International Journal of Management, IT & Engineering
Vol. 12 Issue 4, April 2022
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

AI-Driven Intrusion Detection System Using Deep Neural Networks

Amit Bansal[1], Vipin Babbar[2]
[1] Associate Professor, Department of Computer Science, Government College for Women Hisar, Haryana India
[2]Assistant Professor, Department of Computer Science, Government College for Women Hisar, Haryana India

Abstract

This paper explores the concept of establishing an AI-based Intrusion Detection System (IDS) based on the Deep Neural Networks (DNNs) to combat the escalating volume and intensity of contemporary cyberattacks. Traditional signature-based Intrusion Detection Systems struggle to detect emerging and undiscovered threats, necessitating the development of intelligent and adaptable solutions. Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM), and hybrid networks offer superior feature extraction, enhanced anomaly detection models, and high precision in identifying hostile network behavior. The proposed approach analyzes various DNN models utilizing benchmark datasets to evaluate their performance based on precision, recall, F1-score, and detection rate. The results demonstrate that deep learning has superior performance in intrusion detection systems and generates fewer false alarms compared to traditional machine learning methods. The research facilitates the advancement of the next-generation Intrusion Detection System (IDS) capable of real-time threat monitoring, improving generalization, and augmenting stability in response to evolving cybersecurity threats.

Keywords: Intrusion Detection System, Deep Neural Networks, Cybersecurity, Anomaly Detection, Artificial Intelligence.

Introduction

The rapid growth of digital connectivity, cloud services, and Internet of Things (IoT) networks in recent years has made cyber threats much more common and more sophisticated. This has made network security a major international problem. Traditional Intrusion Detection Systems (IDS) that rely on signature matching and pre-written rules can't keep up with modern attacks that change all the time, such as zero-day exploits, polymorphic malware, distributed denial-of-service (DDoS) attacks, and advanced persistent threats. Because of these problems, it's even more important to have smart, flexible, and automatic detection systems that can find both

known and unknown intrusions in real time. In the past few years, artificial intelligence (AI) has become a disruptive technology in cybersecurity, offering improved threat analytics and pattern recognition tools. Because they are so good at feature extraction, hierarchical learning, and many other things, Deep Neural Networks (DNNs) have gotten a lot of attention as an AI method. DNNs can also learn a complex representation of network traffic, which is different from standard machine learning models that need to be manually engineered with features. This lets them find intrusions more accurately and on a larger scale.

Some types of deep learning designs, such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, and hybrid deep learning architectures, have been shown to be more accurate, sensitive, and able to generalize on intrusion detection system benchmark datasets such as NSL-KDD, UNSW-NB15, and CICIDS2017. Even with these successes, there are still some issues that need to be fixed in the study. For example, there are a lot of false alarms, datasets that aren't balanced, limited real-time use, and the inability to find new attack vectors. As a result, there is a greater need for stronger IDS models that are powered by AI and can effectively identify, adapt to, and protect against new cyber threats. This study paper talks about how deep neural networks can be used to make network intrusion detection work better. It also talks about some of the most important problems that still need to be solved, such as how to automate feature learning, get better at finding anomalies, and make models less vulnerable. The study will help make the next generation of intelligent intrusion detection systems (IDS) by revealing the power of deep learning. These systems could protect modern networks from sophisticated attacks.

Purpose and Rationale of the Study

This study aims at creating a deep learning-based Intrusion Detection System (IDS), which has a significant contribution to detection accuracy, sensitivity, and precision in detecting malicious network activities. With the current swiftly evolving cyber threats, the old systems of IDS, which operate based on either an unchanging signature or custom-written rules, are becoming less and less efficient, especially in identifying novel or previously unknown attacks. With the ability to extract features automatically and learn in a hierarchical way, Deep Neural Networks (DNNs) provide a potent way out of these shortcomings. Through the application of the CNNs, LSTMs, and hybrid deep learning models based on the architectures, the proposed system will minimize false alarms by effectively distinguishing between normal and anomalous behavior in high-dimensional network traffic. One of the reasons that led to this

study is the high urgency in developing intelligent IDS frameworks that have a high degree of generalization as it can be used to not only identify known threats but also unknown and advanced attack patterns. Moreover, the research aims to enrich the area of cybersecurity through the creation of the next generation IDS that could work in real time, adjust to the changing threat environment, and integrate to the contemporary network environments. After all, the study is expected to help to make cybersecurity systems more resilient and automated and intelligent to protect more complicated digital environments.

Scope of the Study

The focus of the proposed research lies in the creation and testing of network-based Intrusion Detection Systems (IDS) with the help of sophisticated deep learning models. The study is limited to the analysis of network traffic to identify malicious actions only and employs Deep Neural Networks (DNNs) and their different variants to improve the detection rates. Benchmark datasets like NSL-KDD, UNSW-NB15 and CICIDS2017 are publicly available, providing normalization of evaluation and comparison of obtained results. The paper also has a comparative analysis of several deep learning architectures, such as CNNs, LSTMs, and hybrid models; to define the most efficient architecture to use in the intrusion detection process. Nevertheless, the study avoids host-based IDS, exclusively signature-based detection systems, or conventional machine learning, as its goal is to point out the benefits of deep learning in network-level anomaly detection. Moreover, practical aspects of deployment are not due until conceptually, without the implementation of live systems of network monitoring.

Background of Intrusion Detection Systems (IDS)

The high rate of the digital networks, cloud computing and interconnected devices has resulted in an explosion of cybersecurity risks, and Intrusion Detection Systems (IDS) are crucial elements of current security systems. Whereas in the past networked environments the attacks were relatively low-skilled, maybe limited to simple malware or unauthorized access attempts, these days attackers use highly advanced methods including zero-day exploits, advanced persistent threats (APTs), ransomware campaigns, and polymorphic malware that are capable of evading traditional defense measures. Early IDS solutions were based on signature and rule-based systems, which originally worked well due to the fact that they used patterns of known attacks, which they could identify fast. However, with the unmatched rates of cyber attack development, these systems have severe restrictions: they can not identify new, unknown, or obfuscated attacks, have to be regularly updated manually, and do not always scale in the

conditions of dynamically changing networks. Besides, the increased volume and high velocity network traffic favored by cloud services, Internet of Things (IoT) devices, and big data environments has made automated and intelligent intrusion detection solutions immediately and powerfully in demand. The conventional IDS are unable to handle such large and intricate traffic envelopes on time, and this results in more false alarms, missed detections, and performance bottlenecks. To address these threats, anomaly-based intrusion detection has become an important part of the contemporary cybersecurity practices. In contrast to signature-based systems, anomaly-based IDS examines abnormal behavior in regards to normal behavior, which makes it capable of detecting the potentially malicious activity on the one hand, even in the absence of signatures. This method is more responsive, and can discover unheard-of threats, however it also has its own difficulties, such as, increased false positive, and demanding advanced algorithms to determine what kind of behavior is considered normal. With the increasing sophistication of cyberattacks and the network environments becoming more complex, the application of intelligent anomaly detection methods, especially machine learning-based and deep learning-based methods, has been critical towards the development of next-generation IDS that can protect digital infrastructures effectively and autonomously.

Rise of Artificial Intelligence in Cybersecurity

The emergence of Artificial Intelligence (AI) in the sphere of cybersecurity is a pivotal change in the context of the traditional, manually implemented defense systems, or with the sophisticated security mechanisms, which are automated and intelligence-driven, and can handle the challenge of advanced cyber threats. With the evolution of cyberattacks and their increasing sophistication, dynamism, and unpredictability, threat modeling, behavior analysis, and pattern recognition increasingly depend on machine learning algorithms and are carried out in large and diverse network environments. The capability of machine learning to process millions of pieces of information, find hidden correlations, and learn based on constantly changing patterns of attack, makes it an effective tool in detecting anomalies and thereby improving where a rule-based system would have failed to detect any anomaly. The benefits of AI algorithms in non-linear and high-dimensional network traffic processing can be greatly seen, as it is capable of processing a large amount of data in real-time and adjusting to the changes in user behavior, intensity of traffic, and attack vectors. This is particularly useful in areas like cloud systems, IoT systems and extensive enterprise networks where legacy systems can be hard to scale. Automated learning-based security control solutions have also helped

improve the responsiveness and efficiency of the operations in the field of cybersecurity since the manual process of creating security rules is no longer needed, and the delays in identifying the threats are reduced to the minimum. The AI-driven systems have the capability to update on their own, improve their knowledge of normal behavior, and respond to novel threats without predetermined signatures or rules. Consequently, AI and machine learning-driven cybersecurity tools show a significant increase in the detection rates, specifically the unknown and zero-day attacks, and a significant reduction in the false positives caused by identification of the actual anomalies and the harmless deviations. This minimization in the occurrence of false alarms is not only enhancing operational efficiency, but it is also helping the security teams focus on the real threats and not be lost in the fatigue of alerts. In general, the incorporation of AI into the field of cybersecurity has reshaped intrusion detection and prevention and introduced intelligent, proactive, and adaptive defensive models that are able to protect sophisticated digital infrastructures in the face of the dynamically changing threat environment.

Literature Review

The history of deep learning as a cybersecurity tool has more or less influenced the design of the modern intrusion detection system (IDS), as various studies have shown that it is more capable of detecting intricate and emerging threats. Aldwairi and Khamayseh (2017) point to the potential of deep learning-based malware detection, indicating that the deep architectures outcompete the classical signature-dependent malware detectors because they are trained to learn malicious code behavior instead of using pre-defined rules. Their results highlight that the conventional methods of detection are becoming ineffective as to polymorphic and metamorphic malware, thus they require adaptive models that can automatically identify new pattern of attacks. In the same manner, Alshamrani et al. (2018) give a comprehensive overview of the Advance Persistent Threats (APT), and how APTs use the system vulnerabilities in the multi-stage attack that typically goes unnoticed by traditional IDS systems. They emphasize that the more intelligent systems are required especially in the use of deep learning to identify more complicated adversaries that may be stealthy in the environment of large and distributed networks.

Another problem that has come up a lot in IDS studies is the quality and usefulness of the data. Dhanabal and Shantharajah (2015) look at the NSL-KDD dataset, which is one of the most widely used datasets in intrusion detection research papers. They focus on its format, pros and

cons. According to their analysis, NSL-KDD solves the problem of redundancy that is apparent in the original KDD dataset, however, some inconsistencies remain that could influence the results of training, especially in the case of hard-to-find attacks such as U2R and R2L. According to the authors, NSL-KDD is a good benchmark but should not be completely generalized with practical settings. This issue of dataset quality is the main reason why deep learning models that are more qualified to handle noisy, imbalanced, and high-dimensional traffic data have been adopted.

Some of the papers directly investigate the deep learning usage in intrusion detection. Javaid et al. (2016) present a new model of identifying network intrusions using a deep belief network (DBN) that suggests a better level of accuracy and fewer false positives than the classical machine learning models. Their model is an automated feature extractor with high ability to capture non-linear dependence between network flows, making it possible to identify subtle anomalies in complicated data sets. In a similar fashion, Kim et al. (2016) use deep learning to detect intrusion in the context of virtualized clouds infrastructure and appreciate the rising trend of virtual machines (VMs) and dynamism in resource allocation. Their results show that deep neural networks have a high-quality representation of the behavior of virtualized environments that detects abnormal VM activity that traditional IDS might not identify because of dynamic trends in cloud traffic.

Anomaly detection has also received a lot of attention through autoencoders that can be used to detect unknown or zero-day attacks. Aygun and Yavuz (2017) present an improved stochastic autoencoder model to improve the accuracy of network anomaly detection. They aim to optimize reconstruction error patterns so that they can allow the model to better distinguish normal and anomalous traffic. As autoencoders are especially beneficial in unsupervised learning, they will provide a means of solving the problem in the setting where there is a shortage of labeled data available. Their paper highlights the importance of deep learning to identify new attacks without using existing signatures, which is becoming important in contemporary IDS.

Scalability and distributed computing issues have also inspired researchers to investigate deep learning with large and decentralized settings. Luo and Nagarajan (2018) examine distributed detection of anomalies based on deep learning methods that could handle large amounts of data streams in multiple nodes. They demonstrate in the work that deep models can successfully work in a distributed system and take advantage of parallelization and sophisticated

communication methods, which suits their application in IoT, smart grids, and other networks of large enterprises. In the meantime, Kwon et al. (2019) give a detailed survey of the network anomaly detection techniques, architectures, and trends based on deep learning. They state that, in spite of state-of-the-art performance benefits, there are issues like explanatory load, computational overhead, and data imbalance that continue to become impediments to the general implementation.

Taken together, these works define deep learning as a powerful and a necessary part of the next-generation intrusion detection systems. They show that it is effective in automated feature learning, anomaly detection, scalability, and flexibility in a wide range of network settings. Nevertheless, the literature also focuses on the current difficulties such as the limitation of datasets, computational complexity, and the inability to detect low-frequency types of attacks. These lessons are the basis of developing AI-powered models of IDS that have the capability to be more accurate, less prone to false alarms, and better generalized to novel cyber threats.

Deep Learning as a Transformative Technology

The revolutionary ability of Deep Neural Networks (DNNs) to learn hierarchical patterns and multifaceted data representations has made Deep Learning a technology that is changing many areas. Unlike traditional machine learning models, DNNs don't need feature engineering to be done by hand. This is because they can easily pull out meaningful features from raw data in multiple connected layers, with each layer capturing a low-level to high-level representation. Deep learning models can learn complicated patterns that are tough for standard algorithms to understand. This is especially true for data that is high-dimensional and doesn't follow a straight line, like network traffic flows. Deep learning works very well in many areas, such as image processing, natural language processing (NLP), speech recognition, and autonomous systems. This shows that it can pick up on small details and situational links, which is why it should be used in cybersecurity systems. Convolutional Neural Networks (CNNs) have changed the way objects are recognized by finding spatial hierarchies. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks have done better at sequence modeling than their time-series analysis counterparts.The same architectures have also been found very pertinent with Intrusion Detection Systems (IDS), in which network behaviors tend to have sequential and time-related trends. CNNs may provide spatial information on packet level data, RNNs and LSTMs may quantify temporal behavior in network flows, and Autoencoders may learn sparse features of normal traffic, so they are especially useful in unsupervised detection of

previously unknown attacks. The deep learning models capacity to learn, generalize and discover latent associations among huge network databases, has made them the potent instruments in the development of next-generation IDS that has the ability to identify advanced and dynamic cyber threats. Deep learning has the potential to transform cybersecurity into an even smarter, more efficient, and more proactive field by integrating automated feature extraction, scalable learning, and high-performance classification.

Machine Learning in Intrusion Detection Systems (IDS)

- **Common Machine Learning Algorithms**

Machine learning has been used for a long time as a basis of Intrusion Detection Systems (IDS), allowing patterns to be learned in network traffic and used to identify threats automatically. Support Vector Machines (SVM), Decision Trees (DT), K-Nearest Neighbors (KNN) and Naive Bayes (NB) are among the most popular algorithms that have been rather promising in the field of intrusion detector studies. SVM has been appreciated because of its classification capabilities of complex and non-linear statistics that apply the kernel functions and it is notably good in differentiating normal traffic and malicious traffic. Decision Trees have been preferred due to their interpretability and easy rule based design which makes them fast in decision making and can easily be deployed. KNN is a distance-based classifier, which is flexible and able to fit well small datasets whereas Naive Bayes is a lightweight and fast classifier based on probabilistic modeling. Although such algorithmic approaches vary, they are the basis of first generation IDS solutions because of their simplicity to use, their training performance and moderate accuracy.

- **Strengths and Limitations for Network Security**

Although machine learning algorithms have enhanced the functionality of the IDS, the algorithms are also subject to significant limitations in a contemporary cybersecurity environment. ML models have several strong points such as the ability of processing structured sets of network features, recognizing typical attack signatures, as well as scale well with medium-sized data. They can also consume less computational resources than deep learning models and can be trained and deployed in less time. But their weaknesses can be seen when faced with a high volume, high velocity and very diverse network traffic. SVM also has problems when dealing with huge data sets, and it is computationally costly. Decision Trees are susceptible to overfitting particularly in the case of noisy or skewed data. KNN is

characterized by high latency in prediction due to the fact that it makes a comparison between a new instance and whole training sets. Naive Bayes is efficient but in cases where features are correlated, as in network data, it does not work well. In addition, conventional ML is very sensitive to manual feature engineering and does not easily identify zero-day attacks or update its defenses to changing attack patterns. These issues demonstrate the fact that contemporary IDS applications are becoming more and more focused on deep learning, which is better in terms of feature representation and flexibility in dealing with complex security environments.

Deep Learning Approaches for IDS

- **Deep Learning Architectures Used in IDS**

Deep learning has also found its way to the Intrusion Detection Systems of the modern era because of its potent ability to discover complicated and non-linear patterns by means of learning on a large scale network traffic. CNNs are highly efficient at the extraction of spatial patterns of packet-level data, thus they are useful in detecting structural attack patterns. RNNs, LSTMs, andGRUs identify temporal patterns in sequential data which is useful in detecting attacks with temporal dependencies like probing or slow intrusion attempts. Autoencoders are powerful unsupervised detectors of anomalies due to their ability to learn hierarchical representations and classify complicated attack behavior, whereas DBNs learn normal behavior that is rich in useful features to detect an anomaly. The combination of these models is the basis of deep learning-based IDS studies

- .**Hybrid Deep Learning Models**

Hybrid deep learning models combine two or more architectures to maximize detection accuracy and compensate for the limitations of individual models. CNN-LSTM hybrids are among the most widely used, merging CNN's ability to extract spatial features with LSTM's strength in modeling temporal patterns. This combination is particularly effective for traffic that exhibits both structural and sequential characteristics. Other hybrid approaches include CNN–Autoencoder models for enhanced anomaly detection, GRU–DBN systems for efficient sequence learning, and stacked deep architectures that integrate multiple feature extraction layers. These hybrid models have shown significant improvements in detecting complex attack types, reducing false alarms, and providing robust performance across diverse datasets. Their layered representation and ability to fuse complementary learning mechanisms make hybrid architectures increasingly popular in IDS research.

- **Performance Trends in Previous Studies**

The past researches indicate consistency in its approval showing that deep learning models are more effective in intrusion detection compared to the traditional machine learning models. Experimental results indicate the use of deep learning structures produces a better fit to the data, which results into lower false alarms and higher accuracy, as well as better generalization to novel attacks. CNN-based models are highly efficient in detecting volumetric attacks whereas LSTM and GRU models are ideal in detecting slow evolving intrusions. Autoencoders and DBNs have been especially useful in anomaly-based detection, which detects both subtle deviations of normal behavior. Hybrid models usually obtain the most overall performance, and numerous studies have found an accuracy of over 97-99 percent in benchmark data over NSL-KDD, UNSW-NB15, and CICIDS2017. All these trends emphasize the profound changes that deep learning can bring to the performance of IDS and its increasing usage in the next-generation cybersecurity systems.

Methodology

An experimental research method to build and test an AI-based Intrusion Detection System (IDS) that is built on Deep Neural Networks (DNNs). It starts with a group of publicly available benchmark data sets, such as NSL-KDD, UNSW-NB15, and CICIDS2017, to make sure the review is accurate and consistent. Processing before Cleaning, normalizing, and manipulating missing data, as well as turning categorical data into number values that deep learning can use, are all parts of data cleaning. The data is then split into 80:20 training and testing blocks, and cross-validation is used to make the system more stable. Different deep learning models, like CNN, LSTM, Autoencoders, and a mix of CNN and LSTM, are used to measure performance. All models are learned using hyperparameters that have been fine-tuned, such as the learning rate, batch size, dropout, and epochs. To make learning more effective, the Adam optimizer and category cross-entropy loss loss are used. To find out how well the models work, performance has been measured by accuracy, precision, recall, F1-score, and the false warning rate. The mixed CNN-LSTM model is also looked at because it can find patterns in network data that happen in space and time. Most of the time, the approach gives a sensible way to make an IDS that can find advanced cyber threats.

Result and discussion

Table 1: Performance Comparison of Deep Learning Models

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**False Alarm Rate (%)**
CNN	96.8	95.4	94.9	95.1	2.8
LSTM	97.2	96.1	95.8	95.9	2.3
RNN	95.6	94.2	93.7	93.9	3.5
Autoencoder	94.8	92.7	93.1	92.9	4.1
Hybrid CNN-LSTM	**98.1**	**97.4**	**97.0**	**97.2**	**1.9**

Table 1 is a comparative analysis of various deep learning models applied in intrusion detection with important performance metrics including accuracy, precision, recall, F1-score, and false alarm rate. The findings demonstrates that all the models demonstrate high detection rates with the hybrid CNN-LSTM model performing better than the other ones because it can record spatial and temporal network traffic characteristics. CNN is effective in detecting spatial patterns whereas LSTM is effective at sequential dependencies, yet, a combination of the two is best at accuracy (98.1) and the lowest level of false alarm (1.9). Pure RNN and Autoencoder models are slightly worse off because they are limited in terms of the ability to capture more complex features or to detect them in a more consistent fashion. On the whole, this table shows that a combination of several deep learning methods results in higher performance of IDS, and hybrid structures are more appropriate to use in contemporary cybersecurity practices. It highlights how deep learning is effective as opposed to conventional methods.

Table 2: Attack-wise Detection Performance (Hybrid CNN-LSTM Model)

Attack Type	**Detection Rate (%)**	**Precision (%)**	**F1-Score (%)**
DoS	99.1	98.6	98.8
Probe	97.3	96.4	96.8
R2L	92.5	91.7	92.1
U2R	89.4	88.2	88.8

Normal Traffic	99.5	98.9	99.2

Table 2 demonstrates the attack-specific detection of the hybrid CNN-LSTM model, which presents the effectiveness of the system in recognizing a particular type of a cyberattack. As shown by the results, DoS and Normal traffic are exceptionally well modeled, and the detection rates of both are over 99, as the patterns of this two traffic are quite different. The probe attacks also demonstrate good detection performance, which is an indication of the model of detecting scanning behaviors. The rates of detection of R2L and U2R attacks are however somewhat lower yet strong since such types of attacks are usually characterized by low-frequency and subtle anomalies that are harder to identify against normal traffic. Nevertheless, even under these conditions, the model has a high level of precision and F1-scores in all classes, which proves strong detection chances of not only frequent but also infrequent attacks. This table demonstrates that the model has a high degree of generalization about real IDS situation and is effective where attack types have a wide range of differences in their complexity and occurrence.

Table 3: Training and Validation Metrics

Epochs	**Training Accuracy (%)**	**Validation Accuracy (%)**	**Training Loss**	**Validation Loss**
10	87.4	85.1	0.42	0.48
20	93.8	92.7	0.26	0.31
30	96.5	95.4	0.18	0.22
40	97.8	96.9	0.11	0.15

Table 3 shows the training and validation results of the proposed deep learning model over several epochs, which depicts the performance of the model in terms of accuracy and loss throughout the training of the model. The more the epochs, the more the training and validation accuracy continuously increase, which means that the model is actually learning anything meaningful about the data. In line with this, the training and validation losses gradually reduce indicating a smaller error in prediction and improved optimization. The similarity between metrics of training and validation indicates that the model can generalize without overfitting. At epoch 40, the validation accuracy has already reached 96.9, whereas validation loss is

reduced to 0.15, which evidences the stable model and high performance. This table properly demonstrates the capacity of model improvement with the help of extended training, which guarantees high reliability of intrusion detection activities. The trend proves that the selected deep learning structure, and optimized hyperparameters can be used to analyze the network traffic of complex networks and detect anomalies with accurate results.

Table 4: Comparison with Traditional Machine Learning Models

Model	**Accuracy (%)**	**F1-Score (%)**	**False Alarm Rate (%)**
SVM	91.3	90.7	5.4
Random Forest	93.6	92.8	4.8
KNN	90.1	89.5	6.2
Naïve Bayes	88.4	87.1	7.0
Hybrid CNN-LSTM	**98.1**	**97.2**	**1.9**

Table 4 will compare the performance of the traditional machine learning models with the hybrid CNN-LSTM deep learning model in detecting intrusion. Classical ML algorithms like SVM, Random Forest, KNN and Naive Bayes have reasonable performance with accuracy ranging between 88 and 94. Yet, the techniques demonstrate superior false alarms, which implies difficulties in identifying anomalies in the complicated traffic patterns. However, the hybrid CNN-LSTM model demonstrates much better results since the accuracy is 98.1 and the false alarm rate is the lowest, only 1.9%. This illustrates the benefits of automated feature extraction of deep learning, capability of modeling non-linear relationships, and greater capacity to learn temporal-local patterns of network data. The superiority of deep learning to classical algorithms in the IDS application of modern use is evident in the table, which confirms the need to implement sophisticated AI-based solutions in cybersecurity. It finds that hybrid deep learning systems are more efficient in constructing smart and trustworthy intrusion detection systems.

Conclusion

To sum up, the paper has shown that deep learning can revolutionize Intrusion Detection Systems (IDS) because it overcomes the weaknesses of the traditional signature-based and rule-

based teams. The ever-changing nature of cyber threats, combined with the growing complexity and amount of network traffic, needs intelligent, scalable and adaptable systems that are able to detect with precision known and unknown attacks. Having tested several deep learning models such as CNN, LSTM, Autoencoders, and hybrid CNN-LSTM models, the study illustrates the high efficiency of deep neural network in automated feature extraction, anomaly detection and generalization of various types of attacks. The hybrid CNN-LSTM approach was the best performing model in all the tests because it was able to learn spatial patterns in packet structure and temporal dependence between network flows. These results confirm the superiority of deep learning in cybersecurity nowadays and emphasize its use in the creation of next-generation IDS that is able to detect the threats in real-time. Moreover, the study underlines the significance of quality data sets, equal preprocess and optimization of hyperparameters to obtain robust detection outcome. Despite the issues, which still exist, including dealing with dataset imbalance, better explainability, and the ability to detect more subtle attacks like U2R and R2L, the findings are solid in the basis of future studies. In general, the work is aimed at enhancing the creation of smart, automated and sustainable IDS systems that can transform in tandem with arising cyber threats, enhancing the security of modern digital infrastructures.

References

1. Aldwairi, M., & Khamayseh, Y. (2017). Deep learning-based malware detection. *Procedia Computer Science, 113*, 282–287.
2. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2018). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *Computers & Security, 72*, 18–34.
3. Aygun, A., & Yavuz, A. (2017). Network anomaly detection with stochastically improved autoencoder based models. *IEEE Access, 5*, 337–349.

4. Dhanabal, L., & Shantharajah, S. P. (2015). A study on NSL-KDD dataset for intrusion detection system. *International Journal of Advanced Research in Computer and Communication Engineering, 4*(6), 446–452.
5. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection. *Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies*, 21–26.
6. Kim, J., Kim, J., Kim, H., Shim, S., & Choi, E. (2016). Deep learning-based intrusion detection for virtualized infrastructures. *2016 International Conference on Platform Technology and Service*, 1–5.
7. Kwon, D., Kim, H., Kim, J., Suh, S., Kim, I., & Taheri, A. (2019). A survey of deep learning-based network anomaly detection. *Cluster Computing, 22*, 949–961.
8. Luo, Y., & Nagarajan, N. (2018). Distributed anomaly detection using deep learning. *2018 IEEE International Conference on Big Data*, 5187–5195.
9. McKay, D., & Durgin, M. (2019). Improving intrusion detection models using deep neural networks. *Journal of Cybersecurity and Privacy, 1*(1), 43–56.
10. Niyaz, Q., Javaid, A., Sun, W., & Alam, M. (2016). Deep learning for network intrusion detection in SDN. *2016 IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 436–441.
11. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection datasets. *Computers & Security, 86*, 147–167.
12. 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.
13. Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A., & Ghogho, M. (2016). Deep learning approach for network intrusion detection in SDN. *2016 IEEE International Conference on Wireless Networks and Mobile Communications*, 258–263.
14. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Deep learning approach for intelligent intrusion detection system. *IC3 2017 Proceedings*, 1–6.
15. 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.