Detection of Attacks in Pervasive Computing Using Gated Recurrent Unit Based on Bidirectional Weighted Feature Averaging

P. Rajasekaran (rajasekarphd01@yahoo.com)
PSNA College of Engineering and Technology https://orcid.org/0000-0003-1588-1544
V Magudeeswaran
PSNA College of Engineering and Technology

Research Article

Keywords: Cyber-attacks, Pervasive computing, SNMP-MIB dataset, Enhanced Salp Swarm Optimization (ESSO), Gated Recurrent Unit-Neural Networks based on Bidirectional weight average, detection rate.

Posted Date: December 6th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-1137724/v1

Detection of Attacks in Pervasive Computing Using Gated Recurrent Unit Based on Bidirectional Weighted Feature Averaging

[*1]P. Rajasekaran, [2]V. Magudeeswaran

[*1]Assistant Professor, Department of ECE, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India.

[2]Associate Professor, Department of ECE, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu, India.

[*]Corresponding Author Mail ID: p.rajasekaran537@psnacet.edu.in

Abstract:

In the era of information technology, the new types of cyber-attacks affect the performance of the network, which is very risky and cannot be restored quickly. In pervasive computing, there are more chances for such types of attacks since the personal data of the user is closely connected to the social environment. The research is performed using SNMP-MIB dataset, and feature selection are made by using the Enhanced Salp Swarm Optimization to select the optimal features to identify the attacks by using wrapper techniques. Then, various types of attacks are appropriately distinguished with proposed classifier Gated Recurrent Unit Neural Network based on Bidirectional Weighted Feature Averaging for high detection rate and accuracy. The value of performance metrics obtained from the proposed method outperforms the existing methods in terms of 99.9% accuracy, 99.8% in precision and detection rate is 99% in classifying different types of attacks.

Key Words: Cyber-attacks, Pervasive computing, SNMP-MIB dataset, Enhanced Salp Swarm Optimization (ESSO), Gated Recurrent Unit-Neural Networks based on Bidirectional weight average, detection rate.

I. INTRODUCTION

Pervasive computing is a model which indicates a paradigm where it is connected by computing element and sensors linked to all types of everyday objects, which is easily accessible to the users[1]. It is the best example of pervasive computing in the context of automobile networks which can be implemented as computational elements in automobiles, road infrastructure and also in user's equipment interoperated to enhance the efficacy in safe measures even without the user's surveillance. It is termed as 'pervasive' in nature as it brings forth a series of security alarms. So here the computing elements are pervasive, which can track the daily routines of the users, and in turn, raises the privacy concerns. Moreover, the rapidly increasing number of devices enlarges the networks, that signifies the opponent have several targets to attack. So it leads to a huge disaster if the network is not Secured intensely. Leaving this system unprotected led to the Miraj Botnet attack[2]. Many components of pervasive computing are reactive, which performs actions in response according to changes in environmental behaviour. The applications are generally attracted in the high-level, complex event in alter to a low-level primitive event generated by sensors. So many researches are performed to detect the multiple events by aggregating, filtering and combining the first events. There are many machine learning algorithms, and deep learning techniques are implemented in the detection and classification of network attacks. The neural networks play a significant role in decision making at the time of an attack and protect the rest of network by classifying and identify the characteristic features and also distinguish the type of attack by training the defence mechanism of the pervasive computing system effectively.

The main application of pervasive computing is to make the life more sophisticated by offering mobile equipment, and digital infrastructure is proficient at offering the distribution of any sort of services within the environment where people socialize, live or work[3]. Besides, it experiences many types of attacks which should be eliminated by effective techniques. The pervasive system is embedded and participate in demanding services without the explicit knowledge of the user. The working of pervasive computing is done by sharing the mutual information which includes personal data even their preferences also like surfing in browsers, time spent in social media, sourcing of various products etc. At a particular time, there are many probabilities for third party attack in user profiling, suggestions in social network connection and targeted advertising related to the user's search keywords. In the context-based text or connection, the device fails to identify the trusted domain and do not have centralized control; there occurs security chaos.

The pervasive computers acts as a game-changer in the health care industries which throws multiple features to patients such as continues observation of heart rate, blood pressure, glucose level and so on by connecting with health experts all over the world [4, 5]. There are a better awareness and engagement of customers with concern to their health results in a boosted growth for remote and personalized health care services. There are various types of attacks such

as TCP-SYN, UDP flood, ICMP-echo, HTTP flood, Slowloris, Slow post and Brute force attacks is discussed in this paper. The proposed method used to detect and differentiate all the mentioned attacks with high accuracy and reliability. A TCP-SYN attack is a method of denial of service attacks in which a hacker uses the communication protocol of the cyberspace, IP, to bombard an objective system with SYN requests in an attempt to overcome the connection queue and push a system to become insensitive to authentic requests. An SYN attack is also called an SYN flood whereas SYN stands for synchronization. UDP flood attack affects the enormous number of user datagram protocol which are transmitted to the targeted server with the focus of overcoming the ability of the device to response and process. The firewall defending the target server can become exhausted as the outcome of UDP flood, which in turn affect in Dos to legitimate traffic[6]. A ICMP echo is called a ping flood, where the hacker attempt to devastate a targeted device with ICMP echo request packets, causing the target to become unreachable to general traffic. When the attack occurs from multiple devices, it turns into a distributed denial-of-service attack. The HTTP flood exploits the authentic HTTP GET to attack web applications or web servers. It is a volumetric attack, which uses a zombie army to attack the group of computers connected to the internet, which maliciously overrides the system with the assistance of malware Trojan Horses. The Slow Loris attack enables a single machine to bring down the webserver of the other machine with minimal bandwidth which impacts on unrelated ports and services. It holds many connections to target web server open and holds it as long as possible by establishing the connection by sending a partial request to target web server. In the Slow Post attack, the hacker sends an authentic HTTP POST headers to a web server. Here the message is transmitted painfully at slow speeds such one byte for every 120 seconds. A Brute Force attack is made to crack the username or passwords to identify the hidden web pages or encrypt a text by repeated trial and error method until the correct guess. Even though it is a very traditional method, it remains popular among hackers. Deep learning methods are implemented effectively in recent days for the detection of network attacks in the pervasive computing environments. But the existing techniques are not reliable and efficient in higher dimensional networks. So the proposed method is based on the feature selection and classification of deep learning methods.

1.1 The objective of the research

- The feature selection is made by using Enhanced Salp Swarm Optimization. It is used to improve the detection rate of various attacks by selecting only the optimal features using the wrapper technique, and in turn, increases the accuracy as it is highly dependent on the classifier.
- The proposed classifier used in GRU-NN based on Bidirectional weighted feature averaging is used to achieve high prediction rate and classify different types of attacks depending on the weights by analyzing the characteristic features of the attacks and prevent frequent lags in the performance metrics of the proposed architecture.

1.2 Paper Organization:

The following section II describes the literature review about the pervasive computing associated with various attacks. Moreover several techniques also discussed. Section III elaborated the proposed methodology of GRU based Bidirectional weighted feature averaging. Section IV illustrated the results and discussion of the proposed work. Finally in section V the paper is concluded.

II. REVIEW ON EXISTING WORKS

In this section, explained the different types of attack in pervasive computing by various methods which are implemented in existing researches. The benefits of each technique are inferred in the proposed method. The limitations are overcome to improve the performance metrics of our proposed research.

This study, proposed the learning ability of detection performance based on deep neural networks by using gated recurrent units. It comprises of neural network with softmax layers and multilayer perceptron. The recurrent neural networks consist of gated units to store central memory units merged with multilayer perceptron to find the network attacks. The KDD dataset is used here for the intrusion detection and classification, and it doesn't require any human efforts in feature selection. The process is more suitable in the RNN memory unit than LSTM in intrusion detection. The advantage of this method, such as time consumption and performance metrics, are attracted. Still, it should be more updated to be applied in real-time environments as suggested by network experts since it is only reliable up to a particular extent[7]. Further, this research explained the capability of learning from the previous attacks by supervised intrusion detection using recurrent neural networks. The developed Learning is based on fast learning networks based on particle swarm optimization applied in KDD dataset. It is processed by comparing with a wide range of existing algorithm for training the extreme machine learning and Fast learning classifiers. The calculated performance metrics overcome various algorithms. So the process of PSO is inferred, and advantages can be considered for our proposed work[8].

This study proposed research to achieve network security by managing the traffic flow in detecting the malicious host attacks. So many techniques are adapted for controlling the cyber-attack. The suggested paper is used to identify the malware attack based on the characteristics at the time of sending the SYN packets. The matrix method is used to transform the series of SYN packets to an input visual image for neural networks. The image comprises of distinctive features of the behavioural characteristics of the host and the convolutional neural network effectively segregates the malevolent host from the general ones. The evaluation of real-world traffic showed a detection accuracy of 98%. Still, it only detects at the time of sending the packets of SYN. It

isn't able to identify any other malware attack. So it is not efficient in distinguishing different types of attack and cannot be applied in a real-time system[9]. This paper deliberated the detection of known and unknown attacks by a defence mechanism that prevents the counterfeit packets from the destiny point of the victim. It enables only the original packets to pass through by training the dataset with neural networks. It focuses on the detection of known attacks in the higher volume of traffic without any packet drop. The dataset is trained, deployed and tested in physical circumstances as a desperate to the simulators and it is trained to lower the impact and strength of the attack before it reaches the victim by the intrusion detection system and the evaluated method is analyzed by computing the performance metrics. But this method cannot be able to differentiate the type of attack and cannot be implied in real-time environments[10].

This research explained the attacks and impacts about the advanced paradigms in pervasive computing. This method revealed the detection model in pervasive computing architecture to attain the close resemblance of human decision making by using the neural networks. Here the Apriori algorithm is used to extract the behavioral sequences adapted from the users at network interactions. Then, Naïve classifier is implemented for final decision to check the trustworthy of the network. The neural network is used in the detection of intrusion. Still, it does not achieve a reliable metric when applied in the sizeable dimensional dataset and doesn't able to classify many types of network attacks[11, 12]. This study explained the intrusion detection system to correct the abnormalities in pervasive environments. It is a traditional method that manages the security of the node and network and always is cautious on the network security and isolates the affected node from the rest of the system. This suggested method implemented authentication methods to develop the user profile, which enables flexible detection and analysis to avoid updating the general profile database. The investigation methods to explore the audit information form IDS is performed by processing the orchestration of network clusters. In this method, three phases are completed, such as the initialization phase, detection phase and isolation phase. The Georgia Tech Network Simulator is used for the simulation process, which is updated to demands of the current environment with many machine learning and deep learning concepts in pervasive computing[13].

This study explained the intrusion detection method to find malicious detection by improvised convolutional neural networks. The traffic data is characterized and preprocessed by optimizing the network parameters in extracting the sample features using stochastic gradient descent algorithm in the convergence model. The sample test and simulation result are used to test the performance metrics of the existing system in the KDD dataset. But the network flow has given a minimum performance in detecting the malicious attack at the time of traffic management in the wireless network system[14, 15]. This paper deliberated the extensive analysis of deep learning methods for intrusion detection in networks. This method used the Restricted Boltzmann machine based on clusters. The supervised machine learning approach is based on adaptively supervised and clustered hybrid ID. The Restricted Boltzmann device is comprised of two layers hidden and visible, is used for the weight selection of the cluster head in the pseudo-code, which is used for the cybersecurity. Even though it shows high-performance outcomes, it cannot be applied in large scale networks[16].
This research described the joint intrusion learning on pervasive systems by detecting the different intrusion sequences simultaneously. The K-neighborhood method is used for grid-based clustering for detecting the occurrence or presence of interferences. The joint learning approach showed the performance metrics with minimum FPR by conducting experiments using Zigbee. But it should be improved by using the collative detection efforts among the multiple pairs of transmitter-receiver[17]. This study explained to overcome the security challenges in ubiquitous health care systems. The pervasive computing system and ubiquitous is similar involves computational, complicated and expensive task in simultaneous execution of the algorithm. It is responsible for characterizing any attack in the networks and should be capable of computing the physical parameters of attacks which can be used for future researches. In this method, the collective computing capability with wireless connected local mobile networking grid and various sensors. Here the sensor plays a data providers by offloading the task which executes a different intensive algorithm, and the raw data is sent via zig bee to manage the elastic data pool. So if any attack exists, the computational load on node is decreased since the parallelism of data is performed. The vital signs are collected and process for contextual information which is used for patient-centric decision making and also can be further used for research application by converting it as a dataset[18] [19].

III. Proposed Methodology- Gated Recurrent Unit Neural Network based on Bidirectional Weighted Feature Averaging

In the proposed method, the SNMP-MIB dataset is used for training and classification, which can be implemented as testing data in the pervasive computing environment. The preprocessing is applied to remove the noises in the dataset, which is fed for feature selection by using Enhanced Salp Swarm Optimization technique to find the optimal features to detect any attack in the pervasive computing. Then, GRU-NN based Bidirectional weighted feature averaging is used as a classifier to differentiate various types of attacks such as TCP-SYN, UDP flood, ICMP echo, HTTP flood, Slowloris, Slow Post and Brute Force. It is made by analyzing the characteristic features and weighted average of the attack with the help of trained SNMP-MIB dataset. The overview of the proposed method with the various process is shown in Fig.1, and a brief explanation is given in the below section.

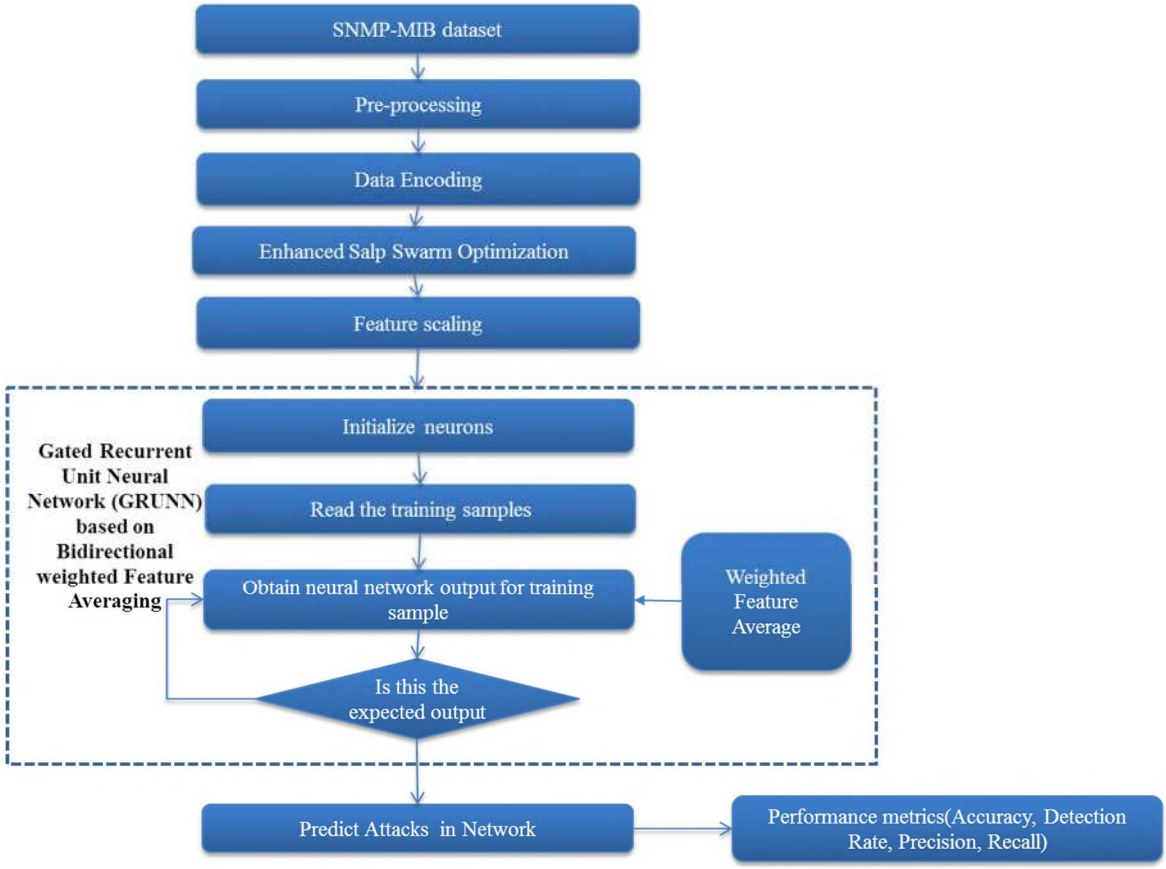

Fig.1 Overview of the Gated Recurrent Unit Neural Network based on Bidirectional Weighted Feature Averaging (GRU-BWFA)

A. Dataset Description

The significant fact in using dataset SNMP-MIB for attack detection is that the variables of SNMP-MIB are utilized since there is no single variable which can be able to capture all abnormalities on networks. This research used only particular variables for accurate attack detection. It focused on the router to collect MIB variables[6]. The proposed method selected thirty-four MIB variables from five different MIB groups in MIB-II. The variable of this group is collected from concern interface of the router such as UDP, ICMP, TCP and IP. The data types of thirty-four MIB variables were counted thirty-two and the non-negative 4-byte integer, which is continuously incremented from 0 to 232. When it reaches a threshold value, it again wraps back to zero. After going through many detailed investigations, these values are selected among these MIB variables in groups since they are impacted more by the attack variables which are persistently refreshed with outgoing and incoming traffic across the network which is more reliable for detection[20].

B. Preprocessing

Preprocessing is a mandatory step which is made to transformations applied to the dataset before pushing it to the algorithm. It is used to change the raw data with multiple flaws into a clean dataset without any noises. Whenever the information is collected from varied resources, it has possibilities of noises or any data errors, miss imputation, repetitive values, mislaid values. The format may also be not feasible to feed into an algorithm for analysis, so it should be formatted in a proper way suitable for the understanding of machine learning algorithm or deep learning techniques which should be executed in the proposed method. The preprocessing in the proposed method is made with filtering techniques which are used to eliminate the errors and noise data.

C. Data encoding

Once the preprocessing is completed, the data is encoded for better clarity and security purposes. The encoder is used to encode every string into numerical values into binary formats. The data loss, data threat and hack are avoided and thus the data can transmitted in a secured packet to the destination point. It also removes the glitches made at preprocessing since the data is completely purified and secured before it is fed into the optimization algorithm.

D. Feature Selection using novel Enhanced Salp Swarm Optimization (ESSO)

The general Salp Swarm Algorithm undergoes the difficulty of population diversity and trapped into local optima. So in the proposed algorithm is implemented to overcome the limitations by making two strategies in the usual Salp Swarm Optimization algorithm[21, 22]. The first strategy is the implementation of Opposition Based Learning (OBL) method at the initializing phase of SSO to enhance the population diversity. The second strategy is implemented with the development of local search algorithm, which is applied at the ending phase of SSO. It is used to increase the SSO utilization and prevent it from being stuck at local optima. So the Enhanced Salp Swarm Optimization is used to resolve the feature detection and choose the optimum subset of features by wrapper technique.

Opposite based Learning is an optimization method used to increase the quality of commenced population solution by the diversity of solutions. It works by searching in both directions in space search. The two directions involve one of the original solutions is symbolized by its opposite solution, which is used to take the fittest answer from all the generated solutions. The Local Search Algorithm is used at the end of every iteration in Salp Swarm Optimization to improve the obtained best solution, E. Initially, the LSA executes by storing the value of obtained best solution received from SSO. At the final iteration of SSO, it is stored as a temporary variable.

The proposed Enhanced Salp Swarm Optimization works with GRU-NN based Bidirectional Weighted Feature Averaging classifier by wrapper function for feature selection. It is implemented on the training dataset to compute the feature subset for training the proposed classifier. The binary values 1 and 0 are performed to choose the unselected and selected features. The value 1 represents the selected feature which is mentioned in the given label or index, whereas the value of 0 indicates the unselected features in the label or index.

The following equations describes the enhanced Salp swarm optimization for feature selection,

$$\widehat{y_r} = ta_i + va_i - y_i \text{ where } r = 1,2,\ldots G \quad (1)$$

$$E_1 = 2d - \left(\frac{4t}{T}\right)^2 \quad (2)$$

$$y_i^1 = \{ E_i + e_1 ((va_i - ta_i)e_2 + ta_i)\, e_3 \} >= 0.5$$

$$\{ E_i + e_1 ((va_i - ta_i)e_2 + ta_i)\, e_3 \} < 0.5 \quad (3)$$

$$y_i^j = \frac{1}{2}(y_i^j + y_i^{j-1}) \quad (4)$$

Algorithm 1

1. Set salps position Y as y_i(j = 1,2,…..m)
2. Compute salp opposite population OY as $\widehat{y_j}$ (j = 1,2,… m) using eq 1.
3. Choose m fittest salps from {Y ∪ OY} which now denote the initial SSA population define fitness value of individual salp.
4. E = best salp (search agent)
5. While (h < max iterations)
6. Update value of e_1 parameters using eq 2
7. for each salp (y_j)
8. if (j==1)
9. update leader positing by eq 3
10. else
11. update follower position by eq 4
12. end if
13. end for
14. reposition salp based on upper and lower bounds of problem variables.
15. Determine the fitness value of individual salp
16. E = best salp (search agent)
17. Apply LSA on E to discover if there is the enhanced solution (if found enhanced solution then, update E; otherwise E left unchanged)
18. L = l+1
19. End while
20. Return E

Algorithm for ESSO

- Initialization of ESSO is made by a randomly generated number of salps based on the size of the population. The generated solution comprises a subset which is randomly chosen from the entire set of features.
- The OBL is applied to find the opposite solution of every obtained answer of step 1.

The suitable fitness value 'E' is obtained, which also signifies the lower classification accuracy error.

- Each position of a slap is updated by choosing the leader of salp chain by eqn 3.
- The fitness value of all solved slap is determined to find the 'E' best solution
- LSA is implemented in the end phase of 'E' to find the best solution, then, the iteration is repeated thrice or more.
- The best solution is determined with ESSO and this signifies the suitable subset features to be selected and applied

F. Feature Scaling

It is also a standardization method which is similar to preprocessing that is executed in independent features or variables of data to normalize within an applicable range. It also helps in speed up the computation in the algorithm. Here, the standard scalar is used to scale the obtained data which should be further used as input for the classifier.

G. Gated Recurrent Unit –Neural Networks based new Bidirectional Weighted Feature Averaging (GRU-BWFA)

The GRU-NN based on bidirectional weighted feature averaging is used to train, test and classify the data. The Gated Recurrent Units is considered a modest version of LSTM [23]. Here two gates are involved as a reset gate which alters the integration of new input with preceding memory. Another is update gate which controls the preservation of the prior memory that is implemented. The hidden units of Gated Recurrent Units are represented as transition functions. The integrated bi-directionality of the recurrent method can enhance the proposed design's flexibility and capability.

GRU:

Due to additional weight matrices in LSTM, the computational complexity increased. Thus by introducing GRU the complexity is reduced by joining the input and LSTM forget gate into single update gate. The hidden and cell states are combined into single hidden state. The equations are expressed as,

V = transformation matrix b = bias value

$$g_k = \varphi\ (\ V^g y_k + S^g g_{k-1} + a^g\ ) \qquad (19)$$

y_k current input g_{k-1} previous activation

$$s_k = \delta\ (\ V^s y_k + S^s g_{k-1} + a^s) \qquad (20)$$

$$z_k = \{\ \delta\ (\ V^z y_k + S^z g_{k-1} + a^z)\ \} \qquad (6)$$

$$\widetilde{g_k} = \{\ \delta\ (V^g y_k + S_k \odot (S^g g_{k-1}\ ) + a^g))\quad \} \qquad (7)$$

$$g_k = \{\ z_k \odot g_{k-1} + (1- z_k) \odot \widetilde{g_k}\qquad \} \qquad (8)$$

s_k, z_k and g_k are the update, reset and hidden states correspondingly.

$$F = -\sum_{m=1}^{M} \| K_m \log \widehat{K_m} + (1- K_m) \log (\ 1 - \widehat{K_m})\ \| \qquad (9)$$

$$\widehat{K_m} = (1 + \exp (-U))^{-1} \qquad (10)$$

Bidirectional GRU with weighted feature averaging

The bidirectional recurrent process operates in two directions, such as backward and forward directions includes two hidden layers. The function of the hidden layer is to capture the past and future context together. The property of bi-directional method can emphasize the memory at initial and final stages of input raw time-series. The complete hidden component is represented at the final step is the output concatenated vector of the forward and backward process, which can be considered as the raw sensor signal. Moreover, the information in the middle range of sequence that might be lost in the bidirectional gated recurrent unit. Hence the weighted feature average is to give another view of selected features which indicates the novelty of this study. The equations are expressed as,

$$g_L = \overrightarrow{g_L} \oplus \overleftarrow{g_1} \qquad (11)$$

g^L rept hidden elements

$\rightarrow rept\ forward\ process$

$\leftarrow$ rept backward process

$$\overrightarrow{g_l} = \vec{G}\ (\ y_l\ ,\ \overrightarrow{g_{l-1}}\ ) \qquad (12)$$

$$\overleftarrow{g_l}\ = \overleftarrow{G}\ (y_l\ ,\ \overleftarrow{g_{l+1}}\ ) \qquad (13)$$

The Gis defined by the following equation

$$z_l = \sigma\ \{\ (V^z\ y_l\ ) + (W^z\ g_{l-1}\ ) + (a^z\ )\} \qquad (14)$$

$$s_l = \{\ (V^s\ y_l\ ) + (W^s\ g_{l-1}\ ) + (a^s)\} \qquad (15)$$

$$\widetilde{g_l} = \tan g\ \{(\ V^e y_l\ ) + (W^e (s_l \odot g_{l-1}))\} \qquad (16)$$

$V \in S^{c \times t}$, $W \in S^{c \times c}$

$\odot$ Represents as element wise operator

t = hyperparameter represents as dimensionality of hidden vector

e = local feature

$$\bar{e} = \sum_{t=1}^{L} v_t \, e_t \quad (17)$$

T denote index for time step

To highlight impact of middle local features, weight are designed as

$$V_t = \frac{\exp(p(t))}{\sum_{i=1}^{L} \exp(p(i))} \quad (18)$$

Where p(t) = min(t-1, L-t) (19)

$$O = \{ g_L \oplus E_l (\bar{e}) \} \quad (20)$$

$$Q \left(\frac{\bar{x}=i}{E_2(o)}\right) = \frac{d^{E_2(o)^L v_i}}{\sum_{t=1}^{T} d^{E_2(o)^L v_t}} \quad (21)$$

T no of labels

V parameter of softmax layer

Supervised learning layer can be linear regression layer given by

$$\bar{x} = VE_2(o) + a \quad (22)$$

H. Predict Attacks in Network

From the obtained value, it predicts the type of attacks such as TCP-SYN, UDP flood, ICMP echo, HTTP flood, Slow Loris, Slow Post and Brute Force attacks. The experimental values are collected and compared with the attack based on its obtained weighted average values. So analyzing the characteristics of attack and computing the weight average and comparing with estimated values, it can be detected and classified the types of attacks by using the well-trained SNMP-MIB dataset.

I. Performance metrics (Accuracy, Detection Rate, Precision, Recall)

The performance metrics such as accuracy, detection rate, precision, recall of the proposed method is calculated and explained briefly in the upcoming section, and obtained results are compared with the existing techniques to prove the efficacy of the proposed technique.

IV. RESULTS AND DISCUSSION

The experimental analysis is performed by using SNMP-MIB dataset and compared with various existing methods. The value of accuracy, precision, recall and F-Measure is calculated for different types of attacks in the proposed method. In the detection of an attack, the proposed method gives a high recognition rate and also provide increased accuracy in classifying different types of attacks[24].

- Accuracy is computed to analyze the performance and efficiency of the proposed system. It is calculated by finding the ratio of summation of true positive and real negative to the summation of total positive and negative values.
- Detection rate is defined as calculating the total number of correctly detected attack by the total number of mentioned attacks.
- Precision is a significant performance metrics evaluated to find the positively predicted attacks to the total number of a mixture of attacks along with probable values of correct or wrong identification attacks
- The recall is referred to as sensitivity of a proposed method which is the ratio of the total quantity of related instances are truly associated instances.
- F-Measure is used to test the accuracy of the proposed technique by computing the weighted harmonic mean of tested standards of precision and recall.

The performance metrics of the proposed method is high in detection and classification of various types of attacks is explained in table.1, and the comparison of multiple attacks is illustrated in the fig.2

Table.1 Performance Metrics in the detection of attacks by the GRU-BWFA.

	TCP - SYN	UDP Flood	ICMP ECHO	HTTP Flood	Slow Loris	Slow post	Brute force
Accuracy	1	1	1	0.9	0.98	0.98	1
Precision	1	1	0.98	1	0	1	1
recall	1	1	1	0.98	0.95	0.9	0.91
F-Measure	1	1	1	0.92	0.9	0.9	1

From the table.1, it is shown that, the value of the performance metrics in the detection of attacks such as TCP-SYN, UDP flood, ICMP-echo, HTTP flood, Slow Loris, Slow Post and Brute force. The proposed techniques is efficient in detecting the attacks since higher accuracy is obtained. But in case of slow post, the precision value is higher where it detect various types of malware occurred in the system. Since the value of precision is high in identifying the different types of attack, and thus the loss in network is avoided.

The value of recall is high in TCP-SYN, UDP flood, ICMP-echo and Brute force which can be able to classify the affected systems precisely. But in HTTP flood, Slow Loris and Slow post, recall is low, but the F-measure is high which at least can identify the various attacks in the system.

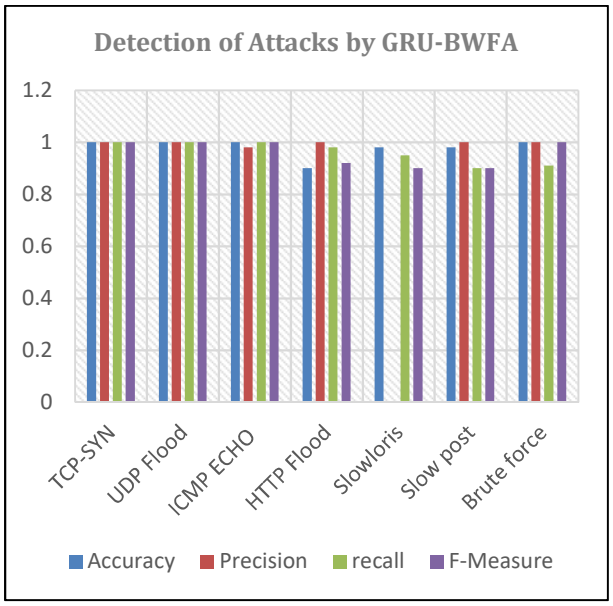

Fig.2. Performance metrics in detection and classification of attacks

The performance metrics for the proposed method in the detection and classification of attacks is shown in fig.2. From the fig.2, it is shown that the in the detection of TCP-SYN, UDP-flood and ICMP-echo the values of accuracy, precision, recall and F-measure are high which signifies the correct classification of attacks which can be used to get the optimal solution for the recovery of the network. In the detection of HTTP flood, the value of precision is high when compared to other performance metrics which at least indicate the presence of attack in the system. In slow Loris and slow post, there is the only average value of accuracy, f-measure and recall, which identifies the attack in system.

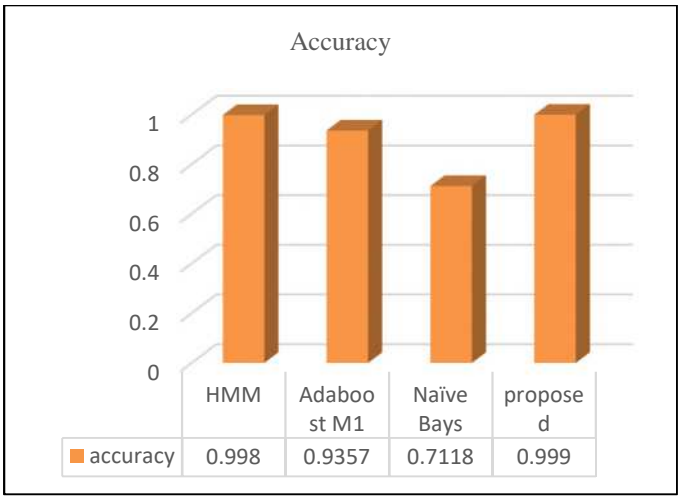

Fig.3. Comparison of Accuracy by different methods [25]

From the fig.3, the comparison of accuracy by the different existing method and proposed method is shown. The proposed method, GRU-BWFA outperforms the existing process by achieving an efficiency of 99.99%.

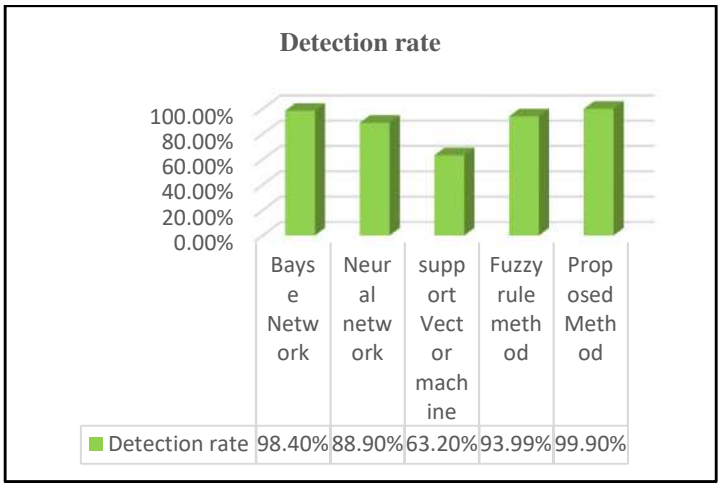

Fig.4. Comparison of detection rate by different methods[26]

From the fig.4, the comparison of detection rate by the different existing method and the proposed method is shown. The proposed method outperforms the existing process by achieving an accuracy of 99.9%. If the detection rate is minimum, the system may fail to identify the attack spontaneously and system failure is possible and thus detection rate helps in the classification of various types of attacks to take a suitable solution as soon as possible to restore the working of the network. Since our proposed method, gives a high value of detection rate.

Table.2 Confusion Matrix of detection mechanism.

Confusion matrix of an existing detection mechanism[26]			
	Normal tariffs test	Up normal tariffs test	Total no of instances
Total no of instance	350	1648	1998
Up normal tariffs	115	1643	1758
Normal tariffs	235	5	240
Confusion matrix of the proposed detection mechanism, GRU-BWFA			
	Normal tariffs test	Up normal tariffs test	Total no of instances
Total no of instance	350	1648	1998
Up normal tariffs	115	1645	1763
Normal tariffs	235	3	235

The confusion matrix for the proposed and existing system is explained in table.2 which comprises of the total number of instances, normal tariffs test and up normal tariff tests.

From the figure5 and figure 6, it shows that the proposed system GRU-BWFA resulted in higher precision and F-measure value by compared with the existing system such as Lazy.blk, trees.Random forest and meta.Random committee. Thus the proposed system is secure against various attacks.

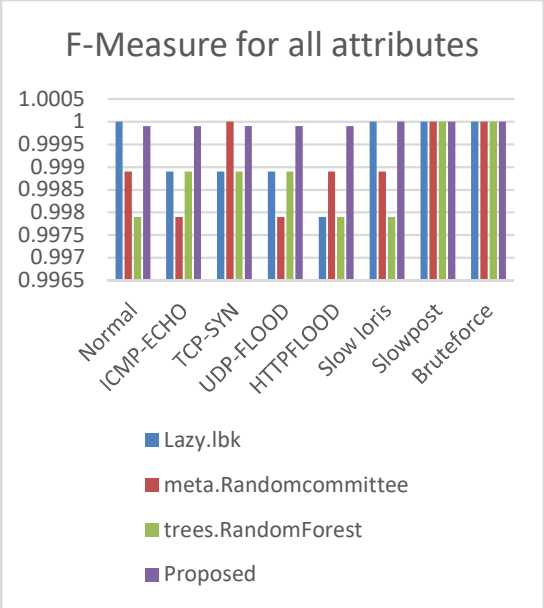

Fig.5. Comparative analysis- F-measure value for all attributes[27]

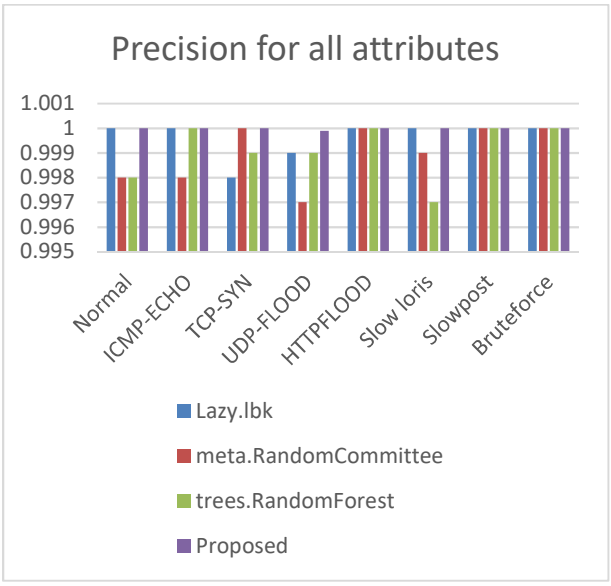

Fig.6. Comparative Analysis- Precision for all attributes[27]

V. CONCLUSION

There are different types of cyber-attacks impacting pervasive computing in recent days. Even though there are many existing methods in detection of attacks there is no reliability in classifying the types of attacks which may lead to false identification and in turn affects its restoring capacity and originality of the network. So the proposed technique with novel Enhanced Salp Swarm Optimization for feature

selection is used to select the optimal features in SNMP-MIB dataset. Once the detection of attack is made, the appropriate classification is made using the proposed classifier, Gated Recurrent Unit Neural Network based on Bidirectional weighted feature averaging. The obtained performance metrics with a value of 99.9% accuracy and detection rate proved that the proposed method outperforms the existing methods in classification and detection of various attacks by effectively training the SNMP-MIB dataset. Hence it is used to identify and eradicate the attack by analyzing its behavioral characteristics. So it helps to isolate the rest of the system from the attack and used to restore the system effectively in minimal time.

CONFLICT OF INTEREST

Dear Editor-in-Chief

- I confirm that this work is original and has not been published elsewhere, nor is it currently under consideration for publication elsewhere. This research work was not funded by any organization/institute/agency. None of the authors have any competing interests in the manuscript.

AUTHOR CONTRIBUTIONS STATEMENT

I Am P. Rajasekaran Hereby State That The Manuscript Title Entitled “Detection Of Attacks In Pervasive Computing Using Gated Recurrent Unit Based On Bidirectional Weighted Feature Averaging” Submitted To Soft Computing, I and my Co-author V. Magudeeswaran Confirm That This Work Is Original And Has Not Been Published Elsewhere, Nor Is It Currently Under Consideration For Publication Elsewhere. And I Am Assistant professor In the Department of ECE at PSNA College of Engineering and Technology, Dindigul and TamilNadu, India.

REFERENCES

[1] A. K. Sharma and M. K. Rewadia, "Security Attacks and Algorithms," *Journal of Software Engineering Tools & Technology Trends,* vol. 5, pp. 22-25, 2019.

[2] N. Papageorgiou, D. Apostolou, Y. Verginadis, A. Tsagkaropoulos, and G. Mentzas, "A Situation Detection Mechanism for Pervasive Computing Infrastructures," in *2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA)*, 2018, pp. 1-8.

[3] M. N. Abdullah and A. M. Al-Chalabi, "Performance Assessment of RSA, ElGamal and Proposed DHOTP for File Security in Pervasive Computing Environment," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 5, 2016.

[4] T. Lemmey and S. Vonog, "Management of data privacy and security in a pervasive computing environment," ed: Google Patents, 2019.

[5] P. Sarkar and D. Sinha, "Application on pervasive computing in healthcare–a review," *Indian Journal of Science and Technology,* vol. 10, 2017.

[6] M. Al-Kasassbeh, G. Al-Naymat, and E. Al-Hawari, "Towards generating realistic SNMP-MIB dataset for network anomaly detection," *International Journal of Computer Science and Information Security,* vol. 14, p. 1162, 2016.

[7] C. Xu, J. Shen, X. Du, and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units," *IEEE Access,* vol. 6, pp. 48697-48707, 2018.

[8] M. H. Ali, B. A. D. Al Mohammed, A. Ismail, and M. F. Zolkipli, "A new intrusion detection system based on fast learning network and particle swarm optimization," *IEEE Access,* vol. 6, pp. 20255-20261, 2018.

[9] R. Nakamura, Y. Sekiya, D. Miyamoto, K. Okada, and T. Ishihara, "Malicious Host Detection by Imaging SYN Packets and A Neural Network," in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*, 2018, pp. 1-4.

[10] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing,* vol. 172, pp. 385-393, 2016.

[11] G. D’Angelo, S. Rampone, and F. Palmieri, "Developing a trust model for pervasive computing based on Apriori association rules learning and Bayesian classification," *Soft Computing,* vol. 21, pp. 6297-6315, 2017.

[12] G. DAngelo, S. Rampone, and F. Palmieri, "An artificial intelligence-based trust model for pervasive computing," in *2015 10th international conference on P2p, parallel, grid, cloud and internet computing (3pgcic)*, 2015, pp. 701-706.

[13] L. Sellami, D. Idoughi, A. Baadache, and P. Tiako, "A novel detection intrusion approach for ubiquitous and pervasive environments," *Procedia Computer Science,* vol. 94, pp. 429-434, 2016.

[14] H. Yang and F. Wang, "Wireless network intrusion detection based on improved convolutional neural network," *IEEE Access,* vol. 7, pp. 64366-64374, 2019.

[15] M. Abedin, K. N. E. A. Siddiquee, M. Bhuyan, R. Karim, M. S. Hossain, and K. Andersson, "Performance analysis of anomaly based network intrusion detection systems," in *43nd IEEE Conference on Local Computer Networks Workshops (LCN Workshops), Chicago, October 1-4, 2018*, 2018, pp. 1-7.

[16] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Networking Letters,* vol. 1, pp. 68-71, 2019.

[17] J. Lv, D. Man, W. Yang, X. Du, and M. Yu, "Robust WLAN-based indoor intrusion detection using PHY layer information," *IEEE Access,* vol. 6, pp. 30117-30127, 2017.

[18] P. Mukherjee and A. Mukherjee, "Advanced processing techniques and secure architecture for sensor networks in ubiquitous healthcare systems," in *Sensors for Health Monitoring*, ed: Elsevier, 2019, pp. 3-29.

[19] S. Monicka, C. Suganya, S. N. Bharathi, and A. Sindhu, "A ubiquitous based system for health care monitoring," *International Journal of Scientific Research Engineering & Technology (IJSRET),* vol. 3, pp. 2278-0882, 2014.

[20] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Computers & Security,* vol. 86, pp. 147-167, 2019.

[21] S. Dutta, S. Ghatak, A. K. Das, M. Gupta, and S. Dasgupta, "Feature selection-based clustering on micro-blogging data," in *Computational Intelligence in Data Mining*, ed: Springer, 2019, pp. 885-895.

[22] S. Mirjalili, A. H. Gandomi, S. Z. Mirjalili, S. Saremi, H. Faris, and S. M. Mirjalili, "Salp Swarm Algorithm: A bio-inspired optimizer for engineering design problems," *Advances in Engineering Software,* vol. 114, pp. 163-191, 2017.

[23] Y. Xu, Q. Kong, Q. Huang, W. Wang, and M. D. Plumbley, "Convolutional gated recurrent neural network incorporating spatial features for audio tagging," in *2017 International Joint Conference on Neural Networks (IJCNN)*, 2017, pp. 3461-3466.

[24] M. Alkasassbeh, "A novel hybrid method for network anomaly detection based on traffic prediction and change point detection," *arXiv preprint arXiv:1801.05309,* 2018.

[25] S. Alhaidari, A. Alharbi, M. Alshaikhsaleh, M. Zohdy, and D. Debnath, "Network traffic anomaly detection based on Viterbi algorithm using SNMP MIB data," in *Proceedings of the 2019 3rd International Conference on Information System and Data Mining*, 2019, pp. 92-97.

[26] M. Almseidin, M. Alkasassbeh, and S. Kovacs, "Fuzzy rule interpolation and snmp-mib for emerging network abnormality," *arXiv preprint arXiv:1811.08954,* 2018.

[27] G. Al-Naymat, A. Hambouz, and M. Al-Kasassbeh, "Evaluating the Impact of Feature Selection Methods on SNMP-MIB Interface Parameters to Accurately Detect Network Anomalies," in *2019 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 2019, pp. 1-6.