Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

# A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing

Jitendra Kumar Samriya, Narander Kumar *

*Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow 226025, India*

ARTICLE INFO

*Article history:*
Received 13 September 2020
Accepted 24 September 2020
Available online xxxx

*Keywords:*
Cloud Computing
Intrusion detection system
Machine Learning
Fuzzy-C-Means
Spider Monkey Optimization

ABSTRACT

In this study, a new hybridization approach for the intrusion detection system is proposed to improve the overall security of cloud based computing environment. In addition this approach is also helps to handle various type of security hurdles on the cloud for e.g., fake identity detection, Data leakage and Phishing attacks etc to maintain Security over the cloud. The method uses fuzzy based ANN for efficient clustering of anomalies whereas the fuzzy based clustering which is further optimized using spider-monkey optimization algorithm. This hybridization approach will overcome the iterative classification and selection process of fuzzy clustering approach by automatically updating the fitness value. In addition, the SMO optimization approach will result in dimensionality and the reduced dataset was forwarded into neural network. The proposed approach results reduced computational time and enhanced accuracy when compared with other existing hybridization methods.
© 2020 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

## 1. Introduction

The cloud provides remote access to both hardware and software resources for the user by placing distributed services worldwide. Cloud Computing (CC) is a branch of Information Technology (IT) that offers infrastructures, platforms, software applications and much more in the form of a request-service and usage [1]. The foremost requirement of CC is virtualization of the cloud resources, their storage and implementations [2]. The entire operational function of the cloud structures are managed by a central hypervisor machine. Therefore, this technology had became eye-catching platform for the intruders and hijackers of application softwares, due to its enormous traffic generated in cloud environment [3].The evolving threat for cloud information mainly the Distributed denial of service attack are found to be a well-known cyber attack in this CC environment. Also, flooding of packets in transmission protocols can lead to damage of resources and bandwidth utilization. This will result in a short term problem or the entire environment will be collapsed. These security concerns paved the way for the deployment of intrusion detection software mainly to protect against zero-day attacks [4]. The prevailing problems with Intrusion detection system (IDS) includes false alarms that contributes to the problem of misuse and certain anomaly detection methods can be implemented in cloud for reducing these kind of attacks [5].

However, implementing these detection approaches lead to increase in the number of events within the cloud, thus detection process becomes burden for which soft computing helps. These include Genetic Algorithm (GL), Fuzzy Logic (FL), Artificial Neural network (ANN), and so on [6] and suchenhances the efficiency and accuracy of detection rate of anomalies. Among these ANN is widely used because of the capability to deal with data which is not complete. The mining rule association approach is also a currently adopted technique for intrusive data detection [7]. ANN in intrusion detection can be used in many ways.

The major drawback of IDS is that requires appropriate amount of time and increased amount of training sets for efficient implementation [8]. The ANN incorporated detection system in cloud is a well-built secured technique and this can append GA for further effectiveness. Artificial Bee Colony [11], Harmony Search [10] and Particle Swarm Optimization (PSO) [9] are some among them used along with ANN based IDS systems. There are also some approaches that combine two or more such for optimization and

* Corresponding author.
*E-mail address:* nk_iet@yahoo.co.in (N. Kumar).

https://doi.org/10.1016/j.matpr.2020.09.614
2214-7853/© 2020 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the Emerging Trends in Materials Science, Technology and Engineering.

Please cite this article as: Jitendra Kumar Samriya and N. Kumar, A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing, Materials Today: Proceedings, https://doi.org/10.1016/j.matpr.2020.09.614

increased resource utilization in CC. The IDS's competence can be improved by search techniques which perform deciding the optimum network parameters and types used by these heuristic approaches. For instance, in order to detect VM attacks hybridization approaches are proficient that combines classification and selection of features [12]. A security system with GA incorporation with PSO tested on NSL based KDD data can be found in existing studies. An overall accuracy of such hybrid approaches achieves around 95% as per the prevailing approaches and the rate of classification attained by classifiers of Denial attacks ha to be addressed. Fuzzy approach concerns with the indefinite invader problems and are implemented in detection schemes for particular function which are also called fuzzy variables.

Moreover, fuzzy rule based detection schemes which include e-mail bombs, phishing, eavesdropping, FTP/Telnet port scanning, UDP SYN floods and password guessing are powered to deal with intrusions that occur in the network to resolve unauthentic entry on cloud platform. Requiring a particular amount of time period and diversity of variables for training are being addressed by these rules. On contrary, only limited training samples are being used by SVM for detecting such intrusions in networking environment which is an efficient classifier that offers enhanced solutions. This can also keep-up with the classification accuracy concerned with data dimensions. Better results are produced in case of Support Vector Machine classifiers in terms of false positives. In this work a novel hybridized ANN network is used that combine's fuzzy logic with SMO algorithm for efficient detection and complexity reduction.

## 2. Literature survey

An approach for Intrusion Detection is proposed [13]. The main techniques used to enhance the accuracy in this approach are support vector machine (SVM) and fuzzy c means clustering (FCM) algorithm. This work is then compared with other existing methods with the help of NSLKDD dataset. The outcomes so obtained reveal that the proposed approach performs well and the analysis shows increase in accuracy and reduction in false positive rates. Also this hybrid approach is said to obtain better performance while implemented in cloud environment. A three level machine leaning approach is implemented in [14] for detecting intrusion in computing environment which is a cluster based neural network approach. In the foremost step the fuzzy clustering technique will generate the training sets. Then the base models are induced on these generated subsets with the help of ANN. Finally, the system files, registry keys and the database are added as restore points and the Fuzzy aggregation module performs tests and classification.

A double layer classifier hybridized with classifier for detection as an infrastructural cloud IDS is introduced in [15]. Fuzzy clustering, improved SVM are used for this approach whereinthe clustering is performed by Bayesian Fuzzy clustering and GG-SVNN which stands for search-based support vector neural network recognizes intruders in the cloud network. This search based gravitational network approach is thus a novel optimization scheme. The classifier contains two level of performance where level 1 deals with compact data and level 2 with nodes invaded by network intruders.

A wrapper based WAO algorithm that addresses the drawback of traditional Whale Optimisation Algorithm is implemented in [16]. This scheme is introduced to overcome the problem of attaining optimal position value due to early convergence by WAO which is handled by a crossover operator. This will somehow improves the mutation operation and prevents the optimal position value by using the valuable informative features in the network and thus detects anomalies easily. The results of this approaches shows better performance when compared with traditional WAO and other state of arts methods.

A hybrid clustering, QALO-K that efficiently combined quantum-inspired ant lions with optimized k-means thus inherits both of its advantages is presented in [17]. This hybrid approach will direct the clusters of k-means to attain its global direction. It's a novel approach that induces the clustering technique with the help of the mentioned intelligence algorithm. The performance analysis of this proposed method using many UCI Machine Learning Repository datasets and compared with other well-knownalgorithms.

The GA for a large quantity of data which contributes to multiple technologies for intrusion detection is presented in [18]. The approach obtains reduced optimal number of features and are then classified network packets ith the help of Multi-Layer perceptron as a classifier. The suggested solution in [19] uses the SVM classifier to separate network data into normal and attack operations, and due to the obsolete and redundant features in the datasets, IG is used to select the correct features and delete unnecessary features.

## 3. Methodology

The detection rate and accuracy of IDS is based on the classifiers capability to track the events in a proper way so that it will not compromise with the detection performance. In addition, these systems face a major occurrence of false alarms in cases it turn to be heavy burden for internal operators who handle such activities. The lack of time and adequate resources for the organization to deal with these generated false alarms have evolved as a major concern, creates warning and produces the possibility of undetected anomalous behaviour. Now-a-days MLs and DL techniques are well-equipped to be implemented as IDS. Because of the architecture of these approaches with the capability to monitor and detect any kind of new threats in the network they are implemented for IDS. Also the structures of IDS are simple and are based on domain-specific. With the usage of high quality data ML techniques will achieve higher precision rate and so the deep learning better fitted for handling enormous volume of data. In accordance with the hybrid optimization and nature-based algorithms and fuzzy clustering techniques can reduce the execution time. Certain algorithms such as PSO, GA, ABC, and SA are certain algorithms derived from nature-inspired processes. The spider monkey optimization algorithm as evolved new can be incorporated in detection schemes for better performance. For instance to detect a plant leaf disease in a high-dimensional subset this technique is employed. The hybridization of SMO with FCM is an efficient approach to attain optimized classification of intruders in the network. Such hybrid systems were successfully applied to address complex real-world problems, offering solutions that are streamlined and resource intensive. This work implements and the results obtained shows it performs detection with higher accuracy in cloud computing IDS environment.

This recent approach will make use of a Euclidean distance for the calculation update to obtain optimal solutions. In addition, this algorithm is combined with fuzzy rules to build a strong wall to deal with optimization problems which are even complex since it is a recent and yet effective swarm intelligence algorithm which can also monitor and process the location of processor and sizing problems. Thus it is implemented in cloud environment for optimal resource utilization and reduced energy consumption. Fig. 1 illustrates the design of the proposed approach. Fig. 2. algorithm flow diagram shows the pictorial representation of flow of algorithm.

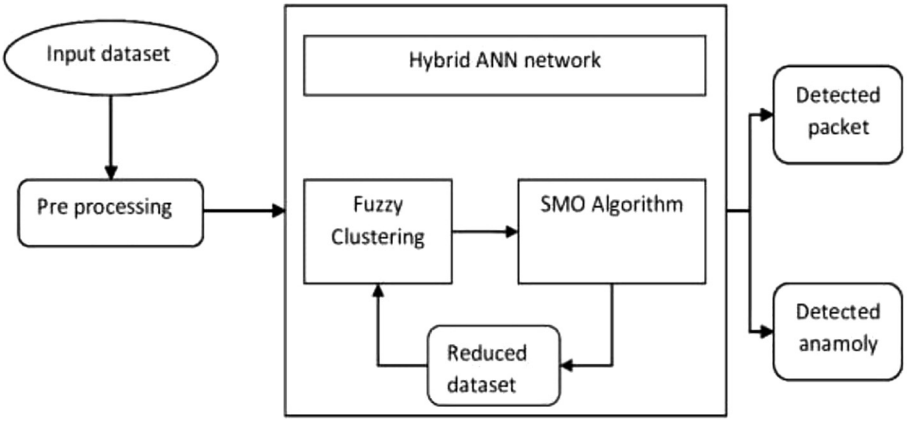


**Fig. 1.** Schematic representation of the proposed work.

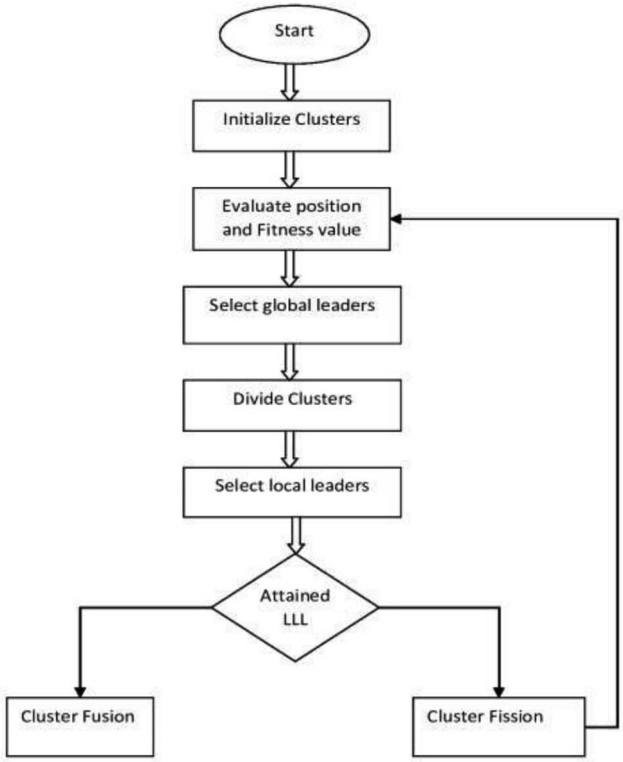


**Fig. 2.** Algorithm flow diagram.

### 3.1. Fuzzy C-means (FCM) clustering technique

FCM is an eminent method for clustering. This technique changes the data points in each cluster; hence the clusters which are small are compulsorily made to gather inneighbouringclusters which are of larger. It is presumed that the point between two cluster centres has a continuing membership of both clusters. The FCM suggests a method in which based on the membership level the data points are assigned with a cluster where the data point can be at the same time a member of two or more clusters. All clusters(c) should have same scale and there should be a prior knowledge of the cluster numbers.

Step 1: Separation of data points in k-dimensional vector.

Step 2: Find cluster centres in each cluster using objective function.

Step 3: Apply fuzzy separation.

When compared with hard c-mean this method is completely different. The elements of the membership matrix are within the range of [0, 1].

### 3.2. Spider-Monkey optimization (SMO) algorithm

SMO is a metaheuristic strategy, influenced by the advanced spider monkeys foraging behaviour. The Spider monkeys' foraging activity focuses on the social system of fission–fusion. The characteristics of this algorithm depend on a group's social structure, which a female participant wants to split or combine from. The association's delegate as a whole is here called the national leader while the regional grouprepresentatives are called as local leaders. The shortage of food of this algorithm doesn't have any impact on the solution. And this algorithm is a swarm intelligence based one, there will be a minimum number of apexes at any small group. One logical solution in this algorithm is the Spider Monkey (SM). Next it describes the SMO processes involved.

#### 3.2.1. Global leader selection

The algorithm begins the step towards the process of the global leader, where it detects the packets in the cluster which is different in the cluster location. The location value is the IP address that is in each packet's header. On behalf of the selection probability the solution is updated, which is calculated by Equation below.

$$fn(fit)_k = \begin{cases} \frac{1}{1+f_k}, if\, f_k \geqslant 0 \\ 1 + abs(f_k), if\, f_k < 0 \end{cases} \quad (1)$$

In the global leader phase, the selected fitness value probability is computed by the formula

$$PROB = 0.9 \times \frac{fn(fit)_k}{\max[fn(fit)]} + 0.1 \quad (2)$$

In the next phase the position is updated,

$$Cnew_{l,m} = Cnew_{l,m} + dis(0,1) * (gl_{n,m} - Cnew_{lm}) + dis(-1,1) \times (C_{rm} - C_{lm}) \quad (3)$$

Where (dis) is a random number representing the global leader in the range (−1, 1), gl.

The persistence of the current packet is shown in the first component, the attraction of the packet towards the global leader is exposed in the second component, and the algorithms stochastic behaviour can be retained using the final component. In this equation the second component is applied to enhance the efficiency of the search space which is specified already, while premature con-

vergence or the risk of being stuck in the optimum locale is prevented in the final component. The global leader's selection process identifies the anomalous packets based on the location value that comes from a specific user differing from the other packets in the cluster and splitting the cluster. Further, a local leader is identified among the other packets and the clusters are isolated, depending on the local leader, for refined anomaly detection.

*3.2.2. Local leader phase (LLP)*

That's an essential process for SMO algorithms. All clusters get a chance to update themselves here. Changing packet location in the cluster is mainly due to the local community leaders and the local-leader's response. Each packet fitness is computed and the fitness is updated if it is higher than that of its previous one,

$$Cnew_{l,m} = Cnew_{l,m} + dis(0,1) * (ll_{n,m} - Cnew_{lm}) + dis(-1,1) \times (C_{rm} - C_{lm}) \quad (4)$$

Where, $dis()$ is a random number in the range $(-1, 1)$ , $ll$ represents the local leader.

*3.2.3. Local leader decision Phase:*

In this phase the Local leaders had partnered with the global leader prior to this process. When no local leader is updated to a certain level, identified as the Local Leader Level, then the cluster members change their positions. The position is changed using Eqn (5). In Eqn the disturbance intensity is applied.

$$Cnew_{l,m} = Cnew_{l,m} + dis(0,1) * (gl_{n,m} - Cnew_{lm}) + dis(0,1) \times (C_{rm} - ll_{lm}) \quad (5)$$

The above equation shows that the obtained search directions and positions are being changed by the global leader. Also, the solutions are rejected by the prevailing local leaders, which is the local leaders does not updated to TL. Where, TL is the threshold counter that will be incremented when it attains a fixed value.

*3.2.4. Global leader decision phase*

Another limit namely the global leader limit, is the limit at which the global leader is not recognized. The swarm is splitinto two sub groups or combined together. The parameter GLL monitors for premature convergence within a given range, and GLC is set to zero when GLL exceeds is exceeded by GLC and the number of groups are compared with the standard groups. When the entire clusters are fewer than the predefined substantial groups, then the group is separated by the gl that will be combining to form develop into parent or a cluster.

*3.3. Hybrid FCM-SMO approach*

The packets are initially clustered using FCM and the packets are grouped into n number of clusters. The clusters are then initialized from k initial starting values. Each cluster starts finding the global and local leaders based on the position value which is the IP address of the incoming packets, fitness value that is the function of the selection probability. Finally when the algorithm reaches its optimal the clusters without anomalies (global or local leaders) are fused and clusters with these global or local points are futher divided to find the different intrudes.

The algorithm steps are given below

Step 1: Set k –Choosethe desired number of clusters, k.

Step 2: Initialization – For initial starting values k is selected.

Step 3: Classification -Find the local and global leaders;

Step 4: The local leaders updates its position value

Step 5: The global leaders updates its position value

Step 6: The learning of global leaders are performed

Step 7: The learning of local leaders are performed;

Step 8: Local leader decision and update of position.

Step 9: Use the global leader decision phase to elect fission or fusion.

Step 10: When endcriteria is attainedhalt and state the best solution or else go to step 3.

SMO works in a step by step procedure where the local leaders account for search region and global leader accounts for position updates. In local leader level every member of the cluster makes its position update and in global leader phase only the best points in the clusters updates its position value. Among other algorithms which are of search based, this feature of SMO makes it an improved one and the proposed algorithmhas got a naturalmethodfor checking the stagnation. The global leader and local leader learning phase are engaged to monitor the search operation during deadlock periods. In such cases both the leaders makes decision and anadvance exploration is made by the local leader in the decision phase, afission or fusion decision is taken. Thus the search speed is well balanced in the classification using SMO approach by the fore mentioned step being accomplished.

*3.4. Dimensionality reduction in SMO*

In this section the optimization algorithm for SM is used for the dimension reduction of the dataset. When the number of features is high during the classification, then the issue of over fitting the model occurs. The presented approach uses the SMO, which is based on the behaviour of FFSS, interacted to reduce the dimensions to resolve this problem. The various dimensional subsets will be higher in number for a dimension set size D, and the number of dimensions would allow a large dimensional space to be carefully searched for. Therefore, SMO is utilized to perform searching operation in a unique way for obtaining an optimal dimension of datasets. The dataset with better accuracy and less in error rate along with number of extracted dimensions will be the optimal one. In general, dimensional reduction is subject to objective conflicts in intrusion detection problems; to minimize the dimension count and to increase classification accuracy or decreased error rate. The presence of trade-offs between opposing priorities created difficulties in achieving optimal results. Therefore, various constraints for one goal cannot effectively address this situation. In this situation more importantly a multi-objective optimization approach is used to optimize or minimize or the objective functions. The proposed approach was intended to test a subset of dimensions, to achieve the maximum accuracy (A). This study uses precision as output metric to measure the classification error (E) of the SMO. In the evolutionary training process the fitness function FD evaluates any possible sub-set of measurements to find one that maximizes the classification accuracy used in the reduction of measurements. In SMO the fitness function fit (fn) is used to calculate individual causes, as described below;

$$fit(fn) = \lambda \times (1 - C) + (1 - \lambda) \times SD \quad (6)$$

For the extracted dimension subset C represents the classifier accuracy, λ is a constant for regularizing the dimension reduction and classification accuracy, the dimension subsets extracted is represented as S, the total number of dimensions in the [0, 1] range is represented as D. Then, for further classification the datasets resultant dimensions are passed. The classified cluster contain either of a group of detected normal packet or group of anomalous packets. The optimized classification using this hybrid approach results in high detection ratio and accuracy while reduced resource allocation.

## 4. Results and discussion

The presented method is related to existing methods and the outcomes shows better performance of the proposed work in term of, recall, F-measure, accuracy, precision, sensitivity and specificity. For results evaluation the NSL-KDD test dataset which comprise the labels for all cases in the data. For performance evaluation these observed labels are used to align with the expected labels. Attacks against networks are habitually because they appear to break into accounts with poor combinations of usernames and passwords. In order to handle some of the complications the original KDD99 dataset NSL-KDD is used.

a) Precision:

In Fig. 3 the number of data is displayed in the x-axis which is 250, 500, 750 and 1000 and y-axis shows the precision. The proposed work is matched with the prevailing methods such as hybrid FCM and SVM, hybrid FCM and ANN in terms of precision and the proposed approach attains an optimal value of 0.857, 0.884, 0.866, 0.847.

b) Recall:

In Fig. 4 the x-axis represents the number of data which is 250, 500, 750 and 1000 and y-axis shows the recall. The proposed work is matched with the prevailing methods such as hybrid FCM and SVM, hybrid FCM and ANN in terms of recall and the proposed approach attains an optimal value of 0.844, 0.842, 0.810, 0.884.

c) F measure:

The x-axis of Fig. 5 signifies the number of data which is 250, 500, 750 and 1000 and y-axis shows the f-measure. The proposed work is matched with the prevailing methods such as hybrid FCM and SVM, hybrid FCM and ANN in terms of f-measure and the proposed approach attains an optimal value of 0.850, 0.863, 0.837, 0.865.

d) Sensitivity:

The x-axis in Fig. 6 signifies the number of data which is 250, 500, 750 and 1000 and y-axis shows the sensitivity. The proposed work is matched with the prevailing methods hybrid FCM and SVM, hybrid FCM and ANN in terms of sensitivity and the proposed approach attains an optimal value of 0.887, 0.875, 0.86, 0.930.

e) Specificity:

The x-axis of Fig. 7 signifies the number of data which is 250, 500, 750 and 1000 and y-axis shows the specificity. The proposed work is matched with the prevailing methods such as hybrid FCM and SVM, hybrid FCM and ANN in terms of specificity and the proposed approach attains an optimal value of 0.805, 0.853, 0.815, 0.762.

f) Accuracy:

The x-axis in the Fig. 8 represents the number of data which is 250, 500, 750 and 1000 and y-axis shows the accuracy. The proposed work matched with the prevailing methods such as hybrid FCM and SVM, hybrid FCM and ANN in terms of accuracy and the

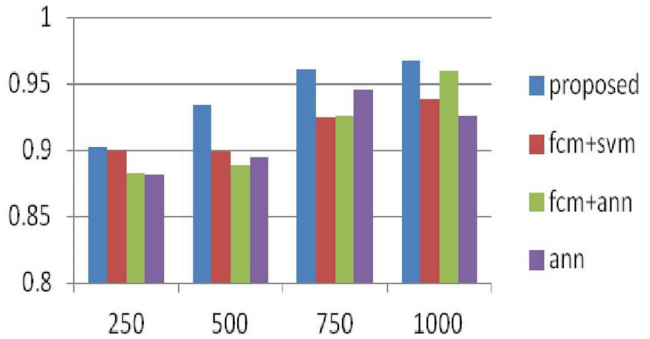


**Fig. 3.** Precision.

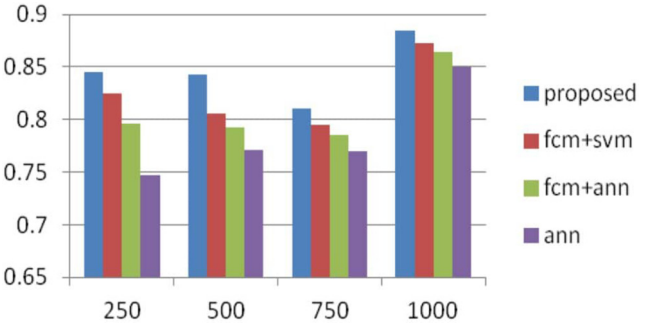


**Fig. 4.** Recall.

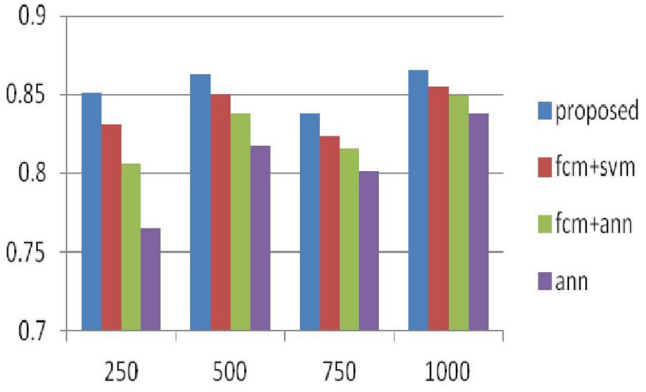


**Fig. 5.** F-measure.

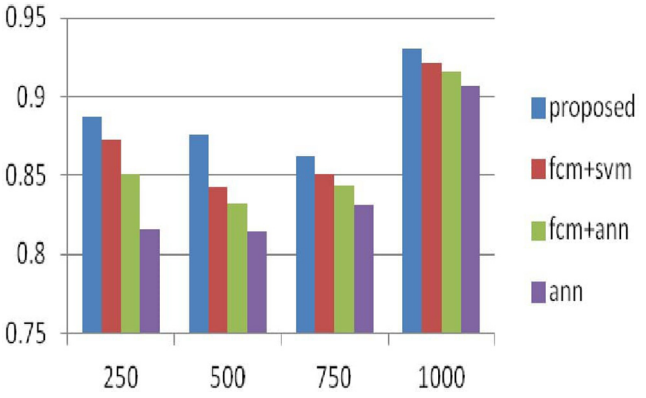


**Fig. 6.** Sensitivity.

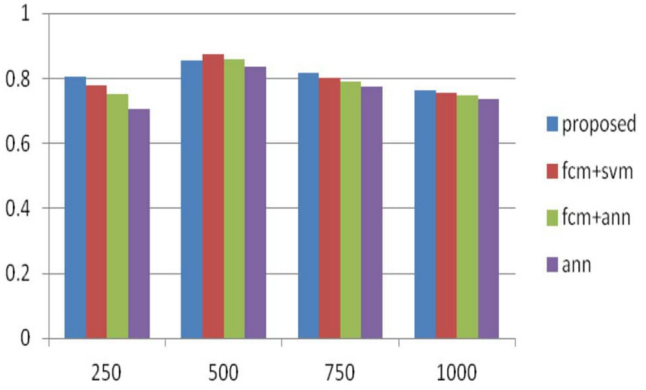


**Fig. 7.** Specificity.

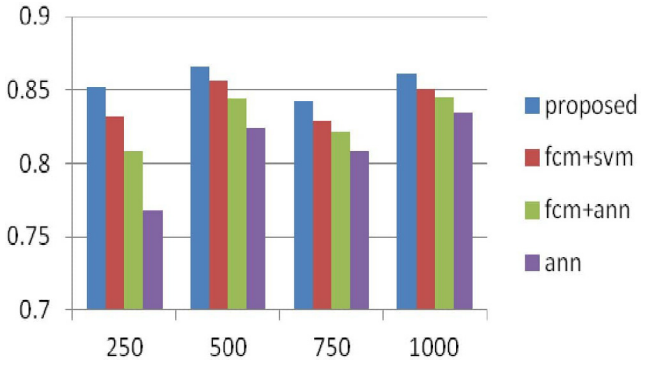


**Fig. 8.** Accuracy.

proposed approach attains an optimal value of 0.852, 0.866, 0.842, 0.86.

## 5. Conclusion

The cloud computing environment needs an improved IDS or security handler and the proposed work implements awell-established a hybrid approach of detection scheme that better suits for high traffic networks like cloud. The combined FCM-SMO clustering classification optimized approach is analyzed and tested using a standard benchmark NSL-KDD dataset. Moreover, this technique had inherited the advantages of dimensionality reduction using SMO and the classification is performed by Fuzzy clustering with SMO. Therefore, the results obtained shows that it achieves optimal values for parameters used for testing such as accuracy, precision, recall, TP rate, FN rateand F-1 score under several attacks. The performance results of the proposed approach reveals that it outperforms the compared techniques like ANN, FCM + SVM, FCM + ANN. Hence, the proposed mechanism can thus efficiently detect the anomalies to provide better security that causes increased traffic in the cloud computing environment with higher accuracy than prevailing techniques.

## CRediT authorship contribution statement

**Jitendra Kumar Samriya:** Methodology, Software, Data curation, Writing - original draft, Investigation, Software, Validation. **Narander Kumar:** Supervision, Conceptualization, Writing - review & editing, Visualization.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## References

[1] A. Velte, T. Velte, Cloud Computing: A Practical Approach, McGraw-Hill, New York, 2019.
[2] S. Prakash, Role of virtualization techniques in cloud computing environment. In: Bhatia, Advances in Computer Communication and Computational Sciences, Springer, Singapore (2019) 439–450.
[3] P. Bawa, S. Rehman, S. Manickam, Enhanced mechanism to detect and mitigate economic denial of sustainability (EDoS) attack in cloud computing environments, Int. J. Adv. Comput. Sci. Appl. 8 (9) (2017) 51–58.
[4] P. Singh, S. Manickam, S. Rehman, A survey of mitigation techniques against Economic Denial of Sustainability (EDoS) attack on cloud computing architecture. In: Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization. IEEE (2014) 1–4.
[5] O. Osanaiye, K.K. Choo, M. Dlodlo, Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework, J. Netw. Comput. Appl. 67 (1) (2016) 147–165.
[6] F. Kuang, W. Xu, S. Zhang, A novel hybrid KPCA and SVM with GA model for intrusion detection, Appl. Soft Comput. 18 (1) (2014) 178–184.
[7] C. Nkikabahizi, W. Cheruiyot, A. Kibe, Classification and analysis of techniques applied in intrusion detection systems, Int. J. Sci. Eng. Technol. 6 (7) (2017) 216–219.
[8] P. Ghamisi, J. Benediktsson, Feature selection based on hybridization of genetic algorithm and particle swarm optimization, IEEE Geosci. Remote Sens. Lett. 12 (2) (2014) 309–313.
[9] A. Saljoughi, M. Mehrvarz, H. Mirvaziri, Attacks and intrusion detection in cloud computing using neural networks and particle swarm optimization algorithms, Emerg. Sci. J. 1 (4) (2017) 179–191.
[10] K. Costa, C. Pereira, R. Nakamura, L. Pereira, J. Papa, Boosting Optimum-Path Forest clustering through harmony Search and its applications for intrusion detection in computer networks. In: 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), (2012) 181-185.
[11] S. Aljawarneh, M. Aldwairi, M. Yassein, Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model, J. Comput. Sci. 25 (1) (2018) 152–160.
[12] S. Raja, S. Ramaiah, Performance comparison of neuro-fuzzy cloud intrusion detection systems, Int. Arab J. Inf. Technol. 13 (1A) (2016) 142–149.
[13] A.N. Jaber, S.U. Rehman, FCM–SVM based intrusion detection system for cloud computing environment, Clust. Comput. (2020) 1–11.
[14] A.A. Chormale, Cloud intrusion detection system using fuzzy clustering and artificial neural network, J. Phys. Conf. Ser. 1478 (2020) 012030.
[15] S.R.K. Tummalapalli, A.S.N. Chakravarthy, Intrusion detection system for cloud forensics using bayesian fuzzy clustering and optimization based SVNN, Evolut. Intell. (2020) 1–11.
[16] R. Vijayanand, D. Devaraj, A novel feature selection method using whale optimization algorithm and genetic operators for intrusion detection system in wireless mesh network, IEEE Access 8 (2020) 56847–56854.
[17] J. Chen, X. Qi, L. Chen, F. Chen, G. Cheng, Quantum-inspired ant lion optimized hybrid k-means for cluster analysis and intrusion detection, Knowl.-Based Syst. 106167 (2020).
[18] J. Ghosh, D. Kumar, R. Tripathi, Features Extraction for Network Intrusion Detection Using Genetic Algorithm (GA). In Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough, Springer, Cham, (2020) 13-25.
[19] E. Mugabo, Q.Y. Zhang, Intrusion detection method based on support vector machine and information gain for mobile cloud computing, IJ Netw. Security 22 (2) (2020) 231–241.

## Further Reading

[1] L. Akoglu, H. Tong, D. Koutra, Graph based anomaly detection and description: a survey, Data Min. Knowl. Discov. 29 (3) (2015) 626–688.
[2] Y. Gao, Y. Liu, Y. Jin, J. Chen, H. Wu, A novel semi-supervised learning approach for network intrusion detection on cloud-based robotic system, IEEE Access 6 (2018) 50927–50938.
[3] S. Ghribi, Distributed and cooperative intrusion detection in cloud networks. In Proceedings of the Doctoral Symposium of the 17th International Middleware Conference (2016, December) 1-2.