Radial Basis Kernel Regressive Feature Extraction and Robert Ensembled Brown Boost Classifier for Attack Detection in Cloud Environment

K. Padmaja*
Department of Computer Science and Engineering, Sri Venkateswara University, Tirupati, Andhra Pradesh, India.
E-mail: padmajaskrishna@gmail.com

R. Seshadri
Department of Computer Science and Engineering, Sri Venkateswara University, Tirupati, Andhra Pradesh, India.

Received March 06, 2021; Accepted July 02, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18I2/WEB18306

Abstract

Cloud computing shares the resource in information technology field. The existing technique is failed to provide better results for identifying unknown attacks with higher accuracy and lesser time consumption. In order to address these problems, Radial Basis Kernel Regressive Feature Extracted Brown Boost Classification (RBKRFEBBC) method is introduced for performing the attack detection in cloud computing. The main objective of RBKRFEBBC method is to improve the attack detection performance with higher accuracy and minimal time consumption. Dichotomous radial basis kernelized regressive function is used in RBKRFEBBC method to extract the relevant features through determining the correlation between the output and one or more input variables (i.e., features of patient transaction data). After extracting relevant features, GRNBBC algorithm is used in RBKRFEBBC method to improve the secured data communication performance through classifying the patient data transaction as attack presence or attack absence. By this way, attack detection is carried out in accurate manner. Experimental evaluation is carried out by NSL-KDD dataset using different metrics like attack detection accuracy, attack detection time and error rate. The evaluation result shows RBKRFEBBC method improves the accuracy and minimizes the time consumption as well as error rate than existing works.

Keywords

Cloud Computing, Intrusion Detection System, Attack Detection, Machine Learning, Radial Basis Kernelized Regressive Function, Network Administrators.

Introduction

Cloud computing deliver the services from one application to storage server through internet connection. Cloud security denotes collection of policies and technologies used to protect virtualized IP, data, services and infrastructure. Many techniques were introduced to perform the secured communication through performing the attack detection process. A rule based approach was introduced in (Rakesh Rajendran, et al., 2019) for attack detection with better knowledge. However, the attack detection accuracy was not improved. A voting extreme learning machine (V-ELM) was introduced in (Gopal S. K. & V Ranga, 2020) for identifying the DDoS attacks in cloud environment. But, the time consumption was not minimized.

A DDoS attack detection was carried out in (Mohamed Idhammad, et al., 2018) depending on ensemble learning algorithm. But, the error rate was not minimized. DDoS attack detection was carried out in (Karan B. Virupakshar, et al., 2020) through bandwidth flooding and connection flooding process. However, the attack presence was not accurately detected. An online cloud anomaly detection approach was introduced in (Michael R. Watson, et al., 2016) with detection components. However, the computational cost was not minimized.

An intrusion detection approach was introduced in (Adnan Rawashdeh, et al., 2018) based on attack activities among virtual machines. But, the anomaly intrusion detection complexity was not minimized. An intrusion detection model was introduced in (Wang Yichuan, et al., 2015) for reduce the internal attack threat of cloud cluster. But, the accuracy was not improved. A secure data transmission was carried out in (Deevi Radha Rani and G. Geethakumari, 2020) for early detection of Anti-Forensic Attack (AFA). However, time complexity was not improved.

An efficient approach was designed in (Kriti Bhushan and B. B. Gupta, 2018) to detect the existence of attack in cloud. But, the complexity was not minimized. An efficient fuzzy and taylor-elephant herd optimization (FT-EHO) was introduced in (S. Velliangiri and Hari Mohan Pandey, 2020) with deep belief network (DBN) classifier for identifying the DDoS attack. But, the attack detection was not carried out in accurate manner.

Motivation

Attack prediction is a key problem in cloud computing. Machine learning algorithms and ensemble methods are used to detect the attack during the data communication. Cloud security is a demanding process because it is an integral part of cloud service. Distributed denial of service attack is the most risky attacks in the cloud computing. Many conventional methods were introduced a few limitations such as higher time consumption, lesser attack detection accuracy, higher error rate, higher computational cost, and higher complexity. These types of issues are overcome and motivated by the RBKRFEBBC method is introduced for obtaining secure data communication during attack detection performance via secured data communication with maximum accuracy and minimum time consumption. Dichotomous radial basis kernelized regressive function is used to extract the features as relevant or irrelevant for diminishing the attack detection time. Generalized Recurrent Neural Brown Boosting Classifier (GRNBBC) algorithm is applied to categorize the data transaction as attack presence or attack absence for enhancing the detection accuracy with minimum error rate.

Objective of the Research Works

The main objective of the research work described as follows,

- To perform attack detection through secured data communication in the cloud as compared to state-of-the-art works, the RBKRFEBBC method is proposed.
- To determine the relevant features with lesser attack detection time as compared to state-of-the-art works, a dichotomous radial basis kernelized regressive function is introduced.
- To enhance the attack detection accuracy and reduce the error rate as compared to state-of-the-art works, a GRNBBC algorithm is introduced for classifying the data as attack presence or attack absence.

Contributions

The major contribution of the proposed RBKRFEBBC method is listed as,

- Radial Basis Kernel Regressive Feature Extracted Brown Boost Classification (RBKRFEBBC) method is introduced for performing the attack detection in cloud computing with higher accuracy and minimal time consumption. RBKRFEBBC method is designed with the novelty of dichotomous radial basis kernelized regressive function and Generalized Recurrent Neural Brown Boosting Classifier (GRNBBC) algorithm.

- Proposed RBKRFEBBC method uses the Dichotomous radial basis kernelized regressive function to extract the relevant features through determining the correlation between the output and one or more input variables. The dichotomous radial basis kernel regression function is used to give the output values in the range of ‘0’ and ‘1’. The threshold is assigned to classify the given input into dissimilar classes. If the value is greater than 0.5, then the feature is categorized into a relevant class. Otherwise, it is said to be an irrelevant feature. Then, each feature is classified into a particular class. This helps in minimizing the time consumption for attack detection.
- Proposed RBKRFEBBC method introduces the GRNBBC algorithm to improve the secured data communication performance through classifying the patient data transaction as attack presence or attack absence. GRNBBC algorithm helps to improve the accuracy and reduce the error rate.
- Robert Similarity-based Recurrent Neural Network (RS-RNN) used in GRNBBC algorithm. Robert similarity function is used to measure the similarity value among the training and testing feature value of patient transaction data. Robert similarity function introduces the similarity value among ‘0’ to ‘0.5’, then patient transaction data is said to be attack absence. If the similarity value among ‘0.5’ to ‘1’, then the patient transaction data is said to be attack presence.
- Brownboost classifier is applied in the GRNBBC algorithm for achieving the strong classifier result by combining each weak classifier result. The classification process is used to accurately classify each patient transaction data into two different classes. The positive margin is said to attack presence data. The negative margin is said to be attack absence.
- The paper is outlined into five different sections. In section 2, related works in the attack detection techniques are discussed. Section 3 portrays the proposed RBKRFEBBC method in brief manner with architectural diagram. In section 4, experimental settings are listed with detailed dataset description. Section 5 describes the results analysis for three different metrics. Section 6 concludes the paper.

Related Works

A new ensemble technique was introduced in (Daniel T. Ramotsoela, et al., 2019) to combine the parametric algorithm in application atmosphere. But, the time consumption was not minimized. A new mechanism was introduced in (Abdelmadjid Benarfa, et al., 2020) for attack detection and mitigation through minimizing memory consumption and traffic. But, the error rate was not reduced through minimizing the traffic.

An attack detection and mitigation model was introduced in (Nitesh Bharot, et al., 2018) with feature selection process. But, the computational cost was not minimized during attack detection. The network traffic characteristics were analyzed in (Dan Tang, et al., 2020) with variance and entropy to determine TCP characteristics. However, the error rate remained unaddressed.

A DDoS attack detection was carried out in (Bin Jia, et al., 2017) with hybrid heterogeneous multi-classifier ensemble learning model. But, the computational cost was not minimized. A new auditory filter-based relative phase (RP) features were employed in (Zeyan Oo, et al., 2019) for replay attack detection. But, the attack detection performance was not improved.

A cloud based trust management scheme (CbTMS) was introduced in Shih-Hao Chang and Zhi-Rong Chen, 2016) to identify the Sybil attacks. But, the attack detection accuracy was not improved. A valued feature was employed in (Abdulaziz Aborujilah and Shahrulniza Musa, 2017) with cloud-based websites. Covariance matrix approach was employed to identify the attacks. But, the complexity level was not reduced.

Optimisation based Deep learning was introduced in (S. Velliangiri, et al., 2020) with Taylor series for DDoS attack detection. Different DDoS attacks with defense mechanism were studied in (Neha Agrawal and Shashikala Tapaswi, 2019) to preserve the cloud infrastructure. But, the taxonomy of possible variants of cloud DDoS attacks solutions was not performed in efficient manner.

Proposed Methodology

In this section, proposed Radial Basis Kernel Regressive Feature Extracted Brown Boost Classification (RBKRFEBBC) method is introduced for attack detection in cloud environment. The architecture diagram of RBKRFEBBC method is described in figure 1.

Figure 1 explains the architecture diagram of RBKRFEBBC method. Initially, patient transaction data is collected from the dataset. Then, the relevant features are extracted from the dataset for performing the attack detection during secured communication. After that, the patient transaction data get classified into attack presence data and attack absence data. The brief explanation of feature extraction and classification is given below.

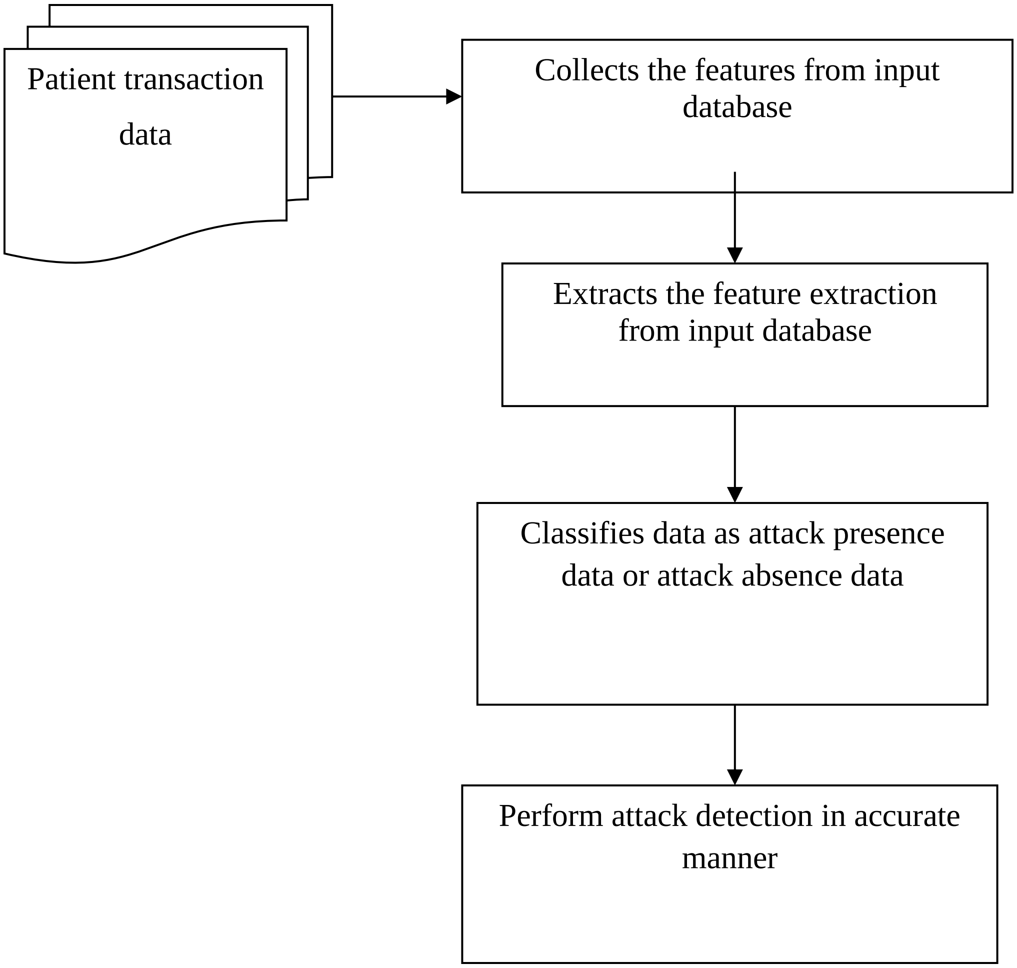
Patient transaction data
Collects the features from input database
Extracts the feature extraction from input database
Classifies data as attack presence data or attack absence data
Perform attack detection in accurate manner

Figure 1 Architecture Diagram of RBKRFEBBC method

Radial Basis Kernel Regressive Feature Extracted Brown Boost Classification

In smart healthcare application, security is the key role for providing the better and effective health facilities to the patients. The proposed system collects the patient health status and send to the server (i.e., hospitals) through the internet.

Figure 2 portrays the structure of attack detection in cloud environment. The proposed RBKRFEBBC technique collects the patient's data for performing the disease diagnosis. After that, the collected information is sent to the cloud server through the internet for further processing. During the data transmission, security needs to be assured through preventing from attackers. In order to achieve secure communication through attack prediction, the proposed RBKRFEBBC technique performs the two different processes, namely feature extraction and classification.

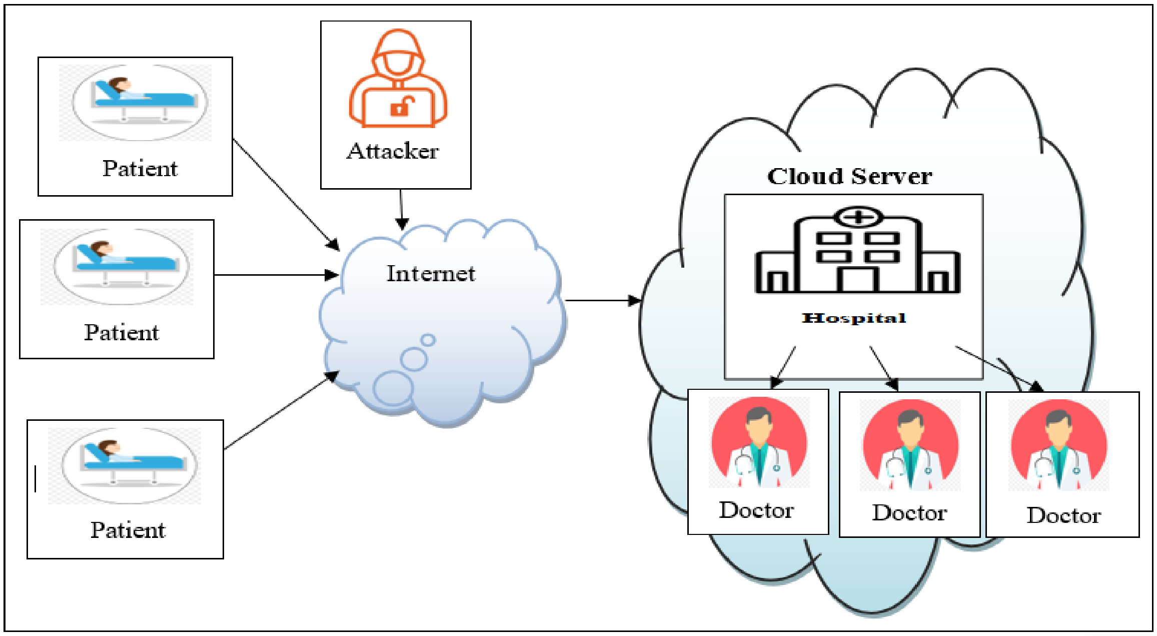

Figure 2 Attack Detection in Cloud Environment

- ### Dichotomous Radial Basis Kernelized Regressive Function

The proposed RBKRFEBBC technique performs the feature extraction through the dichotomous radial basis kernelized regressive function. The dichotomous regression function determines the relationship between dependent variable (i.e., relevant feature and irrelevant feature) and one or more independent variables (i.e. features of patient transaction data). Let us consider, the number of patient transaction data collected is denoted as $ptd_1, ptd_2, ptd_3, \ldots\ldots ptd_n$. The features of each patient transaction data is represented as $fe_1, fe_2, fe_3, \ldots\ldots fe_m$. After that, the dichotomous radial basis kernelized regression function examines the input for categorizing into two output classes.

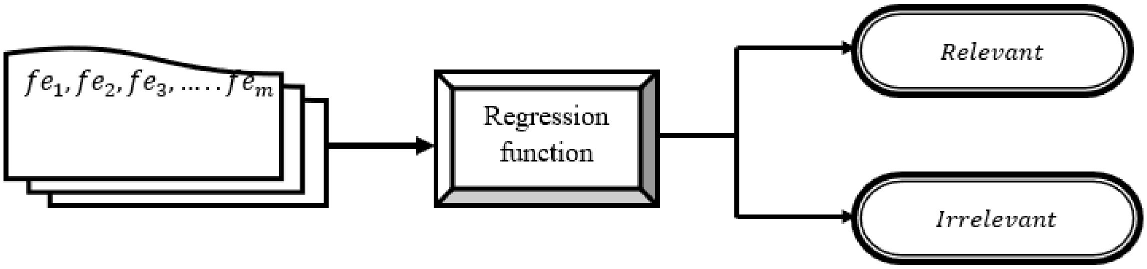

Figure 3 Dichotomous Radial Basis Kernel Regression Function

Figure 3 describes the dichotomous radial basis kernel regression function to analyze the features of input patient transaction data. After that, the designed function get classified into two classes for identifying which set of categories it belongs to. For each class, the mean value 'μ_r and μ_i' is allocated to identify similar data. It is given by,

$$\mu_r \text{ and } \mu_i \rightarrow relevant\ class\ and\ irrelevant\ class \qquad (1)$$

From equation (1), the mean value of both classes is determined. The dichotomous radial basis kernel regression analysis between the input and output is formulated as,

$$DRBKRF = exp\left[-\frac{(fe_i-\mu_j)^2}{2D^2}\right] \tag{2}$$

From equation (2), '$DRBKRF$' symbolizes the dichotomous radial basis kernel regression function. 'fe_i' denotes features of patient transaction data. 'μ_r and μ_i' denotes the mean of two classes (i.e., relevant and irrelevant). 'D' symbolizes the deviation from mean value. The kernel function analysis is used to identify the data near the mean value and classified into particular class. The dichotomous radial basis kernel regression function provides the output values in range from '0' and '1'. After that, the threshold is predefined to categorize the given input into different classes. When the obtained value is greater than 0.5, then feature is classified into relevant class. Otherwise, the features of patient transaction data are irrelevant feature. In this way, all the features are categorized into particular class. Therefore, the radial basis kernel regression analysis reduces the attack detection time during secure data transmission. The algorithmic process of dichotomous radial basis kernel regression function is given below,

```
\\ Algorithm 1 Dichotomous Radial Basis Kernel Regression Function
Input: Dataset, patient transaction data 'patient transaction data '$\boldsymbol{ptd_1, ptd_2, ptd_3, \ldots\ldots ptd_n}$, features '$fe_1, fe_2, fe_3, \ldots\ldots fe_m$'
Output: Improve feature extraction performance
Step 1: Begin
Step 2: Collect the patient transaction data with their features
Step 3: Initialize number of classes '$\boldsymbol{C_1 and\ C_2}$'
Step 4: For each class
Step 5: Assign mean value '$\mu_1$ and $\mu_2$'
Step 6: Perform regression analysis
Step 7: If ($DRBKRF > 0.5$) then
Step 8: Classify the feature into particular class
Step 9: End if
Step 10: End for
Step 11: End
```

Algorithm 1 explains the dichotomous radial basis kernel regression function process. Initially, the number of features from patient transaction data is considered as input and number of classes are initialized. After that, the mean value of each class is determined and assigned. Then, the regression analysis is carried out to identify the feature as relevant feature or irrelevant feature. Finally, the relevant feature of patient transaction data is considered for performing the classification process. The brief explanation of classification is explained in next sub-section.

- **Generalized Recurrent Neural Brown Boosting Classifier**

In RBKRFEBBC technique, Generalized Recurrent Neural Brown Boosting Classifier (GRNBBC) algorithm is introduced to improve the performance through classifying the patient data transaction as attack presence or attack absence. GRNBBC algorithm is introduced through applying brown boosting ideas in weak learners. GRNBBC algorithm considers the Robert Similarity based Recurrent Neural Network (RS-RNN) as the weak learner. The weak RS-RNN is a supervised learning binary classifier. In weak RS-RNN classifier, neurons discover the elements in the training set (i.e., relevant features of patient transaction data) at a time. The weak RS-RNN classifier learns the weight for input patient transaction data to determine the linear decision boundary that distinguishes into two classes. In weak RS-RNN classifier, the input relevant features of patient transaction data are then multiplied with weights to classify the patient data transaction into attack presence or attack absence. The weak RS-RNN classifier is not at the required level. GRNBBC algorithm constructs the 'n' number of weak RS-RNN classifier results for every input patient transaction data. Finally, the weak RS-RNN classifier results are combined to obtain strong classifier result. The process of GRNBBC algorithm is given in below figure 2.

Figure 4 illustrates the process of RS-RNN algorithm to enhance attack detection accuracy for performing the secured data communication. As described in above figure, GRNBBC algorithm initially collects the number of patient transaction data with relevant features. After taking the input, GRNBBC algorithm constructs 'n' number of weak RS-RNN classifier for each input patient transaction data. The weak RS-RNN algorithm comprises the three layers, namely one input layer, one hidden layer and one output layer for performing attack detection process.

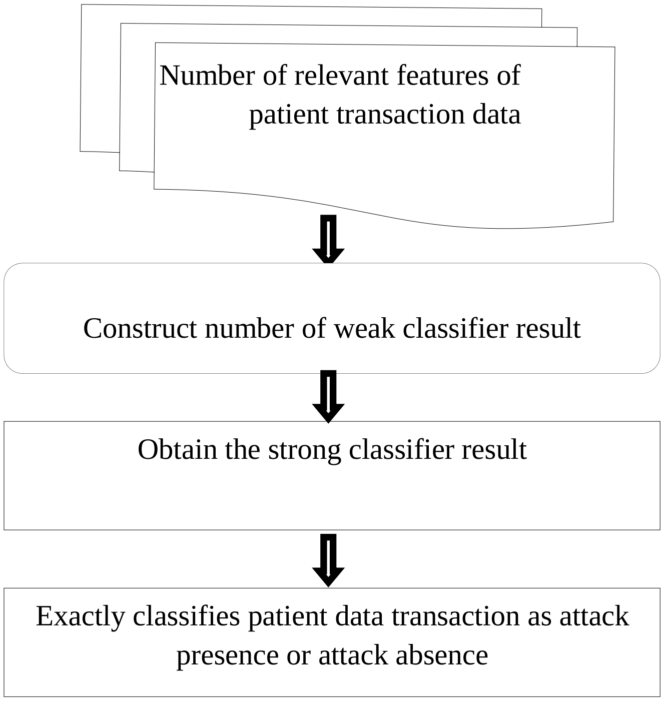
Number of relevant features of patient transaction data
Construct number of weak classifier result
Obtain the strong classifier result
Exactly classifies patient data transaction as attack presence or attack absence

Figure 4 Flow Process of Robert Similarity based Brown Boosting Classifier

Input Layer: The relevant features of patient transaction data are considered as input for weak RS-BBC algorithm. The input of a RS-RNN algorithm is represented as '$ptd_1, ptd_2, ptd_3, \ldots\ldots ptd_n$' where 'n' represents the total number of patient transaction data. In input layer, the weight and bias are used. At the starting stage, the weight is initialized with some initial value and gets updated for every training error. The weights for weak RS-RNN are represented by '$w_{initial}, w_{\mathrm{ih}}, and\ w_{\mathrm{ho}}$'. A bias neuron allows the weak RS-RNN classifier to find the decision boundary to partition into attack presence and attack absence based on input patient transaction data. Bias helps to train the weak RS-RNN algorithm faster and with better quality. The input layer result is obtained as,

$$I(t) = \sum_{i=1}^{n} ptd_i(t)\ w_{initial} + bias \qquad (3)$$

From equation (3), 'ptd_i' denotes the patient transaction data with relevant feature. '$w_{initial}$' symbolizes the initial weight assigned at the input layer. After that, the input layer result is sent to the hidden layer.

Hidden layer: In the hidden layer, an activation function is used to identify the classification results for each patient transaction data. Activation function in weak RS-RNN classifier used Robert similarity measurement to separate information in an input dataset into a two classes (i.e., attack presence or attack presence) based on the patient transaction data. Robert similarity analysis computed the similarity value between the training feature value of patient transaction data 'X_i' and attacker testing feature value 'Y_i' in given dataset using formula,

$$RS(X_i, Y_i) = \frac{\sum_i (X_i, Y_i) \frac{\min(X_i, Y_i)}{\max(X_i, Y_i)}}{\sum_i (X_i, Y_i)} \qquad (4)$$

From equation (4), 'min' and 'max' symbolizes the pointwise operators. '$RS(X_i, Y_i)$' denotes the Robert similarity function. When similarity value lies between '0' to '0.5', then patient transaction data is considered as attack absence. When the similarity value lies between '0.5' to '1', then the patient transaction data is considered as attack presence. The result obtained at the hidden layer is formulated as,

$$H(t) = \sum_{i=1}^{n} I(t)\ * w_{initial} + [w_{ih} * RS(X_i, Y_i)] \qquad (5)$$

From equation (5), '$H(t)$' denotes the hidden layer result. 'w_{ih}' symbolizes the weight assigned between the input layer and hidden layer. After that, the result of the hidden layer is feedback to the input layer for attaining the accurate results with minimum error. The hidden layer results are transmitted to an output layer.

Output Layer: An output unit in weak RS-RNN classifier renders the classification output for each input patient transaction data. The weak RS-RNN classifier finds the related information for each patient transaction data. The result of output layer is given as,

$$O(t) = w_{ho} * H(t) \qquad (6)$$

From equation (6), '$O(t)$' represent the output layer result. 'w_{ho}' denotes the weight assigned between the hidden layer and output layer. But, classification accuracy was not satisfactory to detect the attackers with minimal time complexity. Therefore, Brownboost classifier is used in GRNBBC algorithm. The GRNBBC algorithm obtains the strong classifier result through combining all weak classifier results using following expression,

$$Strong\ classifier = \sum_{i=1}^{n} O(t)\{ptd_i\} \qquad (7)$$

From equation (7) '$O(t)_i(ptd_i)$' represents the weak classifier output for each patient transaction data 'ptd_i'. After that, GRNBBC algorithm provides the weight to every weak classifier consistent with the residual time after classification and margin of the information. In GRNBBC algorithm, a positive margin represents the patient transaction data is considered as attack presence data whereas the negative margin denotes the patient transaction data is attack absence. Consequently, the magnitude of margin value shows that how much the weak RS-RNN classifier categorizes the patient transaction data into particular class in more accurate manner. In GRNBBC algorithm, weight value is assigned for every weak RS-RNN classifier based on the time consumed to classify the patient transaction data. The, weight of weak RS-RNN classifier is determined as,

$$V_j = \exp\left(-\frac{\left(ma_j(ptd_i)+t\right)^2}{r}\right) \qquad (8)$$

From equation (8), 'V_i' denotes the weight allocated to the weak classifier at iteration 'j'. 'ma_j' represent the margin of the information for patient transaction data. 't' represents the time consumed for processing and 'r' indicates the residual time of weak classifier. Then, the probable loss for every classified patient transaction data with margin 'ma_j' is determined as,

$$PL = 1 - \varepsilon rror\sqrt{x} \qquad (9)$$

From equation (9), 'PL' indicates the probable loss of function and 'x' represents the positive real value. Consequently, margin of the each weak RS-RNN classifier is updated based on the loss value using mathematical equation,

$$ma_j(t+1) = ma_j(ptd_i) + \sum_{i=1}^{n} V_j\, O(t)\{ptd_i\}Y_i \qquad (10)$$

From the equation (5) '$ma_i(t+1)$' denotes the updated margin of the input patient transaction data, 'Y_i' symbolizes the actual output of the weak classifier. As a result, the strong classifier result is determined as,

$$Strong\ classifier\ result = sign\left\{\sum_{i=1}^{n} V_j\, O(t)\{ptd_i\}\right\} (11)$$

From equation (11), the final strong classification results are obtained. By designing the strong classifier, the proposed RBKRFEBBC method correctly classifies all the patient transaction data into corresponding class with higher accuracy and lesser time consumption. The algorithmic process of Generalized Recurrent Neural Brown Boosting Classifier is shown in below, Algorithm 2 explains the step by step process of Generalized Recurrent Neural Brown Boosting Classifier Algorithm. With help of the above algorithmic process, RBKRFEBBC method achieves better attack detection performance through classification when compared to conventional works.

```
/ Generalized Recurrent Neural Brown Boosting Classifier Algorithm
Input: Number of patient transaction data with relevant features
Output: Improve attack detection accuracy with minimal time consumption
Step 1:Begin
Step 2: For each input patient transaction data '$ptd_i$'
    Step 3: Construct 'n' number of weak classifier
    Step 4: Ensemble all weak classifier results
    Step 5: Set margin value '$ma_i\ (ptd_i) = 0$'
    Step 6: For each weak classifier result '$O(t)(ptd_i)$'
        Step 7: Assign the weight ' $V_j$'
        Step 8: Determine the probable loss '$PL$'
        Step 9: Update margin '$ma_j\ (t + 1)$'
        Step 10: Obtain strong classification results
    Step 11: End for
Step 12: End for
Step 13:End
```

Algorithm 2 Generalized Recurrent Neural Brown Boosting Classifier

Experimental Settings

Experimental evaluation of proposed RBKRFEBBC method and existing methods namely rule based approach (Rakesh Rajendran, et al., 2019) and voting extreme learning machine (V-ELM) (Gopal S. K. & V Ranga, 2020) are implemented using Java language with help of NETBEANS8.2 IDE tool. The experiments of RBKRFEBBC method is conducted using NSL-KDD dataset taken from https://www.kaggle.com/hassan06/nslkdd/version/1.This dataset is an development of KDD'99 dataset where the duplicate instances gets removed and improved the classification results. The dataset comprises the 42 attributes. The dataset has different files includes the training and testing with various instances. Every instance in the dataset is considered as the patient transaction data. The attributes are termed as class attributes that represent given instance is normal instance or attack instance. Among the different attributes, relevant attribute are selected to perform the classification for attack detection. Performance analysis of RBKRFEBBC method are compared with existing results with certain parameters listed below,

- Attack detection accuracy
- Attack detection time
- Error Rate

Results and Discussions

In this section, results of proposed RBKRFEBBC method and two existing methods namely rule based approach (Rakesh Rajendran, et al., 2019) and voting extreme learning machine (V-ELM) (Gopal S. K. & V Ranga, 2020) are analyzed. The description of different metrics such as attack detection accuracy, attack detection time and error rate are presented with number of patient transaction data to show the improved performance analysis of the proposed RBKRFEBBC method. The three parameters are evaluated with table and graphs.

Performance Analysis of Attack Detection Accuracy

Attack detection accuracy is defined as ratio of the number of patient transaction data that are correctly classified as attack presence or attack absence data to the total number of patient transaction data taken. Attack detection accuracy is formulated as,

$$ADA = \left(\frac{Correctly\ classified\ N_{apa}\ as\ attack\ presence\ or\ attack\ absence\ data}{N}\right) * 100 \quad (12)$$

From equation (12), 'ADA' represents the attack detection accuracy. 'N_{apa}' denotes the number of patient transaction data. 'N' denotes the total number of patient transaction data. It is measured in terms of percentage (%).

Table 1 Tabulation for Attack Detection Accuracy

Number of patient transaction data	**Attack detection accuracy (%)**		
	RBKRFEBBC method	**Rule based approach**	**V-ELM**
500	94	88	85
1000	92	85	83
1500	90	81	76
2000	89	78	73
2500	91	87	81
3000	93	76	70
3500	94	82	73
4000	92	84	78
4500	92	82	79
5000	93	90	86

Table 1 explains the attack detection accuracy of proposed RBKRFEBBC method and existing Rule based approach (Rakesh Rajendran, et al., 2019) and voting extreme learning machine (V-ELM) (Gopal S.K. & V Ranga, 2020) with a number of patient transaction data taken in the range from 500-5000. Totally ten various results for attack detection time are attained for different number of number of patient transaction data. When considering number of patient transaction data is 2000, the number of patient transaction data that are correctly classified as attack presence or attack absence data by RBKRFEBBC method is 1773 whereas 1564 and 1453 is obtained by existing Rule based approach (Rakesh Rajendran, et al., 2019) and voting V-ELM (Gopal S.K. & V Ranga, 2020) respectively. Therefore, the attack detection accuracy obtained by proposed RBKRFEBBC method, Rule based approach (Rakesh Rajendran, et al., 2019) and voting V-ELM (Gopal S.K. & V Ranga, 2020) are 89%, 78% and 73% respectively. From the table, it is clear that the attack detection accuracy of proposed RBKRFEBBC method is higher when compared to other two existing methods.

This is due to the application of dichotomous radial basis kernelized regressive function and Generalized Recurrent Neural Brown Boosting Classifier (GRNBBC) algorithm. Radial basis kernelized regressive function determines the relationship between the features to identify the relevant features. GRNBBC algorithm classifies the patient data transaction as attack presence or attack absence with help of relevant features. By this way, attack detection is carried out in accurate manner. The average of ten results shows that the of attack detection accuracy is said to be improved using RBKRFEBBC method by 11% compared to Rule based approach (Rakesh Rajendran, et al., 2019) and 18% compared to voting extreme learning machine (V-ELM) (Gopal S. K. & V Ranga, 2020).

Performance Analysis of Attack Detection Time

Attack detection time is defined as an amount of time required to categorize the patient transaction data as attack presence or attack absence data. The attack detection time is determined as,

$$ADT = N * time\ (classifying\ one\ patient\ transaction\ data\ ) \quad (13)$$

From equation (12), 'ADT' represents attack detection time, 'N' denotes the number of patient transaction data. Attack detection time is measured in terms of milliseconds (ms).

Table 2 explains the attack detection time of proposed RBKRFEBBC method and existing Rule based approach (Rakesh Rajendran, et al., 2019) and voting extreme learning machine (V-ELM) (Gopal S.K. & V Ranga, 2020) with different number of patient transaction data taken in the range from 500-5000. In the table, ten various results for attack detection time are listed for considering different number of patient transaction data. Let us consider, number of patient transaction data is 1000. The amount of time consumed for performing the one patient transaction data to detect the attack presence or attack absence by RBKRFEBBC method is 0.013s whereas 0.018s and 0.02s is consumed by existing Rule based approach (Rakesh Rajendran, et al., 2019) and voting V-ELM (Gopal S.K. & V Ranga, 2020) respectively. Thus, the attack detection time obtained by proposed

RBKRFEBBC method, Rule based approach (Rakesh Rajendran, et al., 2019) and voting V-ELM (Gopal S.K. & V Ranga, 2020) are $13ms$, $18ms$ and $20ms$ respectively. From the table, it is observed that the attack detection time of proposed RBKRFEBBC method is lesser when compared to other two existing methods. The graphical result of attack detection time is shown in figure 5.

Table 2 Tabulation for Attack detection time

Number of patient transaction data	Attack detection time (ms)		
	RBKRFEBBC method	Rule based approach	V-ELM
500	10.5	14	16
1000	13	18	20
1500	18	21	25.5
2000	20	26	30
2500	22.5	27.5	32.5
3000	24	30	33
3500	24.5	31.5	36.75
4000	26	32	38
4500	27	33.75	40.5
5000	27.5	35	42.5

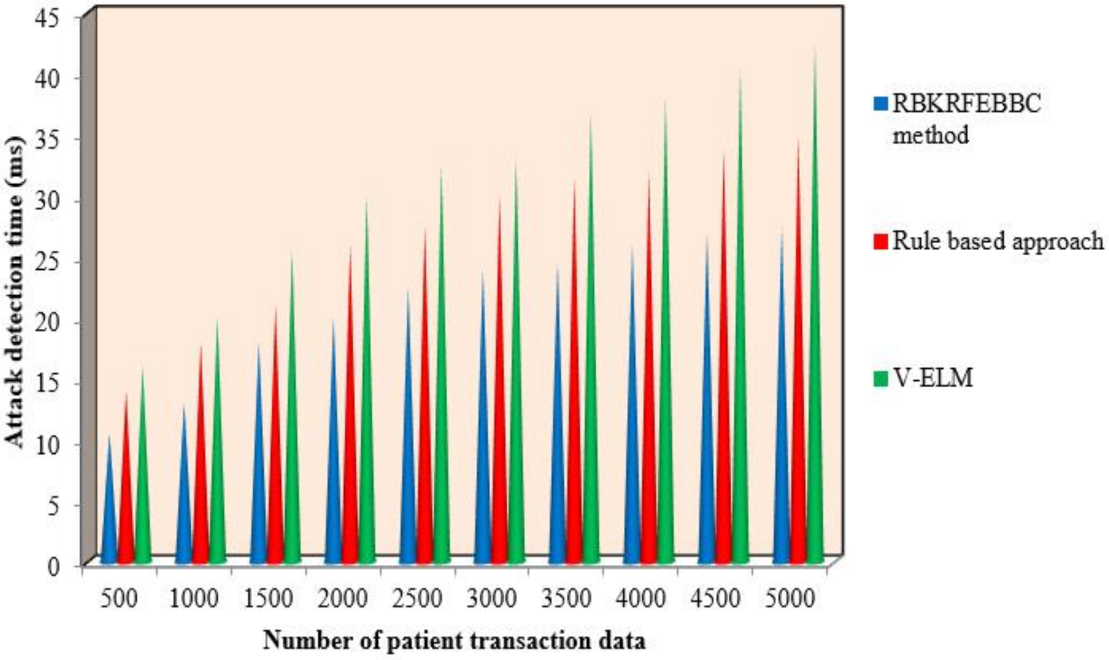

Figure 5 Measurement of Attack detection time

Figure 5 explains the graphical illustration of attack detection time with respect to number of patient transaction data. As illustrated in the figure, 'X' axis denotes the number of patient transaction data and 'Y' axis denotes the attack detection time. The blue color cone denotes the attack detection time of RBKRFEBBC method whereas red color and green color cone symbolizes the attack detection time of Rule based approach (Rakesh Rajendran, et al., 2019) and voting extreme learning machine (V-ELM) (Gopal S.K. & V Ranga, 2020). Let us consider, number of patient transaction data is 1000. The amount of time consumed for performing the one patient transaction data to detect the attack presence or attack absence by RBKRFEBBC method is $0.013s$ whereas $0.018s$ and $0.02s$ is consumed by existing Rule based approach (Rakesh Rajendran, et al., 2019) and voting V-ELM (Gopal S.K. & V Ranga, 2020) respectively. Thus, the attack detection time obtained by proposed RBKRFEBBC method, Rule based approach (Rakesh Rajendran, et al., 2019) and voting V-ELM (Gopal S.K. & V Ranga, 2020) are $13s$, $18s$ and $20s$ respectively. When the attack detection time is lesser, method is said to be more efficient. The graphical result proves that RBKRFEBBC method consumes lesser attack detection time than the existing techniques.

This is because of applying the dichotomous radial basis kernelized regressive function to determine the relationship between the features for performing the feature extraction process. After that, GRNBBC algorithm classifies the patient data transaction as attack presence or attack absence with minimum time consumption with the aid of relevant features. This in turn helps in minimizing an attack detection time. The results shows that of attack detection time consumption gets reduced using RBKRFEBBC method by 21% compared to Rule based approach (Rakesh Rajendran, et al., 2019) and 32% compared to voting extreme learning machine (V-ELM) (Gopal S.K. & V Ranga, 2020).

Performance Analysis of Error Rate

Error rate is ratio of the number of patient transaction data that are incorrectly classified as attack presence or attack absence data to the total number of patient transaction data taken. Error rate is formulated as,

$$Error\ Rate = \left(\frac{Incorrectly\ classified\ N_{pta}\ as\ attack\ presence\ or\ attack\ absence\ data}{N}\right) * 100 \quad (14)$$

From equation (12), 'N_{apa}' denotes the number of patient transaction data with attack presence or attack absence data. 'N' denotes the total number of patient transaction data. It is measured in terms of percentage (%).

Table 3 Tabulation for Error Rate

Number of patient transaction data	Error Rate (%)		
	RBKRFEBBC method	Rule based approach	V-ELM
500	6	12	15
1000	8	15	17
1500	10	19	24
2000	11	22	27
2500	9	13	19
3000	7	24	30
3500	6	18	27
4000	8	16	22
4500	8	18	21
5000	7	10	14

Table 3 illustrates the error rate of proposed RBKRFEBBC method and existing Rule based approach (Rakesh Rajendran, et al., 2019) and voting extreme learning machine (V-ELM) (Gopal S.K. & V Ranga, 2020) with different number of patient transaction data taken in the range from 500-5000. Ten different results for error rate are listed for different number of patient transaction data. Let us consider, number of patient transaction data is 3000. The number of patient transaction data that are incorrectly classified as attack presence or attack absence data by RBKRFEBBC method is 198 whereas 719 and 905 is obtained by existing Rule based approach (Rakesh Rajendran, et al., 2019) and voting V-ELM (Gopal S.K. & V Ranga, 2020) respectively. Thus, the error obtained by proposed RBKRFEBBC method, Rule based approach (Rakesh Rajendran, et al., 2019) and voting V-ELM (Gopal S.K. & V Ranga, 2020) are 7%, 24% and 30% respectively. From the table, it is clear that the error rate of proposed RBKRFEBBC method is lesser when compared to two existing methods.

This is because of using dichotomous radial basis kernelized regressive function and GRNBBC algorithm for performing the efficient attack detection. The designed function performed the feature extraction process to identify the relevant features. Then, GRNBBC algorithm categorizes the attack presence or attack absence data with help of relevant features. In this way, the error rate gets reduced during the attack detection. The average results shown that error rate is reduced using RBKRFEBBC method by 50% compared to Rule based approach (Rakesh Rajendran, et al., 2019) and 61% compared to voting extreme learning machine (V-ELM) (Gopal S.K. & V Ranga, 2020).

Conclusion

In this manuscript, RBKRFEBBC method is introduced with feature extraction and classification. Initially, number of patient transaction data is considered as an input. After that, the relevant features are extracted by kernelized regression function for performing the attack detection process. Finally with relevant extracted features, the classification process is carried out to detect the attack presence or attack absence with higher accuracy and lesser error rate. The comprehensive experimental evaluation is conducted using NSL-KDD dataset with patient transaction data. The result analysis is carried out to prove the enhancement of proposed RBKRFEBBC method. The quantitative results are verified in terms of higher attack detection accuracy and lesser time when compared to other conventional methods. As a result, proposed RBKRFEBBC method improves the attack detection accuracy by 14% as well as minimizes the time consumption time and overhead by 27% and 56% respectively while performing the data communication in cloud environment.

References

Benarfa, A., Hassan, M., Losiouk, E., Compagno, A., Yagoubi, M.B., & Conti, M. ChoKIFA+: an early detection and mitigation approach against interest flooding attacks in NDN. *International Journal of Information Security*, 1-17.

Rawashdeh, A., Alkasassbeh, M., & Al-Hawawreh, M. (2018). An anomaly-based approach for DDoS attack detection in cloud environment. *International Journal of Computer Applications in Technology*, *57*(4), 312-324.

Agrawal, N., & Tapaswi, S. (2019). Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, *21*(4), 3769-3795.

Jia, B., Huang, X., Liu, R., & Ma, Y. (2017). A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning. *Journal of Electrical and Computer Engineering*, *2017*, 1-9.

Chang, S.H., & Chen, Z.R. (2016). Protecting mobile crowd sensing against sybil attacks using Cloud based trust management system. *Mobile Information Systems*, *2016*, 1-10.

Tang, D., Dai, R., Tang, L., & Li, X. (2020). Low-rate DoS attack detection based on two-step cluster analysis and UTR analysis. *Human-centric Computing and Information Sciences*, *10*(6), 1-20.

Ramotsoela, D.T., Hancke, G.P., & Abu-Mahfouz, A.M. (2019). Attack detection in water distribution systems using machine learning. *Human-centric Computing and Information Sciences*, *9*(1), 1-22.

Kushwah, G.S., & Ranga, V. (2020). Voting extreme learning machine based distributed denial of service attack detection in cloud computing. *Journal of Information Security and Applications*, *53*.

Bhushan, K., & Gupta, B.B. (2018). Hypothesis test for low-rate DDoS attack detection in cloud computing environment. *Procedia computer science, 132*, 947-955.

Virupakshar, K.B., Asundi, M., Channal, K., Shettar, P., Patil, S., & Narayan, D.G. (2020). Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. *Procedia Computer Science*, *167*, 2297-2307.

Idhammad, M., Afdel, K., & Belouch, M. (2018). Detection system of HTTP DDoS attacks in a cloud environment based on information theoretic entropy and random forest. *Security and Communication Networks*, *2018*, 1-13.

Aborujilah, A., & Musa, S. (2017). Cloud-based DDoS HTTP attack detection using covariance matrix approach. *Journal of Computer Networks and Communications*, *2017*, 1-8.

Bharot, N., Verma, P., Sharma, S., & Suraparaju, V. (2018). Distributed denial-of-service attack detection and mitigation using feature selection and intensive care request processing unit. *Arabian Journal for Science and Engineering*, *43*(2), 959-967.

Oo, Z., Wang, L., Phapatanaburi, K., Liu, M., Nakagawa, S., Iwahashi, M., & Dang, J. (2019). Replay attack detection with auditory filter-based relative phase features. *EURASIP journal on audio, speech, and music processing*, *2019*(1), 1-11.

Rajendran, R., Kumar, S.S., Palanichamy, Y., & Arputharaj, K. (2019). Detection of DoS attacks in cloud networks using intelligent rule based classification system. *Cluster Computing*, *22*(1), 423-434.

Rani, D.R., & Geethakumari, G. (2020). Secure data transmission and detection of anti-forensic attacks in cloud environment using MECC and DLMNN. *Computer Communications*, *150*, 799-810.

Velliangiri, S., Karthikeyan, P., & Vinoth Kumar, V. (2020). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *Journal of Experimental & Theoretical Artificial Intelligence*, 1-20.

Velliangiri, S., & Pandey, H.M. (2020). Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms. *Future Generation Computer Systems*, *110*, 80-90.

Yichuan, W., Jianfeng, M., Di, L., Liumei, Z., & Xianjia, M. (2015). Game optimization for internal DDoS attack detection in cloud computing. *Journal of Computer Research and Development*, *52*(8), 1873-1882.

Watson, M.R., Marnerides, A.K., Mauthe, A., & Hutchison, D. (2015). Malware detection in cloud computing infrastructures. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 192-205.

Singh, A.K., & Sharma, S.D. (2020). Digital Era in the Kingdom of Saudi Arabia: Novel Strategies of the Telecom Service Providers Companies. *Webology, 17*(1), 227-245.