International Journal of Computer and Engineering Optimization (IJCEO)
Volume 02, Issue 03, May – June (2024)

RESEARCH ARTICLE

HYBRID GRAPH BASED CONVOLUTIONAL NEURAL NETWORK FOR INTRUSION DETECTION IN IOT

Vishnu Karthik Ravindran[1, *]

[1]Independent Researcher.

[*]*Corresponding e-mail: vkacharaya@gmail.com*

Abstract – Cyberattacks on critical Internet of Things (IoT) systems must be detected using Intrusion Detection Systems (IDS). It is necessary to enhance the protection of these devices from cyberattacks in order to safeguard their users. A common feature of IDSs' anomaly detection components is deep learning (DL) techniques.ML approaches have been used for many years to increase the reliability and resilience of Network Intrusion Detection Systems (NIDS). In the last few years, to identify intrusions in the Internet of Things (IOT), deep learning algorithms are employed. Intrusion is one of the major issues in IOT due to lack of security, attacks on network, accuracy etc., in the network. In order to overcome this problem, a novel Hybrid Convolutional neural network and Graph convolutional network (CNN-GCN) technique has been proposed in this work for IOT intrusion detection. The proposed CNN-GCN deals with attacks issue on network, accuracy rate and lack of security in IOT. The proposed work improves feature extraction, accuracy and attention-based classification. Performance evaluation of the suggested method will be done using the MATLAB simulator. The proposed technique performance has been assessed using specific metrics such as accuracy, classification and error detection. In comparison to the existing methods, the findings demonstrate that the proposed work exhibits 99.86% error detection in IOT.

Keywords – *Cyberattacks, Internet of Things, Convolutional neural network, Graph convolutional network.*

1. INTRODUCTION

Cybersecurity is one of the most challenging topics to study in information technology [1]. As more cutting-edge apps that depend on networked devices are developed, there has been a greater emphasis on IoT security in recent years [2]. As IoT usage increases, assaults on linked devices have grown to be a serious problem. There are several ways that IoT devices might be attacked, including privilege escalation, spying, and denial of service [3]. Therefore, it's becoming more and more vital for protecting IoT devices from these threats [4]. Furthermore, because IoT devices are physically dispersed, it is simple for unauthorized individuals to access them. Hence, IoT devices require enhanced and extremely robust intrusion detection solutions [5]. In order to swiftly analyze enormous volumes of data and enable automatic security system modifications in reaction to the identification of malware or security breaches, deep learning requires fewer processing resources [6].

Intrusion detection may be greatly aided by selecting a suitable DL method for Internet of Technology [7]. There are various benefits to the suggested work's application of deep learning techniques, including increased accuracy and reduced number of false alarms for intrusion detection [8]. By enhancing its security, it might positively affect people's life as well, the economy, technology, and the IoT ecosystem. For IOT intrusion detection, a new approach CNN-GCN is proposed using convolutional neural network and graph neural network for intrusion.

- The paper's goal is to enhance intrusion detection, by implementing CNN and GCN techniques.
- The CNN has been utilized to investigate for feature extraction and to provide an efficient dense network, The GCN has been used for attention-based classification.
- The integration of CNN and GCN improve the effectiveness of Internet of Things intrusion detection.
- Using evaluation parameters like accuracy, precision, recall, and the F1-score, the CNN-GCN was built.

The sections that follow are arranged as follows: section 2 represents the literature review, section 3 represent the proposed methodology, section 4 represent the results and discussion, section 5 represent the conclusion.

2. LITERATURE REVIEW

In 2021, Abdulaziz fatani et al. [9] proposed an AI-based approach for intrusion detection systems (IDS) in Internet of Things platforms. Convolutional neural networks (CNNs) are used to extract pertinent characteristics. To make use of DL and metaheuristic (MH) algorithm developments that have demonstrated their effectiveness in resolving challenging engineering issues. The study suggests a feature extraction technique that extracts pertinent information by utilizing convolutional neural networks (CNNs). The

accuracy of the suggested TSODE was higher than that of a number of current methods. In subsequent research, several MH optimizers will be taken into account for IDS using various datasets.

In 2022, Vijayakumar Ravi et al. [10] Introduced a method that uses deep learning to identify attacks and group them into the appropriate attack types. Fused GRU network technique is implemented in this work. The gated recurrent unit (GRU) deep learning layers' intrinsic feature representations are extracted by the model. After combining the features, the entire network was utilized to classify and detect attacks. It has been shown that the proposed feature fused GRU network performs better than the GRU model. It's feasible to enhance the improve the SDN-IoT intrusion detection system's efficiency in the future.

In 2023, Jiawei du et al. [11] Proposed a classification model (NIDS-CNNLSTM). To address the problems of previous IIoT intrusion detection algorithms' high detection rate and poor classification accuracy and detection rate, this research suggests NIDS-CNNLSTM. By experimental results, the effectiveness demonstrates a low false alarm rate, high detection rate, and classification accuracy.

In 2023, Mousa'b Mohammad shtayat et al. [12] introduced a method DL-based IDSs in IIoT networks can be made more transparent and resilient by using ensemble DL-based IDS. SHAP and LIME techniques is used to clarify the choices made by DL-based IDSs, professionals in charge of preserving IIoT network security and creating better cyber-resilient systems can get important insights. Experiments demonstrate how well ensemble learning works to enhance outcomes. Advance technique can be implemented to overcome the intrusion in network

In 2022, Kumar Saurabh et al. [13] developed a 13-feature DNN model and an LSTM Autoencoder with Deep Learning capabilities and They greatly increased accuracy on the Bot-IoT and UNSW-NB 15datasets. To find network intrusions, LBDMIDS uses an LSTM architecture. The dataset was appropriately standardized and then fed into LBDMIDS, which yielded good output and results in terms of F1-score and prediction accuracy. Prediction accuracy may be increased in the future by implementing more hybrid DL models and efficient GPUs.

In 2022, Asmaa halbouni et al. [14] proposed CNN and LSTM deep learning algorithms provide the basis of an intrusion detection system. Utilizing 647 LSTM's ability to extract temporal features and 646 CNN's ability to extract spatial properties, in our model, 645 CNN and LSTM layers were layered. The efficiency of the suggested strategy was confirmed by experimental results that demonstrated a low FAR in comparison, a high detection rate, and good accuracy. Due to the dataset's 669 unbalanced records, Future improvements could improve the performance in terms of its high FAR and 668 poor detection rates.

In 2022, Badr lahasan and Hussein samma [15] introduced a deep encoder technique to overcome intrusion in IOT. To do this, a lightweight deep autoencoder model is constructed using an effective two-layer optimizer that simultaneously selects the input features, training instances, and hidden neuron count. The suggested approach used a lightweight autoencoder model to achieve 99% anomaly detection accuracy.

3. PROPOSED METHOD

In this section a novel convolutional neural network and graph neural network (CNN-GCN) approach is proposed for intrusion detection in IOT network. The introduced work GCN goal is to increase the transmission efficiency in IOT, by implementing CNN and GCN algorithms. The CNN has been utilized to investigate for feature extraction and to provide an efficient dense network, The GCN has been used for attention-based classification. The integration of CNN and GCN technique to improve Internet of Things intrusion detection effectiveness. Figure 1 represents the flow-chart of CNN-GCN technique.

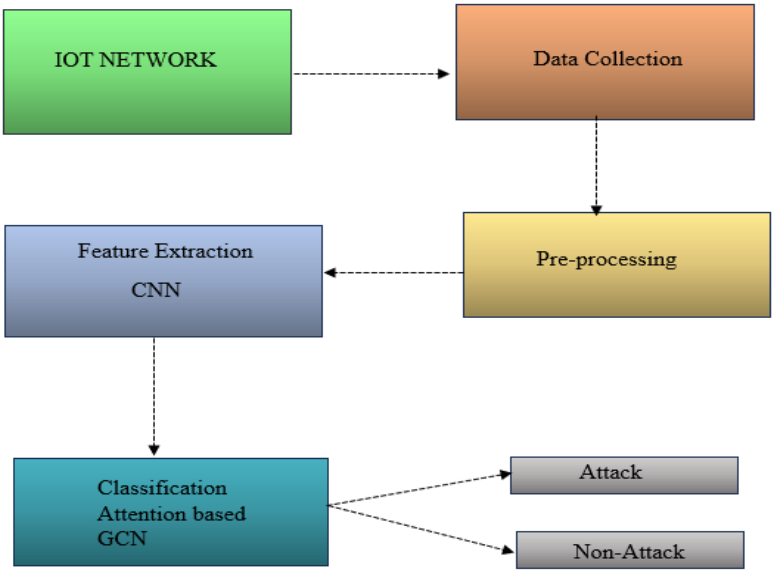

Figure 1. Block diagram of CNN-GCN technique

3.1. Pre-processing

The input data or information is given to data collection. The collected data is preprocessed by two methods such as normalization and standardization.

Normalization

A popular technique for prepping data for DL algorithms is normalization. Changing the numerical data set values in column to a standard scale. While preserving value range fluctuations is the aim of normalization. The values of the IoT Intrusion Detection dataset vary for each feature. Some features have negative values that impair the model's performance, while others have numbers in the thousands. The min-max strategy used to normalize the value between 0 and 1 in order to solve this problem.

Standardization

The z-score can be used to standardize the features of the dataset. By normalizing a dataset's feature values, it offers the capability of normalizing a standard distribution.

3.2. Convolutional neural network (CNN)

In proposed GCN technique, an effective CNN is deployed to extract the specific data from the exploited data. With their flexible designs, the CNN models are well-known feature extractors used for a range of tasks and applications. A basic CNN design consists of convolutional, activation, pooling, and fully connected layers arranged in a certain topology. From low-level features to more complicated features, the retrieved features can vary depending on the model's topological depth. When utilizing a fixed kernel, the CNN block executes a 1D convolution operation after receiving the pre-processed input dat., generating maps of activation.

Let's say that the CNN's input characteristic is the feature map of layer j, which is $Q_j(Q_0 = Y)$

$$Q_j = f(Q_{j-1} \otimes U_j + a_j) \quad (1)$$

where U_j is the j layer's convolution kernel weight vector, accordingly; Convolution is represented by the operation symbol "$\otimes$ "; The activation function is f (y), and a_j is the offset vector of the j layer. By defining various window values, the convolutional layer retrieves distinct feature information from the matrix of data Q_{j-1}, and it uses various convolution kernels to extract distinct features Q_j from the data. The same convolution kernel uses the "parameter sharing" approach in the convolution operation, Therefore, by using the same weight and offset, drastically reduces the neural network's overall number of parameters. The pooling layer typically follows the convolutional layer in sampling the feature map using various sampling techniques.

Assume that the pooling layer receives Q_j as input and outputs Q_{j-1}.

Thus, the pooling layer can be expressed as

$$Q_j = Subsampling(Q_j) \quad (2)$$

Typically, the sample criterion selects the mean or maximum value in the window region. The pooling layer's primary purpose is to reduce the dimension of redundant features so that they have less of an impact on the model.

3.3. Graph convolutional network

Among graph neural networks, the GCN is one of the most fundamental designed to operate on graphs. A graph and a collection of feature vectors, with each node linked to its corresponding feature vector, are inputs to a GCN. The feature vectors at each node are changed sequentially by a series of graph convolutional layers that make up the GCN. The GCN layers gather data from nearby nodes and incorporate it into the representation of the current node using the previously described message-passing method. Every node goes through the same process. Each GCN layer's output is used as the input data for the one after it. As a result, the layers convert the graph data into new embeddings, which are then used by the last neural network layer to handle tasks like node and graph categorization. Each layer's nodes' hidden states are composed of two successive processes: aggregation and update. The concept of "convolutional" is relevant here. The following formula can be used to update each GCN layer's hidden states:

$$K^{(m)} = \sigma(BI^{(m-1)}N^{(m-1)} + d^{(m)}) \quad (3)$$

B: represents graph adjacent matrix.

K: represents node feature matrix.

N: represents weight matrix of GCN layer.

D: represents the bias number and σ the activation function.

The information is updated at each node in the lth layer according to the connections between that node and its neighbors. It may be thought of as a node's "mask." The function of this mask is comparable to that of a CNN model's kernel. By dragging these "masks" over each vertex and executing information aggregation directly there, the graph's nodes are updated one after the other. According to the preceding formula, this aggregation is usually accomplished by multiplying two matrices, K and N. But at its foundation, it still combines data from each node's neighbors to represent the essence of "convolution."

4. RESULT AND DISCUSSION

The proposed CNN-DCN has high accuracy of intrusion detection compared to existing techniques. The collected data are pre-processed using normalization and standardization method. The pre-processed datas are given has input data to the feature extraction, then attack and non-attack in IOT is detected by using classification attention based GCN. MATLAB similar is used to evaluate the proposed CNN-GCN technique.

Figure 2 represents a graphical representation on accuracy, precision, recall, f1-score comparison of the proposed CNN-GCN technique with the existing technique. The proposed technique achieves 0.86% and 0.23% has higher accuracy than CNN-LSTM and SHAP-LIME technique respectively.

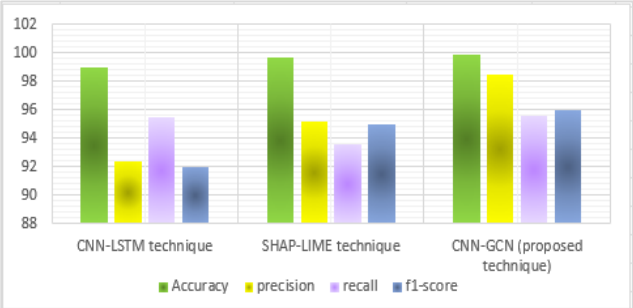

Figure 2. Performance Metric Comparison

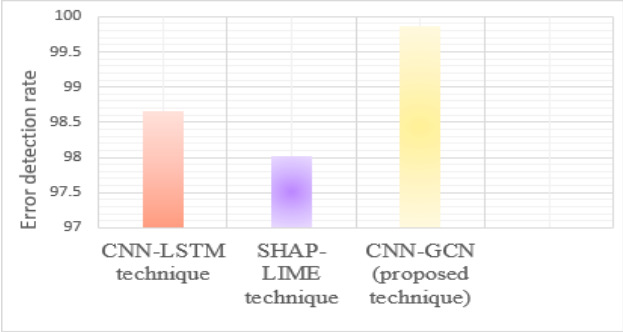

Figure 3. Error Detection Rate

Figure 3 represents a graphical representation of error detection rate, a comparison between proposed CNN-GCN technique with the existing technique. The proposed technique achieves 0.2% and 1.84% has higher error detection rate than CNN-LSTM and SHAP-LIME technique respectively.

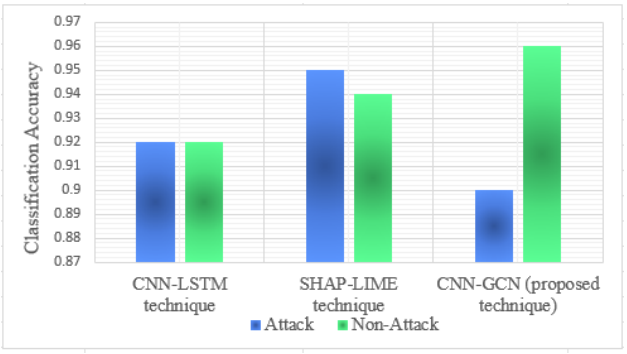

Figure 4. Classification Accuracy

Figure 4 represents a graphical representation of classification accuracy rate a comparison between proposed CNN-GCN method with the existing method. The proposed technique has high classification in non-attack and low ratio in attack classification than the existing techniques.

5. CONCLUSION

In this paper, a novel CNN-GCN Hybrid neural network for intrusion detection in IOT technique has been proposed for intrusion detection in Internet of things. The proposed CNN-GCN deals with convolutional neural network (CNN) technique for feature extraction and Graph convolutional neural network (GCN) for intrusion detection on Internet Of Things. The suggested CNN-GCN aims to enhance intrusion detection in network. Performance evaluation of the suggested strategy is done using the MATLAB simulator. The proposed technique performance has been assessed using specific metrics such as accuracy, classification and error detection. The results show, the proposed work shows 99.86% error detection in IOT and high classification ratio in non-attack and low classification ratio in attack classification than the existing techniques. In the future, complex IOT attacks may be prevented by advanced methods like autoencoders and real-time monitoring and error detection can be improved.

CONFLICTS OF INTEREST

This paper has no conflict of interest for publishing.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher, and M. Portmann, "E-graphsage: A graph neural network based intrusion detection system for iot," In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, pp. 1-9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] A. Alferaidi, K. Yadav, Y. Alharbi, N. Razmjooy, W. Viriyasitavat, K. Gulati, S. Kautish, and G. Dhiman, "Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles," *Mathematical Problems in Engineering*, vol. 2022, no. 1, pp. 3424819, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] S. Tsimenidis, T. Lagkas, and K. Rantos, Deep learning in IoT intrusion detection. *Journal of network and systems management*, vol. 30, no. 1, pp. 8, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] A. Li, and S. Yi, "[Retracted] Intelligent Intrusion Detection Method of Industrial Internet of Things Based on CNN-BiLSTM," *Security and Communication Networks*, vol. 2022, no. 1, pp. 5448647, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] H. Alkahtani, and T.H. Aldhyani, "Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications," *Security and Communication Networks*, vol. 2021, no. 1, pp. 3806459, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] K. Gayathri, N. Uma Maheswari, R. Venkatesh, and A. Appathurai, "Automatic left ventricle segmentation via edge-shape feature-based fully convolutional neural network," *International Journal of Imaging Systems and Technology*, vol. 34, no. 1, pp. e22947, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] M. Kodyš, Z. Lu, K.W. Fok, and V.L. Thing, "Intrusion detection in internet of things using convolutional neural networks," In *2021 18th International Conference on Privacy, Security and Trust (PST)*, pp. 1-10, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] T. A. B. Raj, C. Pushpalatha, and A. Ahilan, "An optimized profound memory-affiliated de-noising of aerial images through deep neural network for disaster management," *Signal, Image and Video Processing*, vol. 17, no. 8, pp. 3983-3991, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] A. Fatani, M. Abd Elaziz, A. Dahou, M.A. Al-Qaness, and S. Lu, "IoT intrusion detection system using deep learning and enhanced transient search optimization," *IEEE Access*, vol. 9, pp. 123448-123464, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] V. Ravi, R. Chaganti, and M. Alazab, "Deep learning feature fusion approach for an intrusion detection system in SDN-based IoT networks," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 24-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] J. Du, K. Yang, Y. Hu, and L. Jiang, "NIDS-CNNLSTM: Network intrusion detection classification model based on deep learning," *IEEE Access*, vol. 11, pp. 24808-24821, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] M.S. Mousa'B, M.K. Hasan, R. Sulaiman, S. Islam, and A.U.R. Khan, "An explainable ensemble deep learning approach for intrusion detection in industrial Internet of Things," *IEEE Access*, vol. 11, pp. 115047-115061, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] K. Saurabh, S. Sood, P.A. Kumar, U. Singh, R. Vyas, O.P. Vyas, and R. Khondoker, "Lbdmids: LSTM based deep learning model for intrusion detection systems for IOT networks," In *2022 IEEE World AI IoT Congress (AIIoT)*, pp. 753-759, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] 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. [CrossRef] [Google Scholar] [Publisher Link]

[15] B. Lahasan, and H. Samma, "Optimized deep autoencoder model for internet things intruder detection," *IEEE Access*, vol. 10, pp. 8434-8448, 2022. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Vishnu Karthik Ravindran earned his Bachelor of Engineering in Computer Science and Engineering from Sri Ramakrishna Institute of Technology, India, in 2008. He later pursued a Master of Science in Computer Science at Syracuse University, New York, USA. Currently, he is a Software Engineer at a leading cloud-based company and actively contributes to open-source projects.

Arrived: 17.05.2024
Accepted: 19.06.2024