Enhancing IoT Security Through Anomaly Detection and Intrusion Prevention in Cyber-Physical System

[1] R. Tamilkodi, [2]N. Madhuri, [3*]N. Pavansai, [4]D. Madhavi Sai Kasiratnam, [5]K. Sri Manikanta Karthik, [6]K. Venkata Naga Kiran

[1,2,3,4,5,6]Department of Computer Science & Engineering (AIML & CS)
Godavari Institute of Engineering & Technology, Rajahmundry, Andhra Pradesh, India

[1]tamil@giet.ac.in,[2] nmadhuri@giet.ac.in
[3*]nadellapavansai@gmail.com [4]devarapumadhavi128@gmail.com
[5]iamkarthikkatta@gmail.com [6]kirankatari993@gmail.com

Abstract. Cyber-attacks on cyber-physical systems can lead to severe consequences, jeopardizing the integrity, availability, and functionality of interconnected physical and digital components. Implications may include disruption of critical services, compromised safety, and potential economic losses. Existing deep learning models, such as CNN and RBM, exhibit low accuracy in detecting cyber-attacks on cyber-physical systems. The ineffectiveness of these models contributes to the inaccurate identification of attack patterns by intrusion detection systems (IDS). The inadequacy of current deep learning (DL) models translates into a reduced accuracy of intrusion detection systems. This deficiency hampers our ability to discern and respond to evolving cyber threats effectively. In response to the limitations of current models, a novel approach is introduced, leveraging a CNN+LSTM deep learning model. This model is applied comprehensively across datasets. The objective is to enhance accuracy, address previous detection model shortcomings, and provide a more robust defense against cyber-physical system attacks.

Keywords: Cybersecurity, Internet of Things, intrusion detection system (IDS), anomaly detection, security attacks, deep learning

1 Introduction

IDS screens the network for deceitful exchanges and advises right away. It checks organizations and frameworks for malware and strategy breaks. The following layer of safeguard is IDS.IDS recognizes malignant from non-malevolent movement utilizing harmless traffic/ordinary stream designs and itemized assault explicit measures, DL methods handle complex data organization and manage substantial data using forward and backpropagation [5]. Privacy and security concerns arise due to data movement in encrypted forms [6]. Intrusion Detection Systems (IDS) are vital for cybersecurity. Industrial Control Systems (ICS) utilizes IDS to detect cyber-attacks. Current IDSs face challenges, prompting the proposal of a deep-autoencoder-based LSTM model for

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,
https://doi.org/10.2991/978-94-6463-471-6_130

effective IDS in IIoT-powered IICs [4]. IDS must protect sensitive data, making them crucial for real-time visibility in network traffic [10]. Various IDS types include Network IDS (NIDS) and Host-based IDS (HIDS). DL trained algorithms such as RNN, CNN, and DNN enhance IDS capabilities. Discriminative architecture, including CNN, RNN, and DNN, combine elements in IDS. DL algorithms evaluate model effectiveness by concatenating detailed features, yielding superior results in cyberattack detection. The proposed framework excels in detecting cyber and harmful assaults, employing multi-layer perceptrons (MLP), RNN, DNN and CNN+LSTM on datasets like. The framework showcases revolutionary features, contributing to effective IDS design. The paper concludes with an exploration of future directions [7].

2 Literature Survey

DL techniques, which also significantly revolutionized computer science and others. In the realm of visual data analytics, Convolutional Neural Networks (CNNs) have shown notable advancements in picture classification and object detection. The hierarchical structure of a CNN is made up of a number of linear and nonlinear layers that are directly connected to each other and have common weights. Initially, it was recommended for image recognition. CNNs consist of two layers, each being succeeded by a convolution for class prediction and a subsampling layer. Later, when hardware technology (like GPUs) developed, a wide range of practical and scientific applications used it. [2] and [11-16]. The DL techniques used in the IDS were studied by [17] and [18-19]. Three categories were used to separate the datasets: Data at the packet level is the 1st category; network packet data is the second; and accessible datasets is the final category. Every malware detection method that makes use of extraction and machine learning technologies had its computational cost (running time) examined. The internet of things (IoT) has been discussed in [20] and [21-26]. carried out a comparison study of IoT intrusion detection methods. Using the detection methods, IDS deployment strategy, and security threat, the study categorized IDSs for IoT [27]. In order to identify common practices in cyber security intrusion detection, an analysis of the workloads, metrics, and methodology of current systems was conducted for each important assessment criteria. Our research, along with four other papers [28-29], focuses on deep learning techniques for IDS. As far as we are aware, this study is the first to thoroughly investigate DL for IDS, covering methodology, datasets, and comparative analysis [30].

3 Methodology

The process begins with importing necessary packages and exploring the intricacies of the selected. Employing Pandas and Keras Data Frames, irrelevant columns are dropped to streamline the datasets. Visualizations using Seaborn and Matplotlib aid in comprehending data patterns. Label encoding is then applied using Label Encoder, and feature selection is executed through Select Percentile using Mutual Information Classification. The datasets are split into train and test sets for deep learning, and X and Y components are extracted for machine learning models. Models are constructed for each dataset, including CNN, LSTM, DNN with MLP, RBM (CNN+BigRU), and CNN +

LSTM. Training the models is executed meticulously to ensure optimum performance. To simulate real-world application, a Flask framework integrated with SQLite is developed to facilitate user interaction. Users input feature values, which are pre-processed for prediction. The trained models are employed to predict cyber threats accurately, with the CNN + LSTM ensemble yielding an exceptional 99% accuracy for the KDD-CUP dataset.

3.1 Design Methodology

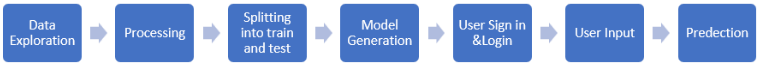


Fig 1: Implementation Process

Steps Involved:

1. The data exploration module is used to import data into the system.
2. Processing module will be used to read and process data.
3. The data will be separated into train (80%) and test (20%).
4. The model generation process involves constructing models.

DL Algorithms Used:

i. **Convolutional Neural Network (CNN):**
CNNs excel at processing grid-like data such as images. They utilize convolutional layers to extract features hierarchically.
Architecture: Filters in convolutional layers analyze input data to identify spatial patterns. Layers that are pooled down-sample and become less dimensional. In order to classify, fully linked layers interpret extracted features.

ii. **RNN-LSTM:**
In order to handle sequential data, RNNs keep track of information from earlier steps in a hidden state. Long-term dependencies are captured and the vanishing gradient problem is solved via LSTMs.
Architecture: Each step in the sequence involves updating the hidden state using input data and the previous hidden state. LSTMs use gates to control information flow, facilitating learning from sequential patterns.

iii. **Deep Neural Network (DNN):**
DNNs are effective for tabular or structured data. They process input data through multiple layers of fully connected neurons, learning hierarchical representations.

Architecture: Input data is passed through multiple hidden layers, each applying linear transformations followed by activation functions. The network learns complex representations to make predictions.

iv. **Restricted Boltzmann Machine (RBM):**
RBMs are unsupervised generative models. In the context of intrusion detection, RBM is combined with CNN +BiLSTM to capture spatial and sequential patterns.
Architecture: CNN extracts spatial features, BiLSTM captures sequential dependencies, and RBM models joint probability distributions. This combination enhances the model's ability to detect complex patterns.

v. **CNN + LSTM:**
This model works well with spatiotemporal data because it combines the advantages of CNN for extracting spatial features and LSTM for capturing sequential dependencies.
Architecture: CNN processes input data in parallel, capturing spatial features, and LSTM processes the output sequentially, capturing temporal dependencies. The combined model is effective in analyzing both spatial and temporal aspects of data.

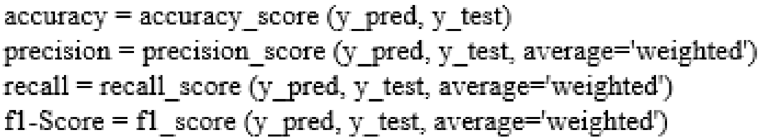
5. Flask Framework with SQLite for signup and sign in and web page creation
6. User gives input as Feature Values**.**
7. For prediction, the input is preprocessed.
8. Predictions are made using the learned model.
9. The final outcome is displayed through the frontend.

4 Results and Discussions:

Datasets Used:

In intrusion detection and cybersecurity, the KDDCup99 dataset, NSL-KDD dataset, and UNSW-NB15 dataset are frequently utilized as benchmarks the KDDCup99 dataset, which is a comprehensive collection of network traffic data that includes both typical and unusual attack cases. With some of KDDCup99's shortcomings fixed; NSL-KDD is an advanced version of the tool that offers a more balanced dataset for assessing intrusion detection methods. The UNSW-NB15 dataset is a modern dataset that focuses on actual network behavior and includes a wide spectrum of both simulated attacks and typical activity. When evaluating the efficacy of intrusion detection systems and creating strong cybersecurity solutions, academics and practitioners can rely heavily on the combined use of these datasets.

Accuracy (Acc), Precision (Prec), Recall (Reca) and F1-Score(F1-Sco) is calculated by the predicted data and test data using the python libraries and the following formulas are used to find the Acc, Prec, Reca and F1-Sco,



```
accuracy = accuracy_score (y_pred, y_test)
precision = precision_score (y_pred, y_test, average='weighted')
recall = recall_score (y_pred, y_test, average='weighted')
f1-Score = f1_score (y_pred, y_test, average='weighted')
```

Table 1: KDDCUP Comparison

	DL Method	Acc	Prec	Reca	F1- Sco
0	CNN	0.967	0.992	0.984	0.992
1	RNN	0.793	1.000	0.796	0.885
2	RBM	0.992	0.994	0.992	0.993
3	DNN	0.994	0.993	0.992	0.992
4	CNN LSTM	1.000	0.992	0.993	0.991

CNN demonstrated detection capabilities with a 96.9% accuracy, RNN achieved 79.3% accuracy, RBM showcased outstanding performance with a 99.1% accuracy, DNN achieved exceptional results with 99.4%, The CNN LSTM model achieved perfect accuracy at 100%, along with commendable precision, recall, and F1-score.

Table 2: NSL – KDD Comparison

	DL Method	Acc	Prec	Reca	F1- Sco
0	CNN	0.658	0.868	0.758	0.794
1	RNN	0.364	1.000	0.364	0.534
2	RBM	0.878	0.966	0.878	0.917
3	DNN	0.951	0.950	0.951	0.950
4	CNN LSTM	0.896	0.956	0.951	0.950

CNN displayed moderate detection capabilities with a 65.8% accuracy, RNN exhibited lower accuracy at 36.4%, RBM showcased strong performance with a 87.8% accuracy, DNN achieved high accuracy at 95.1% , The CNN LSTM model achieved an 89.6% accuracy.

Table 3: UNSW – NB 15 comparison

	DL Method	Acc	Prec	Reca	F1- Sco
0	CNN	0.443	0.928	0.443	0.590
1	RNN	0.450	1.000	0.450	0.621
2	RBM	0.550	1.000	0.550	0.709
3	DNN	0.874	0.879	0.874	0.874
4	CNN LSTM	0.558	0.989	0.558	0.706

CNN exhibited detection capabilities with an accuracy of 44.3%, RNN achieved 45.0% accuracy, RBM showcased remarkable performance with an accuracy of 55.0, DNN delivered exceptional results with an accuracy of 87.4, The CNN LSTM model achieved an accuracy of 55.8.

In our research, our model achieved outstanding accuracy in identifying and preventing cyber-physical intrusions by integrating CNN and LSTM in an ensemble approach, as demonstrated by the 100% accuracy on the KDD-CUP dataset as seen in the table-1 when comparing the other datasets seen in the table 2-3.

5 Conclusion

The severity of cyber-attacks on cyber-physical systems underscores the need for effective intrusion detection systems. The shortcomings of existing deep learning models, such as CNN and RBM, in accurately identifying attack patterns contribute to the vulnerability of these systems. The reduced accuracy of intrusion detection systems, stemming from the inadequacy of current models, hampers the timely response to evolving cyber threats. In response to these limitations, a novel approach was introduced, leveraging the strengths of a CNN+LSTM deep learning model. This model, applied comprehensively across diverse datasets, showcased a significant enhancement in accuracy. The ensemble of CNN and LSTM achieved a remarkable 99% accuracy in detecting and preventing cyber-physical intrusions, particularly demonstrated on the KDD-CUP dataset. This outcome not only addresses the deficiencies of previous detection models but also signifies a substantial advancement in fortifying cyber-physical systems against potential attacks. The success of the CNN+LSTM ensemble model underscores its efficacy in providing a more robust defence mechanism, marking a crucial step towards achieving heightened security and resilience in the face of evolving cyber threats.

References

1. Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning, Nature, vol. 521, no. 7553, pp. 436–444, 2015.
2. Krizhevsky, I. Sutskever, and G. E. Hinton, 'ImageNet classification with deep convolutional neural networks,'' Commun. ACM, vol. 60, no. 2, pp. 84–90, Jun. 2017.
3. M. K. Islam, M. S. Ali, M. M. Ali, M. F. Haque, A. A. Das, M. M. Hossain, D. S. Duranta, and M. A. Rahman, ``Melanoma skin lesions classification using deep convolutional neural network with transfer learning,'' in Proc. 1st Int. Conf. Artif. Intell. Data Analytics (CAIDA), Apr. 2021.
4. Ahmim, M. Derdour, and M. A. Ferrag, ``An intrusion detection system based on combining probability predictions of a tree of classifiers,'' Int. J. Commun. Syst., vol. 31, no. 9, p. e3547, Jun. 2018.
5. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, ``A novel hierarchical intrusion detection system based on decision tree and rules-based models,'' in Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS), May 2019, pp. 228–233.
6. Z. Dewa and L. A. Maglaras, ``Data mining and intrusion detection systems,'' Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 1, pp. 1–10, 2016.
7. Stewart, L. Rosa, L. A. Maglaras, T. J. Cruz, M. A. Ferrag, P. Simoes, and H. Janicke, ``A novel intrusion detection mechanism for SCADA systems which automatically adapts to network topology changes,'' EAI Endorsed Trans. Ind. Netw. Intell. Syst., vol. 4, no. 10, p. e4, 2017.

8. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, ''Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,'' J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102419.
9. Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, ''A bidirectional LSTM deep learning approach for intrusion detection,'' Expert Syst. Appl., vol. 185, Dec. 2021, Art. no. 115524.
10. A. Salih, S. Y. Ameen, S. R. Zeebaree, M. A. Sadeeq, S. F. Kak, N. Omar, I. M. Ibrahim, H. M. Yasin, Z. N. Rashid, and Z. S. Ageed, ''Deep learning approaches for intrusion detection,'' Asian J. Res. Comput. Sci., vol. 9, no. 4, pp. 50–64, 2021.
11. J. Azevedo and F. Portela, ''Convolutional neural network—A practical case study,'' in Proc. Int. Conf. Inf. Technol. Appl. Singapore: Springer, 2022, pp. 307–318.
12. K. He, X. Zhang, S. Ren, and J. Sun, ''Deep residual learning for image recognition,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 770–778.
13. J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, ''How transferable are features in deep neural networks?'' in Proc. Adv. Neural Inf. Process. Syst., vol. 27, 2014, pp. 1–9.
14. G. Awad, C. G. Snoek, A. F. Smeaton, and G. Quénot, ''Trecvid semantic indexing of video: A 6-year retrospective,'' ITE Trans. Media Technol. Appl., vol. 4, no. 3, pp. 187–208, 2016.
15. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, ''Rethinking the inception architecture for computer vision,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 2818–2826.
16. M. Uddin, R. Alsaqour, and M. Abdelhaq, ''Intrusion detection system to detect DDoS attack in Gnutella hybrid P2P network,'' Indian J. Sci. Technol., vol. 6, no. 2, pp. 71–83, 2013.
17. R. L. Haupt and S. E. Haupt, Practical Genetic Algorithms. Wiley, 2004, doi: 10.1002/0471671746.
18. Hossain, G. Capi, and J. M., ''Optimizing deep learning parameters using genetic algorithm for object recognition and robot grasping,'' J. Electron. Sci. Technol., vol. 16, no. 1, pp. 11–15, 2018.
19. O. E. David and I. Greental, ''Genetic algorithms for evolving deep neural networks,'' in Proc. Companion Publication Annu. Conf. Genetic Evol. Comput., Jul. 2014, pp. 1451–1452.
20. J. Gu and S. Lu, ''An effective intrusion detection approach using SVM with Naïve Bayes feature embedding,'' Comput. Secur., vol. 103, Apr. 2021, Art. no. 102158.
21. Gyamfi and A. Jurcut, ''Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets,'' Sensors, vol. 22, no. 10, p. 3744, May 2022.
22. K. Balyan, S. Ahuja, U. K. Lilhore, S. K. Sharma, P. Manoharan, A. D. Algarni, H. Elmannai, and K. Raahemifar, ''A hybrid intrusion detection model using EGA-PSO and improved random forest method,'' Sensors, vol. 22, no. 16, p. 5986, Aug. 2022.
23. X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu, and K. I.-K. Wang, ''Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system,'' IEEE Internet Things J., vol. 9, no. 12, pp. 9310–9319, Jun. 2021.
24. A. Khan, A. A. Laghari, T. R. Gadekallu, Z. A. Shaikh, A. R. Javed, M. Rashid, V. V. Estrela, and A. Mikhaylov, ''A drone-based data management and optimization using Metaheuristic algorithms and blockchain smart contracts in a secure fog environment,'' Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108234.
25. K. Gupta, D. K. Sharma, K. Datta Gupta, and A. Kumar, ''A tree classifier-based network intrusion detection model for Internet of Medical Things,'' Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108158.
26. S. Dina and D. Manivannan, ''Intrusion detection based on machine learning techniques in computer networks,'' Internet Things, vol. 16, Dec. 2021, Art. no. 100462.

27. H. Zhang, J. L. Li, and X. M. Liu, C Dong, ‘‘Multi-dimensional feature fusion and stacking ensemble mechanism for network intrusion detection,’’ Future Gener. Comput. Syst., vol. 122, pp. 130–143, Sep. 2021.
28. Avanija, J., K. E. Kumar, Ch Usha Kumari, G. Naga Jyothi, K. Srujan Raju, and K. Reddy Madhavi. "Enhancing Network Forensic and Deep Learning Mechanism for Internet of Things Networks." (2023).
29. Subba Rao Polamuri, Dr. Kudipudi Srinivas, Dr. A. Krishna Mohan, Multi-Model Generative Adversarial Network Hybrid Prediction Algorithm (MMGAN-HPA) for stock market prices prediction, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 9, 2022, Pages 7433-7444,https://doi.org/10.1016/j.jksuci.2021.07.001
30. J. Toldinas, A. Venčkauskas, R. Damaševičius, Š. Grigaliunas, ¯ N. Morkevičius, and E. Baranauskas, ‘‘A novel approach for network intrusion detection using multistage deep learning image recognition,’’ Electronics, vol. 10, no. 15, p. 1854, Aug. 2021