ISSN: 0976-3104
ISSUE: Computer and Allied Sciences

ARTICLE

HYBRID METAHEURISTIC ALGORITHM TUNED BACK PROPAGATION NEURAL NETWORK FOR INTRUSION DETECTION IN CLOUD ENVIRONMENT

Ayyappan Thirumalairaj[1*], Mohan Jeyakarthic[2]

[1]*Dept. Of Computer Science, Kunthavai Naacchiyaar Govt. Arts College for Women, Thanjavur, Tamil Nadu, INDIA*

[2]*Tamil Virtual Academy, Kottur, Chennai, Tamil Nadu, INDIA*

ABSTRACT

Background: *Cloud computing (CC) being the representation of the technology utilizes the infrastructure for computing in a proficient way. This kind of computing provides massive amount of significance in enhancing the productivity that minimizes the cost and verifies the risk handling management. Intrusion detection systems (IDS) are commonly employed to detect malicious activities in the network of communication and also its host.* ***Methods:*** *This paper presents new clustering based hybrid metaheuristic algorithm tuned back propagation neural network (BPNN) based IDS, called C-HMT-BPNN for effective identification of intrusion in the network. The proposed model involves two stages namely threshold based K-means clustering technique and back propagation neural network (BPNN) based classification. To optimize the weights and biases of BPNN, Particle Swarm Optimization (PSO) with Gravitational Search Algorithm (GSA) called PSO-GSA model has been developed.* ***Results:*** *The proposed model has been tested using a set of two IDS dataset namely, NSL-KDD 2015 and CICIDS 2017 dataset. The obtained experimental outcome clearly ensured the superior characteristics of the proposed model over the compared methods in a significant way.* ***Conclusions:*** *The proposed HMT-BPNN model resulted to a maximum accuracy of 99.51% which is increased to 99.75% by the inclusion of clustering techniques.*

KEY WORDS
Clustering, Cloud computing, Metaheuristic, Intrusion detection

Received: 1 Mar 2020
Accepted: 24 Mar 2020
Published: 30 Mar 2020

***Corresponding Author**
Email:
a.thirumalairaj@gmail.com

INTRODUCTION

At present times, cloud computing (CC) becomes familiar and offers on-demand computing services ranging from applications to storage and processing power using the internet and on a pay-as-you-go basis. [1]. The cloud satisfies the requirement of users for trustworthy access to data and the corresponding resources. More number of businesses has been applying CC through the features of on-demand self-service, broad network application, resource pooling, quick elasticity and valid facilities. These metrics enables several clients to concentrate on business processes and controlling the computational resources using Cloud Service Provider (CSP) [2]. This cloud method tends to minimize the business cost with respect to simple installation of hardware and its procedures with software as well as the hardware updates by ensuring suitability and accessibility of diverse computational resources [3]. Generally, the deployment of CC takes place in three ways, namely Private cloud, Public cloud and Hybrid cloud. Public cloud can be used by common people and owned by a private or academic, government or combined organizations. This private cloud infrastructure has been maintained by a broad as well as individual organization. The Hybrid cloud is referred as an appropriate integration of different architectures which might be private, public which becomes as an individual cloud [4].

In recent times [5], Google, Amazon and the Salesforce.com are the important providers of cloud services (CS) and expand the facilities of storing the applications as well as processing enhancement for every year. The data non-availability of services and applications have been induced interms of denial of service (DOS) or distributed DoS (DDOS) where the attackers use CS [6]. The IDS becomes a required unit of defensive metrics which is capable of protecting the systems from a dangerous attack. Furthermore, safeguarding a system is considered to be the most important potion of CC platform. The main theme of IDS is to find and response to the events of intrusion as emerged from selfish nodes [7]. The IDS is defined as a model applied for detecting and responding the intrusion events. Also, it is referred as a method applied for predicting the intrusions of a network. IDS is a process of detecting actions which happens in a network and tries to satisfy the confidentiality, security or network accessibility to apply the trust procedures [8, 9]. Misuse prediction relied method is assumed to be the analysis of intrusions that exhibits forecasting intrusions uses an effective intrusion strategy [10]. These models are more efficient in detecting predefined attacks. Alternatively, the anomaly based prediction shows the performance conducted by an investigation of modified patterns in a system. These modifications are applied for detecting the difference in patterns of predetermined and unknown attacks. Furthermore, the abnormal nature can be identified. Also [11], IDS has 2 features which are based on the host network. The IDS is found at defense system that helps to monitor the harsh events existing in a system. CC has 2 various modules that are knowledge-based IDS as well as behavior-based IDS to analyze the IDS of CC platform.

Several types of meta-heuristic frameworks are used in solving the issues related with scheduling. [12] deployed a model in-depth analysis of PSO and the application of workflow scheduling techniques has presented for CC environment in this study. Also, it offers the classifications of developed system according to PSO that has been used in research directions. A method for PSO-optimized Back Propagation (BP) which is assumed to be an NN based MapReduce on a Hadoop platform along with PSO as well as corresponding model was presented by Cao et al. [13]. It is applied for optimizing BP NN from the initial

IIOAB JOURNAL
ISSN: 0976-3104

weights and thresholds helps in developing classification methodologies as well as the accuracy. The MapReduce based parallel programming technique is applied to attain the simultaneous process of BP methods to deal hardware and communication problems while addressing BP and NN datasets. Furthermore, the system depicts a maximum accuracy of classification and enhanced efficiency of time which denotes an increment that is attained from parallel processing to smart models of big data. Hyper-heuristic methodologies helps in finding essential solutions to schedule in CC systems and further extension of allocating the simulation outcome to enhance the network lifetime. [14] deployed an alternate new Multi-Objective PSO (MOPSO) and Genetic Algorithm (GA) based hyper-heuristic technologies to schedule the resource in the form hybrid model. The working function of this method is estimated under the application of Cloud Sim toolkit. Various researchers made a comparison over hybrid scheduling technique by using recent heuristic as well as scheduled models [15]. The attained outcome has exhibited an optimal performance when compared with current approaches with respect to cost reduction and enhanced network lifetime. Consequently, proposed system has implemented a maximum resources application with span and throughput.

This paper presents new clustering based hybrid metaheuristic algorithm tuned back propagation neural network (C-HMT-BPNN) based IDS for effective identification of intrusion in the network. The proposed model involves two stages namely threshold based K-means clustering technique and back propagation neural network (BPNN) based classification. To optimize the weights and biases of BPNN, Particle Swarm Optimization (PSO) with Gravitational Search Algorithm (GSA) called PSO-GSA model has been developed. The proposed model has been tested using a set of two IDS dataset namely, NSL-KDD 2015 and CICIDS 2017 dataset.

MATERIALS AND METHODS

Figure-1 shows the process involved in C-HMT-BPNN model. The proposed model involves two main stages, namely clustering and classification. For clustering process, thresholding based K-means clustering technique is applied to cluster the data prior to classification. Next to that, the HMT-BPNN based classification model is applied to classify the clustered data to identify the existence of intrusions exist in the network data.

Threshold based K-means clustering

K-means is defined as a simple as well as effective unsupervised classification technique. K-means is a popular division based clustering models which tries to explore a user with definite clusters given by the centroids. It is said to be a common distance-based clustering method where the distance has been applied as a value of similarity, in which a minimum distance objects exhibits a higher affinity.

- Initiate $k = 2$ as the expected variable has 2 feasible results namely, normal and anomaly.
- Compute the input data for every nearby cluster center with the application of Eq. (1).

$$S_i^{(z)} = \left\{ x_p : \left\| x_p - m_i^{(z)} \right\|^2 \le \left\| x_p - m_i^{(z)} \right\|^2 \forall_j, 1 \le j \le k \right\} \quad (1)$$

- Using Eq. (2), upgrade the cluster centers by re-evaluating the mean of all input data allocated to every cluster.

$$m_i^{(z+1)} = \frac{1}{|S_i^{(z)}|} \sum_{x_j \in S_i^{(z)}} x_j \quad (2)$$

- In order to implement the k-means cluster to a terminate step, it has looped through step (b) and (c) till a convergence of a mean value is attained.

As a result, k-means cluster provides the result by eliminating unwanted clustered data as well as to make a decision of exploring a novel dataset to classify using Eq. (3). When a novel data size is maximum then, supervised classification is applied, otherwise, it repeats k-means clustering technique till obtaining an adoptable cluster size.

$$newsize = \frac{leftdata}{totalsum} \quad (3)$$

In this paper, a thresholding mechanism is incorporated, which enables the clustering technique to group at least 70% of entire data. The clustering process gets iterated till 70% of clustered data is attained.

Classification Methods

Once the clustering process gets completed, HMT-BPNN model is applied for data classification. The HMT-BPNN is actually a BPNN based classifier which undergoes tuning by the use of hybrid metaheurisitc algorithm, named PSO-GSA. The PSO-GSA is applied to tune the weights and biases of BPNN. Generally, PSO is referred to be an optimizing model which depends upon the foraging behavior of birds, and random initialization of population as well as regular extension of searching task. When exploring an optimized solution, every bird has been assumed to be a particle with no mass and volume.

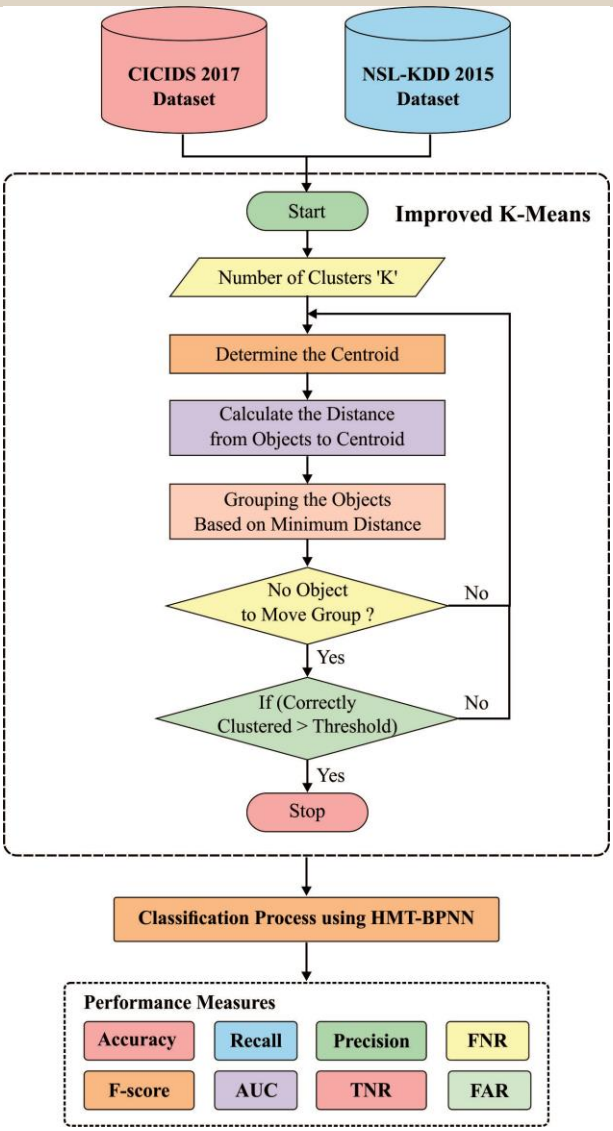

Fig. 1: Overall Process of Proposed Method

At the time of processing a search operation, the particles are capable of recording the recent best position (*pbest*) as well as global best position (g*best*). Velocity and position of every particle are estimated as given below:

$$v_i^{z+1} = w \cdot v_i^z + c_1 \cdot \text{rand} \cdot (\text{pbest} - x_i^z) + \text{c}_2 \cdot rand \cdot (gbest - \text{x}_\text{i}^\text{z}) \quad (4)$$

$$x_i^{z+1} = x_i^z + v_i^{z+1} \quad (5)$$

where v_i^z and x_i^z are referred as current velocity and position of ith particle at jth iteration, c_1 and c_2 are said to be acceleration coefficients which helps to manage the influence of $pbest$ and $gbest$ in searching task, correspondingly, rand denotes a random value in [0, 1], $pbest(z)$ represents the recent best position of every particles at tth iteration, $gbest$ implies a best position over the compared particles, and w signifies inertia weight.

GSA model has been named as a novel strategy which depends upon the law of gravity. The agents present in GSA are assumed as objects along with masses. Agents are inspired with one another by using a gravity force. If the quality becomes higher then, the gravity is stronger. Hence, position of an agent with higher mass is termed as best solution. Let N agents have d-dimension where the position of ith agent is given by,

$$X_\text{i} = \left(x_i^1, x_i^2, \ldots, x_i^d\right)(\text{i} = 1,2,\ldots,N) \quad (6)$$

In a tth time, the force is working on ith agent from jth agent which is written as,

$$F_{ij}^d = G(\text{z})\frac{M_i(\text{z})M_j(\text{z})}{R_{ij}(\text{z}) + \varepsilon}\left(\text{x}_j^d(\text{z}) - \text{x}_i^d(\text{z})\right) \quad (7)$$

IIOAB JOURNAL
ISSN: 0976-3104

where $M_i(z)$ and $M_j(z)$ are signified as masses of ith agent as well as jth agent, correspondingly , $G(z)$ denotes a gravitational constant at zth time, ε refers a lower constant, and R_{ij} depicts the Euclidian distance from ith and jth agent. In zth time, overall force has been used on ith agent as defined in the following:

$$F_i^d(z) = \sum_{j=1, j\neq i}^{N} \text{rand} \cdot F_{ij}^d(z) \tag{8}$$

where $rand$ represents a uniform random variable in $[0, 1]$. Based on the law of motion, the acceleration of an agent in zth time could be expressed as follows:

$$a_i^d(z) = \frac{F_i^d}{M_i(z)} \tag{9}$$

For every iteration process, velocity and position of ith agent gets updated under the application of 2 given functions:

$$v_i^d(z+1) = \text{rand} \times v_i^d(z) + a_i^d(z) \tag{10}$$
$$x_i^d(z+1) = x_i^d + v_i^d(z+1) \tag{11}$$

where $rand$ implies a uniform random variable from the interval $[0, 1]$ and $x_i^d(z)$ and $v_i^d(z)$ are the current position and velocity, correspondingly.

In GSA, an agent does not distribute the population details by one another and contains a vulnerable ability of developing. BY exploiting the global optimum searching potential of PSO as well as local searching capability of GSA, every agent are upgraded with using the velocity of PSO as well as the acceleration of GSA. This technique is named as PSO-GSA [16]. Hence, exploration and exploitation ability has been integrated with modified variables. The velocity and position of ith agent are extended by given 2 equations:

$$v_i^{z+1} = w \cdot v_i^z + c_1' \cdot \text{rand} \cdot ac_i + c_2' \cdot rand \cdot (gbest - x_i^z) \tag{12}$$
$$x_i^{z+1} = x_i^z + v_i^{z+1} \tag{13}$$

where w denotes the inertia weight, v_i^z , x_i^z , and $ac_i(z)$ are said to be the velocity, position, and acceleration of ith particle at tth iteration, whereas c_1' and c_2' are constant acceleration coefficients, correspondingly. In this study, it is assumed with that c_1' and c_2' is exponential functions expressed as:

$$c_i' = c_{start} \cdot \left(\frac{c_{end}}{C_{Start}}\right)^{1/(1+k/Z_{max})} \tag{14}$$

where c_{start} denotes an initial value, c_{end} implies the final value, Z_{max} signifies the higher iteration value, and k represents a current iteration value. To differentiate from GSA-PSO, GSA-PSO with functional acceleration coefficients (14) it is termed as I-PSO-GSA.

The PSO-GSA model is used for optimizing the weights and biases of BPNN as well as Mean Square Error (MSE) which is employed as Fitness Function (FF) of HPT-BPNN model. The FF of kth training sample is described as:

$$MSE = \frac{1}{q}\sum_{k=1}^{q}\sum_{i=1}^{m}\left(o_i^k - d_i^k\right)^2 \tag{15}$$

where q refers a count of training samples, d_i^k shows an required outcome of ith input unit from a kth training instance, and o_i^k reflects the original result of ith input unit from kth training sample.

When a structure of BPNN is a $r - s - z$ structure, where r indicates the node count present in an input layer, s depicts the value of nodes from a hidden layer, and z shows a number of the nodes from a resultant layer. Then,N agents of population has $L_i(i = 1,2,\ldots,N)$ as d-dimension vector$\left(l_{i,1}, l_{i,2}, \ldots, l_{i,d}\right)$, where $d = rs + s + sz + z$. By mapping L_i as the weights on the basis of BPNN, the components $l_{i,1}, l_{i,2}, \ldots, l_{i,rs}$ of $L_i$is assumed to be the weights acquired from input and hidden layer, the components $l_{i,rs+1}, \ldots, l_{i,rs+s}$ of L_i is based on hidden layer, and the components $l_{i,rs+s+1}, \ldots, l_{i,rs+s+sz}$ of L_i are the weights among hidden layer as well as output layer, and components $l_{i,rs+s+st+1}, \ldots, l_{i,D}$ depends upon the output layer.

RESULTS

Dataset Description

For assessing the effective performance of the presented C-HMT-BPNN model, an experimental validation takes place using a set of two benchmark dataset namely NSL-KDD 2015 [17] and CICIDS 2017 [18]. The first NSL-KDD 2015 dataset holds a sum of 125973 instances with 41 attributes. Among the 125973 instances, around 67343 and 58630 instances fall into the Normal and Anomaly categories respectively. The second CICIDS 2017 dataset comprises 2830743 instances with the occurrence of 80 features.

IIOAB JOURNAL
ISSN: 0976-3104

Among the total number of instances, 2273097 instances comes under Normal class and rest of the instances comes under Anomaly class.

Results Analysis

Fig. 2 illustrates the confusion matrix generated by the proposed model on the applied dataset. Fig. 2a shows the confusion matrix offered by the proposed model before clustering on the applied NSL-KDD 2015 dataset. The figure clearly stated the proposed model offers a maximum of 67138 instances as Normal and 58219 instances as Anomaly. Similarly, Fig. 2b shows the confusion matrix offered by the proposed model after clustering on the applied NSL-KDD 2015 dataset. The figure clearly stated the proposed model offers a maximum of 50724 instances as Normal and 45897 instances as Anomaly. Fig. 2c shows the confusion matrix offered by the proposed model before clustering on the applied CICIDS 2017 dataset. The figure clearly stated the proposed model offers a maximum of 2223538 instances as Normal and 553235 instances as Anomaly. Similarly, Fig. 2d shows the confusion matrix offered by the proposed model after clustering on the applied CICIDS 2017 dataset. The figure clearly stated the proposed model offers a maximum of 2189257 instances as Normal and 491513 instances as Anomaly.

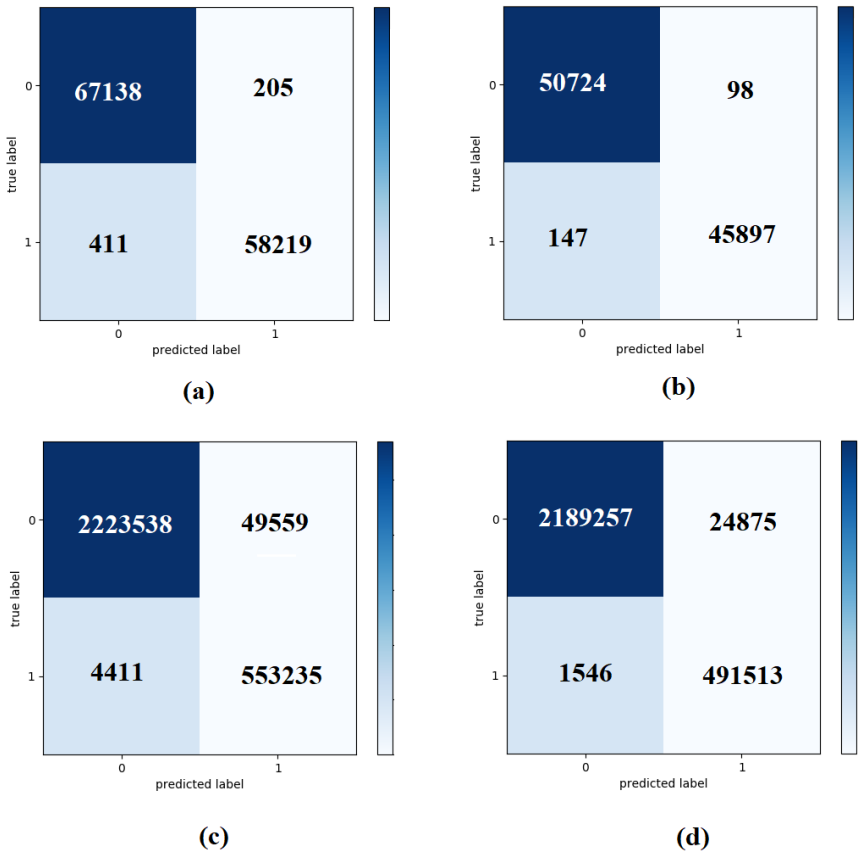

Fig. 2: Confusion Matrix Generated at the Time of Execution a) Before Clustering NSL-KDD 2015 b) After Clustering NSL-KDD 2015 c) Before Clustering CICIDS d) After Clustering CICIDS

Figures - 3 and -4 show the classification outcome of the proposed model on the applied dataset, with and without clustering interms of different measures namely false acceptance rate (FAR), true negative rate (TNR), false negative rate (FNR), area under curve (AUC), precision, recall, accuracy and F-score are employed. On measuring the results on the applied NSL-KDD 2015 dataset, it is noted that the C-HMT-BPNN model before clustering offers effective results with minimum FAR value of 0.04 and is further reduced to 0.002 after clustering. Similarly, the C-HMT-BPNN model attains minimum FNR values of 0.007 and 0.003 under before and after clustering respectively. At the same time, the C-HMT-BPNN model provides a higher TNR rate of 99.65% before clustering and gets increased to 99.79% after clustering. The proposed C-HMT-BPNN model also demonstrated maximum AUC value of 99.52% before clustering and is raised to 99.75% after clustering. In the same way, the C-HMT-BPNN model achieves a maximum precision value of 99.70% before clustering and is increased to 99.81% by the inclusion of clustering process. Afterwards, the C-HMT-BPNN model shows its effective results by offering maximum recall values of 99.39% and 99.71% before and after clustering respectively. In these lines, the C-HMT-BPNN model exhibits maximum classification accuracy of 99.51% before clustering and the clustering process

enhances it to 99.75%. At last, the C-HMT-BPNN model reaches to an F-score value of 99.54% and is raised to 99.76% by the use of clustering process.

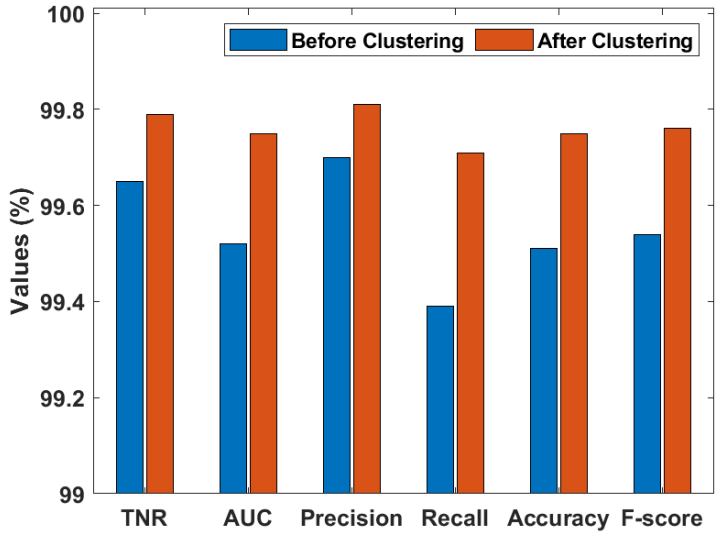

Fig. 3: Classifier results analysis of C-HMT-BPNN model on NSL-KDD 2015 dataset

To validate the classifier outcome on the tested CICIDS 2017 dataset, it is observed that the C-HMT-BPNN model before clustering provides supreme outcome with a lower FAR value of 0.082 and is further reduced to 0.048 after clustering. Likewise, the C-HMT-BPNN model reaches to minimum FNR values of 0.008 and 0.003 under before and after clustering respectively. Simultaneously, the C-HMT-BPNN model attains a high TNR of 91.78% before clustering and gets increased to 95.18% after clustering. The proposed C-HMT-BPNN model additionally exhibited higher AUC value of 95.79% before clustering and is raised to 97.56% after clustering. Similarly, the C-HMT-BPNN model resulted to a maximum precision value of 97.82% before clustering and is increased to 98.88% by the inclusion of clustering process. Afterwards, the C-HMT-BPNN model shows its effective results by offering maximum recall values of 99.80% and 99.93% before and after clustering respectively. In these lines, the C-HMT-BPNN model provides a maximum classification accuracy of 98.09% before clustering and the clustering process enhances it to 99.02%. Finally, the C-HMT-BPNN model leads to a maximum F-score value of 98.80% and is raised to 99.40% by the use of clustering process.

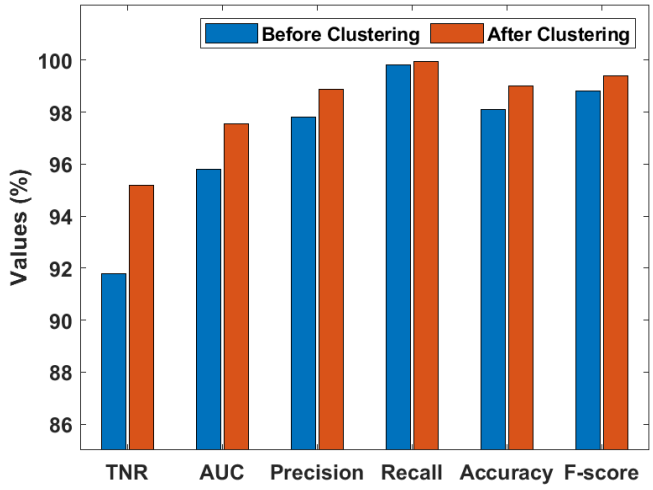

Fig. 4: Classifier results analysis of C-HMT-BPNN model on CICIDS 2017 dataset

DISCUSSION

To validate the consistent results of the presented C-HMT-BPNN model on the IDS dataset, an extensive results analysis is made with the lately presented IDS models [19] namely Cuckoo optimization, cuckoo search with PSO (CS-PSO), PSO-SVM, Behaviour Based IDS, Gaussian Process, Deep Neural Network with SVM, GA+Fuzzy, Fuzzy C-means and Gradient Boosting models interms of accuracy. The resultant values are shown in Fig. 5. After observing the values exist in the table, it is evident that the CS-PSO model exhibited poor outcome with a least accuracy of 75.51%. Then, it is apparent that the Gradient Boosting

IIOAB JOURNAL
ISSN: 0976-3104

model has reached to an accuracy of 84.25%, which is superior to the accuracy provided by the CS-PSO algorithm. On the other hand, the Gaussian Process and the DNN+SVM models show better results over the existing models by the attainment of near identical accuracy values of 91.06% and 92.03% respectively. Besides, even higher detection performance is showed by Fuzzy C-means model by offering an accuracy value of 95.30%. Concurrently, the GA+ Fuzzy and Cuckoo Optimization algorithms have accomplished manageable and identical detection results by offering accuracy values of 96.53% and 96.888% respectively. In line with, even higher detection outcome is achieved by Behaviour Based IDS model which can be noticed from the accuracy value of 98.89% whereas competitive results of 99.10% and 99.36% of accuracy are provided by the existing PSO-SVM and IPSO-NN models. But, it is interesting that the HMT-BPNN model has outperformed all the existing methods and achieved a higher accuracy of 99.51% on the applied dataset. Furthermore, it is noted that the C-HMT-BPNN model has shown superior performance and offered a maximum accuracy of 99.75%.

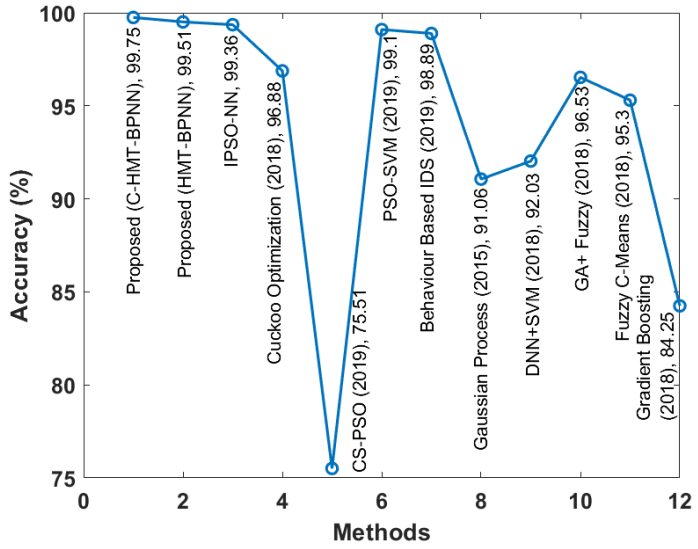

Fig. 5: Accuracy analysis of C-HMT-BPNN model with state of art models

CONCLUSION

This paper presents new C-HMT-BPNN model for effective identification of intrusion in the network. The proposed model involves two main stages, namely clustering and classification. For clustering process, thresholding based K-means clustering technique is applied to cluster the data prior to classification. Next to that, the HMT-BPNN based classification model is applied to classify the clustered data to identify the existence of intrusions exist in the network data. The proposed model has been tested using a set of two IDS dataset namely, NSL-KDD 2015 and CICIDS 2017 dataset. The obtained experimental outcome clearly ensured the superior characteristics of the proposed model over the compared methods in a significant way. The proposed HMT-BPNN model resulted to a maximum accuracy of 99.51% which is increased to 99.75% by the inclusion of clustering techniques.

CONFLICT OF INTEREST
The authors have expressed no conflict of interest.

ACKNOWLEDGEMENTS
None

FINANCIAL DISCLOSURE
None

REFERENCES

[1] Shiraz M, Gani A, Khokhar RH, Buyya R. [2012] A review on distributed application processing frameworks in smart mobile devices for mobile cloud computing. IEEE Communications surveys & tutorials, 15(3):1294-313.
[2] Popović K, Hocenski Ž. [2010] Cloud computing security issues and challenges. In The 33rd international convention mipro, IEEE, 344-349.
[3] Carlin A, Hammoudeh M, Aldabbas O. [2015] Defence for distributed denial of service attacks in cloud computing. Procedia computer science,1;73:490-497.
[4] Murugan S, Jeyakarthic M. [2019] An Efficient Bio-Inspired Algorithm Based Data Classification Model For Intrusion Detection In Mobile Adhoc Networks. The International journal of analytical and experimental modal analysis, 11(11): 834-848.

[5] Carlin A, Hammoudeh M, Aldabbas O. [2015] Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges. International Journal of Advanced Computer Science and Applications, 6(6): doi: 10.14569/IJACSA.2015.060601
[6] Shelke MP, Sontakke MS, Gawande AD. [2012] Intrusion detection system for cloud computing. International Journal of Scientific & Technology Research, 1(4):67-71.
[7] Butun I, Morgera SD, Sankar R. [2013] A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials,16(1):266-82.
[8] Peddabachigari S, Abraham A, Grosan C, Thomas J. [2007] Modeling intrusion detection system using hybrid intelligent systems. Journal of network and computer applications, 30(1):114-32.
[9] Mohod AG, Alaspurkar SJ. [2013] Analysis of IDS for cloud computing. International Journal of Application or Innovation in Engineering & Management, 2:344-9.
[10] Rowland CH, Psionic Software Inc [2002]. Intrusion detection system. US Patent, 6405318.
[11] Liao HJ, Lin CH, Lin YC, Tung KY. [2013] Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1):16-24.
[12] Masdari M, Salehi F, Jalali M, Bidaki M. [2017] A survey of PSO-based scheduling algorithms in cloud computing. Journal of Network and Systems Management, 25(1):122-58.
[13] Cao J, Cui H, Shi H, Jiao L. [2016] Big data: A parallel particle swarm optimization-back-propagation neural network algorithm based on MapReduce. PloS one, 11(6):e0157551.
[14] Kumari KR, Sengottuvelan P, Shanthini J. [2017] A hybrid approach of genetic algorithm and multi objective PSO task scheduling in cloud computing. Asian Journal of Research in Social Sciences and Humanities, 7(3):1260-71.
[15] Zaman S, El-Abed M, Karray F. [2013] Features selection approaches for intrusion detection systems based on evolution algorithms. InProceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 1-5.
[16] Hu H, Cui X, Bai Y. [2017] Two Kinds of Classifications Based on Improved Gravitational Search Algorithm and Particle Swarm Optimization Algorithm. Advances in Mathematical Physics. 2017.
[17] CICIDS2017 data set. [2019] https://www.unb.ca/cic/datasets/ids-2017.html (Accessed on 14 Jan, 2020)
[18] NSL-KDD Dataset of NSL-KDD University of new Brunswick. [2019] http://www.unb.ca/research/iscx/dataset/iscx-NSL-KDD-dataset.html. (Accessed on 14 Jan, 2020)
[19] Chiba Z, Abghour N, Moussaid K, Rida M. [2019] Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms. Computers & Security, 86:291-317.