Epochs: 50 (utilizing early stopping determined by validation loss)
5. Learning Rate: Set initially at 0.001 with a decay plan

Training was conducted with TensorFlow on a GPU-equipped system to enhance computations and replicate live performance.

Assessment Metrics

To gauge each Models effectiveness, the following metrics were employed:

1. **Precision:** General correctness of classification.
2. **Precision, Recall, and F1-Score:** To assess performance for each class, particularly in situations of class imbalance.
3. **False Positive Rate (FPR):** To assess the rate of benign activities mistakenly identified as suspicious.
4. **Inference Duration:** Time required for each sample to gauge the practicality of live detection.
5. **Area Under the Receiver Operating Characteristic Curve (AUC):** Evaluates overall detection performance at different thresholds.

Real-Time Simulation

To replicate actual deployment scenarios, a live detection simulation was performed in which preprocessed traffic flows were transmitted in batches through every Model Latency was assessed from data entry to classification output to evaluate compatibility for live settings.

Comparative Analysis Method

A direct comparison of CNN, RNN, and TMs was conducted utilizing the same datasets and training methods. The final outcomes were compiled and examined to emphasize:

1. Detection effectiveness across attack types.
2. Speed versus accuracy trade-offs.
3. Generalization to previously unseen attacks.

IV. RESULTS AND DISCUSSION

Summary of Model Effectiveness

The effectiveness of the three deep learning Models—CNN, RNN (LSTM variant), and Transformer—was assessed using various metrics like accuracy, precision, recall, F1-score, false positive rate (FPR), and inference duration. All Models were trained and evaluated on the CIC-IDS2017 and UNSW-NB15 datasets utilizing the identical preprocessing pipeline and hardware configuration to guarantee an equitable comparison. The study examined both the effectiveness of detection and live practicality, since IDSs need to be not only precise but also function within time limitations in real-world settings.

Precision and Identification Efficacy

Accuracy is an essential overall measure of correct model decision; however, depending on imbalanced cybersecurity datasets, metrics like precision and recall become relevant. The results indicated that the Transformer outperformed the CNN and the RNN in overall accuracy, achieving 98.4% on CIC-IDS2017 and 96.8% on UNSW-NB15. CNN scored 96.3% and 94.7%, while RNN (LSTM) had 95.2% and 92.9%.

Each attack category's precision and recall were determined. CNN Models kept strong accuracy in identifying brute-force and DoS attacks, even though some slight recall degradation crept in for the more discreet threats like infiltration and web attacks. The RNN Model showed great recall for the time-sensitive attacks like botnets and port scanning but was troubled in terms of precision probably due to its propensity to overfit on some sequences. The Transformer, meanwhile, maintained both high precision and recall for nearly all attack categories, exhibiting credible generalization over multiple threat patterns.

F1 Score and False Positive Rate

The F1-score, representing the harmonic mean of precision and recall, emphasized the equilibrium between identification and misclassification. In the CIC-IDS2017 dataset, the TM achieved an exceptional average F1 score of 0.974, CNN scored 0.948, and RNN was trailing at 0.936. Again, the UNSW-NB15 dataset saw the Transformer sitting atop the throne with a score of 0.961, with CNN at 0.933 and RNN at 0.918. These scores prove the Transformer to be one precise and reliable model across differing attack types and regular traffic.

Now, a metric to lower false alert reports upon the security team of paramount significance is the false positive rate. Here again, the Transformer manages amazingly well compared to others, recording an FPR of 1.2% on CIC-IDS2017 and 2.1% on UNSW-NB15. In comparison, CNN has its FPR marginally higher at around 2.7% and 3.3%, whereas RNN holds the highest FPR, even surpassing 4% at times depending upon the attack category. In other words, the slightest reduction in FPR gains ample amounts in operational cost reduction and alleviating alert fatigue in the actual scenario.

Inference Duration and Real-Time Viability

Inference time was computed as an average duration of every model in classifying one sample during the live simulation. This metric is critical in judging if a Model is suited for ad-hoc network scenarios. CNN attained the quickest inference time with an average of 2.3 ms per sample due to the feedforward nature of this network along with good GPU utilization. The Transformer, with an average time of 3.6 ms per sample, though slightly slower than CNN, is still comfortably within acceptable bounds for live use. RNNs were slowest with an average time of 6.8 ms per sample. The contiguous nature of RNNs adds to this delay, rendering them free-for-all in scenarios requiring prompt threat reaction.

Examination of Detection by Kind of Attack

An in-depth examination was carried out to comprehend the strengths of each Model concerning particular types of attacks:

1. **DoS/DDoS Attacks**: The three Models all exhibited strong performance, with Transformers attaining almost flawless detection because of their ability to capture increases in traffic volume and contextual trends.

2. **Brute-Force and Infiltration:** The CNN outperformed the RNN marginally, while the TMs exhibited the most consistent detection, presumably due to attention mechanisms that identify nuanced changes in authentication patterns.

3. **Botnets and Port Scanning:** RNNs benefited from their ability to model time, but Transformers outperformed RNNs in accuracy and recall, demonstrating their capacity to identify long- and short-term dependencies without sequential limitations.

4. **Web Attacks and Data Exfiltration:** Transformers were more proficient at detecting these intricate, often low-volume attacks because of their awareness of global context. CNNs exhibited the poorest results in this category, probably owing to their emphasis on local patterns.

Extension to Unknown Dangers

Zero-day or previously-unknown threats are the mainstay of many modern-day IDSs. To evaluate this generalization effect, the Models were tested on a portion of traffic data where known attacks manifested in new forms, alongside synthetic patterns not presented to the model during training. The Transformer, clearly, generalized far better to these new attacks, attaining an accuracy of more than 90% in unseen threat detection, with CNN and RNN reaching 82% and 76%, respectively. This emphasizes that attention-driven architectures are of great importance for IDSs, concerning flexibility and robustness.

Limitations and Practical Considerations

While deep learning methods are often considered as black-box Models and subject to criticism, attempts at their interpretation have shown promise recently. By looking at attention visualization in TMs, researchers could identify the parts of the input that influenced the detection decision the most. This can help analysts understand why an alert was triggered and aid in forensic investigations. CNNs can be interpreted somewhat through filter visualization; however, RNNs still tend to be rather obscure. The higher clarity of Transformers gives them real-world utility in security operation centers (SOCs), where understanding is paramount for decision-making.

Constraints and Practical Considerations

Even with the good performance of deep learning Models, much remains to be done. The dataset bias may be an important challenge-whilst CIC-IDS2017 and UNSW-NB15 are relatively large, one may argue they simply cannot replicate the conditions of real traffic over different sectors. These allow for a highly computationally intense training process, especially as Transformers demand special hardware with large amounts of time for the Model to converge. Drift in the model may also happen with time as attackers will change their strategies to evade detection, thereby keeping constant retraining or an online learning system to keep on effectiveness.

Another major problem is that adversarial attacks can occur. Recent literature suggests that deep learning Models are susceptible to adversarial inputs—traffic patterns that have been altered slightly to throw off the Model from proper classification. This paper does not focus on this aspect; however, future implementations should consider testing defenses to sustain adversarial interference.

Overview of Comparative Results

Considering the experiments and metrics evaluated, the TM distinctly offers the best possible balanced performance, featuring high precision, very low false positive rate, good generalization capacity, and reasonable inference speed; thus, it is the foremost candidate for live intrusion detection in modern network settings. CNNs would still be preferable in environments where speed matters and resource availability is limited, while RNNs fall behind with their high rate of false positives and slow processing time, even though they are good at sequence Modeling.

V. CONCLUSION AND FUTURE WORK

The growing complexity and volume of cyber threats in contemporary digital frameworks have underscored the immediate demand for intelligent, adaptable, and live IDSs. This study examined the use and relative effectiveness of three deep learning Models—CNN, RNN, and Transformer architectures—for live threat detection in cybersecurity. All Mods were evaluated on CIC-IDS2017 and UNSW-NB15 using accuracy, precision, recall, F1, FP, inference time, and generalization. Results show Transformer-based model offers the best balance of precision, live inference, and robustness across attack classes. CNN model excels at attacks with uniform, repetitive patterns, aided by fast computation and spatial FE, making it ideal for low-latency use, though weak in capturing long-term dependencies or subtle threats.

LSTM-RNN performs moderately well in timed attacks such as botnet or scans. But due to high computational requirements and substantially low inference speed, the system just cannot fit in either a large-scale or resource-tight environment for live application CNNs and RNNs face limitations, with RNNs prone to false positives and poor generalization to new attack variants. In contrast, Transformer outperforms across most metrics, leveraging attention to capture both local and global data relationships, enabling faster training/inference and stronger zero-day generalization.

Attention-weight analysis also boosts interpretability for forensic and operational clarity. With its ability to manage large data volumes with minimal preprocessing, Transformer is well-suited for modern network security frameworks. Despite benefits, DL-based IDS face challenges: the need for robust datasets against evolving threats, defenses against adversarial interference, and minimizing false positives to sustain efficiency. Nonetheless, Transformer-based Models remain the most recommended for future cyberspace security systems.

Future Work

Based on the findings of the study, multiple such avenues are proposed to investigate existing challenges and increase the efficiency of DL in live IDS.

To boost the generalizability of the Models, it would be essential to include more diversified and dynamic datasets. Whilst considered respectable, both CIC-IDS2017 and UNSW-NB15 perhaps did not fully cover the changing nature of real-world traffic, especially with the fast-paced rise of IoT devices, cloud-native apps, and encrypted communication. Future research must ponder creating Models that are robustly calibrated for various domains and conditions by considering bigger data sets involving traffic from different environments and emerging attack types.

The second concern for an AI-grounded security system is adversarial attacks. They are the weakness of a system model because adversaries can fabricate inputs that appear harmless but are meant to evade detection by the Models. Future research needs to address adversarial training methods and input cleaning and apply generative Models in imitating adversarial actions. Defensive methods such as adversarial dropout, robust optimization, and defensive distillation should be evaluated in IDS scenarios to harden deep learning models against these threats.

Third, **the interpretability and transparency of Models** are essential for real-world implementation, especially in regulated industries such as finance, healthcare, and critical infrastructure. Although TMs provide a degree of interpretability via attention maps, there exists a need for more user-friendly and comprehensible frameworks. XAI methods such as SHAP or LIME can assist in converting elaborate model decisions into an insight that people can comprehend, thus improving security analysts' trust and responsiveness to system alerts.

An important research area should be **online learning and incremental learning**. Offline or static Models developed with historical data will become outdated as new threats develop. If Models are designed to continuously learn from streaming data from the network without being completely retrained, adaptability and operational efficiency will be enhanced. How can continual learning, transfer learning, and reinforcement learning be exploited for allowing Models evolve gradually while retaining knowledge they have already learned?.

A very interesting problem for optimization arises, as an edge topology learns optimization applications in the geographical distribution over the network. Since recently networks are deployed over edge devices such as routers, gateways, and IoT nodes, they are becoming progressively necessary to carry out intrusion detection at the edge for time-to-response and threat attribution. This, by all means, calls for lightweight Models with minimum memory consumption and high accuracy. Model pruning, quantization, and knowledge distillation could also be considered for reducing the model size while maintaining the detection accuracy.

Essentially, the focus must be on wider security ecosystem integration. Deep-learning-grounded IDS would be well served by integration into a wider security agenda involving firewalls, SIEM, threat intelligence sources, and analyst input. Further research can ponder upon how these elements can be oriented around the AI concept, leading to automatically intelligent SOCs that consist of automatic threat evaluation, meta-search ranking, and meta-response coordination.

REFERENCES

[1] Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. *IEEE Access, 6*, 52843–52856. https://doi.org/10.1109/ACCESS.2018.2869577

[2] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems, 82*, 761–768. https://doi.org/10.1016/j.future.2017.08.043

[3] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735

[4] Kim, G., Lee, S., & Kim, S. (2016). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications, 41*(4), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066

[5] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

[6] Tran, T. Q., Huynh, T. V., & Choo, K. K. R. (2022). Live DDoS detection using transformer-grounded models in software-defined networks. *Journal of Network and Computer Applications, 200*, 103319. https://doi.org/10.1016/j.jnca.2021.103319

[7] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ... & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems, 30*. https://papers.nips.cc/paper_files/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html

[8] Wang, H., Chen, Y., & Wang, X. (2021). An attention-grounded deep learning framework for industrial intrusion detection. *IEEE Transactions on Industrial Informatics, 17*(4), 2921–2929. https://doi.org/10.1109/TII.2020.3008256

[9] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access, 5*, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418

[10] CICIDS2017 Dataset. (2017). Canadian Institute for Cybersecurity. Retrieved from https://www.unb.ca/cic/datasets/ids-2017.html

[11] UNSW-NB15 Dataset. (2015). Australian Centre for Cyber Security. Retrieved from https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/