ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

DEEP LEARNING FOR INTRUSION DETECTION SYSTEMS

SADAF ISHTIAQ
Email: sadafirshad729@gmail.com
Department of Computer Science, Lahore Leads University, Lahore, Pakistan
FAZAL UR REHMAN
Email: rehmantahir2003@gmail.com
Department Information Technology, Lahore Leads University, Lahore, Pakistan
SARIM SALEEM
Email: sarim.new.inception@gmail.com
Department of Computer Science, Lahore Leads University, Lahore, Pakistan
AHMAD YAAR (Corresponding Author)
Email: hafizahmad1048@gmail.com
Department of Computer Science, Comsats University Islamabad, Sahiwal Campus

Abstract:
In recent years, computer networks have faced a rapid and continuous rise in diverse and sophisticated cyberattacks, posing significant challenges to data integrity and system reliability. Intrusion detection therefore remains a critical research area in network security. The present work examines the implementation of deep learning (DL) methodologies aimed at optimizing the accuracy and adaptability of Intrusion Detection Systems (IDS), alongside a performance comparison among different models feature representation, and benchmark datasets to highlight the advantages of DL-based methods in accurately identifying emerging threats. In the 2024–2025 context, deep learning continues to advance IDS capabilities through automated feature extraction, improved generalization to unseen attacks, and real-time detection across dynamic network environments.

Keywords: *Intrusion datasets*, *intrusion detection*, *Deep learning*, *security service*

I. INTRODUCTION

The network's security has become increasingly important as hostile assaults occur more frequently, protecting user information. There are numerous methods for identification and prevention network service and security. To safeguard the systems, however, network security administration and control are difficult. Various things, including software, hardware, Network attacks, virus assaults, un authorized data access, etc. To ensure the protection of computing environments from diverse attack vectors, a comprehensive security architecture must be established. An Intrusion Detection System (IDS) serves this purpose by analyzing network traffic in real time to detect irregular or malicious actions. The possibility that each new kind of assault may be recognized presents an even bigger gap for intrusion detection systems[1].In addition, the rapid growth of modern communication technologies has created new difficulties. One major issue is the huge amount of data being generated and exchanged across networks in a very short time. Because of the sheer volume of data and the lightning-fast network speeds, it's almost impossible to spot any suspicious activity. Artificial intelligence and machine learning may be used to identify a suspect attack. Deep learning, rather than standard machine learning, is being used and studied by academics . Big data may be mined for useful information . Network intrusion detection uses deep learning techniques to find hidden patterns and recognize threats. The ability of deep learning to simultaneously conduct feature extraction and classification tasks is another key feature[2]. The intrusion exhibits several characteristics and actions.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Using feature selection and extraction, deep learning can automatically decrease the complexity of traffic actions and extract only the most pertinent aspects from the data. Deep Learning has proven effective in a variety of applications. It improves the efficiency and intelligence of everyday life through the use of mobile devices, automation systems, robots, and other technologies (such as image, audio, and video processing) [3].

This paper describes the various assault types and discusses the use of intrusion detection in different applications. They also use deep learning techniques to create a system for identifying malicious attempts. The remainder of the paper is organised as follows: IDS's deep learning techniques are described in Section iii, while deep learning is covered in Section ii of the study. Section iv gives background data, while Section v wraps up the conversation.

II. IDS AND DEEP LEARNING

There are four components in this paragraph. the background of deep learning in the first segment. The second section provides a description of the deep learning architecture and methods. Applications for intrusion detection are covered in the third section. The fourth segment discusses network attacks, and the last section discusses computer network security data sets.

A. Deep Learning

As an extension of traditional machine learning, deep learning employs neural networks with numerous hidden layers, enabling the model to capture high-level abstractions from large datasets. [4]. In deep learning neural networks, there are more inputs and more sophisticated neural layers, making them more difficult to train. Deep learning, a branch of artificial intelligence, expands upon machine learning by using deep neural architectures to extract complex representations from large-scale data. Three forms of learning are included in deep learning. Feature extraction begins with supervised feature learning. In order to accomplish tasks like classification and detection, these properties will be obtained via the use of simple machine learning algorithms. For unsupervised feature learning in its second iteration, just the model's most salient features are used. Using generative feature learning models, a hybrid deep neural network accelerates deep neural network training. The ability to handle complex problems, providing the best results at the lowest cost, eliminating the need for data labelling, and training a large number of parameters in intelligent applications are some of these advantages. However, there are drawbacks, such as difficulties with understanding, a high need for exact data, a high processing cost, and more complicated algorithms [5]. Deep learning is mostly used in applications today to generate decisions, predictions, and classifications. Deep learning relies on both learnable and automatically extractable features.

The use of computer-aided intelligence (AI) tactics in conjunction with a growing internet area and a range of attack elements has been found to be ineffectual. Deep learning methods are recognized for their strong capabilities in extracting features, classifying data, and reducing dimensionality. Their adaptability has enabled their application across numerous fields, such as language processing, visual recognition, and cybersecurity intrusion analysis.

B. Methods of deep learning

Artificial neural network (ANN) methods with several layers of neural networks are being developed using deep learning. Deep learning algorithms are designed to perform tasks such as feature extraction and classification. Another challenge is sifting through enormous amounts of data in search of patternsDeep learning methods can be grouped into three broad categories: those that learn from labelled data (supervised/discriminative), those that generate insights from unlabelled data (unsupervised/generative), and those that combine both strategies (hybrid models). In predictive analysis, supervised models make use of labelled inputs to detect meaningful correlations and trends.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

. Convolutional neural networks (CNN) are one of the most widely used discriminative deep learning techniques for feature selection and image identification. Unsupervised learning, sometimes referred to as generative learning, uses sparse amounts of training data and unlabeled data to learn each lower layer individually. The Auto Encoder (AE), Boltzmann Machine (BM), and Recurrent Neural Networks (RNN) are a few examples of unsupervised methods. Deep neural network (DNN) and generative adversarial networks (GAN) techniques are combined in a method known as "deep hybrid" to achieve the best results possible.

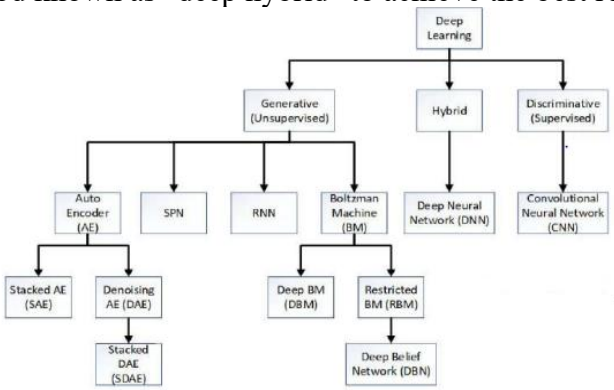

Fig. 1 Deep Learning *Architectre* [7]

C. *IDS for applications*

Cyberattacks now manifest in numerous ways and affect a variety of domains, including communication networks, web platforms, cloud infrastructures, and Internet of Things (IoT) environments. In network and computer security, intrusion detection is one of the most important research areas. An analysis of network traffic is required to detect malicious assaults. Several businesses, including IoT, the internet, wireless, and the cloud, rely on intrusion detection systems. IoT devices require a robust IDS to handle the various threats that originate from various networks. IoT could connect to hundreds of nodes via the internet as the communication devices. There are numerous algorithms that aid in the discovery of various dangers that are used by machine and deep learning techniques to safeguard IoT applications. Smart homes, smart cities, industrial, building, shopping, and transportation applications have all used IoT devices in recent years; all of these applications have to do with device security .Software that can detect unknown and unknown malicious assaults using various intelligent techniques is required for IoT device protection .

Web apps have recently become widely available in many various services, including retail, banking, and social networking [8]. Systems for detecting anomalies are required to protect the web against multiple dangerous activities. Anomaly detection in HTTP request parameters is one of the technologies used to secure the web. The number of threats has increased. Despite applying a variety of data sets on the attack threats that may target web applications conducted in various intelligent ways, including machine learning and deep learning, they have reported on the efficiency, quality, results, and protection of such attacks on their websites.

D. *Network Attacks*

The technological world needs greater defenses against malicious attacks as the communication network continues to grow. Digital data can be protected from infiltration in a variety of ways. Know information about various security attack kinds first. Security services come in third, followed by security mechanisms.

The first step towards safe communication between nodes is always the detection of malicious attempts [9].There have been more dangerous assaults recently. Various circumstances are used

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

to categories a variety of attack types. The two main types of attacks are. The primary objective of an active attack is to exhaust the system's resources. The data stream is altered by this type of assault, which results in false messages like Daniel of service. A passive assault, on the other hand, seeks to gain access to or exploit system data without endangering the system's resources or transmission monitoring.

E. ***Security Mechanism***

The network can use a variety of solutions for intrusion detection and prevention. The security attributes specified in a particular security policy may be enforced via a variety of security mechanisms:

By rejecting attempts to contact an unauthorized person, the firewall guards against outside attacks on the devices in the internal network. To get access to the system, the user is normally asked to provide a name and a password in plain text.

The encryption process transforms a message into a format that conceals its information based on a set of transformation criteria. It is critical to protect systems and data from outside attackers by using intrusion detection.

F. ***Security service***

Detecting and responding to attacks is made possible by effective security technologies called intrusion detection systems (IDS). It does out network traffic monitoring.

A hardware or piece of software known as an intrusion prevention system (IPS) analyses and keeps track of network traffic, guards against malicious attacks, and prevents attacks from ever happening [10].

G. ***Intrusion detection data set***

Network traffic flows that contain information about the host, user activity, and system parameters may be used to create an intrusion detection dataset. This data is essential for analyzing attack patterns and other oddities in different kinds of network assaults. Every day, enormous amounts of data are produced, making secure data transmission crucial . The era of big data is here. the managerial computer security collection organization a wide range of features in a large data collection. This dataset includes a large number of characteristics of many attacks. In order to extract and eliminate unnecessary characteristics and reduce the amount of data, deep learning is essential [11].

The researcher has been studying clever tactics that are essential for developing computer security utilizing a variety of data sets. Several security datasets used for intrusion detection categorization make use of attack features like KDD, CUP99, and NSL-KDD to identify malicious attacks. Since they offer the most crucial characteristics for attack detection in academia, the most popular datasets include the ECML-PKDD 2007, HTTP CSIC 2010, CTU 13, ADFA, and UNSW-NB15; as well as the CIDS, Kyoto, 2006+ ,CICIDS, and CTU 13 datasets, such as KDD99 and NSL-KDD. Furthermore, collecting real-time system traffic data proved to be exceedingly difficult for researchers.

III. DEEP LEARNING ALGORITHEMS FOR INTRUSION DETECTION SYSTEN

After Because deep learning algorithms have the capacity to evaluate and extract relevant information from enormous volumes of data, several scholars have concentrated on IDS issues with them. As a result, some deep

For incursion, learning strategies have been employed systems for detection. The primary goal of deep gaining knowledge of building intrusion systems tasks including feature extraction and categorization[12]. Automatic encoding (AE), Hybrid Deep Learning (HDL), and Deep Belief (DB) are some of the deep learning approaches utilized in the field of artificial intelligence for the detection of intrusions. Deep learning frequently, if not every day, uses a new tactic or methodology. The summaries and comparisons of the published works on deep

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

learning-based intrusion detection are provided in Table 1. The dataset used to build and test the model, along with the deep learning architecture, determined the classification method.

IV. GENERATIVE ARCHITECTURES

Unsupervised learning can use deep learning techniques. Given that there are more unlabeled data than labelled data, this is a significant advantage.

A. *Auto-Encoder (AE)*

The method with the most descriptions in the literature is the auto-encoder (AE), this is applied to classification and dimensionality reduction tasks. Duplicating the input encoder to the output decoder is the goal of this technique. It is utilized in numerous applications that provide features for compression and classification. Stacking AE (SAE), sparse AE, and deposing AE are a few AE extensions.

2020 saw a focus on dimension reduction to simplify and speed up model construction. Large volumes of data may be compressed by using an auto encoder (AE), a deep neural network with a reduced feature space. Data normalization and preprocessing were conducted on the KDD99 dataset. Decision trees, Naive Bayes, and decision tables are other categorization methods that may be used to sort data streams. Five and thirteen features were omitted from the model after it had been tested with all 41 features without the use of (AE) deep learning. The trials demonstrated that using a decision tree classifier with 13 features produced the best results. Three criteria were used to evaluate a system: accuracy of 98.2162 percent, false positives of 0.0066 percent, and false negatives of 0.0180 percent.

The data preprocessing stage uses the Min-Max normalization. The training model for this model was created using the NSL KDD dataset. When compared to traditional machine learning techniques, the recommended model performs best with an accuracy of 91.28 percent. Both the Soft Max Classifier and the Deep Auto-Encoder (DAE) for the last hidden layer were shown. Using all characteristics, 10% of the KDD99 dataset was used to train the model. The proposed model's accuracy of 94.71% prevents overfitting. In 2020, a random forest technique was employed for feature extraction and categorization, and the Auto Encoder deep learning technology was created.

This approach simplifies the system and speeds up processing time by deleting certain functionalities. Data from CICIDS 2017 is utilized to develop the model that has been proposed. The results of the study showed that the proposed AE-RF is 98% accurate.

B. *Recurrent Neural Networks (RNN)*

In regression and classification, the recurrent network is a variant of the ANN known as an ANN. Long-Short-Term Memory (LSTM) and Gated Recurrent Units are two common RNN kinds (GRU). Time-series data prediction is used in this kind of deep learning. To forecast the next time step, the RNN should feed the next time step with its edges. The current cycle necessitates the use of historical data. Aside from robot control, he was also employed in voice recognition and intrusion detection. The use of RNNs for intrusion detection has been the subject of several studies.

In [13] reported on long-short-term memory using four neural networks (LSTM) . In this technique, gates are used to control the memory of the cells. To handle output, input, and forgetting, the LSTM has three gates. On the CIDDS dataset, the proposed model is evaluated. This investigation yielded a 0.85 accuracy rate, which is acceptable. Deep learning recurrent neural networks (RNN) and convolutional neural networks (CNN) were used by researchers to build an intelligent system[12]. In the last stage, deep learning classification attacks are applied to the preprocessed data that was selected as the features for this method.

A strong intrusion detection system is created by combining the deep learning RNNs algorithm with LSTM and gated recurrent units (GRU). According to the data, there is a 97% difference in accuracy, F1, recall, and precision between CNN and RNN. When it comes to wireless

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

intrusion detection systems, Kasongo and Yanxia Sun created a DLSTM-based classifier (IDS).

The Information Gain (IF) filter is used to choose characteristics that provide the most value to the user. The model is trained on the NSL-KDD dataset. Several machine learning approaches are compared to the proposed model. It seems that 99.51 percent of the validation data was accurate according to the results shown.

C. *Deep Belief Networks (DBN)*

Multiple Restricted Boltzmann Machine (RBM) techniques are stacked in the Deep Belief Network (DBN). DBN includes drawing conclusions about unobserved data and learning a probability distribution from an initial dataset. DBN is also employed for applications involving regression, classification, and dimensionality reduction. The goal of DBN is to enhance the ability to learn new features. During the training phase, each hidden layer is taught to rebuild the inputs by altering weights using rapid algorithms [14]. Exhibited a network intrusion detection solution based on deep learning in 2019.

Back Propagation (BP) Neural Network Classifier and Deep Confidence Neural Network (DBN) both employ this feature extraction technique. Using the KDD CUP'99 dataset, the effectiveness of the intrusion detection system was assessed. Character-type features that require data transformation must be numerical features. The data were normalised due to the size of the dataset. Comparing DBN's study of feature learning approaches to PCA and gain ratio. The outcome indicates that the DBN-based feature learning algorithm is more practical for high-dimensional feature learning tasks with s4 get high accuracy of 95.45 percent.

Algorithm for optimization built on a deep belief network. Particle swarm optimization (PSO), genetic algorithm optimization back propagation (GAPSO), and an artificial fish swarm algorithm were the three optimization methods employed in this study. The suggested model was created and tested on the NSLKDD dataset. Predictions made by the model have an accuracy of 83.86 percent. Dai and Pan suggested an intrusion detection system using a Deep Belief Network and Extreme Learning Machine to improve classification accuracy [108]. The DBN-ELM approach trains features using the NSLKDD data set. The suggested model is 97.82% accurate, according to the incremental results.

V. DISCRIMINATIVE ARCHITECTURES

A class of models used in supervised learning data labelled specifically for classification tasks are referred to as discriminative methods.

A. *Convolutional Neural Network (CNN)*

Convolutional Neural Networks (CNNs) are a class of supervised, discriminative deep learning models designed to classify and recognize complex data patterns. Within a Deep Neural Network (DNN), CNNs strengthen inter-layer connections and utilize multiple nonlinear, fully connected layers to extract hierarchical features. The hidden layers of a CNN perform convolution operations, typically involving matrix multiplication, to detect spatial relationships in numerical input data. CNNs are particularly effective in handling complex information with higher precision, enabling applications such as image and video analysis, facial recognition, feature extraction, and intrusion detection [15].

Among the prominent deep learning algorithms for classification, CNNs have shown exceptional performance. Lin et al. (2019) proposed a five-layer CNN architecture for feature extraction and applied a Softmax classifier to categorize various attack types. When evaluated on the KDD99 dataset, their model achieved a notable accuracy rate of 97.53%, demonstrating CNN’s strong potential for intrusion detection tasks.

A method in 2019 that uses a number of deep learning models to categories and identify data. They employed CNN, LSTM, and patched auto encoder, three deep learning models, to extract features from various angles of view. In this programme, the stacked auto encoder

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

extracted sentence-level features, the RNN extracted time series-level features, and the CNN extracted local feature information. The automatic method is effective. It currently has a perfect score after passing the ISCX 2012 test battery. The process of extracting an image feature's noisiest properties is a beneficial algorithm detection technique.

VI. HYBRID DEEP LEARNING

In hybrid architectures, models from both the generative and discriminative domains are present. a deep learning model that successfully combines a variety of deep learning techniques (including Bi LSTM, LSTM with GRU, and CNN with other techniques). In this learning under progressive settings, a variety of deep learning approaches were employed to extract features, integrate the features, and categorise them.

TABLE I. PREFORMANCE OF THE INTRUTION DETECTION SYSTEM USING DEEP LEARNING APPROACHES

Dataset	***Algorithm***	***Feature***	***Accuracy***	***Ref***
NSL-KDD	DBN-ELM	DBN	97.82 %	[16]
KDD99	Soft max	SAE	94.71 %	[17]
CICIDS 2017	Random forest	AE	98%.	[18]
KDD'99	decision trees, Naive Bayes	FE and SAE	98.21 %.	[19]
KDD	DLSTM	Information Gain	99.51 %,	[16]

For the classification phase, several deep learning architectures—such as autoencoders, deep belief networks (DBN), deep neural networks (DNN), and extreme learning machines (ELM)—have been proposed [20]. Using the NSL-KDD dataset, these models achieved an accuracy rate of approximately 93%. In a related study, Malik et al. (2020) incorporated CUDA-enabled computing to enhance detection speed and efficiency, allowing rapid identification and mitigation of multi-vector attacks. Their hybrid deep learning framework combined Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, reaching a detection accuracy of 98.6% on the CICIDS2017 dataset. Furthermore, a hybrid classification approach integrating Deep Learning and Binary Algorithms was also introduced for Intrusion Detection Systems (IDS), demonstrating improved adaptability and precision.

[21]. The Deep Neural Network , Binary Genetic Algorithm (BGA), Binary Bat Algorithm (BBA), and Binary Gravitational Search Algorithm (BGSA) were introduced as the best fit models in a different section of this work to boost the rates of detection. From network traffic, the genetic algorithms choose more than 80 features.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

According to the results, the BGSA performs the hybrid method's inaccuracies the best, with a 99.002 recall rate, a 99.02 precision rate, a 98.98 sensitivity rate, a 98.984 specificity rate, and a 0.997 cost error rate. The suggested model was used with the CICIDS2017 dataset, a brand-new dataset.

Literature Review

From 2018 onward the IDS research community strongly shifted from conventional machine-learning (ML) pipelines toward deep learning (DL) architectures that perform automated feature learning and hierarchical representation. Early comparative and taxonomy studies in this period summarized how DL techniques (CNN, RNN/LSTM, AE, DBN and hybrid schemes) outperform traditional classifiers on standard benchmarks—while also highlighting trade-offs in complexity and deployability. These reviews established a baseline understanding of where DL approaches add value for IDS tasks. ScienceDirect

Autoencoders and unsupervised learning (2018–2021). Autoencoders (AEs) became popular for anomaly detection and dimensionality reduction in IDS research because they learn compact representations of "normal" traffic and flag deviations as anomalies. Studies applying stacked and denoising AEs on datasets such as NSL-KDD and CIC-IDS2017 reported strong compression and detection performance while reducing noisy or redundant features. Work that combined AE feature extraction with classical classifiers (e.g., Random Forest) demonstrated notable gains in detection rates — for example, AE+RF pipelines on CIC-IDS2017 reported accuracy figures near reported state-of-the-art levels for that dataset. manuscriptlink-society-file.s3-ap-northeast-1.amazonaws.com

Temporal models — RNNs and LSTM (2018–2022). Because network traffic exhibits temporal dependencies, recurrent architectures (RNNs, LSTMs, GRUs) were widely explored to capture sequential behavior of flows and session patterns. LSTM-based IDS models demonstrated improved detection of time-dependent attacks (e.g., slow DoS, multi-stage probes) compared with purely feedforward models; however, they introduced latency and heavier training costs in some real-time contexts. Comparative studies in this period emphasized LSTM suitability for sequence modeling while noting resource constraints for large-scale deployment.

Spatial & hybrid feature learning — CNNs and CNN–LSTM (2019–2023). Researchers adapted CNNs (originally for images) to learn local feature patterns in transformed network feature matrices. CNNs produced strong local pattern detection and low false positive rates when used standalone or as feature extractors. Hybrid models that fuse CNNs for spatial feature extraction with LSTMs for temporal modeling (CNN–LSTM) repeatedly achieved superior robustness and accuracy across KDD, NSL-KDD, CIC and UNSW datasets, making hybridization a widely adopted design pattern.

Data augmentation and generative approaches (2020–2024). Data imbalance and scarcity of labeled attack traffic drove the adoption of generative models. GAN-based augmentation and VAE–GAN hybrids were used to synthesize realistic minority attack samples, improving class balance and classifier generalization. Recent augmentation studies (including VAE/WACGAN variants) reported measurable improvements on CIC-IDS2017 and UNSW-NB15 benchmarks, indicating generative augmentation is an effective strategy to mitigate dataset skew and improve recall for rare attack classes.(MDPI)

Transformers and sequence-modeling advances (2022–2024). Inspired by successes in NLP, transformer architectures and attention mechanisms have been adapted to flow-level IDS tasks. Transformer-based frameworks (e.g., FlowTransformer and other transformer-NIDS studies) model long-range dependencies more efficiently than classical RNNs and can be parallelized for higher throughput. Initial 2023–2024 work shows promising detection accuracy and

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

improved handling of long sequences in cloud/IoT contexts, indicating transformers are an emerging direction for time-sensitive IDS.

Graph Neural Networks (GNNs) and structure-aware detection (2021–2024). With network traffic naturally forming graph structures (flows, host relations, provenance), GNNs have been investigated to capture structural and relational attack patterns that tabular features miss. Recent surveys and studies (2023–2024) show GNNs can improve detection for lateral movement, multi-host attacks, and stealthy campaigns by exploiting topological cues; however, graph construction and scalability remain active challenges.

Recurring challenges (2018–2025). Across these years common limitations persisted: (1) dataset quality and realism (many benchmarks are dated or lack modern IoT/cloud traffic); (2) class imbalance and rare attack detection; (3) adversarial vulnerability of DL models; (4) computational/training cost impeding real-time deployment on edge devices; and (5) explainability — DL models remain opaque, complicating incident response. The literature therefore increasingly emphasizes hybrid pipelines (combine DL feature learning with lightweight classifiers), data augmentation, adversarial robustness techniques, and research into interpretable DL to make IDS outputs actionable for security operators.

Synthesis and trend (2018–2025). The literature from 2018 to 2025 shows a clear trajectory: from applying individual DL building blocks (AE, CNN, RNN) to designing hybrid and structure-aware models (CNN–LSTM, GAN-augmented pipelines, Transformers, and GNNs). Recent work focuses on practical constraints — dataset realism, class imbalance, latency, and robustness — marking the field's maturation from proof-of-concept accuracy gains toward operational readiness and resilient, interpretable IDS solutions.

VII. DISCUSSIONS AND COMPARISON

In order to compare the effectiveness of various strategies for improving intrusion detection systems, As shown in Table (1), this paper examines the use of deep learning techniques between 2018 and 2020. In the parts that came before this one, research on deep learning methods used to develop IDS was previously discussed. Network intrusion detection systems (NIDS) are enhanced using deep learning to better recognize various malicious attempts.

A huge number of features are handled by an intrusion detection system. The deep learning approach's main function is feature earning through the simplification of huge data additionally, the data preparation feature Deep learning does not employ extraction. The AE generative models have mostly been employed for accurately learning features from features. The use of deep learning to perform the classification problem learning methods produced high detection rates. Accuracy RNNs are mostly employed as categorization for various assault types that achieved excellent outcomes. Because intrusion detection frequently had to deal with different big data, the hybrid deep learning and ensemble learning approaches are a progressive approach that take advantage of the best qualities of each group of algorithms. By combining different algorithms, these approaches could be able to fill in the model's gaps and produce the best outcomes. To demonstrate the effectiveness of deep learning in intrusion detection, various deep learning approaches are compared.

On the other hand, deep learning has a lengthy training period and requires a lot of machine storage. Deep learning exhibits significant benefits in feature extraction. It has been extensively applied to feature selection and has increasingly taken the role of older machine learning algorithms. Accurate detection and classification were necessary for the intrusion detection system to be improved. Most researchers utilized accuracy as the key parameter for assessing the effectiveness of deep learning algorithms based on several indicators.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

The data collection, feature learning methods, and deep learning algorithm are all compared in this research. The results of this study, which tries to demonstrate how well several profound learning algorithms perform, are shown in Table 1.

VIII. CONCLUSION

An intrusion detection system (IDS) can be built using deep learning techniques to identify many forms of attacks. The primary goal of applying deep learning techniques is anomaly detection, which may be applied to both dimensionality reduction and classification problems. In addition, it outperforms conventional machine learning techniques and handles complex huge data sets in a better way. This study examined a number of studies and came to the conclusion that the hybrid deep learning approach is being used more frequently to accurately identify risks.

References

[1] A. Tabassum, A. Erbad, and M. Guizani, "A survey on recent approaches in intrusion detection system in IoTs," *2019 15th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2019*, no. June, pp. 1190–1197, 2019, doi: 10.1109/IWCMC.2019.8766455.

[2] S. N. Mighan and M. Kahani, "Deep Learning Based Latent Feature Extraction for Intrusion Detection," *26th Iran. Conf. Electr. Eng. ICEE 2018*, pp. 1511–1516, 2018, doi: 10.1109/ICEE.2018.8472418.

[3] J. Wang, B. Cao, P. Yu, L. Sun, W. Bao, and X. Zhu, "Deep learning towards mobile applications," *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 2018-July, pp. 1385–1393, 2018, doi: 10.1109/ICDCS.2018.00139.

[4] M. A. M. Sadeeq and A. M. Abdulazeez, "Neural Networks Architectures Design, and Applications: A Review," *3rd Int. Conf. Adv. Sci. Eng. ICOASE 2020*, pp. 199–204, 2020, doi: 10.1109/ICOASE51841.2020.9436582.

[5] S. V. A. Amanuel and S. Y. A. Ameen, "Device-to-device communication for 5G security: A Review," *J. Inf. Technol. Informatics*, vol. 1, no. 1, pp. 26–31, 2021.

[6] N. Riaz, S. O. Gilani, S. I. A. Shah, Emad-Udin, and F. Rehman, "Fault signal detection of linear actuators based on intelligent remnant filter," *2019 8th Int. Conf. Inf. Commun. Technol. ICICT 2019*, pp. 180–184, 2019, doi: 10.1109/ICICT47744.2019.9001965.

[7] G. Noh, J. Kim, S. Choi, N. Lee, H. Chung, and I. Kim, "Feasibility Validation of a 5G-Enabled mmWave Vehicular Communication System on a Highway," *IEEE Access*, vol. 9, pp. 36535–36546, 2021, doi: 10.1109/ACCESS.2021.3062907.

[8] A. A. Salih *et al.*, "Deep Learning Approaches for Intrusion Detection," *Asian J. Res. Comput. Sci.*, pp. 50–64, 2021, doi: 10.9734/ajrcos/2021/v9i430229.

[9] A. S. Abdulraheem *et al.*, "Home Automation System based on IoT," *Technol. Reports Kansai Univ.*, vol. 62, no. 05, pp. 2453–2464, 2020, [Online]. Available: https://www.researchgate.net/publication/342561938.

[10] A. Thakkar and R. Lohiya, "A Review of the Advancement in Intrusion Detection Datasets," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 636–645, 2020, doi: 10.1016/j.procs.2020.03.330.

[11] W. Zhong, N. Yu, and C. Ai, "Applying big data based deep learning system to intrusion detection," *Big Data Min. Anal.*, vol. 3, no. 3, pp. 181–195, 2020, doi: 10.26599/BDMA.2020.9020003.

[12] N. Riaz, S. I. A. Shah, F. Rehman, and M. J. Khan, "An Intelligent Hybrid Scheme for Identification of Faults in Industrial Ball Screw Linear Motion Systems," *IEEE Access*, vol. 9, pp. 35136–35150, 2021, doi: 10.1109/ACCESS.2021.3062496.

[13] N. Riaz, S. I. A. Shah, F. Rehman, S. O. Gilani, and E. Udin, "A Novel 2-D Current Signal-Based Residual Learning with Optimized Softmax to Identify Faults in Ball Screw Actuators," *IEEE Access*, vol. 8, pp. 115299–115313, 2020, doi:

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

10.1109/ACCESS.2020.3004489.

[14] S. A. Althubiti, E. M. Jones, and K. Roy, "LSTM for Anomaly-Based Network Intrusion Detection," *2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018*, pp. 1–3, 2019, doi: 10.1109/ATNAC.2018.8615300.

[15] Q. Tian, D. Han, K. C. Li, X. Liu, L. Duan, and A. Castiglione, "An intrusion detection approach based on improved deep belief network," *Appl. Intell.*, vol. 50, no. 10, pp. 3162–3178, 2020, doi: 10.1007/s10489-020-01694-4.

[16] J. A. Nada and M. R. Al-Mosa, "A Proposed Wireless Intrusion Detection Prevention and Attack System," *ACIT 2018 - 19th Int. Arab Conf. Inf. Technol.*, pp. 1–5, 2019, doi: 10.1109/ACIT.2018.8672722.

[17] P. R. Chandre, P. N. Mahalle, and G. R. Shinde, "Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification," *Proc. - 2018 IEEE Glob. Conf. Wirel. Comput. Networking, GCWCN 2018*, pp. 135–140, 2019, doi: 10.1109/GCWCN.2018.8668618.

[18] A. A. Salih and M. B. Abdulrazaq, "Combining Best Features Selection Using Three Classifiers in Intrusion Detection System," *2019 Int. Conf. Adv. Sci. Eng. ICOASE 2019*, no. April, pp. 94–99, 2019, doi: 10.1109/ICOASE.2019.8723671.

[19] A. Othman et. al., "An Energy-Efficient MIMO-Based 4G LTE-A Adaptive Modulation and Coding Scheme for High Mobility Scenarios," *Int. J. Comput. Netw. Technol.*, vol. 03, no. 02, pp. 69–74, 2015, doi: 10.12785/ijcnt/030204.

[20] P. Kottapalle, "A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data," *J. Inf. Comput. Sci.*, vol. 10, no. March, pp. 1362–1370, 2020.

[21] S. A. Ludwig, "Applying a Neural Network Ensemble to Intrusion Detection," *J. Artif. Intell. Soft Comput. Res.*, vol. 9, no. 3, pp. 177–188, 2019, doi: 10.2478/jaiscr-2019-0002.