GENERATIVE ADVERSARIAL RECURRENT NEURAL NETWORK SCHEME BASED INTRUSION DETECTION SYSTEM FOR THREE-DIMENSIONAL WIRELESS SENSOR NETWORK

DIVYA.S.S Research Scholar, Department of Computer Science, Mother Teresa University, Kodaikanal, Tamilnadu, India, Email id: divya2ss@gmail.com
DR.B.ASHADEVI Assistant professor, Department of Computer Science, M.V Muthiah Government Arts College for Women, Dindigul, Tamilnadu, India. (Affiliated to, Mother Teresa University, Kodaikanal.) Email id: asharajish2005@gmail.com

Abstract

Intrusion Detection System (IDS) is an important component in the overall network and data security. With the rapid advancement in network technologies, detection of attacks based on the analysis of contextual information may be specific to individual applications and networks. A malicious node can behave abnormally in various ways like holding the data incoming the route by itself, it forward the incoming data to another abnormal route, a node receives the data by using other ID as Sybil node etc. These activities create leads data loss, data misuse, data corruption, utilizing the network resources without network permission, destroy the network resources etc. The existing IDSs cannot resolve flow distribution imbalances where provide a low resulting in poor IDS detection performance and false alarm rates are increasing, especially due to low frequency attacks. To address this problem, the proposed new model uses a Generative Adversarial Recurrent Neural Network (GARNN) with an attack prevention system to handle traffic and malicious user detection visualized in 3Dimension WSN. These attacks are detected using IDS obtained by a deep learning model using KDD CUP99 set trained data. Then collected dataset trained into pre-processing for reducing noise, check null values. After that, traffic analysis for identifying the suspicious activity trained into impacts of features scaling analysis selects the best features of attack detection such as network impact ratio, Adversary Behavior, scaling transmission. Finally, the proposed GARNN algorithm is used to classify and 3D visual representation to reflect the attacks in WSN.The prevention system can help to block the malicious users and provide a security. The network activities are monitor store on event recording for analysis the traffic. The attack prevention method tracks the packet capture activity, network behaviors form buffer content. When the attack classifier form deep learning model the prevention system execute network protocol analysis for other network route. In this overall process for improve the attack detection accuracy and network prevention.

Keywords: Intrusion Detection System (IDS), attack identification, Generative Adversarial recurrent neural network (GARNN), 3Dimension, Wireless sensor network.

1. Introduction

As the Internet has grown in popularity and development, it has become increasingly relevant to people's lives. However, the Internet is a double-edged sword, and although it is convenient, it also has many problems. Among countless issues, network security is the primary issue. The number of network intrusions is increasing in Wireless Sensor Network (WSN), and the losses caused are great, especially the consumption of server resources by the intrusions.3D deployment represents an essential role in establishing an efficient WSN. Three-Dimensional (3D) WSNs are at the forefront of many advanced industrial applications.3D WSN also requires a very complex and computationally intensive analysis of insect coverage of sensor nodes placed in the 3D field.

IDS are playing an important role in development as computer and network attacks increase. IDS monitor's intrusion patterns by analyzing events that occur in computer systems or networks.A network Intrusion Detection (ID) system is used to detect malicious or unwanted intrusion in the

network. Network IDS is typically used to classify network traffic to protect computer systems from various network intrusions. Intrusion is described as an attempt to break the information system security services.

The ability of IDS to detect unknown attacks has led to increase in anomaly detection. The pre-processing phase removes irrelevant functionality in the dataset, reducing functionality for building high-performance models. On the other hand, the classification phase reduces the functionality of the basic classifiers to predict attack categories. In this paper, presents GARNN algorithm detects intrusion and detection in all directions using 3D in WSN environment. The proposed Generative Adversarial Recurrent Neural Network (GARNN) system identifies malicious user detection reflects the 3D visual representation to reflect the attacks in WSN. This paper aim is to improve the detection rate in IDS and reduce the false alarm rate.

The remaining of this paper chapter 2 contains the related wok, chapter 3 describes proposed methodology of IDS detection, chapter 4 defines the proposed implementation result analysis and finally chapter 5 defines the conclusion.

2. Related Work

N. K. Mittal et al. (2016),the author investigate Wireless Sensor Networks (WSN) have proven to be one of the most promising technologies, with applications going from complex military systems to common housing systems. WSNs are easy to deploy and inexpensive to install, but they have some security issues.IDS has become an effective solution for addressing multiple security vulnerabilities. These IDSs can be used in residential or workplace areas where WSNs are used.Butun et al. (2014), therefore, to operate the WSN securely, detect all types of intrusions before an attacker can loss the network (i.e., sensor nodes) or information destinations (i.e., data receivers or base stations).

Warzyński et al. (2018), Anomaly-based ID in a network refers to the problem of outcome atypical events that do not match the normal patterns expected in observed network traffic.Assume that all atypical/unusual things are dangerous and may be associated with a particular security incident. Many security systems use sorting or clustering algorithms to detect anomalies.

I. Ullah et al. (2021), the author introduces the Convolutional Neural Network (CNN) algorithm to identify intrusion and detection in 3D using the IoT-23 ID dataset. In that method is the inefficient process to detect the IDS.

Duttet al. (2020), the authors present the Statistical modeling based Anomaly Detection (SMAD) for IDS detection using standard datasets are KDDcup99 and UNSW-NB15.It acts as an innate immune system interface, capturing early network traffic and finding direct vulnerabilities. However in that method didn’t work proper results.

ID has been a common research area for many years, and several IDS have been recommended in cyber-physical and Industrial Control Systems(ICS).A. Khan et al. (2019),the author uses a Supervisory Control and Data Acquisition (SCADA) method for a hybrid model that takes advantage of the expected consistent nature of the communication patterns between terrestrial equipment in the ICS configuration.

W. Zhonget al. (2020), the author presents Big Data-based Hierarchical Deep Learning System (BDHDLS) uses behavioral and content characteristics to understand the characteristics and load of network traffic.Each deep learning model in BDHDLS focuses on learning the unique data distribution within the cluster.S. Amaranet al. (2021), the author introduces Optimal Support Vector Machine (OSVM) is used for IDSin WSN.

K. Lin et al. (2016), carries out Software-defined radio (SDR), and Markov prediction (MP) was used to predict the ID and increase the performance in all directions. That study takes much more time and doesn't provide proper results.

S. Otoumet al. (2019),Deep Learning (DL) based Restricted Boltzmann Machine-Based Clustered IDS (RBMBC-IDS) used for monitoring IDSin WSN.IDS is widely used in WSNs to protect against internal attacks by implementing the appropriate trust-based mechanisms.W. Meng et al. (2018),Bayesian-based trust management and traffic sampling are used for wireless intrusion detection under a hierarchy.

Z. Sun et al. (2018), Modify the V-detector algorithm by taking advantage of the cooperative advantages of base stations, detector nodes, and regular nodes, considering their different capabilities, and modifying the detector generation rules to optimize the detector.

R. Vinayakumar et al. (2019), Deep Neural Networks (DNNs) are deep learning models designed to develop flexible and effective IDSs for detecting and categorizing unexpected and unpredictable cyber-attacks.Due to the constant changes in network behavior and the rapid evolution of attacks, it is necessary to evaluate the integration of various data generated in static and dynamic methods over the years.However, malicious attacks are constantly changing, are so numerous, and require scalable solutions that pose many challenges.

H. Moosaviet al. (2014), the author to summarize this issue, assume that the player does not fully understand the game data and uses robust optimization techniques to resolve this data uncertainty.To evaluate the effectiveness of the framework, have generated an example of a game model developed.Equilibrium analysis reveals how the conflicting goals of intruder and intrusion detection systems force different conservative positions on data uncertainty.

V. T. Alaparthyet al. (2018), Efforts are being made to ensure the security of WSNs using a theoretical immune technique called Danger theory. In short, a multi-level IDS was designed based on the capabilities of various immune cells.It is achieved by monitoring WSN parameters (energy, amount of data, frequency of data transmission, etc.) and developing outputs based on their weights and concentrations.

F. Raza et al. (2015), the author studied the effect of different node densities on a non-uniform network of uniform Gaussian distribution on calculating detection probabilities under the K-sensing model.K. Ramasamy et al. (2021), the author explore a hashing distance computation (HDC) and reading-based dual validation (RbDV) algorithm to identify the IDS and suspicious node in 3D reconfigurable.

MamounAlazabet al. (2014), the author uses the hybrid wrapper filter model for malware feature selection. It combines the maximum correlation filter heuristic and the Artificial Neural Net Input Gain Measurement Approximation (ANNIGMA) wrapper heuristic method. However, that method is a challenging task didn't provide proper solutions.

3. Proposed Methodology

This paper proposes new model of GARNN framework for IDS detecting malicious users and attacks detection reflects based on 3D in WSN environment. To proposed implement the attack detection and prevention system to improve the performance of attack identification. In this proposed model Generative Adversarial Recurrent Neural Network (GARNN) with attack prevention system handle the traffic and malicious user detection. These attacks are detected using IDS obtained by a deep learning model using KDD CUP99 set trained data.

Figure 1 defines the framework of proposed for identifying the malicious users and attacks. In this proposed algorithm, the first step input the KDDCup99 dataset is preprocessed. The pre-processing is done to remove noise, irrelevant data and identifying the missing values. Then pre-processed data is trained into GARNN for detecting malicious users and attacks reflects in 3D virtualization. The GARNN algorithm is to produce the best accuracy performance results.

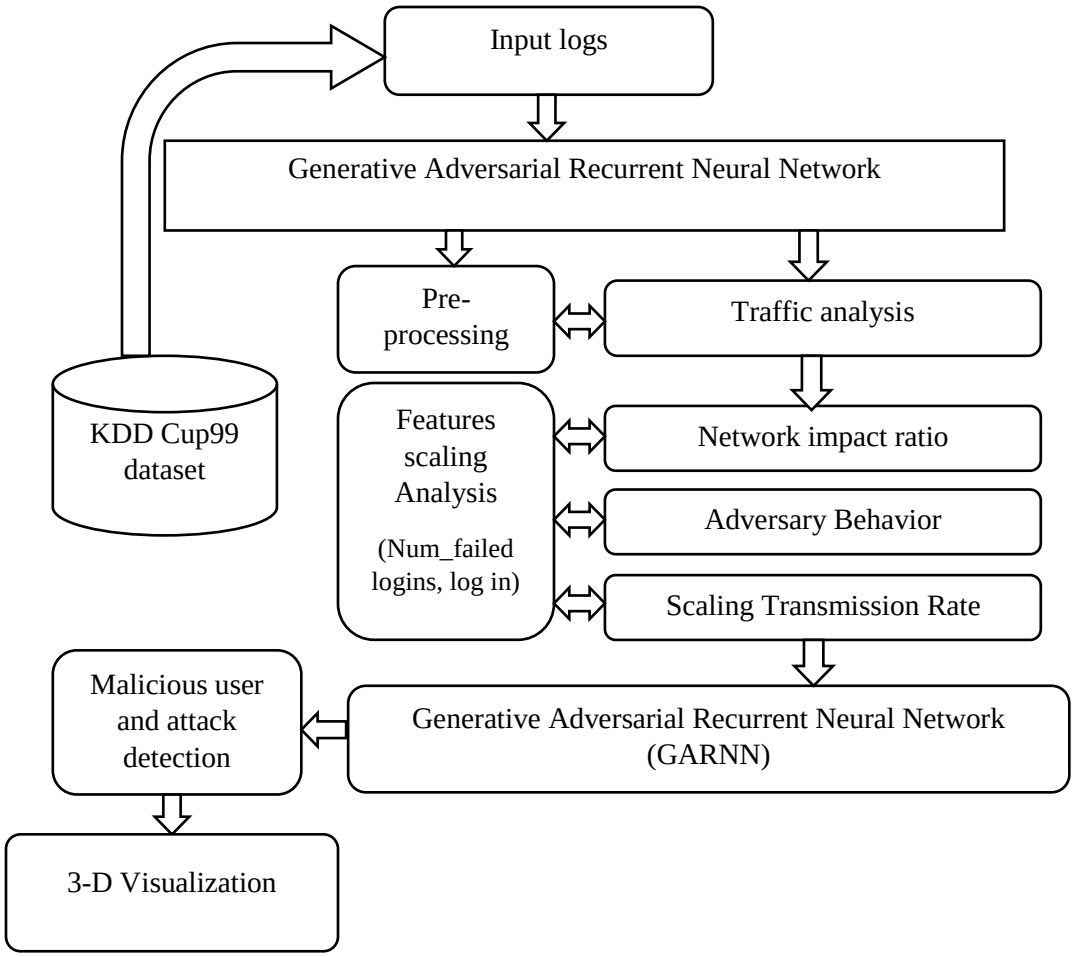

Figure 1: Block Diagram

3.1 Pre-processing

Preprocessing is a very important stage for improving classification process. Preprocessing is a proven method of resolving various issues of real-world data such as incompleteness, inconsistency, lacking in certain behaviors or trends, and the likelihood of containing errors. Data normalization is a process of scaling the value of each attribute into a well-proportioned range, so that the bias in favor of features with greater values is eliminated from the dataset.

$$T_{nor} = \frac{(T-\mu)}{\sigma}, \sigma \neq 0 \; and \; T-\mu, \sigma = 0 \qquad (1)$$

Let assume T_{nor} is denotes the normalized data, T is the test data with n column traits, μ is refers to mean σ is refers to standard deviation for each n traits.

$$\text{Mean } (\mu) = \frac{\sum O}{n} \qquad (2)$$

The above equation finds mean values. Where O presents the observed values and n denotes the number of records. The below equation find the standard deviation values,

$$\text{Standard Deviation} \sigma = \sqrt{\frac{\sum (O-\mu)^2}{n}} \qquad (3)$$

The below equation is used to find the pre-processed (P) dataset

$$P = \frac{T_{nor} - min(a_t)}{max(a_t) - min(a_t)}, for \; t = 1,2, \ldots n \qquad (4)$$

Let assume T_{nor} is the normalized dataset of attribute value, P is the pre-processed dataset, and $max(a_t), min(a_t)$ are the minimum and maximum values of attributea_t and n is the number of records.

3.2 Network Traffic Analysis

Network traffic analysis examines to identify threats that generate unusual traffic, such as Intrusion Detection (ID) attacks and some forms of malware. The proposed method monitors network traffic analysis for specific network segments or devices and analyzes network and application protocol activity to identify suspicious activity related to the protocol.

To calculate the some reached trafficT_R, let assume P refers to pre-processed data, A_T refers to average traffic for iteration$i$.

$$T_R = \sum_{i=1} P * A_T \quad (5)$$

Buffer utilization (b_f) can be expressed as equation 6, Let assume $S(bf)$ refers to size of the buffer data.

$$b_f = \sum_{i=0} \frac{T_r}{S(bf)} \quad (6)$$

In this stage done to identify the network traffic suspicious activity related to the protocol.

3.3Impacts of features scaling analysis

In this stage, after pre-processing, this process calculates the proposed feature scaling analysis based on the network transmission of the training dataset. This stage selects the most relevant attack detection features, so it is used to reduce the time during classification for normal or attack. The features are number failed login, number success login, and wrong fragment based on KDD Cup 99 dataset.

Let assume$fs_1, fs_2, \ldots fs_n$ is the feature value used for forming the set of transmission records given training dataset S.

$$S=\left\{s_1, S_2, \ldots . S_n \forall_s = \{Val(fs_1), Val\ (fs_2), \ldots Val(fs_i), Val(fs_{i+1}), \ldots Val(fs_n)\}\right\} \quad (7)$$

The features set values associated with each network transaction as the Transmission value set vs and all transmission value sets asA_{vs}.The above equation 5Val(fs_i) can be expressed as Val$(fs_i) \in \{fs_{iC1}, fs_{iC2} \ldots fs_{iCn}\}$ is refers to current features of attack detection.

Algorithm steps:

Input: Pre-processed (P) Dataset

Output: Feature Scaling Analysis $FSA|_T$dataset

Begin

Step 1: Initialize the preprocessed (P) Dataset

Step 2: The features of edge weight $W_t$calculating as

$$W_t\left(Val(fs_1) \leftrightarrow Val(fs_2)\right) = \frac{\text{vs}}{|A_{\text{vs}}|}$$

Step 3: Computing the categorical features scaling analysis (FSA) values as

$$\text{FSA } (A_{\text{vs}}) = \frac{\sum_{n=1}^{A_{\text{vs}}} \{vs_n : (fs_{iC1} \rightarrow vs_n) \neq 0\}}{\sum_{n=1}^{A_{\text{vs}}} vs_n}$$

Step 4: impact of FSA each transmission value set vs calculating as

$$FSA| \text{ (vs)} = 1 - \frac{\sum\{FSA(\{Val_i \exists Val_j\}) : (Val_j C vs_i)\}}{|vs_i|}$$

Step 5: Calculating the Maximum features of threshold $FSA|_T$

$$FSA|_T = \frac{\sum_{n=1}^{|A_{\text{vs}}|} FSA| \text{ (vs)}}{|A_{\text{vs}}|}$$

Stop

The above algorithm is done to identify the select the features for attack detection to reduce the classification time and dimension.

3.4Generative Adversarial Recurrent Neural Network

In this stage anomaly-based IDS monitors' network activity uses 3D visualization and GARNN to classify it as normal or malicious.Recurrent Neural Networks (RNNs) extend the capabilities of traditional feedforward neural networks and are designed to model continuous data.A GARNN consists of an input layer, a hidden layer, and an output unit, and the hidden unit is considered a memory element. The feature analysis of the dataset consists of input parameters that are passed to the GARNN and targeting output labels so that the model can learn the hidden dependencies between inputs and outputs.

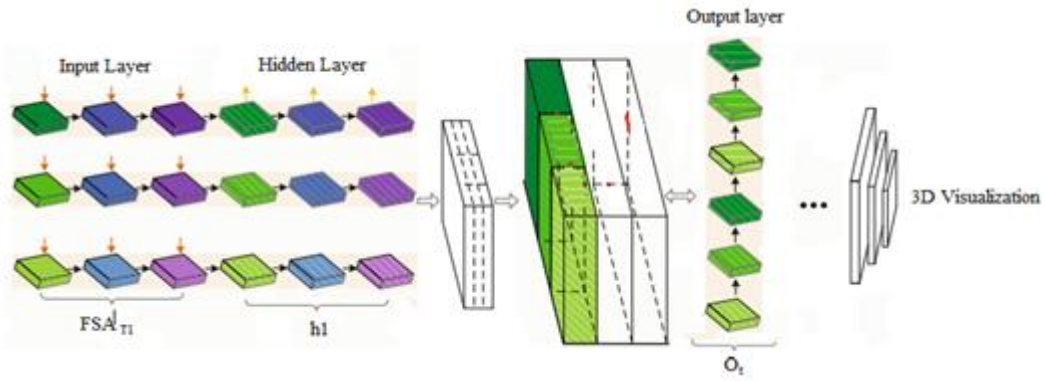

Figure 2: Diagram for Generative Adversarial Recurrent Neural Network

The input layer initializes the preprocessed data there is no calculation that occurred in this layer. The input layer sequence is $FSA|_{T1}, FSA|_{T2} \ldots . n$. the hidden layer is a layer between the input layer and output layer. The hidden layer denotes$h_1, h_2 \ldots n$. This layer performs the calculation of the weights and finally passes the information to the output layer. Each neuron is connected from the next layer, and each connection (black arrow) has a specific weight. The output layer provides the results for normal or malicious attacks shown figure 2.The output layer denotes $o_1, o_2 \ldots n$.the weight for connection weight denotes $w_{lm}^{(1)}$ represent the connection from input to hidden layer weight for the connection, then $w_{lm}^{(2)}$represents the connection from hidden to output layer to identify the DDoS attack detection in 3D WSN.

The transformation from input layer to hidden layer is through the weighted function and activation function $\sigma$and b is refers to V refers to bias shown in equation

$$h = \sigma\left(\sum_{i=1}^{n} P_1 \, w_{lm}^{(1)} + V\right) \qquad (8)$$

The transformation from hidden layer to output layer as follows,

$$O = \sigma\left(\sum_{i=1}^{n} h \, w_{lm}^{(2)} + V\right) \qquad (9$$

Algorithm Steps

Input: Features Scaling Analysis $FSA|_T$dataset
Output: Classify the result (O)as attack or normal
Begin
Step 1: Initializes the $FSA|_T$dataset fed in to the input layer
Step 2: Compute the hidden layer process as (h)

$$h = \sigma\left(\sum_{i=1}^{n} P_1 \, w_{lm}^{(1)} + V\right)$$

Step 3: Check weights of threshold features
For each scaling y do
Check threshold features values
End each
Step 4: Compute output layer process

$$O = \sigma\left(\sum_{i=1}^{n} h\, w_{lm}^{(2)} + V\right)$$

Step 5: Return the result as normal or attack reflect to 3D virtualization
Stop

The above algorithm done to detecting the attack or normal based on KDDCup99 dataset. Assume $FSA|_T$ is presents the Features Scaling Analysis,$y^{th}process$ of features analyzing values, $w_{lm}^{(2)}$ is calculating weights that is tuning the results based features and σ is the activation function to produce the accurate results O.The primary purpose of the GARNN algorithm is to analyze the probability of intrusion detection, assist in the deployment of user behavior and obtain a sufficient 3D WSN security level.

4. Result and discussion

This section presents the simulated experimented results of this work. This paper uses the KDDCup99 dataset as our proposed algorithm for the number of records for testing and training data. The dataset attributes contain duration, protocol, service, flag, src bytes, land, wrong fragment, num_failed logins, logged in, and so on.

Table 1 simulation parameters

Parameters	**Value**
Dataset name	KDD CUP99
Number of Data	494021
Tool	Anaconda
Language	Python
Training data	400000
Testing data	9421

The above table 1 defines the simulation parameters for malicious user and attack detection in WSN using python language. The test result comparing to the proposed method Generative Adversarial Recurrent Neural Network (GARNN) and existing methods are Deep Q-Learning Neural Network (DQNN), Supervisory Control and Data Acquisition (SCADA). The below equation can be calculating the precision performance.

All parameters are based on a calculation by a confusion matrix. A confusion matrix is a two-dimensional matrix that provides information about the actual class and the predicted class.

$$Precision\ (Pn) = \frac{TN}{TN+FP} x100 \qquad (10)$$

Where TN refers to True Negative, FP refers to False Positive, TN is the number of attacks that are accurately classified as attacks. FP is the number of normal data inappropriately classified as attacks

Table 2: Analysis of precision performance

Number of data	SCADA in %	DQNN in %	GARNN in %
200	56	62	75
400	70	72	84
600	74	80	87
800	80	84	92

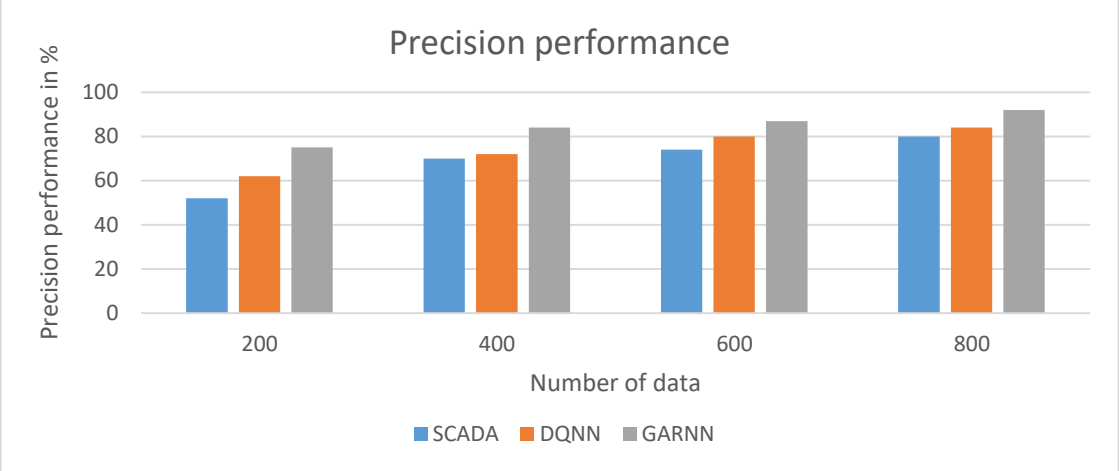

Figure 3: Analysis of precision performance

The above figure 3and table 2 describes the precision performance for detecting the malicious users and attacks in WSN.Precision is the ratio of the correctly predicted attack to all the samples predicted as an attack. The proposed Generative Adversarial Recurrent Neural Network (GARNN)precision performance result is 92%, in this comparison result existing Deep Q-Learning Neural Network (DQNN) 84%, and Supervisory Control And Data Acquisition (SCADA)precision result is 80%.

$$Recall\ (Re)=\frac{TP}{TP+FN}x100 \qquad (11)$$

The above equation can be calculating recall performance. TP refers true positive, and FN refers False Negative. TP is the number of attacks that are accurately classified as a record,

Table 3: Analysis of recall performance

Number of data	SCADA in %	DQNN in %	GARNN in %
200	58	61	76
400	69	73	83
600	75	81	88
800	81	85	93

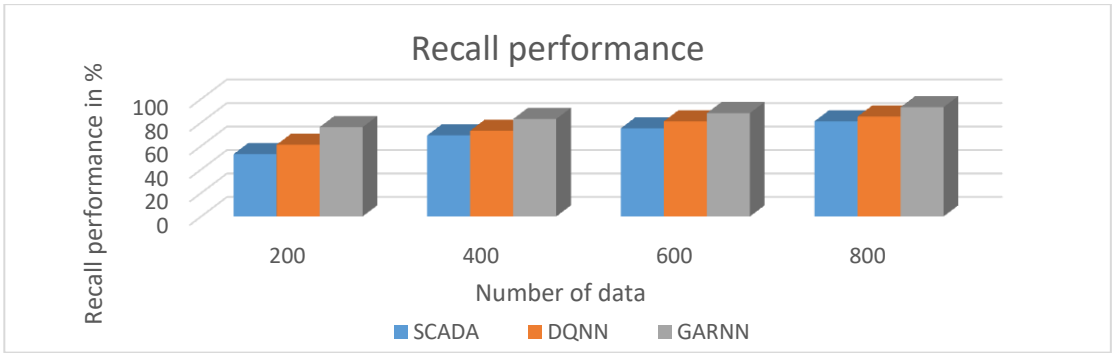

Figure 4: Analysis of recall performance

The above figure 4and table 3 defines analysis of recall performance for malicious user and attack detection in WSN. The recall is the ratio of all samples that are correctly classified as attacks to all actual attack samples.The proposed GARNN algorithm recall performance 93%; likewiseexisting Deep Q-Learning Neural Network (DQNN) 85%, and Supervisory Control And Data Acquisition (SCADA) precision result is 81%.

$$F-measure = 2\left(\frac{PnXRe}{Pn+Re}\right)x100 \qquad (12)$$

The above equation can be calculating F-measure performance. The F-measure is defined as the harmonic mean of precision and recall. It checks the system compliance rate by considering the system compliance precision and recall rate.

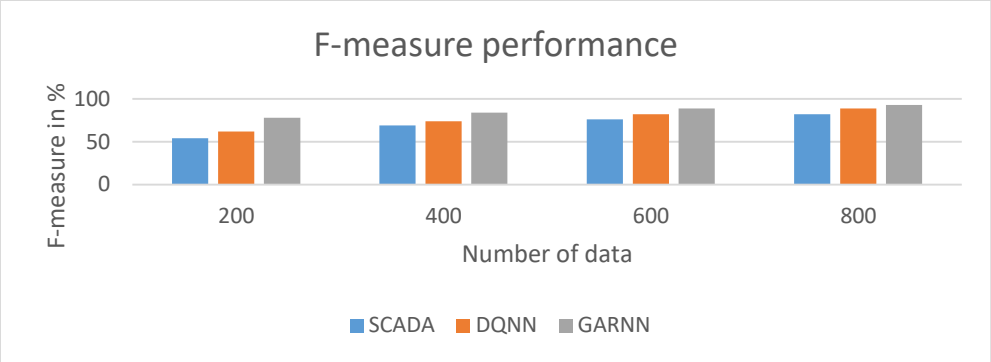

Figure 5: Analysis F-measure Performance

The above figure 5 shows the analysis f-measure performance in the result of proposed F-measure performance has 93% for 800 data. In the comparison result existing Deep Q-Learning Neural Network (DQNN) 89%, and Supervisory Control and Data Acquisition (SCADA) precision result is 82% for 800 data respectively.

Accuracy Detection (AD) is the ratio of the number of properly categorized instances to the whole number of instances. The below equation used to calculate the AD performance

$$AD = \frac{TP + TN}{TP + TN + FP + FN} \quad (13)$$

Table 4: Analysis of Accuracy Detection (AD) performance

Number of data	SCADA in %	DQNN in %	GARNN in %
200	60	66	78
400	71	76	85
600	79	84	90
800	83	87	94

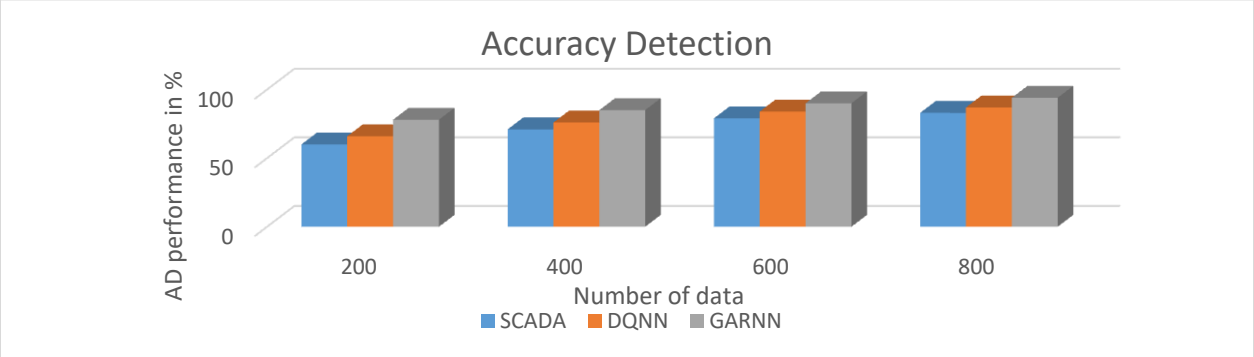

Figure 6: Analysis of Accuracy Detection (AD) performance

Analysis of Accuracy Detection (AD) performance for detecting the malicious user and attacks in WSN the comparison of proposed and existing method results shown in figure 6 and table 4. In the proposed GARNN algorithm AD performance has 94% for 800 data, similarly the existing DQNN has 87% and SCADA has 83% for 800 data respectively. The proposed GARNN provide result high performance compared with previous algorithm. The below equation calculate the False Rate Performance (FAR),

$$False\ Alarm\ Rate(FAR) = \frac{FP}{FP+TN} \quad (14)$$

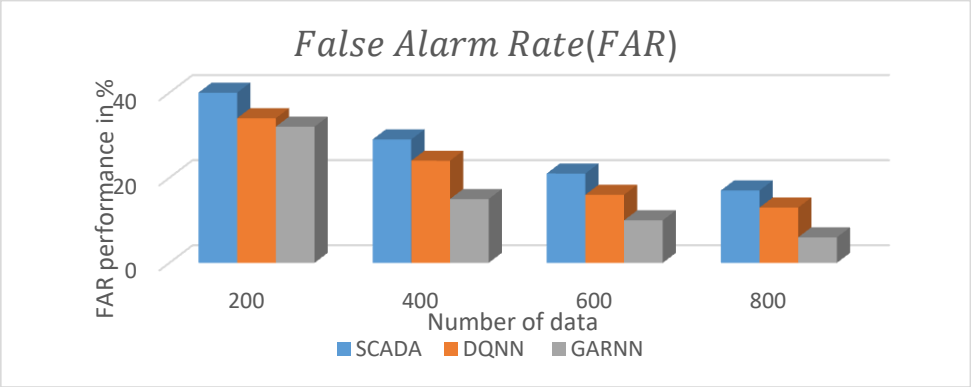

Figure 7: Analysis of False Alarm Rate (FAR) performance

Analysis of False Alarm Rate (FAR) performance results shown in figure 7. The proposed GARNN algorithm FAR performance result is 6%; similarly the previous DQNN algorithm FAR performance 13% and SCADA algorithm FAR performance result is 17% respectively. The GARNN proposed algorithm provide low False Alarm Rate (FAR) than existing algorithm.

5. Conclusion

This paper presents the new model of Generative Adversarial Recurrent Neural Network (GARNN) for detecting malicious users and attacks in WSNis reflect to 3Dimension virtualization using KDDcup99 dataset.This study focuses on enhance on Intrusion Detection System(IDS) the proposed to improve the Accuracy Detection (AD) and reduce the false rate performance.The proposed model effectively increases the accuracy of intrusion detection and identifies malicious users.The proposed GARNN provide results are Precision (Pn) has 92%, and Recall (Re) has 93%, F-measure has 93%, Accuracy Detection (AD) has 94%, and False Alarm Rate (FAR) has 6%.The proposed simulation experimental result shows that our solution is more effective and efficient in terms of Accuracy Detection (AD), Precision (Pn), Recall (Re), F-measure, and reduced False Alarm Rate (FAR) than existing methods.

Reference

[1]. N. K. Mittal, "A survey on Wireless Sensor Network for Community Intrusion Detection Systems," 2016 3rd International Conference on Recent Advances in Information Technology (RAIT), 2016, pp. 107-111, doi: 10.1109/RAIT.2016.7507884.

[2]. Butun, S. D. Morgera and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 266-282, First Quarter 2014, doi: 10.1109/SURV.2013.050113.00191.

[3]. Warzyński and G. Kołaczek, "Intrusion detection systems vulnerability on adversarial examples," 2018 Innovations in Intelligent Systems and Applications (INISTA), 2018, pp. 1-4, doi: 10.1109/INISTA.2018.8466271.

Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," in IEEE Access, vol. 9, pp. 103906-103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[4]. Dutt, S. Borah and I. K. Maitra, "Immune System Based Intrusion Detection System (IS-IDS): A Proposed Model," in IEEE Access, vol. 8, pp. 34929-34941, 2020, doi: 10.1109/ACCESS.2020.2973608.

[5]. W. Zhong, N. Yu and C. Ai, "Applying big data based deep learning system to intrusion detection," in Big Data Mining and Analytics, vol. 3, no. 3, pp. 181-195, Sept. 2020, doi: 10.26599/BDMA.2020.9020003.
[6]. S. Amaran and R. M. Mohan, "Intrusion Detection System using Optimal Support Vector Machine for Wireless Sensor Networks," 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 2021, pp. 1100-1104, doi: 10.1109/ICAIS50930.2021.9395919.
[7]. K. Lin, T. Xu, J. Song, Y. Qian and Y. Sun, "Node Scheduling for All-Directional Intrusion Detection in SDR-Based 3D WSNs," in IEEE Sensors Journal, vol. 16, no. 20, pp. 7332-7341, Oct.15, 2016, doi: 10.1109/JSEN.2016.2558043.
[8]. S. Otoum, B. Kantarci and H. T. Mouftah, "On the Feasibility of Deep Learning in Sensor Network Intrusion Detection," in IEEE Networking Letters, vol. 1, no. 2, pp. 68-71, June 2019, doi: 10.1109/LNET.2019.2901792.
[9]. W. Meng, W. Li, C. Su, J. Zhou and R. Lu, "Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data," in IEEE Access, vol. 6, pp. 7234-7243, 2018, doi: 10.1109/ACCESS.2017.2772294.
[10]. Z. Sun, Y. Xu, G. Liang and Z. Zhou, "An Intrusion Detection Model for Wireless Sensor Networks With an Improved V-Detector Algorithm," in IEEE Sensors Journal, vol. 18, no. 5, pp. 1971-1984, 1 March1, 2018, doi: 10.1109/JSEN.2017.2787997.
[11]. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," in IEEE Access, vol. 7, pp. 41525-41550, 2019, doi: 10.1109/ACCESS.2019.2895334.
[12]. H. Moosavi and F. M. Bui, "A Game-Theoretic Framework for Robust Optimal Intrusion Detection in Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 9, pp. 1367-1379, Sept. 2014, doi: 10.1109/TIFS.2014.2332816.
[13]. V. T. Alaparthy and S. D. Morgera, "A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory," in IEEE Access, vol. 6, pp. 47364-47373, 2018, doi: 10.1109/ACCESS.2018.2866962.
[14]. F. Raza, S. Bashir, K. Tauseef and S. I. Shah, "Optimizing nodes proportion for intrusion detection in uniform and Gaussian distributed heterogeneous WSN," 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 2015, pp. 623-628, doi: 10.1109/IBCAST.2015.7058571.
[15]. K. Ramasamy, M. H. Anisi and A. Jindal, "E2DA: Energy Efficient Data Aggregation and End-to-End Security in 3D Reconfigurable WSN," in IEEE Transactions on Green Communications and Networking, doi: 10.1109/TGCN.2021.3126786.
[16]. MamounAlazab, Shamsul Huda, "A Hybrid Wrapper-Filter Approach for Malware Detection,"ResearchGate, Nov 2014.

