

CYBERATTACK DETECTION USING DEEP LEARNING TECHNIQUES

Tariq Ali (Corresponding Author)

MS Scholar, Mir Chakar Khan Rind University, SIBBI

Email: tariqali550@gmail.com

Shafiq Ahmed

MS Scholar, Mir Chakar Khan Rind University, SIBBI

Email: nish.shah009@gmail.com

Israr Ahmed

MS Scholar, Mir Chakar Khan Rind University, SIBBI

Email: israrshohaaz12@outlook.com

ABSTRACT

The increasing frequency and sophistication of cyberattacks have made traditional rule-based security systems inadequate. Deep learning (DL), a subfield of artificial intelligence (AI), provides a powerful approach for detecting and mitigating cyber threats by automatically learning complex data patterns. This study explores deep learning-based techniques for cyberattack detection, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders. Experimental results from recent studies highlight that DL models outperform traditional machine learning algorithms in accuracy, adaptability, and feature extraction. The paper concludes with recommendations for integrating DL systems into real-world cybersecurity frameworks.

Keywords: Cybersecurity, Deep Learning, Intrusion Detection, Neural Networks, Artificial Intelligence

Introduction

As the internet-related devices and digital infrastructure grow at a high rate, so are the cybersecurity threats. Conventional security solutions like rule-based and firewalls can solely identify familiar attack patterns, exposing the networks to new and advanced threats (Kim et al., 2020). To provide an answer to this, Deep learning is an algorithm inspired by biological neural networks and is capable of learning complex and hidden relationships in large datasets. Autoencoders, RNNs and CNNs are popular DL models used in intrusion detection, anomaly detection, and malware classification. In the given paper, the researcher aims to analyze the improvement of cyberattack detection performance and reliability by the use of DL-based models.

Background of the Study

Cybersecurity is nowadays a burning issue to governments, organizations, and individuals in the inter-religious world. Due to the enormous expansion of digital technologies, IoT gadgets, and cloud services, the exchange of data and network dependence have increased exponentially (Almomani, 2024). This reliance has also exposed networks to cyberattacks, such as malware, denial of service (DoS), phishing and ransomware, which may result in data breaches and costly losses.

The conventional security measures, including firewalls and signature-based intrusion detection systems (IDS), cannot identify zero-day attacks and advanced emerging threats (Sahoo et al., 2020). To address these issues, researchers have resorted to machine learning (ML) and deep learning (DL), which may learn patterns of attacks automatically to work with large datasets and keep pace with new attack patterns (Sharma & Kaushik, 2022).

Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) are some of the deep-learning algorithms that have demonstrated impressive performance in detecting cyberattacks (Bukhari et al., 2024). CNNs are good for extracting spatial features of traffic data whereas LSTMs are suitable to extract sequential dependencies, hence they are effective at detecting both simple and complex attacks (Hasan et al., 2023). This paper suggests a Hybrid CNN-LSTM architecture that combines the two architectures to enhance the detection accuracy and resilience of the model on various datasets.

Scope and Limitations

This study is restricted to the supervised deep learning techniques on NSL-KDD, CICIDS2017, and UNSW-NB15 data. The research is centered on the evaluation of the classification performance in the conditions of the experiment. It does not involve unsupervised or federated learning strategies, real-time deployment, or model explainability. The following areas are suggested to be considered in the future.

Literature Review

Barbhaya, M., Dasari, (2025). The blistering incorporation of network-based control systems vulnerability into the Industry Control Systems (ICS) has exposed them to highly advanced cyber assaults, more so in the chemical process sector. The opponents use these systems to undermine operations and disrupt safety, exploiting sensor data, and going undetected by traditional fault detection systems. Cyberattacks on critical infrastructure are now the new normal, and the World Economic Forum (WEF) has put cyber threats as the seventh highest worldwide risk in terms of probability in the next ten years. Moreover, cybercrime has increased by 600 percent since COVID-19, which underscores the importance of well-developed cybersecurity systems. In this study, a hybrid cybersecurity model is proposed integrating an improved Typicality and Eccentricity Data Analytics (TEDA) algorithm with a Convolutional Neural Network (CNN) to detect and categorize real-time ICS cyberattacks. The improved TEDA code uses a sliding window mechanism in adaptive statistical analysis and a characteristic model to identify advanced cyber threats, which allows the rapid detection of anomalies and mitigation of them without using a lot of historical data. At the same time, CNN classifier correctly recognizes

the type of attacks, which makes it possible to implement the correct mitigation strategies on time. Lab validation of an ICS on a large scale confirms the effectiveness of the framework in various cyberattacks such as Min-Max, Surge, Ramp, and Replay attacks. The findings demonstrate its versatility, compact size, and real-time capabilities, and the suggested framework is a scalable and deployable approach to improving ICS cybersecurity and operational resiliency.

Naveeda, K., & Fathima, S. S. S. (2025). The adoption of the Internet of Things (IoT) and MultiFunction Energy Meter into the power grid highlights the urgent necessity of the effective cybersecurity program to handle the data. The high level of accuracy and integrity of data sent and stored by smart meters needs to be guaranteed to ensure the integrity of the entire energy grid. Any changes in energy consumption data that are not authorized may have a risk of causing financial losses to utility companies, as well as creating a risk of consumers being disrupted in services. Based on machine learning (ML) models, this paper introduces an IoT-enabled cyberattack detection system (IoT-E-CADS) on the advanced metering infrastructure (AMI). As per the industry requirements, the proposed Bi-level IoT-E-CADS is capable of detecting two types of threats in a smart grid environment. The first level is the Isolation Forest algorithm of ML, which detects anomalies and cyberattacks within the real-time systems. The second level then applies the Decision Tree ML algorithm to detect cyberattacks and incidences of false injection of data in real-time systems. The hardware is designed and has been tested successfully in Quantanics TechServ Pvt. Ltd. located in Madurai, Tamil Nadu, India. This business operates an AMI facility of 10 smart meters, information filter, and exclusive server system. This enables complete monitoring and recording of the electrical parameters and power profile of the business. Here, the proposed IoT-E-CADS has been implemented and it has managed to identify two cyberattacks that are manually generated. Evaluating the received findings proves that the IoT-E-CADS can identify cyber threats at an accuracy rate of 95 per cent, which ensures all-encompassing cybersecurity services to secure monitoring departments in business settings.

Anurag, A., Shankar, (2024, January). Robotic systems play an important role in many industries, medicine, disaster management, agriculture, police and the military. They are prone to numerous security threats, such as hardware, software, and application attacks. IoT protocols are susceptible to DDoS attacks because they are vulnerable to the Information, Access, and Functional aspects, which are small, lack computing capabilities, and are not uniform. The solutions based on machine learning (ML) can contribute to better security in authentication, access control, offloading in a secure manner, malware detection, and network performance. Supervised learning, K-nearest neighbour (KNN), neural networks, deep neural networks, and random forest (RF) are useful in classifying and regression of network traffic characteristics using ML algorithms. With reinforcement learning, IoT devices can automatically pick security mechanisms and essential requirements when faced with cyberattacks. Unsupervised learning groups unlabelled network traffic data into useful clusters. This study highlights the prospects of the ML-based solutions in enhancing security even on the diverse robotic systems and IoT gadgets.

AlZubi, A. A., Al-Maitah, (2021). The use of cyber-physical systems has been widely applied in healthcare sectors to provide patients with a high standard of treatment in

complex clinical settings. The heterogeneity of the medical device used in these systems (mobile devices and body sensor nodes) opens up infinite attack surfaces and thus requires the development of efficient security solutions to these compound environments. Therefore, in this research, the cognitive machine learning assisted Attack Detection Framework has been suggested to share healthcare data safely. The Healthcare Cyber-Physical Systems will be competent to disseminate the acquired data to the cloud storage. Machine learning systems forecast the behavior of cyber-attacks and its processing can provide decision support to healthcare professionals. The proposed solution is premised on a patient-based design that protects the information on a trusted device such as the mobile phones of the end users and gives the end users control over access data sharing. The model as proposed by us is shown to work well in experimental results, with a ratio of attack prediction of 96.5, ratio of accuracy of 98.2, ratio of efficiency of 97.8, limited delay of 21.3, and communication cost of 18.9, compared to other models in the field.

Some of the literature has indicated that deep learning models predict better than traditional algorithms in protecting against intrusion. Yin et al. (2017) used recurrent neural networks to predict temporal variations on network traffic with high accuracy. The authors of Javaid et al. (2016) introduced a network intrusion detection system based on the autoencoder network that can be trained on raw data without any supervision. Ferrag et al. (2022) compared various deep learning models and found that hybrid CNN-LSTM models have the highest performance. Nevertheless, there are still issues, such as model interpretability, the necessity of large training data, and the cost of computation. In spite of such limitations, deep learning is still transforming the realm of cybersecurity by offering intelligent and adaptive solutions.

Research Objectives

The objectives of this study are to:

Create a hybrid deep learning network of CNN and LSTM to detect cyberattacks.

Test the model on benchmark data (NSL-KDD, CICIDS2017, UNSW-NB15).

Compare the proposed model to classic deep learning models (CNN, RNN, Autoencoder).

Compare model performance in terms of accuracy, precision, recall, and F1-score values.

Research Questions

How can deep learning models enhance cyberattack detection compared to traditional ML-based methods?

What benefits does the integration of CNN and LSTM provide in detecting complex attack types?

How does the hybrid CNN-LSTM model perform across multiple benchmark datasets?

Significance of the Study

The study will help in advancing the next generation of intelligent intrusion detection systems which use the power of deep learning to enhance precision and flexibility. The hybrid framework suggested will improve both spatial as well as temporal

learning, enabling to detect more advanced and changing cyber threats. The results have the potential to help information security experts, scholars, and network managers create effective and adaptive real-time defense systems.

Methodology

The research relies on the secondary data collected through three popular intrusion detection datasets, including NSL-KDD, CICIDS2017, and UNSW-NB15. Normalization, feature encoding, and class balancing are data preprocessing steps that aid in enhancing model generalization. CNN, RNN, and Autoencoders are trained and evaluated on the basis of accuracy, precision, recall, and F1-score.

Table 1 Dataset Description

Dataset	Number Records	of Features	Classes
NSL-KDD	125,973	41	Normal, DoS, Probe, R2L, U2R
CICIDS2017	2,830,743	80	Normal, 14 Attack Types
UNSW-NB15	257,673	49	Normal, 9 Attack Types

The three benchmark datasets, which are applied to test the performance of cyberattack detection in this study, are displayed in Table 1. The datasets are quite different in terms of size, number of features and varieties of attack categories, which emphasize to test the resilience and the capability of the proposed deep learning structure to be generalized.

The size of the NSL-KDD dataset is rather small (125,973 network connection records and 41 features). It is the classic network attack forms like Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). The dataset can be applied to baseline model training and verify the framework on familiar classical attacks.

CICIDS2017 is significantly larger and more complicated with over 2.8 million records and 80 features. It consists of benign traffic and 14 types of attacks, which are modern and realistic network behaviors. Due to its large size and heterogeneity, it offers a good testing ground to assess how well the deep learning models can perform on the real-world traffic.

UNSW-NB15 dataset is an intermediate sized contemporary dataset consisting of 257,673 records and 49 features. It includes nine categories of attacks that are produced in the present-day environment as a result of a hybrid model that involves normal and malicious traffic. This data set fills the gap between classical and current network worlds and the adaptability of models to changing patterns of attack is put to test.

Altogether, the combination of these datasets will guarantee that the proposed framework will be tested in various network configurations, feature space, and attack

complexities, which will improve the validity and generalizability of the experimental findings.

Proposed Model

The hybrid CNN-LSTM model proposed combines the functions of spatial and temporal feature extraction. CNN layers are used to extract spatial correlations between network packets, and LSTM layers are used to extract temporal dependencies, allowing the model to detect sequential attack behavior. The Adam optimizer is used to optimize the architecture with binary cross-entropy loss.

Table 2 Proposed Model Architecture

Layer Type	Number of Units/Filters	Activation Function	Output Shape
Input Layer	-	-	(None, 100, 1)
Conv1D	64	ReLU	(None, 98, 64)
MaxPooling1D	2	-	(None, 49, 64)
LSTM	128	Tanh/Sigmoid	(None, 128)
Dense	64	ReLU	(None, 64)
Dropout	0.5	-	(None, 64)
Output Layer	1	Sigmoid	(None, 1)

Table 2 demonstrates the specific structure of the proposed deep learning model architecture that is used to detect cyberattacks. The model is a combination of Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) layers to identify both spatial and temporal patterns in the network traffic data.

The architecture starts with an Input Layer which accepts feature sequences reconfigured into the dimensions (None, 100, 1), with 100 being the length of the sequence and 1 being one of the feature channels. A 1D Convolutional (Conv1D) layer containing 64 filters and ReLU (activation) of the convolutional layer, is used as the first processing block to extrapolate the local spatial features of the input data. This layer can be used to identify short term trends like packet bursts or local network flow anomaly.

It is followed by a MaxPooling1D layer of size 2 that down-samples the feature maps, decreasing the dimensionality and computer cost of the computation. This pooling operation preserves the most important properties as well as ignoring the redundant information.

Then, an LSTM layer with 128 units and tanch activation functions/sigmoid activation functions is applied to capture the time series relationships in the data. This layer records the long-term associations and sequential trends that tend to appear in the pattern of cyberattacks (e.g., incremental accumulation of DDoS or brute-force attacks).

The LSTM layer output is fed to a fully connected Dense layer containing 64 neurons and with ReLU activation which allows the model to learn non-linear combinations of features. A Dropout layer of rate 0.5 will be added to address overfitting by randomly

disabling half of the neurons at each training step.

Lastly, an Output Layer that has one neuron and Sigmoid activation function gives a binary response that is the likelihood of a particular network flow being normal (0) or malicious (1). The sigmoid output can be easily classified by threshold.

This CNN-LSTM model successfully incorporates both feature learning and temporal sequence learning and classification functions, which is why it is highly suitable to identify sophisticated and dynamic cyberattack patterns in networks of large scale.

Table 3 Performance Comparison of Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
CNN	98.2	97.6	96.8	97.2
RNN	97.4	96.1	95.8	95.9
Autoencoder	95.8	94.2	93.7	94.0
Hybrid CNN-LSTM	99.1	98.7	98.3	98.5

The relative performance findings of various deep learning models tested to detect cyberattacks are reported in Table 3. The four main measures of Accuracy, Precision, Recall and F1-Score were used to evaluate the models CNN, RNN, Autoencoder and the proposed Hybrid CNN-LSTM.

According to the results, the detection performance of all deep learning models was high; nevertheless, there were significant differences regarding the capacity of the models to generalize and to detect sophisticated attack behaviors. The CNN model obtained the accuracy of 98.2 which indicates a good spatial feature extraction of network traffic. CNNs have been shown helpful in detecting localized attack signatures with convolutional filters, but lose temporal information on long sequences.

RNN (97.4) also had a lower accuracy than CNN, but it had a balanced recall (95.8) and F1-score (95.9) and demonstrated stronger performance in sequential dependencies among network flows. This underscores the RNN capability to identify attacks that are developed over time, including scanning or infiltrations.

The Autoencoder model scored a relatively low accuracy of 95.8% mainly due to the fact that it is not supervised. It is good at noticing unexpected or infrequent abnormalities but can fail to notice subtle attack types when it is trained only on normal data.

The suggested Hybrid CNN-LSTM model ranked above all other baseline models with an overall accuracy of 99.1, precision of 98.7 and recall of 98.3 and F1-score of 98.5. This high performance shows that convolutional layers- plus- LSTM layers (legislating space- and- time-based features and features, respectively) are more effective in improving the model to detect the short- and the long-term patterns of attacks. The hybrid methodology is useful with real-time intrusion detection in dynamic networks as it captures local data variations whilst maintaining sequential dependencies.

The findings verify that hybrid deep learning frameworks offer a stronger and more

reliable mechanism of detecting cyberattacks than unimodal methods. Such a high quality increase in F1-score suggests that there is an equal trade-off between false positives and false negatives, which is essential in a practical intrusion detection system.

Results and Discussion

The proposed Hybrid CNN-LSTM model was tested on three benchmark datasets NSL-KDD, CICIDS2017 and UNSW-NB15 (Table 1). These datasets are varied in size, features, and types of attacks, which gives a general evaluation of how the model is performing on classical and modern cyberattacks.

The proposed architecture (Table 2) integrates Convolutional Neural Networks (CNN) to extract spatial features, and Long Short-Term Memory (LSTM) layers to learn time-based relationships in network traffic. This composite design allows the model to be efficient in capturing complicated attack forms.

Table 3 shows that the Hybrid CNN-LSTM model had the highest performance with the highest accuracy at 99.1, which is better than the standalone CNN (98.2%), RNN (97.4%), and Autoencoder (95.8) models. The accuracy of detection (98.7) and recall (98.3) implies that the model is able to identify attacks with high precision and false alarms are low.

The findings validate the claim that combining convolutional and recurrent layers enhances detection accuracy and strength. The Hybrid CNN-LSTM model is also effective in detecting short-term and long-term behavior of attacks, hence it can be applied in real-time intrusion detection systems.

Discussion

The overall findings of Tables 13 indicate the significance of integrating different datasets, hybrid models, and the learning of deep features to create a powerful intrusion detection paradigm.

The model was able to generalize to datasets with different traffic characteristics and this proves its ability to perform consistently. The high accuracy and recall rates support the fact that the model can predict attacks and false alarms with high precision, which is a critical factor of an efficient security system.

Additionally, the F1-score of 98.5% indicates that there is some kind of a trade-off between precision and recall, meaning that the model can be trusted to distinguish between regular and attack traffic without a high level of a bias.

Nonetheless, the hybrid model requires more computing resources because of its intricate structure, thus might not be applicable to low-power edge hardware. Additional optimization methods to be implemented in the future to minimize processing time and memory usage include pruning, quantization, or lightweight CNN-LM versions of the model.

Conclusion and Future Work

The paper described a Hybrid CNN-LSTM machine learning architecture to identify cyberattacks in network traffic with three benchmark datasets, namely, NSL-KDD, CICIDS2017, and UNSW-NB15. The model was shaped to take advantage of CNNs and LSTMs in extracting spatial features and learning a sequence of values,

respectively. As it was revealed in the experimental results, the hybrid model exhibited higher performance with 99.1% accuracy, 98.7% precision, 98.3% recall, and F1-score of 98.5 that outperformed standalone CNN, RNN, and Autoencoder models. These findings verify that the integration of convolutional and recurrent structures can lead to a substantial increase in the capacity of the model to recognize more sophisticated and dynamic patterns of attacks in the large-scale network setting. The framework proposed is very accurate and reliable in the real-time intrusion detection system and is very efficient in minimizing the false alarms but generalizes well across datasets. Nevertheless, its complexity and memory consumption can be too large to run on devices with limited resources or edges. Another problem to consider is to optimize the model to use in lightweight environments. For future research, the framework can be extended in several directions.

Model optimization:

Using pruning, quantization, or knowledge distillation to achieve faster speeds and smaller models.

State-of-the-art architectures:

Investigating Transformer-based or Graph Neural Network models to identify more profound connections in network traffic.

Federated and distributed learning:

Allowing synergistic training by different organizations without data transfer to improve privacy and scalability

Explainable AI (XAI):

Employing techniques of interpretability, including SHAP or attention visualization, to assist analysts in interpreting detection decisions

Adaptive learning:

Introducing a continuous or online learning to deal with new types of attacks and changing threat environments.

Summing up, Hybrid CNN-LSTM is a powerful, precise, and flexible platform to present-day cyberattack identification and a strong basis to develop the next generation, intelligent, and autonomous network security frameworks.

This study shows that deep learning-based techniques can significantly enhance the accuracy of detection of cyberattacks. The combination of CNN and LSTM models yield better performance than the traditional models. Future research needs to address explainable AI (XAI), to improve the model transparency and create lightweight deep learning models that can be deployed in edge and IoT devices.

References

Alaithman, M., Aldweesh, A., Al-Qerem, A., Al Maqousi, A. Y., Almomani, A., & Alkasassbeh, M. (2024). Cryptographic protocols for internet of things (IoT) security lightweight schemes and practical deployment. *Innovations in Modern Cryptography*, 431-448. <https://www.igi-global.com/chapter/cryptographic->

- protocols-for-internet-of-things-iot-security-lightweight-schemes-and-practical-deployment/354050
- AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. *Soft Computing*, 25(18), 12319-12332. <https://link.springer.com/article/10.1007/s00500-021-05926-8>
- Anurag, A., Shankar, A., Narayan, A., & TR, M. (2024, January). Robotic and Cyber-Attack Classification Using Artificial Intelligence and Machine Learning Techniques. In 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-6). IEEE. <https://ieeexplore.ieee.org/abstract/document/10469153/>
- Barbhaya, M., Dasari, P. R., Damarla, S. K., Srinivasan, R., & Huang, B. (2025). A deep learning framework for cyberattack detection and classification in Industrial Control Systems. *Computers & Chemical Engineering*, 109278. <https://www.sciencedirect.com/science/article/pii/S0098135425002807>
- Bukhari, S. M. S., Zafar, M. H., Abou Houran, M., Qadir, Z., Moosavi, S. K. R., & Sanfilippo, F. (2024). Enhancing cybersecurity in Edge IIoT networks: An asynchronous federated learning approach with a deep hybrid detection model. *Internet of Things*, 27, 101252. <https://www.sciencedirect.com/science/article/pii/S2542660524001938>
- Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2022). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 67*, 103142.
- Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies**, 21–26.
- Kaushik, D., Garg, M., Gupta, A., & Pramanik, S. (2022). Application of machine learning and deep learning in cybersecurity: An innovative approach. In *An Interdisciplinary Approach to Modern Network Security* (pp. 89-109). CRC Press. <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003147176-6/application-machine-learning-deep-learning-cybersecurity-dushyant-kaushik-muskan-garg-anu-ankur-gupta-sabyasachi-pramanik>
- Kim, G., Lee, S., & Kim, S. (2020). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41*(4), 1690–1700.
- Naveeda, K., & Fathima, S. S. S. (2025). Real-time implementation of IoT-enabled cyberattack detection system in advanced metering infrastructure using machine learning technique. *Electrical Engineering*, 107(1), 909-928 <https://link.springer.com/article/10.1007/s00202-024-02552-z>
- Sahoo, K. S., Tripathy, B. K., Naik, K., Ramasubbareddy, S., Balusamy, B., Khari, M., & Burgos, D. (2020). An evolutionary SVM model for DDOS attack detection in software defined networks. *IEEE access*, 8, 132502-132513. <https://ieeexplore.ieee.org/abstract/document/9142183/>
- 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.