Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Enhanced Intrusion Detection System Using Deep Learning Algorithms : A Review

Andy Victor Amanoul[1], Adnan Mohsin Abdulazeez[2]
andy.victor@dpu.edu.krd[1], adnan.mohsin@dpu.edu.krd[2]
[1] Technical College of Duhok, Duhok PolytechnicUniversity , Duhok City , Kurdistan Region, Iraq
[2] Technical College of Engineering, Duhok Polytechnic University, Duhok City , Kurdistan Region, Iraq

Article Information

Submitted : 12 May 2024
Reviewed : 22 May 2024
Accepted : 15 Jun 2024

Keywords

Intrusion Detection Systems (IDS), Deep Learning, Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Cybersecurity.

Abstract

Intrusion Detection Systems (IDS) are crucial for protecting network infrastructures from advanced cyber threats. Traditional IDS, largely reliant on static signature detection, fail to effectively counter novel cyber attacks, leading to high false positive rates and missed zero-day exploits. This study investigates the integration of deep learning technologies into IDS to enhance their detection capabilities. By employing advanced deep learning frameworks, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) and other algorithms , the research explores their efficacy in identifying complex data patterns and anomalies. Furthermore, the use of big data analytics is assessed for its potential to significantly augment the predictive power of these systems, aiming to set new benchmarks in cybersecurity defenses tailored for contemporary threats.

A. Introduction

Intrusion Detection Systems (IDS) play a crucial role in safeguarding network infrastructures against evolving cyber threats. Traditional IDS, primarily based on static, signature-based detection methods, are increasingly inadequate due to their inability to cope with the sophistication of new and evolving threats. These systems often suffer from high false positive rates and struggle with the detection of zero-day exploits, highlighting a significant gap in current network security measures [1], [2].To bridge this gap, there is a growing shift towards incorporating advanced deep learning techniques into IDS. Deep learning offers potent capabilities for automatically detecting complex patterns and anomalies in data, significantly enhancing both the accuracy and adaptability of IDS. Techniques such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are particularly effective, utilizing large datasets to improve detection mechanisms dynamically [3], [4]. Furthermore, the integration of big data analytics enables these systems to process and analyze vast amounts of network data, thereby significantly boosting the predictive capabilities of IDS [5], [6].

This paper will delve into various deep learning frameworks and their implementations within IDS, aiming to advance the capabilities of traditional systems and set new benchmarks for cybersecurity defenses capable of confronting the complexities of modern cyber threats.

The paper is organized as follows: Section II discusses the various Deep Learning Architectures for IDS, enhancing traditional systems with advanced techniques like CNNs and RNNs. Section III delves into Convolutional Neural Networks in Feature Analysis for IDS, highlighting their role in intricate feature extraction. Section IV explores Recurrent Neural Networks for Temporal Data Processing in IDS, essential for analyzing sequential data. Section V examines Autoencoders for Anomaly Detection in IDS, focusing on their use in unsupervised learning scenarios. Section VI addresses Deep Reinforcement Learning for Adaptive IDS, demonstrating its application in dynamic environments. Section VII investigates Generative Adversarial Networks for IDS Enhancement, showcasing their ability to generate synthetic data for training. Section VIII provides a comprehensive Literature Review, outlining related works and previous research. Section IX presents a Summary Table that encapsulates methodologies, advantages, disadvantages, and key results. Section X offers a detailed Discussion on the implications and effectiveness of integrating deep learning into IDS. The paper concludes with Section XI, summarizing the findings and proposing future research directions in the field of IDS enhanced by deep learning technologies.

B. Deep Learning Architectures for IDS

Deep learning architectures significantly enhance the capabilities of Intrusion Detection Systems (IDS), adapting dynamically to the evolving landscape of cybersecurity threats. Techniques like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) effectively process diverse and complex data streams, crucial for detecting sophisticated cyber threats [1]. Additionally, autoencoders play a pivotal role in reducing data dimensionality and identifying anomalous patterns, thus strengthening IDS frameworks against advanced persistent threats [4]. The adaptability of these systems is further exemplified in their application across varied environments, from conventional network settings to fog computing, showcasing their versatility and scalability in real-world [5], [6]. As cyber threats evolve, the integration of advanced deep learning techniques becomes essential, offering robust, real-time detection and ensuring continuous system adaptation to new and emerging threats [2], [3].

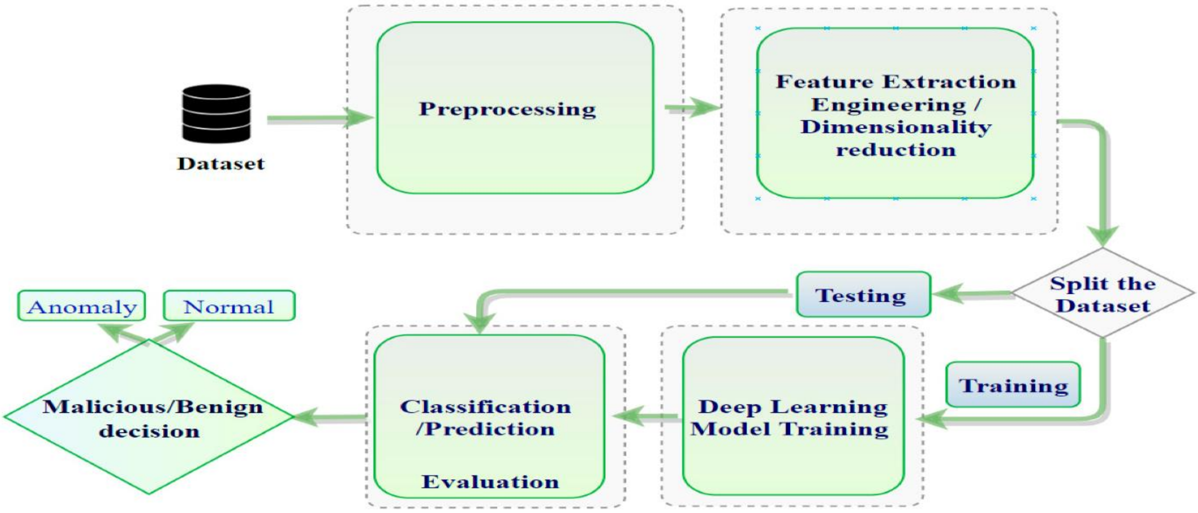
Dataset
Preprocessing
Feature Extraction Engineering / Dimensionality reduction
Split the Dataset
Testing
Training
Deep Learning Model Training
Classification /Prediction
Evaluation
Malicious/Benign decision
Anomaly
Normal

Figure 1. Framework of Implementing deep-learning in Intrusion Detection System[7]

2.1 Convolutional Neural Networks (CNNs) in Feature Analysis for IDS

Convolutional Neural Networks (CNNs) are increasingly applied in Intrusion Detection Systems (IDS) to analyze and detect cybersecurity threats effectively. These networks excel in extracting intricate features from network traffic data without the need for manual feature engineering. For instance, [8] demonstrated how CNNs could classify and predict various types of network attacks by training on traffic datasets, emphasizing the network's ability to learn from data complexity [8]. Similarly, [9] explored CNNs' capability to discern patterns that signify malicious activities, highlighting the adaptability of CNNs to evolving security datasets [9]. [10] presented a comparative analysis showing CNNs' superior performance in feature extraction and classification tasks over traditional machine learning approaches [10]. [11] outlined a novel approach using Siamese CNNs to enhance feature extraction processes, thereby improving detection accuracies in IDS systems [11]. Lastly, [12] discussed the integration of CNNs into IDS frameworks to process large-scale data, ensuring efficient and real-time intrusion detection [12]. These advancements illustrate CNNs' critical role in developing robust and intelligent IDS solutions capable of addressing the complexities of modern cybersecurity threats.

2.2 Recurrent Neural Networks (RNNs) for Temporal Data Processing in IDS

Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), are essential for temporal data processing in Intrusion Detection Systems (IDS). These models excel in handling sequential data, crucial for recognizing patterns in network traffic and detecting anomalies over time. [13] emphasize the effectiveness of RNNs in identifying complex, time-dependent intrusion patterns due to their ability to retain information across time steps. [14], [15] further highlight how LSTM models, by overcoming issues of vanishing gradients, provide robust performance enhancements in sequential pattern recognition tasks. [16] discusses the application of bidirectional LSTM architectures that effectively capture dynamic features in network flows, enhancing the detection capabilities of IDS frameworks. Finally, [17] integrates these concepts within hybrid models, combining convolutional neural networks with RNNs to optimize feature extraction and temporal analysis, leading to improved IDS accuracy and response times.

2.3 Autoencoders for Anomaly Detection in IDS

Autoencoders are pivotal in IDS for anomaly detection, using their ability to compress and reconstruct network traffic data to identify deviations from expected patterns. Particularly effective in unsupervised scenarios due to their capability to learn from unlabelled data, autoencoders distinguish between normal and anomalous traffic based on reconstruction errors. This is underscored by [18], who highlights the use of deep autoencoders in industrial networks, demonstrating significant detection capabilities with minimal false positives . Additionally, [19] discusses their application in IoT, adapting dynamically to diverse network behaviors, which is crucial for robust security frameworks . [20] further illustrate their effectiveness in transfer learning, enhancing anomaly detection across different IoT environments . Similarly, [21] show their application in SDN environments, where they dynamically update to detect new network anomalies efficiently .

2.4 Deep Reinforcement Learning (DRL) for Adaptive IDS

Deep Reinforcement Learning (DRL) is increasingly pivotal in enhancing Intrusion Detection Systems (IDS) across various networks. [22] emphasize its value in anomaly detection within voluminous, unlabeled datasets typical of cloud and IoT environments . [23] illustrate DRL's effectiveness in managing real-time data and security in industrial blockchain networks . Additionally, [24] highlight its capability to refine decision-making in network security, thereby boosting IDS reliability. [25] [26] both demonstrate DRL's ability to adapt and learn from dynamic environments, significantly reducing false positives and enhancing threat detection accuracy.

2.5 Generative Adversarial Networks (GANs) for IDS Enhancement

Generative Adversarial Networks (GANs) significantly enhance intrusion detection systems (IDS) by generating synthetic data that closely simulates real network traffic, including sophisticated cyber threats. This capability allows IDS models to improve their detection mechanisms against novel and evolving threats. [27] emphasized how GANs can effectively address data imbalances in IDS, thereby improving the detection accuracy by training the system with balanced data representing both common and rare attack scenarios. [28] introduced a method using GANs to perform adversarial attacks, which in turn tests and strengthens IDS against such sophisticated manipulations. [29] discussed the integration of GANs in producing synthetic samples to augment training datasets, particularly for emerging technologies within cyber-physical systems, thereby stabilizing the IDS performance during training phases. Additionally, [30] explored the real-time detection capabilities of GANs in network IDS, further advancing the practical applications of this technology in operational environments.

C. Related Works (Literature Review)

Choi et.al.(2019)[31] developed an unsupervised learning approach for network intrusion detection using autoencoders, showcasing its application on the NSL-KDD dataset. Their study emphasizes the advantages of using unsupervised learning methods, which are particularly useful when labeled data is scarce or expensive to obtain. The proposed model achieved an accuracy of 91.70%, significantly improving upon traditional cluster analysis methods which usually achieve around 80% accuracy. This demonstrates the potential of autoencoders in enhancing intrusion detection systems without relying on labeled data.

Otoum et.al.(2019)[32] introduced a novel deep learning-based Intrusion Detection System tailored for IoT environments. Employing advanced algorithms like Spider Monkey Optimization for feature selection and a Stacked Deep Polynomial Network for anomaly classification, their approach effectively addresses IoT's unique security challenges with remarkable accuracy and computational efficiency.

Li et.al.(2019)[33] presented a multi-CNN fusion approach for intrusion detection within Industrial IoT networks, showcasing its effectiveness in complex and varying intrusion scenarios. By converting one-dimensional feature data into a grayscale graph, their model demonstrates superior performance in binary and multiclass classification tasks on the NSL-KDD dataset.

Zhang et.al.(2020)[34] proposed a network intrusion detection method that leverages the strengths of deep learning through the integration of Auto-Encoders (AN) and Long Short-Term Memory (LSTM) networks. This combination aims to map high-dimensional data to a lower-dimensional space and accurately predict intrusion types, showcasing improved detection across various attacks.

Wu et.al.(2020)[35] introduced an innovative network intrusion detection approach leveraging semantic re-encoding combined with deep learning, specifically employing ResNet architectures. This method significantly enhances the classification accuracy and robustness by deeply understanding the semantics of network traffic, demonstrating a substantial improvement over traditional and some deep learning models.

Su et.al.(2020)[36] developed the BAT-MC model, a deep learning-based intrusion detection system utilizing BLSTM (Bidirectional Long Short-term Memory) and an attention mechanism. This model automatically extracts key features from network traffic, demonstrating superior classification accuracy on the NSL-KDD dataset without relying on manual feature engineering.

Hsu et.al.(2020)[37] explored the application of Deep Reinforcement Learning (DRL) for cloud-based intrusion detection, as presented at the 9th International Conference on Cloud Networking (CloudNet). The research demonstrates how DRL can be effectively utilized to enhance the security of cloud services. Using the CloudNetSim++ dataset, the study emphasizes DRL's capability to dynamically adapt and optimize detection strategies in real-time, achieving an impressive accuracy of 97.2%. This highlights the potential of DRL to improve detection rates and response times in cloud environments, showcasing its value in complex and evolving security landscapes.

Shahriar et al. (2020) [38] introduce a Generative Adversarial Network (GAN)-based Intrusion Detection System (G-IDS) for cyber-physical systems, enhancing detection by generating synthetic data to train on imbalanced datasets. Their approach demonstrates improved accuracy and model stability, validating the efficacy of GANs in security applications.

Shende et.al.(2020)[39] investigated the application of Long Short-Term Memory (LSTM) deep learning techniques for intrusion detection in network security. Their research, focused on anomaly detection, utilizes the NSL-KDD dataset for training and testing, demonstrating the effectiveness of LSTM in classifying both binary and multiclass network intrusions.

Nayyar et.al.(2020)[40] explored the efficacy of LSTM-based models in network intrusion detection, demonstrating the model's ability to identify DDoS attacks among others. Utilizing the CICIDS2017 dataset, their approach shows significant promise in distinguishing between benign and malicious network traffic with a high degree of accuracy.

Mighan et.al.(2020)[41] proposed a scalable deep learning-based intrusion detection system utilizing Apache Spark for efficient big data processing. Their hybrid approach combines stacked autoencoders for feature extraction with SVM, decision trees, and other classifiers for intrusion detection, demonstrating notable efficiency and accuracy on the UNB ISCX 2012 dataset.

Kim et.al.(2020)[42] proposed AI-IDS, a deep learning model for real-time web intrusion detection, employing a CNN-LSTM architecture. This model efficiently processes HTTP traffic to distinguish between benign and malicious activities, showcasing the potential of deep learning in enhancing cybersecurity measures in real-time applications.

Kasongo et.al.(2020)[43] developed a model for network intrusion detection that combines deep learning with feature selection techniques. Their method showcases the effectiveness of combining wrapper-based feature selection with deep neural networks to enhance detection capabilities in both wired and wireless network environments, marking a significant advancement in intrusion detection systems.

Hossain et.al.(2020)[44] proposed an LSTM-based IDS for in-vehicle CAN bus communications, achieving remarkable detection accuracies for various attacks. By optimizing neural network parameters and employing techniques like gradient descent, they demonstrate the model's efficacy in identifying malicious activities with minimal false positives and negatives.

Dey et.al.(2020)[45] enhanced intrusion detection with an innovative attention-based CNN-LSTM model, showcasing its capability on the IDS 2018 dataset. This method marks a significant step forward in detecting network intrusions, utilizing the strengths of both CNN and LSTM architectures, augmented by attention mechanisms for refined analysis.

Chen et.al.(2020)[46] addressed the limitations of traditional machine learning methods in network intrusion detection by employing deep learning technologies. Their research signifies a shift towards utilizing deep learning for its ability to autonomously extract and learn features from network traffic, offering a more dynamic and effective detection mechanism.

Muhammad et al. (2020)[47] proposed a deep learning-based intrusion detection system utilizing stacked autoencoders and deep neural networks, tailored to detect financial fraudulent activities. This approach significantly reduces false positives and enhances detection capabilities across various datasets including KDDCup99, NSL-KDD, and AWID, achieving high classification accuracies.

Basnet et.al.(2020)[48] innovated in electric vehicle charging station (EVCS) security with a deep learning-based IDS to detect DoS attacks. Implementing DNN and LSTM models, they achieve over 99% detection accuracy, showcasing LSTM's superiority in precision and recall, thereby enhancing cybersecurity in the smart grid ecosystem.

Tang et al. (2020)[49] presented DeepIDS, an intrusion detection system that combines deep neural networks (DNNs) and gated recurrent unit recurrent neural networks (GRU-RNNs) to secure software-defined networks. This approach significantly reduces false positives and enhances detection accuracy to 80.7% (DNN) and 90% (GRU-RNN) across NSL-KDD datasets, efficiently identifying various attack types.

Louati et.al.(2020)[50] designed a deep learning-based multi-agent intrusion detection system combining autoencoders, MLP, and K-NN. The system aims to improve detection accuracy and speed using the KDD 99 dataset, showcasing a model that surpasses traditional methods by integrating deep learning with a multi-agent approach.

Ahmad et.al.(2020)[51] proposed a deep neural network-based Intrusion Detection System (IDS) aimed at improving network security by efficiently monitoring and classifying network traffic into authentic and malicious. Utilizing deep learning, their model demonstrates high accuracy in segregating malicious traffic, underscoring the advancement in IDS technology through deep learning.

Abdullateef et.al.(2020)[52] proposed a hybrid Intrusion Detection System utilizing Recurrent Neural Network (RNN) and Crow Swarm Optimization (CSO) for feature reduction on the KDD 99 dataset, achieving a high accuracy of 98.34% with reduced feature set, demonstrating the efficiency of combining deep learning with optimization techniques.

Ashiku et.al.(2021)[53] explored deep learning (DL) for network intrusion detection, emphasizing DL's flexibility and learning capabilities in detecting known and zero-day network behavioral features. The UNSW-NB15 dataset, reflecting modern network communications with synthetic attack activities, is used to validate their model's effectiveness.

Hu et.al.(2021)[54] designed and implemented a WiFi sensing system for intrusion detection using Channel State Information (CSI) at the physical layer. They utilized path decomposition algorithms and Convolutional Neural Networks (CNN) to enhance sensitivity to passive intrusion detection, especially for non-line-of-sight (NLOS) motion. This system showcased the effective application of deep learning techniques in network security, achieving high detection accuracy in various experimental scenarios.

Jithu P et.al.(2021)[55] focused on leveraging Deep Neural Networks (DNN) to develop an Intrusion Detection System for IoT Botnet Attacks. Utilizing the Bot-IoT dataset created in a realistic network environment, their study reveals DNN's capability to significantly outperform existing systems in detecting IoT botnet attacks, offering a promising solution to the growing concern of IoT security vulnerabilities.

Laghrissi et.al.(2021)[56] investigated the implementation of deep learning models for intrusion detection, specifically focusing on Long Short-Term Memory (LSTM) networks enhanced with Principal Component Analysis (PCA) and Mutual Information (MI) for dimensionality reduction. Their methodology aims to optimize the detection of network intrusions by reducing feature dimensionality while maintaining high accuracy levels.

Liu et.al.(2021)[57] proposed a hybrid Intrusion Detection System employing scalable K-means+ Random Forest and Deep Learning on the NSL-KDD and CIC-IDS2017 datasets. Their approach combines the strengths of machine learning for initial classification with deep learning for detailed analysis of detected anomalies.

Qaddoura et.al.(2021)[58] introduced a multi-layer classification approach for intrusion detection in IoT networks, leveraging deep learning techniques. By implementing a novel architecture that combines initial intrusion detection with subsequent classification of intrusion types, and incorporating an oversampling technique, they aim to enhance the accuracy and comprehensiveness of intrusion detection.

Ullah et.al. (2021)[59] developed a deep learning-based anomaly detection model for IoT networks, using convolutional neural networks (CNN) in dimensions 1D, 2D, and 3D. Their approach leverages transfer learning for both binary and multiclass classification, validated on datasets including BoT-IoT and IoT-23 among others.

Wang et.al.(2021)[60] explored the enhancement of intrusion detection systems using a combination of deep learning models SDAE-ELM and DBN-Softmax. Their research focuses on the effective detection of various attack types across multiple datasets, demonstrating the potential of deep learning in improving intrusion detection accuracy.

Halbouni et.al.(2022)[61] developed a CNN-LSTM hybrid deep neural network aimed at network intrusion detection, demonstrating significant advancements in accuracy and detection rates across multiple datasets including CIC-IDS 2017, UNSW-NB15, and WSN-DS.

D. Related Work Summary Table:

Tabel 1. Section-by-Section Summary of implementing DL in IDS

No	Author(s)	Dataset	Methodology	Pros	Cons	Accuracy
1	Choi et. al. (2019)[31]	NSL-KDD	Autoencoder	High accuracy (91.70%) using unsupervised learning, useful when labeled data is scarce.	May struggle with complex or noisy data compared to supervised methods.	91.70%
2	Otoum et.al. (2019) [32]	NSL-KDD	Stacked Deep Polynomial Network (SDPN)	High accuracy in IoT security	Computational demands	99.02%
3	Li et.al. (2019) [33]	NSL-KDD	Multi-CNN fusion approach	High accuracy and low complexity	Model adaptation challenges	86.95% for binary,81.33% for multiclass classification
4	Zhang et.al. (2020) [34]	KDD Cup 99	Auto-Encoders and LSTM networks	Improved detection accuracy	Dependency on outdated dataset	5 kind attacks behaviour : 97.6%, 96.8%, 95.3%, 94.8% and 94.7%
5	Wu et.al. (2020) [35]	Hduxss_data1.0, NSL-KDD	Semantic re-encoding and ResNet	Superior classification accuracy	Potential implementation challenges	97%, 97.35%, 97.5% for ResNet models
6	Su et.al. (2020) [36]	NSL-KDD	BLSTM with an attention mechanism	High accuracy in detection	Complexity and computational demands	84.25%
7	Hsu et.al. (2020)[37]	UNSW-NB15	Deep Reinforcemen	High adaptability	DRL can be computationa	97.2% accuracy

			t Learning (DRL)	to dynamic threat environments, utilizing reinforcement learning to optimize detection strategies.	lly intensive and require substantial training data to effectively learn and make decisions.	
8	Shahriar et al. (2020) 38]	NSL KDD-99	Generative Adversarial Networks (GAN)	Enhances attack detection and model stability by generating synthetic data to address data imbalance and missing samples.	Complexity of GAN models may introduce computational challenges and the potential generation of misleading synthetic data.	91.70% ac
9	Shende et.al. (2020)[39]	NSL-KDD	LSTM for binary and multiclass classification	High accuracy in network intrusion identification	Focus on specific dataset limits generalizability	99.2% for binary, 96.9% for multiclass classification
10	Nayyar et.al. (2020)[40]	CICIDS2017	LSTM-based machine learning model for anomaly detection	High detection accuracy	Focus on DDoS attacks	96%
11	Mighan et.al. (2020)[41]	UNB ISCX 2012	Hybrid model with stacked autoencoders and various classifiers	Efficient processing of large datasets	High model complexity	99.49%
12	Kim et.al. (2020)[42]	CSIC-2010, CICIDS2017	CNN-LSTM for real-time HTTP traffic analysis	Efficient real-time detection	Computational demands	91.54%, 93%
13	Kasongo et.al. (2020)[43]	UNSW-NB15, AWID	Deep FFDNN with wrapper-based feature selection	Enhanced detection capabilities	Complex feature selection	99.67% (AWID)
14	Hossain et.al. (2020)[44]	NAIST CAN, Automobile IDS	LSTM optimized for CAN bus attack detection	High accuracy with minimal false rates	Real-time dataset performance unknown	99.995% (binary), near 100% (multiclass)
15	Dey et.al. (2020)[45]	IDS 2018	Attention-based CNN-LSTM	Combines CNN and LSTM strengths	Complexity and resource demands	99.98%
16	Chen et.al. (2020)[46]	CICIDS2017,	Transition to deep learning	Automatic feature	Complexity and	99.56%, 99.07%

		USTC-TFC 2016	for IDS	extraction	overfitting issues	
17	Muhammad et al. (2020)[47]	KDDCup99, NSL-KDD, AWID	Stacked autoencoders, DNNs	High accuracy, versatile	High complexity, overfitting risk	94.2% KDDCup99, 99.7% NSL-KDD, 99.9% AWID
18	Basnet et.al. (2020)[48]	CICIDS 2018	DNN and LSTM for DoS attack detection	High accuracy in smart grid security	Limited to DoS attacks	More than 99%
19	Tang et al. (2020)[49]	NSL-KDD	DNN & GRU-RNN	Flow-based intrusion detection for SDNs	Original structural vulnerabilities remain	80.7% (DNN), 90% (GRU-RNN) accuracy
20	Louati et.al.(2020)[50]	KDD 99	Multi-agent system with autoencoders, MLP, and K-NN	High accuracy, reduced detection time	Complex implementation, computationally intensive	99.8% classification accuracy
21	Ahmad et.al. (2020)[51]	KDD99	DNN for network traffic classification	High accuracy in malicious traffic detection	Overfitting and optimization needs	Up to 99.78%
22	Abdullateef et.al. (2020)[52]	KDD 99	Utilizes RNN with CSO for feature reduction	High accuracy with reduced features	Use of outdated dataset	98.34% accuracy
23	Ashiku et.al. (2021)[53]	UNSW-NB15	Deep learning model incorporating CNN	Significant performance improvements	Room for improvement in feature reduction	95.4% & 95.6% accuracy
24	Hu et.al. (2021)[54]	Custom (WiFi CSI)	Path decomposition algorithms and CNN for analyzing CSI data	High sensitivity to human motion	Reliance on CSI data	98.69% & 98.91% accuracy
25	Jithu P et.al. (2021)[55]	Bot-IoT	Development of a DNN for IoT botnet attack detection	Efficacy of DNN in identifying IoT botnet attacks	Scalability and real-time application concerns	94%
26	Laghrissi et.al. (2021)[56]	KDD99	LSTM networks enhanced with PCA and MI	Effective dimensionality reduction	Reliance on KDD99	99.49%
27	Liu et.al. (2021)[57]	NSL-KDD, CIC-IDS2017	Hybrid model combining K-means and Random Forest for binary classification, followed by	High accuracy in detecting intrusions	Complexity and computational resource needs	85.24% & 99.91% accuracy

			CNN and LSTM			
28	Qaddoura et.al. (2021)[58]	IoTID20	Multi-layer classification system using deep learning techniques	High recall for normal and specific intrusion types	Focus on IoTID20 may limit broader applicability	G-mean value of 78%
29	Ullah et.al. (2021)[59]	Multiple (BoT-IoT, IoT-23, etc.)	Convolutional neural networks in 1D, 2D, and 3D combined with transfer learning	Effectiveness of CNNs across different dimensions	Broad scope of IoT environments challenge	99.95%, 99.82%-100%
30	Wang et.al. (2021)[60]	Multiple (KDD Cup99, NSL-KDD, etc.)	Utilization of SDAE-ELM and DBN-Softmax models for intrusion detection	Versatility in identifying various intrusions	Focus on two models might limit exploration of others	Effectiveness in detecting intrusions
31	Halbouni et.al. (2022)[61]	Multiple (CIC-IDS 2017, UNSW-NB15, etc.)	Hybrid CNN-LSTM model, leveraging convolutional neural networks for spatial feature extraction and LSTM for temporal feature recognition	High detection accuracy across datasets	Complexity may challenge rapid deployment adaptation	Up to 99.67% accuracy

E. Discussion

The studies reviewed reveal that deep learning models like CNNs, RNNs, autoencoders, DRL, and hybrid systems markedly improve intrusion detection capabilities, with accuracies often exceeding 90%. The interpretation of these results indicates that these models are exceptionally adept at handling complex, dynamic data, and they significantly reduce false positives while effectively adapting to new threats. The implications of these findings are profound; as cyber threats evolve, the reliance on advanced computational models becomes crucial for maintaining effective defenses. However, the limitation of these models lies in their high computational and data demands, which can hinder scalability and practical deployment in rapidly changing environments.

Future research should therefore focus on optimizing these models to be less resource-intensive, enhancing their efficiency with limited data, and expanding their applicability to new and emerging sectors such as IoT and cloud security, which are becoming increasingly relevant in our interconnected digital landscape. This approach will ensure that IDS remains robust and capable of confronting modern cybersecurity challenges.

F. Conclusion

This review has highlighted the substantial enhancements deep learning can bring to intrusion detection systems (IDS), offering advanced solutions against increasingly sophisticated cyber threats. Through the integration of deep learning techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and autoencoders, IDS can effectively manage and analyze vast data streams, thereby significantly improving threat detection accuracy and system adaptability. Our examination emphasizes not only the immediate benefits of applying these technologies but also the potential for future innovations that could further revolutionize the cybersecurity landscape. Moving forward, it is crucial to continue exploring these technologies in varied and emerging network environments to develop robust, scalable, and efficient IDS capable of meeting the dynamic demands of modern cybersecurity challenges.

G. References

[1] S. W. Lee et al., “Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review,” Journal of Network and Computer Applications, vol. 187. Academic Press, Aug. 01, 2021. doi: 10.1016/j.jnca.2021.103111.

[2] W. Zhong, N. Yu, and C. Ai, “Applying big data based deep learning system to intrusion detection,” Big Data Mining and Analytics, vol. 3, no. 3, pp. 181–195, Sep. 2020, doi: 10.26599/BDMA.2020.9020003.

[3] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, “Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions,” Security and Communication Networks, vol. 2022. Hindawi Limited, 2022. doi: 10.1155/2022/4016073.

[4] J. Lansky et al., “Deep Learning-Based Intrusion Detection Systems: A Systematic Review,” IEEE Access, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 101574–101599, 2021. doi: 10.1109/ACCESS.2021.3097247.

[5] G. Andresini, A. Appice, N. Di Mauro, C. Loglisci, and D. Malerba, “Multi-Channel Deep Feature Learning for Intrusion Detection,” IEEE Access, vol. 8, pp. 53346–53359, 2020, doi: 10.1109/ACCESS.2020.2980937.

[6] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” Journal of Information Security and Applications, vol. 50, Feb. 2020, doi: 10.1016/j.jisa.2019.102419.

[7] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, “Iot intrusion detection taxonomy, reference architecture, and analyses,” Sensors, vol. 21, no. 19. MDPI, Oct. 01, 2021. doi: 10.3390/s21196432.

[8] W. Jo, S. Kim, C. Lee, and T. Shon, “Packet preprocessing in CNN-based network intrusion detection system,” Electronics (Switzerland), vol. 9, no. 7, pp. 1–15, Jul. 2020, doi: 10.3390/electronics9071151.

[9] R. V. Mendonca et al., “Intrusion Detection System Based on Fast Hierarchical Deep Convolutional Neural Network,” IEEE Access, vol. 9, pp. 61024–61034, 2021, doi: 10.1109/ACCESS.2021.3074664.

[10] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A Survey of CNN-Based Network Intrusion Detection," Applied Sciences (Switzerland), vol. 12, no. 16. MDPI, Aug. 01, 2022. doi: 10.3390/app12168162.

[11] S. Moustakidis and P. Karlsson, "A novel feature extraction methodology using Siamese convolutional neural networks for intrusion detection," Cybersecurity, vol. 3, no. 1, Dec. 2020, doi: 10.1186/s42400-020-00056-4.

[12] M. T. Nguyen and K. Kim, "Genetic convolutional neural network for intrusion detection systems," Future Generation Computer Systems, vol. 113, pp. 418–427, Dec. 2020, doi: 10.1016/j.future.2020.07.042.

[13] C. Yue, L. Wang, D. Wang, R. Duo, and X. Nie, "An Ensemble Intrusion Detection Method for Train Ethernet Consist Network Based on CNN and RNN," IEEE Access, vol. 9, pp. 59527–59539, 2021, doi: 10.1109/ACCESS.2021.3073413.

[14] S. V. Amanoul, A. M. Abdulazeez, D. Q. Zeebare, and F. Y. H. Ahmed, "Intrusion Detection Systems Based on Machine Learning Algorithms," in 2021 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2021 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Jun. 2021, pp. 282–287. doi: 10.1109/I2CACIS52118.2021.9495897.

[15] S. Kaur and M. Singh, "Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks," Neural Comput Appl, vol. 32, no. 12, pp. 7859–7877, Jun. 2020, doi: 10.1007/s00521-019-04187-9.

[16] J. C. Kimmel, A. D. McDole, M. Abdelsalam, M. Gupta, and R. Sandhu, "Recurrent Neural Networks Based Online Behavioural Malware Detection Techniques for Cloud Infrastructure," IEEE Access, vol. 9, pp. 68066–68080, 2021, doi: 10.1109/ACCESS.2021.3077498.

[17] M. A. Khan, "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," Processes, vol. 9, no. 5, 2021, doi: 10.3390/pr9050834.

[18] I. Ortega-Fernandez, M. Sestelo, J. C. Burguillo, and C. Piñón-Blanco, "Network intrusion detection system for DDoS attacks in ICS using deep autoencoders," Wireless Networks, 2023, doi: 10.1007/s11276-022-03214-3.

[19] S. Zavrak and M. Iskefiyeli, "Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder," IEEE Access, vol. 8, pp. 108346–108358, 2020, doi: 10.1109/ACCESS.2020.3001350.

[20] C. W. Tien, T. Y. Huang, P. C. Chen, and J. H. Wang, "Using autoencoders for anomaly detection and transfer learning in iot," Computers, vol. 10, no. 7, Jul. 2021, doi: 10.3390/computers10070088.

[21] L. Yang, Y. Song, S. Gao, B. Xiao, and A. Hu, "Griffin: An Ensemble of AutoEncoders for Anomaly Traffic Detection in SDN," in Proceedings - IEEE Global Communications Conference, GLOBECOM, 2020. doi: 10.1109/GLOBECOM42002.2020.9322187.

[22] K. Arshad et al., "Deep Reinforcement Learning for Anomaly Detection: A Systematic Review," IEEE Access, vol. 10. Institute of Electrical and Electronics Engineers Inc., pp. 124017–124035, 2022. doi: 10.1109/ACCESS.2022.3224023.

[23] W. Liang, W. Huang, J. Long, K. Zhang, K. C. Li, and D. Zhang, “Deep Reinforcement Learning for Resource Protection and Real-Time Detection in IoT Environment,” IEEE Internet Things J, vol. 7, no. 7, pp. 6392–6401, Jul. 2020, doi: 10.1109/JIOT.2020.2974281.

[24] M. Lopez-Martin, B. Carro, and A. Sanchez-Esguevillas, “Application of deep reinforcement learning to intrusion detection for supervised problems,” Expert Syst Appl, vol. 141, Mar. 2020, doi: 10.1016/j.eswa.2019.112963.

[25] K. Sethi, R. Kumar, N. Prajapati, and P. Bera, “Deep Reinforcement Learning based Intrusion Detection System for Cloud Infrastructure,” India: IEEE, Jan. 2020. doi: https://doi.org/10.1109/COMSNETS48256.2020.9027452.

[26] S. Tharewal, M. W. Ashfaque, S. S. Banu, P. Uma, S. M. Hassen, and M. Shabaz, “Intrusion Detection System for Industrial Internet of Things Based on Deep Reinforcement Learning,” Wirel Commun Mob Comput, vol. 2022, 2022, doi: 10.1155/2022/9023719.

[27] J. H. Lee and K. H. Park, “GAN-based imbalanced data intrusion detection system,” Pers Ubiquitous Comput, vol. 25, no. 1, pp. 121–128, Feb. 2021, doi: 10.1007/s00779-019-01332-y.

[28] D. Shu, N. O. Leslie, C. A. Kamhoua, and C. S. Tucker, “Generative adversarial attacks against intrusion detection systems using active learning,” in WiseML 2020 - Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, Association for Computing Machinery, Jul. 2020, pp. 1–6. doi: 10.1145/3395352.3402618.

[29] M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso, “G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System,” in Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020, Institute of Electrical and Electronics Engineers Inc., Jul. 2020, pp. 376–385. doi: 10.1109/COMPSAC48688.2020.0-218.

[30] T. Kim and W. Pak, “Early Detection of Network Intrusions Using a GAN-Based One-Class Classifier,” IEEE Access, vol. 10, pp. 119357–119367, 2022, doi: 10.1109/ACCESS.2022.3221400.

[31] H. Choi, M. Kim, G. Lee, and W. Kim, “Unsupervised learning approach for network intrusion detection system using autoencoders,” Journal of Supercomputing, vol. 75, no. 9, pp. 5597–5621, Sep. 2019, doi: 10.1007/s11227-019-02805-w.

[32] Y. Otoum, D. Liu, and A. Nayak, “DL-IDS: a deep learning–based intrusion detection framework for securing IoT,” Transactions on Emerging Telecommunications Technologies, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3803.

[33] Y. Li et al., “Robust detection for network intrusion of industrial IoT based on multi-CNN fusion,” Measurement (Lond), vol. 154, Mar. 2020, doi: 10.1016/j.measurement.2019.107450.

[34] Y. Zhang, Y. Zhang, N. Zhang, and M. Xiao, “A network intrusion detection method based on deep learning with higher accuracy,” in Procedia Computer Science, Elsevier B.V., 2020, pp. 50–54. doi: 10.1016/j.procs.2020.06.055.

[35] Z. Wu, J. Wang, L. Hu, Z. Zhang, and H. Wu, “A network intrusion detection method based on semantic Re-encoding and deep learning,” Journal of Network and Computer Applications, vol. 164, Aug. 2020, doi: 10.1016/j.jnca.2020.102688.

[36] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, “BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset,” IEEE Access, vol. 8, pp. 29575–29585, 2020, doi: 10.1109/ACCESS.2020.2972627.

[37] Y. F. Hsu and M. Matsuoka, “A Deep Reinforcement Learning Approach for Anomaly Network Intrusion Detection System,” in Proceedings - 2020 IEEE 9th International Conference on Cloud Networking, CloudNet 2020, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/CloudNet51028.2020.9335796.

[38] M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso, “G-IDS: Generative Adversarial Networks Assisted Intrusion Detection System,” in Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020, Institute of Electrical and Electronics Engineers Inc., Jul. 2020, pp. 376–385. doi: 10.1109/COMPSAC48688.2020.0-218.

[39] S. Shende and S. Thorat, “Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security,” International Journal of Engineering Research & Technology (IJERT), Jun. 2020, doi: https://www.doi.org/10.17577/IJERTV9IS061016.

[40] S. Nayyar, S. Arora, and M. Singh, Recurrent Neural Network Based Intrusion Detection System. india: IEEE, 2020. doi: https://doi.org/10.1109/ICCSP48568.2020.9182099.

[41] S. N. Mighan and M. Kahani, “A novel scalable intrusion detection system based on deep learning,” Int J Inf Secur, vol. 20, no. 3, pp. 387–403, Jun. 2021, doi: 10.1007/s10207-020-00508-5.

[42] A. Kim, M. Park, and D. H. Lee, “AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection,” IEEE Access, vol. 8, pp. 70245–70261, 2020, doi: 10.1109/ACCESS.2020.2986882.

[43] S. M. Kasongo and Y. Sun, “A deep learning method with wrapper based feature extraction for wireless intrusion detection system,” Comput Secur, vol. 92, May 2020, doi: 10.1016/j.cose.2020.101752.

[44] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, “LSTM-based intrusion detection system for in-vehicle can bus communications,” IEEE Access, vol. 8, pp. 185489–185502, 2020, doi: 10.1109/ACCESS.2020.3029307.

[45] A. Dey, “Deep IDS : A deep learning approach for Intrusion detection based on IDS 2018,” Bangladesh: IEEE, Dec. 2021.

[46] L. Chen, X. Kuang, A. Xu, S. Suo, and Y. Yang, “A Novel Network Intrusion Detection System Based on CNN,” in Proceedings - 2020 8th International Conference on Advanced Cloud and Big Data, CBD 2020, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 243–247. doi: 10.1109/CBD51900.2020.00051.

[47] G. Muhammad, M. Shamim Hossain, and S. Garg, “Stacked Autoencoder-Based Intrusion Detection System to Combat Financial Fraudulent,” IEEE Internet Things J, vol. 10, no. 3, pp. 2071–2078, Feb. 2023, doi: 10.1109/JIOT.2020.3041184.

[48] M. Basnet and M. H. Ali, "Deep learning-based intrusion detection system for electric vehicle charging station," in 2020 2nd International Conference on Smart Power and Internet Energy Systems, SPIES 2020, Institute of Electrical and Electronics Engineers Inc., Sep. 2020, pp. 408–413. doi: 10.1109/SPIES48661.2020.9243152.

[49] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, M. Ghogho, and F. El Moussa, "DeepIDS: Deep learning approach for intrusion detection in software defined networking," Electronics (Switzerland), vol. 9, no. 9, pp. 1–18, Sep. 2020, doi: 10.3390/electronics9091533.

[50] F. Louati and F. B. Ktata, "A deep learning-based multi-agent system for intrusion detection," SN Appl Sci, vol. 2, no. 4, Apr. 2020, doi: 10.1007/s42452-020-2414-z.

[51] S. Ahmad, F. Arif, Zabeehullah, and N. Iltaf, "Novel Approach Using Deep Learning for Intrusion Detection and Classification of the Network Traffic," Tunis: IEEE, Jun. 2022. doi: https://doi.org/10.1109/CIVEMSA48639.2020.9132744.

[52] A. A. A. Lateef, S. T. F. Al-Janabi, and B. Al-Khateeb, "Hybrid Intrusion Detection System Based on Deep Learning," in 2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy, ICDABI 2020, Institute of Electrical and Electronics Engineers Inc., Oct. 2020. doi: 10.1109/ICDABI51230.2020.9325669.

[53] L. Ashiku and C. Dagli, "Network Intrusion Detection System using Deep Learning," in Procedia Computer Science, Elsevier B.V., 2021, pp. 239–247. doi: 10.1016/j.procs.2021.05.025.

[54] Y. Hu, F. Bai, X. Yang, and Y. Liu, "IDSDL: a sensitive intrusion detection system based on deep learning," EURASIP J Wirel Commun Netw, vol. 2021, no. 1, Dec. 2021, doi: 10.1186/s13638-021-01900-y.

[55] P. Jithu, J. Shareena, A. Ramdas, and A. P. Haripriya, "Intrusion Detection System for IOT Botnet Attacks Using Deep Learning," SN Comput Sci, vol. 2, no. 3, May 2021, doi: 10.1007/s42979-021-00516-9.

[56] F. E. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," J Big Data, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00448-4.

[57] C. Liu, Z. Gu, and J. Wang, "A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning," IEEE Access, vol. 9, pp. 75729–75740, 2021, doi: 10.1109/ACCESS.2021.3082147.

[58] R. Qaddoura, A. M. Al-Zoubi, H. Faris, and I. Almomani, "A multi-layer classification approach for intrusion detection in iot networks based on deep learning," Sensors, vol. 21, no. 9, May 2021, doi: 10.3390/s21092987.

[59] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," IEEE Access, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[60] Z. Wang, Y. Liu, D. He, and S. Chan, "Intrusion detection methods based on integrated deep learning model," Comput Secur, vol. 103, Apr. 2021, doi: 10.1016/j.cose.2021.102177.

[61] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion

Detection System," IEEE Access, vol. 10, pp. 99837–99849, 2022, doi: 10.1109/ACCESS.2022.3206425.