AGLCNet: A Novel Attention-Driven GLC Framework for Enhancing IoT Cybersecurity

R. Nandhini[1] and D. Pradeep[2]
[1]Department of Computer Science and Engineering, K.Ramakrishnan College of Engineering, Trichy, Tamil Nadu, India
[2]Department of Computer Science and Engineering, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India

Keywords: Graph based Neural Network, Convolution Neural Network, Cyber Attack. Cyber Security, Internet of Things.

Abstract: With the Internet of Things expanding, inter-device security is a sensitive issue owing due to the rising number and sophistication of cyberattacks aimed at the IoT networks. In this paper, novel attention-driven GLC model is proposed to enhance detection of cyberattacks on the IoT environment. The model employs Graph Neural Networks (GNN) to model spatial dependency between devices, Long Short-Term Memory (LSTM) networks for temporal dynamics of the network traffic and Convolutional Neural Networks (CNN) for high level feature extraction. Furthermore, an attention mechanism is added to the architecture to focus on relevant features and device interactions needed to optimally improve the performance of the detection. The model was validated on IoT security benchmark dataset UNSW-NB-15 and outperformed traditional models in terms of accuracy, precision, recall and F1 score. These findings support the model's ability to provide effective and efficient cyber security for Internet of Things infrastructure. While the model performs well, certain gaps exist in streamlining the computational complexity to enable efficient execution in real-time for low-power IoT devices. Future work will revolve around optimizing the model as well as conducting more experiments on large-scale real-world IoT datasets to evaluate the model's usability and performance in real-world situations.

1 INTRODUCTION

With an exponential growth of Internet of Things, it is expected around billions of interconnected devices in the next few years. These devices generated vast amount of sensitive data which makes them vulnerable to various cyber attack such as DDoS (Distributed Denial of Service), man in the middle attack. (J. H. Lee et al. 2017) Data breeches and malware. This will lead to inadequate computational and storage capabilities as IoT ecosystem grows. With the rapid advancement of technology, IoT has a great impact in the future (F. Panagiotis et al. 2021). However, this rapid growth has made security paramount concern in networked, independent systems. Hackers, viruses and other malicious software pose a serious threat to the integrity and reliability of data. Data insecurity presents a substantial threat to the entire IoT infrastructure, potentially leading to serious risks. Consequently, there is a growing demand for robust IoT security solutions. (M.A. Ferrag et al. 2020) With the rise in the number of connected devices and new threats, the need to gather and manage the data to protect these devices has become more pressing. This has raised the goal of IoT security to a paramount level. These security measures have mostly been about the adoption of systemic security architectures alongside the use of cryptography. Nevertheless, there are a number of reasons why attacks on networks should be taken seriously. They include the denial of several IoT services through request flooding or the abuse of some services by unauthorized persons. (K.A. Da Costa et al. 2019)

In order to overcome these obstacles, the deployment of an intrusion detection system (IDS) is highly important for detecting hostile interventions for the security and availability of the IoT network. Unfortunately, this can be an issue because of the constraints on technology and power by IoT devices that makes it impractical for them to use sophisticated IDS. An IDS comprises of a configuration that has proximity to the desktop's screen that guarantees the overall monitoring of the vitality and the maneuvers of the network in order to direct a signal to the managers when anomalous activity, or actions that are deemed intrusive are founded (N. Chaabouni et al. 2019). However, most of these systems were created

Nandhini, R. and Pradeep, D.
AGLCNet: A Novel Attention-Driven GLC Framework for Enhancing IoT Cybersecurity.
DOI: 10.5220/0013927200004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 5*, pages 294-300
ISBN: 978-989-758-777-1

for managing the internet alone, but the tidal nature of IoT data volumes and erratic event stream order does not compromise such intrusion detection systems (S. Hajiheidari et al. 2019).

Conventional cyber security methods are insufficient because of decentralized, heterogeneous, and resource-constrained nature of IoT system. Consequently, a cutting edge technology such as deep learning (DL) becomes a viable solution for real-time threat detection and mitigation (J.Asharf et al. 2020). Deep learning can process huge number of datasets to identify potential complex patterns which are making it an effective tool for anomaly detection and the prediction of cyberattacks in IoT environments. (Z. Ahmad et al. 2021).

This paper focuses on utilizing advanced deep learning techniques to enhance the security of IoT networks. This paper also investigates how deep learning algorithms can be used to detect and mitigate various types of attacks while addressing the unique constraints of IoT devices, such as limited computing power, low memory, and network bandwidth limitations. Figure 1 illustrates the General Scenario of Intrusion Attack.

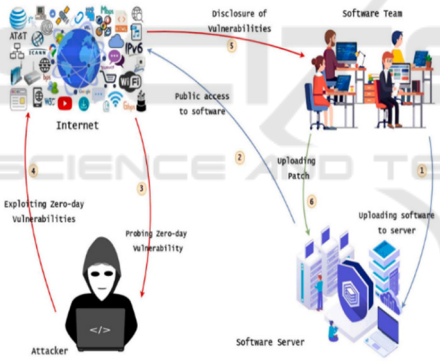

Figure 1: General Scenario of Intrusion Attack.

2 RELATED WORKS

There has been a lot of work done in the direction of employing ML techniques towards enhancing security in the IoT ecosystem. General ML algorithms such as SVM, decision trees, and random forests have been utilized for anomaly detection in IoT networks. But these methods usually do not cope well with massive high-dimensional data streams that are prevalent in an IoT setting. Most recently, deep learning models of the family of models consisting of CNN, LSTM, and RNN file for example showed better results for the applications in cybersecurity.

Alzaqebah et al. (2022) proposed the use of the bio-inspired Grey Wolf Optimization (GWO) technique to overcome such drawbacks by increasing IDS detection rates for both the malicious and normal traffic. The primary enhancement proposed in their work is related to the smart initialization step which consists of both the wrapper and filter strategies to select the most important features at the initial stage of the modeling process. Moreover, they proposed an optimization by adapting GWO to adjust the parameters involved in the high-speed classification mode referred to as Extreme Learning Machine (ELM). For performance, they obtained an accuracy of 81%, F1-score of 78%, and G-mean of 84% when working with the UNSWNB-15 dataset. The downside to this method is high crossover error rate which was only minimized to below 30% for the experiments performed hence it is less suitable for complex attacks.

K.Geetha, et.al (2022) suggested one strategy to safeguard the different connected IoT devices in healthcare system from botlet attacks, this strategy involve constant scrutiny of the traffic patterns in the system and categorization of traffic into normal and malicious. The approach employs the BiLSTM model in IoT traffic analysis, and the IoT-23 dataset is used in the evaluation of the model. To evaluate the performance, a new parameter of attack prediction accuracy was incorporated which reaches the maximum of 84.8% for separation of normal and attack conditions. However, the method has a drawback as it is not accurate always, especially when it comes to more complex and dynamic scenarios compared to the ControlFlow benchmarks used in the paper are not representative of real attacks.

Khatun and Chowdhury (2019) discussed the use of deep learning technique by implementing an Artificial Neural Network towards handling wide range of IoT data. It also proves their method of distinguishing between normal and suspicious IoT traffic and a way of handling suspicious nodes. Their prediction accuracies were 77.51%, and they acknowledged that they would be higher if they include other deep learning methods in a mix model. The main weakness is a quite low accuracy compared to other models that can be a problem in highly connected IoT environments.

Al-Obaidi et al., (2023) have made a comparison on different and distinct machine learning models utilizing the UNSW-NB15 dataset, of which the Voting model was established to have a 99.0% accuracy for a binary classification. On multiclass classification, the accuracy was slightly lower at 82 percent. The authors has implemented a Hybrid

Autoencoder (AE) with Generative Adversarial Network (GAN) on a private database of 1.6 million records for 8 features with 98.24% accuracy and 95% recall rates. One major limitation in both studies is the restricted feature selection which can be problematic for increased or varied data sets.

Koroniotis and Moustafa (2022) proposed the INSAT-DLNF model, which they developed to detect of identify and trace unusual proceedings within smart satellite networks by utilising LSTM-RNN and GRU. They benchmarked their model against five supervised and two unsupervised learning paradigms to prove that the hybrid deep learning solutions can identify cyber attacks including zero-day vulnerabilities and are more flexible and powerful than traditional post-incident forensics. Nevertheless, the qualitative development of the model might attract high computational cost, which will not be ideal for real-time or compact computations.

M.S. Alzahrani et.al (M.S. Alzahrani et al.) employed different machine learning and deep learning techniques to analyze data packets as either normal or containing an attack based on a signature database. They used a correlation analysis approach to define important network features associated with different classes and chose nine such features for their models. The textual categories were converted into numerical attributes by applying the one-shot encoding and the effectiveness of the system was checked with reference to the KDD Cup benchmark data. The packet classification methods used this paper implemented binary and multiclass classifications and performance quantification was done statistically. One limitation of the study is that there are few features employed in modeling, which can limit the model from capturing multivariate attack patterns.

Malik and Singh (2022), pointed out a problem with the current methods in detection since the threats are often new and hence the identification of new threats turns out to be a daunting task when using the existing methods. In response they put forward the Deep Belief Network (DBN)-based intrusion detection engine to detect such attacks. The DBN classifier was compared against a sample of TON-IOT dataset containing the weather data and successfully rated higher than more effective previous approaches averaging at 86.3%.

However, that is the disadvantage because while the method raised the accuracy of such detection, they may still lack to cope with highly changing environments or other more complex and novel zero-day attacks.

3 PROPOSED METHODOLOGY

The proposed methodology aims to enhance cyber-attack detection in IoT networks by integrating GNN (Graph Neural Network), LSTM (Long Short-Term Memory) and CNN (Convolution Neural Network) along with attention mechanism (**AGLCNet**). An attention mechanism is used for score computing, besides GNN and LSTM-CNN hybrid architectures. This method combines the strength of the different techniques in enhancing the account of detection and flexibility to new threats.

3.1 System Architecture

3.1.1 Data Collections

Information and communication data from the different IoT devices will be obtained, such as traffic logs, device records and communication behavior of the connected IoT devices. It will also involve the use of open datasets with a view of training and evaluating the models with reference to UNSW-NB-15 datasets.

3.1.2 Data Preprocessing

During the preprocessing step data cleaning and normalization are performed to reduce noise and variability in input data.

It provides the information that must be used in decision making and analyzed to confirm its reliability. Also, some features will be selected for better differentiativeness between normal activities and malicious ones.

After that, the features are going to be defined, and the dataset will be preprocessed to transform it to a format suitable for both graph representation and time series so that the processing and the performance of the model can be improved.

3.1.3 Graph Construction

During graph construction, a graph is built and each node is an IoT device, and the communication relationship between the devices is represented by the edges shown in the graph. This structural framework enables an enhanced representation of the IoT network. The parameters that characterize the edges can include frequency of contact, amounts of traffic, and type of communication. For eg, Supposing the general set of IoT devices is represented by V then $V = \{v_1, v_2, \ldots, v_n\}$.

Then the communication links can be represented as a set of edges E. Each edge (v_i, v_j) can be assigned a weight w_{ij} based on the connection frequency or data volume, which can be mathematically expressed as:

$$w_{ij}=\alpha\cdot\text{Connection Frequency}_{ij}+\beta\cdot\text{Data Volume}_{ij}+\gamma\cdot\text{CommunicationType}_{ij} \quad (1)$$

where, α, β, γ are constants that represent the degree of influence of each attribute to the formation of an edge.

3.1.4 Graph Representation

Another peculiarity on constructing a graph is that in order to allow GNN processing on the graph, the constructed graph must be represented in a certain format. This involves creating two key matrices: The basic input we have are the adjacency matrix A and the feature matrix X.

3.1.5 Adjacency Matrix A

The matrix A is the one carrying information on connectivity of the nodes where an entry aij stands for the value of the edge connecting a node. vi and node vj. If there is no relation, that is aij will be 0. Combined, it mathematically can be expressed as

$$A_{ij}=\begin{cases} w_{ij}, & if(v_i,v_j)\in E \\ 0, & otherwise \end{cases} \quad (2)$$

3.1.6 Feature Matrix X

The feature matrix X encodes the attributes of the nodes, and each row represents a node, while each feature column can be such as device type, time last communicated, etc. If there are m features, the feature matrix can be represented as:

$$X=\begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1m} \\ f_{21} & f_{22} & \cdots & f_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ f_{n1} & f_{n2} & \cdots & f_{mn} \end{bmatrix} \quad (3)$$

Where f_{ij} represents the j^{th} feature of the i^{th} IoT device.

By constructing these matrices, the graph structure becomes suitable for processing within a GNN framework, enabling effective learning and inference for cyber-attack detection in IoT networks.

3.1.7 Attention Mechanism Integration

To enhance the effectiveness of the Graph Neural Network (GNN), an attention mechanism is integrated into the architecture to assign weights to nodes based on their significance within the network. This attention layer enables the model to focus on critical IoT devices and communication patterns that are more likely to indicate malicious activity. By computing attention weights, the model can dynamically adjust its focus, thereby improving its ability to detect threats.

3.1.8 Attention Weight Calculation

The attention weights are calculated using a dot-product attention mechanism. For a given node vi, the attention score eij for node vj can be computed as follows:

$$e_{ij}=\text{LeakyReLU}\left(a^T\left[Wh_i\middle\|Wh_j\right]\right) \quad (4)$$

where hi and hj are the feature representations of nodes vi and vj respectively, W is a weight matrix, and a is a learnable parameter vector. The attention weights αij are then computed using the softmax function.

$$\alpha_{ij}=\frac{\exp(e_{ij})}{\sum_{k\in N(i)}\exp(e_{ik})} \quad (5)$$

Here, $N(i)$ represents the neighbors of node vi. This process allows the model to learn the importance of each node in relation to the overall task of attack detection, emphasizing those nodes that contribute more significantly to the risk assessment.

3.1.9 Hybrid LSTM-CNN Model

The LSTM (Long Short-Term Memory) layer processes sequential data to capture temporal dependencies in network traffic. This layer is designed to remember patterns over time, making it particularly effective for detecting anomalies in the sequence of data packets. The output ht at time step t can be computed using the LSTM equations.

Forget Gate:

$$i_t=\sigma(W_i\cdot[h_{t-1},x_t]+b_i) \quad (6)$$

Input Gate:

$$f_t=\sigma\left(W_f\cdot[h_{t-1},x_t]+b_f\right) \quad (7)$$

Candidate Memory Cell:

$$\tilde{C} = \tanh(W_c \cdot [h_{t-1}, x_t] + b_c) \quad (8)$$

where σ is the sigmoid activation function, W and b represent weight matrices and biases, and xt is the input at time step t.

In parallel, a CNN (Convolutional Neural Network) layer is integrated to extract spatial features from the time-series data. This layer detects local patterns within the data that may indicate an attack. The convolution operation can be expressed as:

$$Z_{ij} = \sum_{m=1}^{M} \sum_{n=1}^{N} K_{m,n} \cdot X_{i+m-1,j+n-1} \quad (9)$$

where Z is the output feature map, K is the filter (kernel), and X is the input data. Pooling layers can subsequently be applied to reduce dimensionality and focus on the most salient features.

Finally, the outputs from both the LSTM and CNN layers are concatenated to create a comprehensive feature representation that encompasses both temporal and spatial information. This fusion can be represented as:

$$F = \text{Concat}(h_t, Z) \quad (10)$$

where F is the fused feature vector, ht is the output from the LSTM layer, and Z is the output from the CNN layer. This enriched feature set provides the model with a more holistic view of the network, significantly enhancing its capacity to detect cyber attack

4 RESULTS AND DISCUSSION

The UNSW-NB-15 network intrusion detection datasets are being used for experimental purpose. This dataset consists of 9 various attack classes along with normal class which has around 25, 40,044 instances and 49 features including both numerical and categorical attributes. The data is captured from different IoT devices within the network.

4.1 Performance Evaluation

The proposed AGLCNet Model is evaluated using performance metrics such as accuracy, precision, recall and F1 score. The proposed AGLCNet model outperforms traditional models like Auto encoder (AE), LSTM (Long short term mermory), CNN (Convolution Neural Network) and MLP (Multilayer perceptron). The integration of an attention mechanism enhances the ability of the proposed model to concentrate on the most relevant features, which helps to differentiate benign and malicious traffic more effectively and accurately. Traditional model using CNN or LSTM architectures alone achieve low precision-recall score because of their limited ability to capture complex interdependencies among network features. The proposed model achieved high accuracy of 98.75% which is far better than the traditional models. The performance results of proposed model on UNSW-NB-15 datasets are illustrated in Table 1.

Table 1: Proposed Model results on UNSW-NB-15 dataset.

Metrics	Score
Accuracy	98.75
Precision	97.83
Recall	98.92
F1 Score	98.35

The attention mechanism embedded within the model was a valuable addition in enhancing the detection ability as it allowed the model to give priority to certain patterns in the network traffic. This mechanism formatively adjusts the weightage of different features and nodes thus allowing the model to concentrate on the most important areas of a given network graph. For instance, DDoS or Fuzzer attacks would render some links between network devices to be very useful but the attention mechanism embedded in the model allows such linkages to be crowned.

This attention-based approach is especially important because it allows and aids the detection of unusual patterns that would not be captured through CNN or GNN's architectures, thus improving the overall detection strategy.

One common problem with UNSW-NB15 dataset is that of class imbalance, where certain classes of attack such as Generic, Fuzzers, have higher ratio than Backdoor, Worms. Nonetheless the attention based GNN-LSTM-CNN (AGLCNet) model was able to address these balance perturbations as the attention mechanism allowed users to overweight sparse attack patterns resulting in improved recall for all attack types.

The F1 score remains high enough even for the imbalanced situations and continues to generalize across different attack types, making it difficult for the model to become asymmetric towards attacks that are more frequently occurring classes.

Table 2: Performance Evaluation of existing results over UNSW-NB-15 dataset.

Model	Accuracy	Precision	Recall	F1 Score
AE	91.38	91.59	93.84	92.70
CNN	92.30	90.52	91.82	91.15
LSTM	95.97	94.13	96.74	95.41
MLP	93.51	92.88	96.57	94.69
Proposed AGLCNet	98.75	97.83	98.92	98.35

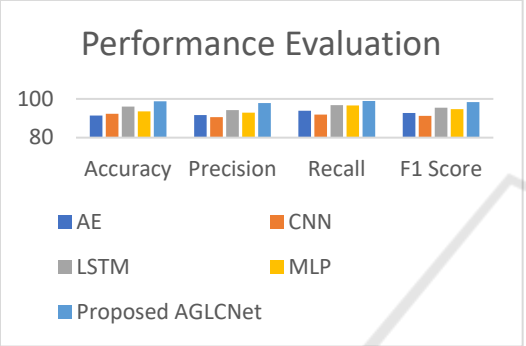

Figure 2: Performance Evaluation over UNSW-NB-15 datasets.

The Table 2 shows the performance comparison of proposed model with traditional models on UNSW-NB-15 datasets. The Figure 2 show the visual representation of performance evaluation.

5 CONCLUSIONS AND FUTURE ENHANCEMENT

In this paper, a new attention-based GNN-LSTM-CNN hybrid model (AGLCNet) for the detection of cyberattacks in IoT networks was developed. The model incorporates the strengths of each of these architectures such as Graph Neural Networks (GNNs) which model the spatial relationships among IoT devices, Long Short-Term Memory networks (LSTMs) which allow capturing of temporal trends in the data and Convolutional Neural Networks (CNNs) which structure the feature extraction. Through the integration of an attention mechanism, the model allocates resources to the most important features and relationships, therefore improving its performance in detecting different kinds of cyber threats. The proposed model achieved better accuracy, precision, recall, and F1 score metrics on the standard datasets UNSW-NB-15. These findings demonstrate the effectiveness of the model towards accurately separating the benign and the malicious traffic in heterogeneous IoT settings.

While the results are quite solid, the model still struggles with certain attack types, especially those which are more sophisticated, or those which occur infrequently within the dataset. For instance, rare attacks such as Worms produced slightly lower recall scores with regard to that technique because of their sparsity within the training set. Future work might investigate the possibility of aggression towards such rare classes of the model, with the use of techniques such as data augmentation or synthetic minority over-sampling SMOTE.

In addition, future studies could work towards the improvement of GNN in order to enable real-time application of the model when deployed in large networks, as this complexity would be a challenge in resource constrained environments.

REFERENCES

J.H.Lee, H. Kim, Security and Privacy challenges in the internet of things [security and privacy matters], *IEEE consumer electronics magazine* 6(3) (2017) 134-136

F. Panagiotis, K. Taxiarxchis, K. Georgios, L. Maglaras, M.A. Farrag, Intrusion Detection in critical infrastructures: a literature review. *Smart Cities* 4(3) (2021) 1146-1157

M.A. Ferrag, L. Maglaras, S. Moschoyiannnis, H. Janicke Deep Learning for cyber security intrusion detection: approaches, datasets and comparative study, *J. Inf. Secur. Appl*. 50 (2020), 102419.

K.A. Da Costa, J.P. Papa, C.O. Lisboa, R. Munoz, and V.H.C. de Albuquerque Internet of Things: a survey on machine learning-based intrusion detection approaches, *Comput. Network*. 151 (2019), 147-157.

N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, P. Faruki, Network Intrusion Detection for IoT security based on learning techniques, *IEEE Commuications Surveys & Tutorials* 21(3) (2019) 2671-2701.

S. Hajiheidari, K. Wakil, M. Badri, N.J. Navimipour, Intrusion detection systems in the internet of things: a comprehensive investigation, *Comput. Network*. 160 (2019) 165-191.

J.Asharf. N. Moustafa, H. Khurshid, E. Debie, W. Haider, A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions, *Electronics* 9(7) (2020) 1177.

Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, F. Ahmad Network Intrusion Detection System: a systematic study of machine learning and deep learning approaches, *Transactions on Emerging Telecommunications Technologies* 32(1) (2021) e4150.

Alzaqebah, Abdullah & Aljarah, Ibrahim & Al-Kadi, Omar & Damaševičius, Robertas. (2022). A Modified Grey Wolf Optimization Algorithm for an Intrusion Detection System.*Mathematics*. 10.10.3390/math10060999.

K.Geetha, S. Brahmananda, Network traffic analysis through deep learning for detection of an army of bots in health IoT network, *Int.J. Pervasive Comput. Commun.* (2022)

M. Khatun, N. Chowdhary, M.N. Uddin, Malicious nodes detection based on artificial neural network in IoT environments. in: *Proceedings of the Twenty Second International Conference on Computer and Information Technology (ICCIT)*, IEEE 2019.

A.AI-Obaidi, A. Ibrahim, A.M. Khaleel, The Effectiveness of Deploying Machine Learning Techniques in Information Security to Detect Nine Attacks: UNSW-NB15 Dataset as A Case Study (2023)

N. Koronotis, N. Moustafa, J. Slay A New Intelligent Satellite Deep Learning Network Forensic Framework for smart satellite networks, *Comput.Electr. Eng.* 99 (2022) 107745

M.S. Alzahrani, F.W. Alsaade, Computational Intelligence approaches in developing cyberattack detection system, *Comput. Intell. Neurosci.* 2022 (2022)

R. Malik, et.al An improved deep belief network IDS on IoT-based network for traffic systems. *J. Adv. Transp.* 2022 (2022).