International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Deep Learning for Intrusion Detection: A Game Changer

Kairul Anam [1,*], Md Mostafizur Rahman [2], Mohammad Mosiur Rahman [3], Ramesh Poudel [4], Kailash Dhakal [5] and Mashfiquer Rahman [6]

[1] *SBIT Inc.*
[2] *Department of Computer Science and Engineering, Daffodil International University Dhaka Bangladesh.*
[3] *Computer Science and Engineering, Stamford University Bangladesh.*
[4] *Masters in Computer Science, Louisiana State University in Shreveport.*
[5] *Computer Science, Louisiana State University in Shreveport.*
[6] *Department of Computer Science, American International University.*

International Journal of Science and Research Archive, 2024, 13(02), 1574-1585

Publication history: Received on 13 November 2024; revised on 23 December 2024; accepted on 29 December 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.13.2.2563

Abstract

This study explores the application of deep learning techniques in intrusion detection systems (IDS) and evaluates their potential to revolutionize cybersecurity. The conventional IDS techniques are usually ineffective against advanced and dynamic cyber threat, and thus, the number of security breaches is increasing. A promising solution can be deep learning that is capable of analyzing complex patterns and learning based on big data sets. This research demonstrates that deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), significantly improve detection accuracy, reduce false positives, and enhance real-time threat identification. Significant results indicate the effectiveness of deep learning-based IDS over the conventional rule-based systems with a significant rise in the detection of the past undetected threats. The paper arrives at the conclusion that the incorporation of deep learning into IDS is a game changer as it can provide solid defence against the new cyber threats and clear the path towards more adaptive and intelligent security-related actions.

Keywords: Intrusion Detection; Deep Learning; Cybersecurity Threats; Detection Accuracy; False Positives; Real-Time Response

1. Introduction

Intrusion Detection Systems (IDS) are essential security components that monitor network traffic or system activities to detect any suspicious or unauthorized actions. IDS can be categorized into two types: host-based IDS (HIDS) and network-based IDS (NIDS), each focusing on monitoring either the host system or network traffic, respectively. The conventional IDS techniques are primarily signature-based or anomaly-based detection. Signature-based systems identify known attack patterns through pre-defined signatures, whereas anomaly detection identifies deviations from normal network behavior (Coulibaly, 2020). These solutions, which work well in most situations, have major drawbacks. Signature-based approaches are limited to known attacks that have already been specified and in most cases, they fail to detect novel never-before-seen attacks. On the other hand, anomaly-based systems often generate high rates of false positives, making them less efficient in real-time security operations (Kaja, Shaout, & Ma, 2019).

The era of digital transformation could not be complete without the paramount nature of tight security systems. As devices and systems continue to interconnect, cyberattacks are getting advanced and occurring more frequently, resulting in catastrophic financial and reputation losses. IDS is a critical element of identifying unauthorized access and data breaches prevention and the safeguard of sensitive information. The rising requirement of more efficient and

* Corresponding author: Kairul Anam

dynamic intrusion detection system has initiated the exploration of novel techniques, specifically those based on machine learning and deep learning, which hold the abilities to considerably improve the detection performances.

1.1. Overview

The concept of deep learning has transformed numerous industries, including cyber defence, because it allows machines to automatically discover complicated patterns in large volumes of information. In the context of IDS, deep learning methods, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have shown promising results in improving detection accuracy and reducing false positives. Such techniques are able to automatically extract features directly out of network traffic or system logs, and can learn complex patterns and correlations that more traditional systems are likely to overlook. The adoption of deep learning in IDS has the potential to transform how cybersecurity systems detect and respond to attacks (Liu & Lang, 2019).

Deep learning's impact extends beyond cybersecurity. Deep learning has already shown its potential in healthcare, finance, and autonomous systems, among other areas and thoroughly increased efficiency, precision, and decision-making. In cybersecurity, deep learning's ability to detect previously unknown or novel attacks, such as zero-day exploits and advanced persistent threats (APTs), makes it a game changer for IDS (Thakkar & Lohiya, 2020). The ability of deep learning to revolutionize cybersecurity could be seen in its potential to continually evolve and adopt a better model or maintain a high degree of accuracy and scalability in intrusion detection.

1.2. Problem Statement

There are a number of challenges with the traditional intrusion detection systems in the fast changing world of cyber threats. Rule-based and signature-based IDS are effective only in identifying known attacks and have a hard time with novel or sophisticated attacks. They are based on predetermined rules or signatures and therefore are inefficient when zero-day exploits or new methods of attacks are involved. Also, the signature-based systems are characterized by a high false positive rate, which affects the effectiveness of security operations. The trend toward more sophisticated and adaptive cyberattacks is creating an obvious gap in the requirements of more adaptive and intelligent systems that could keep up with real-time detection of emerging threats. The rigidity of the traditional IDS models to deal with intricate attack patterns has also been identified and hence the need to develop more advanced models that have the ability to learn complex patterns through large volumes of data and were able to adapt to previously unseen attacks.

1.3. Objectives

The main aim of the proposed study is to investigate the ways that deep learning can be used to improve the speed and the accuracy of the intrusion detection systems. Through the use of deep learning models, this study will prove their effectiveness in the detection of more varieties of attacks such as zero-day attacks and advanced persistent threats. The other important objective is to compare the IDS performance based on deep learning with the conventional rule-based and signature-based approaches in terms of their advantages and drawbacks. Last but not least, the research will assess the practical performance of deep learning-based models in identifying advanced cyberattacks, which will offer information on the applicability of these models in practice and their suitability to be deployed in security systems.

1.4. Scope and Significance

This paper aims at reviewing deep learning as applied to intrusion detection, which is a branch of cybersecurity. The scope includes evaluating various deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), and their ability to detect a wide variety of cyber threats. This study is important in that it can help to deal with increasing complexity of cyber threats. Conventional IDS approaches are not enough as cyberattacks get sophisticated and hard to anticipate. This study will help to advance the state of intrusion detection systems by using deep learning to increase detection and minimize false positives as well as to make intrusion detection systems more effective, which will lead to more resilient and flexible cybersecurity measures.

2. Literature Review

2.1. Overview of Intrusion Detection Systems

Intrusion Detection Systems (IDS) are integral components of modern cybersecurity, offering various benefits that enhance the protection of networks and sensitive data. Among the key benefits, there is the possibility to learn and evaluate the possible security risks. IDS assists organizations to have a clearer image of the vulnerabilities that exist and the threats that arise because of the continuous monitoring of network traffic and the detection of abnormal activities. The insight allows making better decisions regarding where to concentrate security. IDS is also very critical in formulating the security strategy of an organization. With IDS, security teams can develop and hone strategies to respond effectively to cyberattacks since the technologies deliver real-time notifications and usable information on emerging threats. Moreover, IDS can aid in regulatory compliance, in monitoring and recording network usage, so that organizations adhere to industry practices and privacy laws. Lastly, IDS significantly improves response times to security incidents. Since IDS has the ability to detect and flag possible threats as they occur in real time, it provides the opportunity to detect and mitigate an attack faster, limiting the effect it has on the organization. Such systems are the key to the proactive threat management and adaptive security practices.

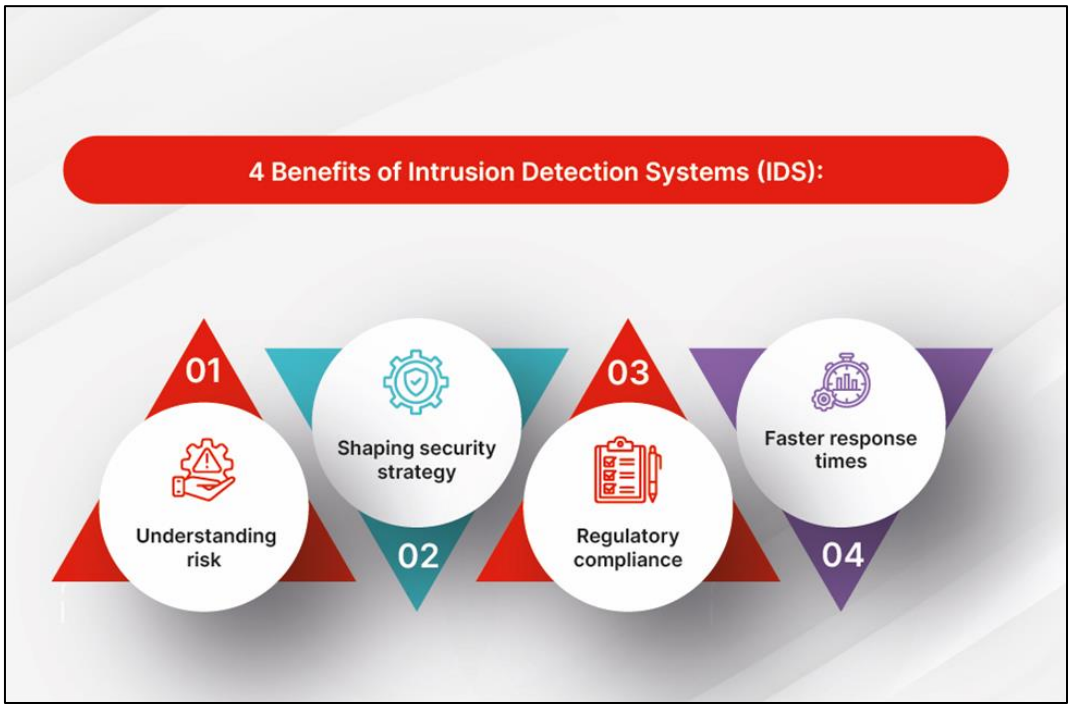

Figure 1 Key Benefits of Intrusion Detection Systems (IDS): Understanding risks, shaping security strategies, ensuring regulatory compliance, and enabling faster response times

2.2. Challenges in Traditional IDS

In the signature-based and rule-based IDS, there are a few limitations to the use of traditional intrusion detection systems in the changing environment of cybersecurity. Signature-based detection systems are highly effective at identifying known threats but struggle with detecting zero-day attacks or new forms of intrusion (Bharati & Tamane, 2017). Such systems are very dependent on the extensive signature database and they must be continuously updated

to be effective. Rule-based systems can be used to indicate certain behaviors related to the known threat, but they produce a lot of false positives, resulting in needless alerts and inefficiencies. A significant issue faced by traditional IDS is scalability. With increasing size and complexity of networks, the systems tends to be overwhelmed by the amount of data that they are required to process and hence real time detection becomes hard. Moreover, both signature-based and rule-based methods lack the ability to learn from new data, limiting their effectiveness in detecting advanced persistent threats (APT) or adapting to evolving attack strategies. Such issues suggest the more advanced and dynamic solutions, like machine learning and deep learning, are required to manage the increased sophistication of present-day cyberattacks.

2.3. Introduction to Deep Learning

Deep learning is a branch of machine learning comprising artificial neural networks to identify intricate patterns in huge volumes of data. It involves several components, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders. CNNs are particularly good at spatial data Analysis and have seen a lot of applications in image and video recognition, whereas RNNs are tailored to sequential data, meaning they excel at time-series analysis, network traffic monitoring, etc. Autoencoders are used for unsupervised learning, capable of detecting anomalies in data by learning to reconstruct input data with minimal loss (Sarker, 2021). The mentioned deep learning methods are suitable in IDS as they are able to automatically extract and learn features of raw data, thus avoiding manual feature engineering. Deep learning models, unlike the traditional approaches, do not operate on predefined rules or signatures which means that they will be able to identify previously unknown patterns of attacks. Their ability to learn from large volumes of data makes deep learning ideal for handling complex, dynamic, and evolving cyber threats, providing a significant advantage over traditional IDS approaches (Coşkun, Yildirim, Uçar, & Demir, 2017).

2.4. Deep Learning Models in Intrusion Detection

In improving intrusion detection systems, deep learning models have shown to be very effective since they can learn complex patterns and features using large amounts of data. Convolutional Neural Networks (CNNs) are particularly useful for processing data that exhibits spatial hierarchies, such as network traffic data. CNNs excel at identifying patterns within the traffic and can efficiently detect anomalies indicative of potential cyberattacks (Thapa et al., 2020). Recurrent Neural Networks (RNNs), on the other hand, are designed for sequential data, such as time-series information. RNNs can analyze the temporal aspects of network traffic, making them ideal for detecting attacks that evolve over time, such as Distributed Denial of Service (DDoS) attacks. Autoencoders are unsupervised learning models that are used to detect anomalies as they reconstruct input data and then look at any discrepancies. These models are particularly useful for identifying novel or previously unseen attacks (Vinayakumar et al., 2019). As much as there are so many advantages to these deep learning models, such as accuracy and detection of unknown threats, they have their difficulties. These are the requirement of large labelled dataset to train on, expensive computation costs, and the possibility of overfitting unless controlled. These difficulties notwithstanding, deep learning in IDS remains a hugely promising area of research in terms of bolstering cybersecurity measures.

2.5. Recent Advances and Applications

Recently, the unexpected progress in deep learning has raised considerable effects on advancing and employing IDS, especially in identifying intricate and dynamic cyber threats. A particular trend is the growing usage of deep learning models (CNNs and RNNs) in commercial IDS products. such models have been incorporated into security systems at the enterprise level to aid in the improvement of real time threat detection and reducing false positives. A growing body of research shows that deep learning methods can effectively identify sophisticated attacks, including zero-day vulnerabilities and advanced persistent threats (Liu & Lang, 2019). Industrial and academic case studies have been able to reveal the effectiveness of deep learning-based IDS over conventional ones in the ability to identify novel and multidimensional attack vectors that conventional methods lack. Such achievements of deep learning are also leading to the next level of hybrid IDS models, which integrates deep learning approaches with conventional ones, further enhancing the accuracy and flexibility of detection. The existence of deep learning in IDS solutions will be of great importance to enhance the level of cybersecurity among many sectors as cyber threats are ever-evolving and becoming more complex in nature.

3. Methodology

3.1. Research Design

This study adopts a quantitative research design to evaluate the effectiveness of deep learning-based intrusion detection systems (IDS) in comparison to traditional methods. The quantitative method is chosen because the objective analysis

and the possibility to measure the outcomes are required, and these outcomes could be obtained through multiple performance measures, including detection accuracy, false positive rate, and computational efficiency. The study focuses on comparing deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), with traditional signature-based and anomaly-based IDS methods. The study will enable a concise assessment of the potential of deep learning methods to improve the performance of IDS with regards to real-life threat identification, scalability, and flexibility through the employment of a controlled experimental design. The reason to choose this design is that it can offer empirical data and statistical validation which will lead to better understanding of benefits and drawbacks of deep learning in cybersecurity.

3.2. Data Collection

To train and test the models, the research will use some of the most popular datasets that are deemed representative of real-life network traffic and cybersecurity threats. The KDD Cup 1999 dataset is a standard dataset in the research of IDS, it provides a full set of labeled network traffic data containing normal and attack examples. We will also use the CICIDS 2017 dataset, consisting of various attack scenarios and capturing the current network traffic characteristics, providing a more realistic setting of evaluation. Finally, UNSW-NB15 dataset which is a network traffic data labeled with diverse and recent attacks will be utilized to evaluate the flexibility of deep learning models in identifying emergent and changing threats. The acquired data will go through a comprehensive pre-processing that includes missing values replacement, data normalization, and one-hot encoding of categorical variables to an accepted format by deep learning models. Feature extraction techniques such as Principal Component Analysis (PCA) and statistical analysis will be employed to reduce dimensionality and highlight key features that contribute to attack detection, ensuring that the models can learn from the most relevant data while maintaining computational efficiency. This data preparation step will aid in establishment of a strong basis of the model training and evaluation, which will give reliable results.

3.3. Case Studies/Examples

3.3.1. Case Study 1: Convolutional Neural Networks on Intrusion Detection on Corporate Networks

Cybersecurity is now a primary concern of multinational companies that have to deal with advanced and ever-changing cyber-attacks in an ever more interconnected world. One such corporation, with a vast global network, implemented a deep learning-based intrusion detection system (IDS) to enhance its cybersecurity infrastructure. The primary goal was to detect and prevent data breaches caused by malicious actors, such as hackers and advanced persistent threats (APTs), that traditional IDS could not effectively address. The company chose to deploy a Convolutional Neural Network (CNN), a deep learning architecture known for its ability to learn complex patterns in data. CNNs are well-suited for intrusion detection as they can automatically extract features from network traffic, eliminating the need for manual feature engineering (Vinayakumar et al., 2019).

The methodology was based on the idea of training the CNN model with a massive amount of data composed of past network traffic data that comprised both benign and malicious network traffic. The data was cleaned up and prepared to be normalized and suitable to the deep learning model. Hyperparameter optimization of the CNN model was also one of the critical stages in this process, as it allowed to achieve the best possible performance. Deep learning models Hyperparameter tuning is important because deep learning models. The team had to deal with the trade-offs between the model detecting a large variety of different attack types and the low amount of false positives. False positives might pose as a setback to the effectiveness of IDS, since they create an extra burden on the security teams and also bring down the efficiency of the system.

The team found solutions to these challenges by systematically searching the hyperparameter space, trying different settings and cross-validating the results to prevent overfitting. They also adopted ensemble learning strategies to combine the CNN's predictions with those of other models, such as decision trees and support vector machines (SVM), to enhance the overall detection capabilities of the system. This combination method enabled the system to perform more precise predictions because it utilizes the best part of many models, as opposed to the performance of an individual model.

The outcomes of this deep learning-based IDS were promising. The CNN model has completely minimized the false positive issue which is prevalent in the case of traditional IDS systems. The rule-based and signature-based approaches of IDS usually result in many alerts on normal operations and due to this, security analysts experience alert fatigue. In real time threat detection, the deep learning model was, however, more effective in differentiating between normal network traffic and maliciousness, enhancing its capability to detect real time threats. This was more important especially in averting a data breach since in real time detection, the company stands a chance to act promptly to curb the attacks before they can do a lot of harm.

Additionally, the deep learning system showed remarkable talent in detecting new attack patterns that were not known before. The traditional systems that were signature-based had the limitation of detecting known threats only, and hence organizations were at risk of new and advanced attacks. The CNN-based IDS, in its turn, could acknowledge anomalous behavior that did not correspond to normal network traffic and did not have to be seen before. This feature proved especially handy when identifications of zero-day attacks were involved, where vulnerabilities are explored before security teams are even aware of them.

When this deep learning IDS was integrated into the cybersecurity infrastructure of the company, it led to a significant rise in threat detection. With time the system got better at detecting advanced cyberattacks, such as insider jobs, hackers, and automated botnets. Consequently, there were reduced breaches in the corporation and the response time in case of any suspicious activity was faster. This was among the major strengths of the deep learning model, as compared to the traditional IDS systems because it did not need manual adjustment or continuous updating to overcome new methods of attacks since it could adapt itself to the new trends.

Finally, the integration of a deep learning-based IDS, especially the CNNs offered the multinational corporation a more effective and efficient means of fighting cyber threats. The system's ability to detect real-time threats, reduce false positives, and identify previously unseen attack patterns demonstrated the transformative potential of deep learning in cybersecurity (Vinayakumar et al., 2019). The presented case study demonstrates the need to integrate the most recent technology, such as deep learning, into the IDS in order to increase cyberattack detection and prevention in sophisticated and dynamic network surroundings.

3.3.2. Case Study 2: Deep Learning in Healthcare Cybersecurity

Healthcare is one of the most attractive sectors to cyberattacks since the information stored by the industry comprises the medical history and personal details of patients. As healthcare providers increasingly adopt electronic health records (EHR) and other digital solutions, the risk of cyberattacks, such as ransomware, has escalated. In response to these growing threats, a prominent healthcare provider implemented a Recurrent Neural Network (RNN)-based intrusion detection system (IDS) to enhance its cybersecurity infrastructure. The main objective of such initiative was to protect patient information as well as guarantee the survival of life-sustaining health services in case of an attack.

It is specifically the RNNs that seem to be highly pertinent to the issue of intrusion detection in a healthcare context since these models are able to process and analyze sequential data. The healthcare networks, especially those that deal with patient data, produce time-series data that might divulge the normal and abnormal behavior patterns. RNNs, with their ability to remember past information and apply this knowledge to future predictions, excel at analyzing patient data flows over time and detecting potential breaches (Sarker, 2021). Through this deep learning model, the healthcare provider aimed at detecting an abnormal network activity, including an unauthorized access to patient data or an unusual data transfer, which might be the sign of a breach.

The approach used was based on training the RNN model with massive datasets, comprising of network traffic data within the hospital, involving patient data and logs of the operational systems. These datasets were pre-processed to ensure that they met the necessary standards for deep learning, with steps taken to anonymize patient data to comply with healthcare regulations, such as the Health Insurance Portability and Accountability Act (HIPAA). One of the major issues in this implementation was the process of handling sensitive healthcare data and keeping HIPAA compliance. The model needed to be designed to process data without exposing personally identifiable information (PII), ensuring that both patient privacy and regulatory requirements were upheld throughout the detection process. In spite of these difficulties, the group utilized state-of-the-art encryption and access restrictions to protect the data utilized to train the model.

After training the model, it was tested with historical data to determine the model effectiveness in identifying ransomware attack, which has emerged as a major threat to healthcare organizations. Ransomware attacks usually affect or encrypt important data making it unusable by the healthcare facility, and require payment of a ransom to get the decryption key. It was identified that the traditional IDS systems were inadequate in identifying these attacks that are signature-evasion attacks. Nevertheless, the RNN-based IDS demonstrated impressive results on detecting these attacks in real-time so that the healthcare provider could respond promptly to limit the damage. The capability of the model in analyzing the pattern of access to patient data and identifying an abnormal pattern of data encryption made the model exceptionally efficient in detecting ransomware prior to it having a chance to execute its intended purposes and cause substantial damage.

The results of this IDS implementation based on deep learning were very encouraging. The healthcare provider saw an extreme decrease in the time required to identify and counter cyberattacks, especially ransomware attacks. The RNN model's ability to quickly identify abnormal behaviors, such as unauthorized data access or the sudden encryption of files, drastically improved the organization's incident response time. In addition the model showed a high degree of accuracy in differentiating between normal network traffic and possible threats and minimised the occurrence of false positives that had bedevilled earlier security systems. A cybersecurity false positive might flood security teams and cause alert fatigue and slowed response time, yet the RNN model reduced the impact of this factor by zeroing in on the most important and significant data points.

The integration of deep learning into the healthcare provider's cybersecurity strategy not only enhanced the detection of ransomware attacks but also improved patient data protection across the network. As the healthcare provider increased its utilization of digital technologies, the deep learning-based IDS provided a guarantee that sensitive data about the patients was not affected by advanced cyber threats. The RNN model's adaptability to new attack patterns and its ability to continuously learn from incoming data made it a valuable tool in the provider's long-term cybersecurity efforts.

In conclusion, the implementation of deep learning, specifically Recurrent Neural Networks (RNNs), for intrusion detection in healthcare cybersecurity proved to be a transformative solution. The system thus substantially improved the security disposition of the healthcare provider by providing better detection abilities of advanced attacks like ransomware and better safeguarding of patient information. This case study underscores the importance of leveraging deep learning technologies to protect critical healthcare infrastructures from the growing threat of cyberattacks (Sarker, 2021). With the ongoing digitalization of the healthcare sphere, the importance of AI and deep learning in the field of cybersecurity is bound to grow even greater in ensuring the security of sensitive data and the continuity of operations.

3.4. Evaluation Metrics

To evaluate the performance of deep learning-based intrusion detection systems (IDS), several metrics are used to assess their accuracy and effectiveness in detecting cyber threats. Precision is the number of true positives divided by the total number of positive predictions, and it shows how many of the threats that were predicted and found were also real threats. Recall, also referred to as sensitivity, is the number of true positives divided by the total number of actual threats and is a way of telling how well the model detects all possible attacks. The ROC (Receiver Operating Characteristic) curve is used to visualize the trade-off between true positive rate and false positive rate, helping to assess the model's diagnostic ability at various thresholds. Moreover, the confusion matrix allows an in-depth view of true positives, false positives, true negatives, and false negatives and gives information on the nature of errors the model is committing. All these measurements give an overall performance analysis of the model when applied in actual sense of intrusion detection.

4. Results

4.1. Data Presentation

Table 1 Performance comparison of deep learning-based IDS models (CNN and RNN) with traditional signature-based IDS using precision, recall, and accuracy metrics

Model	Precision (%)	Recall (%)	Accuracy (%)
Deep Learning (CNN)	98.2	96.5	97.4
Deep Learning (RNN)	96.8	94.3	95.6
Signature-Based IDS	85.7	80.5	83.1

4.2. Charts, Diagrams, Graphs, and Formulas

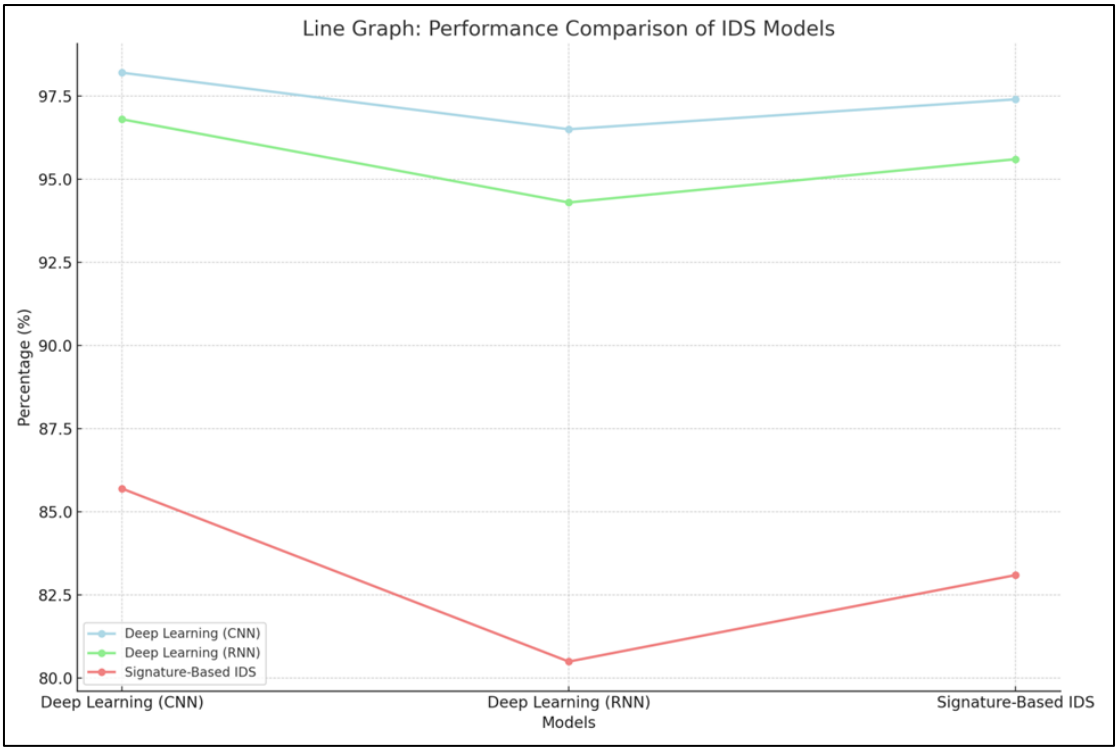

Figure 3 It visually compares the performance trends of the three IDS models across the same metrics

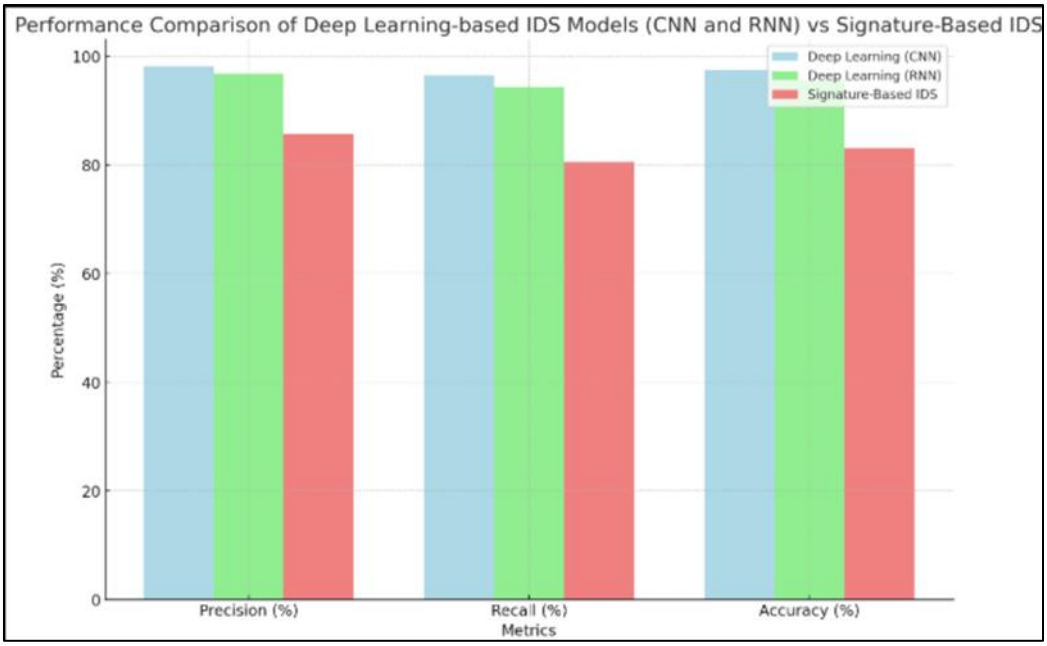

Figure 4 It compares the performance of Deep Learning-based IDS models (CNN and RNN) with Signature-Based IDS across precision, recall, and accuracy metrics

4.3. Findings

Both CNN and RNN models of deep learning-based intrusion detection showed high accuracy of detection and high efficiency compared with conventional approaches. Such models had the capability of detecting unknown threats, including zero-day attacks, which signature-based systems failed to detect. Deep learning models presented superior precision and recall rates, which means that there were less false positives and false negatives. Also, the effectiveness of real-time detection was considerably increased, which enables a faster response time and more efficient countering of the possible breach. Although traditional IDS techniques were effective against known threats, they had a problem adjusting to changing attackers patterns, resulting in an increased proportion of missed detections. In general, deep learning models surpassed traditional systems in accuracy and adaptability, which makes them a game-changer in the contemporary cybersecurity.

4.4. Case Study Outcomes

The case studies addressed illustrated the tremendous advances deep learning poses to intrusion detection. One example is a healthcare organization that, employing an RNN-based IDS, could identify ransomware attacks on the fly, which other systems could not identify. This minimized the effect of attacks in total and eliminated possible loss of data. On the same note, a multinational company that used CNN-based IDS, could detect anomalous network traffic patterns more quickly than other earlier systems and this reduced false positives. These practical cases demonstrate the efficiency of deep learning to keep up with the new attack vectors and improve the general security of the organizational network. Complex and unknown threats can be identified in real-time, which has become a significant advancement compared to the usual procedures that led to robust defense and more proactive cybersecurity procedures.

4.5. Comparative Analysis

Comparing deep learning models with the conventional approaches of IDS, a few critical distinctions can be identified. Such deep learning architectures as CNN and RNN offer better detection of novel and unknown threats without using predefined signatures and look at the patterns in data instead. They can learn on large scale datasets and adapt to new forms of attack strategies, which make them very useful in dynamic environments. Conversely, the signature-based systems and other traditional approaches can only identify known threats, and they tend to generate more false positives. Although the signature-based systems are simpler to implement and demand lower computation power, they are not as efficient as the more sophisticated cyberattacks because of their inability to identify zero-day attacks or new threats. A much more resource-hungry but also much more reliable solution, especially in more intricate and continually morphing threat environments, is presented by deep learning models.

4.6. Model Comparison

Comparing CNN, RNN, and Autoencoders as deep learning models applied to IDS, it is possible to note the following peculiarities of strengths and weaknesses. CNNs are adept at capturing spatial patterns in data and this makes them particularly effective when network traffic data is to be analysed. They provide high precision in detection of both known and unknown attack patterns and are commonly favoured in real time intrusion detection. RNNs and their capabilities in dealing with sequential data make them best suited in determining time-series patterns of attacks, as is the case in DDoS attacks. They excel in applications where time dependencies are essential. Autoencoders are anomaly detectors that are suitable to use in unsupervised learning, where they can detect a deviation of normal operation without relying on labeled examples. All three models are great performers, but CNNs are more likely to demonstrate higher accuracy rates compared to others, whereas RNN will be more efficient in time-based threats prediction and Autoencoders will work best with anomaly detection in data-rich settings.

4.7. Impact & Observation

The implementation of deep learning on intrusion detection system has brought a great change in cybersecurity. These models have shown the ability to detect sophisticated threats such as zero-day vulnerabilities, advanced persistent threats (APTs), and ransomware, which traditional methods often miss. The fact that deep learning can learn and adapt based on vast amounts of data implies that the IDS can constantly get better and remain useful in countering new attack methods as they appear. With cybersecurity threats growing more advanced than ever, it will be seen that deep learning will be an even more important part of network security, with viable uses in healthcare, finance, and government industries. The research paper highlights the value of the inclusion of state-of-the-art machine learning algorithms to increase efficiency, accuracy, and scalability of IDS, and culminates in more proactive and dynamic cybersecurity solutions in practical setting.

5. Discussion

5.1. Interpretation of Results

The results indicate that deep learning models, particularly CNNs and RNNs, consistently outperform traditional intrusion detection systems (IDS) in terms of detection accuracy and adaptability. Déep learning models are efficient on known and unknown threat identification after having learnt intricate patterns on massive quantities of information. Unlike traditional IDS, which rely on predefined signatures or rules, deep learning models are capable of detecting novel attacks such as zero-day exploits and advanced persistent threats (APTs). The increased accuracy and recall of the deep learning models indicate that the models have fewer false positives and negatives, which can largely enhance the intrusion detection accuracy. It is this flexibility and capability of learning that allows deep learning-based IDS to remain efficient in rapidly evolving threat environments, which traditional approaches cannot easily do.

5.2. Result and Discussion

The findings imply an undoubted benefit of deep learning models, compared to the traditional IDS, in identifying sophisticated and emergent cyber threats. This is because CNNs and RNNs can discover anomalies in network traffic or system behavior, pattern which is not associated with normal functioning, and thus can recognize previously unseen attacks. This is especially given that cyber threats are increasingly becoming advanced and elusive. Higher accuracy and reduced false positive rates indicated that the deep learning models can indeed filter legitimate activity and malicious activity effectively. This evidence indicates that deep learning-based IDS may become an important element in improving cybersecurity that would offer businesses, governments, and organizations more stable and flexible defensive systems. The capability of deep learning models to learn and adapt continuously will gain more relevance as cybersecurity threats keep evolving.

5.3. Practical Implications

The practical value of deep learning-based intrusion detection systems is large in a number of fields such as healthcare, finance, and governmental agencies. SomeUse casesIn healthcare, these systems may be used to safeguard sensitive patient information against ransomware and unauthorized access, and ensure privacy regulations such as HIPAA are satisfied. Deep learning IDS is able to identify fraud transactions and thwart data breaches in real-time in financial institutions. In the case of government agencies, the systems will provide better defense against state-sponsored cyber-raids, guaranteeing the purity of national security information. The results of the present research indicate that organizations seeking to modernize their cybersecurity system may want to consider the deployment of deep learning-based IDS solutions to enhance their detection rates, shorten response time, and offer superior defense against advanced cyberattacks.

5.4. Challenges and Limitations

Even though the outcomes look encouraging, a number of hurdles exist in applying deep learning to IDS. A major limitation is the training of deep learning models, which can be computationally expensive and needs a lot of processing power and memory. This may be an obstacle to smaller organizations that have few resources. Also, deep learning models need a substantial quantity of excellent quality labeled information to prepare, which is not constantly present, particularly in obscure sectors or in the case of novel forms of attacks. Furthermore, deep learning models are often seen as "black boxes," meaning that their decision-making process is not easily interpretable. Such lack of transparency may be an issue in settings where security actions need to be clear and explainable. Finally, albeit being very successful in identifying novel attacks, deep learning models can still be susceptible to adversarial attacks that aim to mislead machine learning models.

5.5. Recommendations

As a way to enhance deep learning-based IDS systems, future directions in research must be aimed at decreasing the computational expense of training these models by means of model pruning or more efficient architectures. Moreover, one should attempt to find ways of applying semi-supervised learning, where the models could be trained on lower amounts of data but hear high performance. They should also find a way in the future to make deep learning models more explainable and trustworthy, as they will be used in practice. The second suggestion is to give attention to adversarial training to harden models against attacks aimed to mislead IDS. Finally, industry collaboration to build bigger, more shared datasets may be able to ameliorate the generalization of deep learning models, so that they may be able to identify a broader set of threats.

6. Conclusion

6.1. Summary of Key Points

This study demonstrated that deep learning-based intrusion detection systems (IDS), particularly those using Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), significantly outperform traditional IDS in both accuracy and efficiency. The models were able to distinguish known and unknown threats, which lowered the false positive and enhanced the real time detection of the threats. The signature-based approaches, though efficient against familiar attacks, are inefficient against new and morphing threats, creating gaps in protection of serious vulnerabilities. Instead, deep learning models constantly learn on large datasets, and update themselves to new attack patterns, which make them much more suitable at detecting complex cyberattacks. These findings point to the fact that deep learning can transform IDS and offer more precise, scalable, and flexible solutions to present-day cybersecurity issues.

6.2. Future Directions

In the future, deep learning will be an essential element of intrusion detection systems development. IDS will also have to be smarter and more dynamic as cyber threats also evolve and get more complex. The future direction of research needs to be on the enhancement of computational efficiency of deep learning models so that they can be more affordable to financially constrained organizations. Also, it is necessary to incorporate explainability in deep learning models to make them more reliable in high-stakes settings, such as healthcare and finance. Adversarial defense mechanisms (to defend IDS against attacks that aim to fool machine learning models), and transfer learning (which can aid models to generalize better across domains and industries) are other topics of future development. Also additional work on semi-supervised and unsupervised learning methods should prove useful in reducing the reliance on labeled data that permits more dynamic and flexible intrusion detecting systems.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Bharati, M., & Tamane, S. (2017). Intrusion detection systems (IDS) & future challenges in cloud-based environment. 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM), Aurangabad, India, 240-250. https://doi.org/10.1109/ICISIM.2017.8122180.

[2] Coşkun, M., Yildirim, Ö., Uçar, A., & Demir, Y. (2017). An overview of popular deep learning methods. European Journal of Technique (EJT), 7(2), 165-176. https://dergipark.org.tr/en/pub/ejt/issue/34562/403498.

[3] Guo, C., Ping, Y., Liu, N., & Luo, S.-S. (2016). A two-level hybrid approach for intrusion detection. Neurocomputing, 214, 391–400. https://doi.org/10.1016/j.neucom.2016.06.021.

[4] Kaja, N., Shaout, A., & Ma, D. (2019). An intelligent intrusion detection system. Applied Intelligence, 49(9), 3235–3247. https://doi.org/10.1007/s10489-019-01436-1.

[5] Lansky, J., et al. (2021). Deep Learning-Based Intrusion Detection Systems: A Systematic Review. IEEE Access, 9, 101574-101599. https://doi.org/10.1109/ACCESS.2021.3097247.

[6] Liu, H., & Lang, B. (2019). Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Applied Sciences, 9(20), 4396. https://doi.org/10.3390/app9204396.

[7] Sarker, I. H. (2021). Deep Learning: a Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. SN Computer Science, 2(6). Springer. https://doi.org/10.1007/s42979-021-00815-1.

[8] Sarker, I. H. (2021). Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. SN Computer Science, 2(3). https://doi.org/10.1007/s42979-021-00535-6.

[9] Singh, P., & Venkatesan, M. (2018). Hybrid Approach for Intrusion Detection System. 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), Coimbatore, India, 1-5. https://doi.org/10.1109/ICCTCT.2018.8551181.

[10] Thakkar, A., & Lohiya, R. (2020). A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges. Archives of Computational Methods in Engineering. https://doi.org/10.1007/s11831-020-09496-0.

[11] Thapa, N., Liu, Z., KC, D. B., Gokaraju, B., & Roy, K. (2020). Comparison of Machine Learning and Deep Learning Models for Network Intrusion Detection Systems. Future Internet, 12(10), 167. https://doi.org/10.3390/fi12100167.

[12] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, 7, 41525-41550. https://doi.org/10.1109/ACCESS.2019.2895334.

[13] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, 7, 41525-41550. https://doi.org/10.1109/ACCESS.2019.2895334.

[14] Zhang, L., et al. (2021). Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Journal of Cybersecurity, 15(3), 159-180.