IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8846

AN SEMI SUPERVISED ANOMALY DETECTION IN CLOUD COMPUTING BASED ON CSI-HAC CLUSTERING AND IRLS-cGAN DETECTION TECHNIQUE

Soumya Naga Chinthalacheruvu

Assistant professor, Computer Science and Engineering,Anubose Institute of Technology, palavancha, Telangana

Abstract : Identifying cyber-attacks in cloud infrastructures is essential for protecting the cloud environment from cyber-attacks. It is difficult to detect cyber-attacks in cloud infrastructures due to the complex and distributed nature of cloud infrastructures. In addition, various attacks that happen dynamically or randomly, online attacks, adversarial attacks, and data leakages increase the difficulty and complexity of cyber-attack detection. The work has proposed highly secured semi supervised anomaly detection in a cloud environment using the IRLS-cGAN detection technique. To enhance the capability of the proposed framework, the work has explored Data preprocessing, data extraction, data selection, and finally, attack classification. The approach arrests the probability of attack caused due to unnecessary data by providing a proper structuration with the help of data preprocessing that includes redundant data removal, handling categorical features, data scaling, and handling imbalanced data. In order to bring an optimal relation between the features and the outcome, the approach has extracted the informative data using GRA and selected the relevant data using the MRSO technique. Thereafter, the behavior of various environments based on clouds, VM, networking, and attacks are grouped into a cluster using the CSI-HAC technique, which is then trained to IRLS-cGAN for detecting the attacks. The results obtained demonstrate that the proposed cloud-based anomaly detection model is superior in comparison to the other state-of-the-art models (used for network anomaly detection) in terms of accuracy, detection rate, false-positive rate, and false-negative rate.

Keywords: Cloud Computing, Virtual Machine (VM), cyber security, anomaly detection, Multicollinearity, Grey Relation Analysis (GRA), Mutated Rat Swarm Optimization (MRSO), Cauchy Schwartz Inequality-Based Hierarchical Agglomerative Clustering (CSI-HAC), and Iteratively Reweighted Least-Squares-Based Conditional Generative Adversarial Network (IRLS-cGAN).

1. INTRODUCTION

Nowadays, cyberspace development is increasing rapidly because of cloud computing, big data, the Internet of Things, and software-based network growth [1]. One of the common problems in cyberspace is cyber security. Cyber security is a means of safeguarding the systems, applications, and networks from potential digital attacks [2]. The main aim of the adversaries which conduct these attacks is to modify/access confidential information, laundering money from the users, and interrupting normal business operations [3]. The challenges associated with implementing cyber security policies on organizations are the large number of devices connected to the network and the novel attacks conducted by hackers [4]. The different kinds of attacks are prevented by using tools like the intrusion detection system, firewalls, scanner, and antivirus software, etc. The devices connected to the network are often subjected to various attacks [5]. The cyber security system is affected by different kinds of attacks such as a denial of service, probe, malware, zero-day, phishing, sinkhole, user root, adversarial attacks, poisoning attack, evasive attack, Integrity attack, and causative attack [6, 7].

Modern big data analytics powered by machine learning (ML), data science, and artificial intelligence (AI) capabilities are emerging as a powerful solution [8, 9]. Building a machine powered with adaptive baseline behavior models will be super effective in detecting new unknown attacks [10]. Considering previous and current data with predictive analytics and machine intelligence for security including intelligence will boost the CS perspective tremendously [11, 12]. Most of the researchers have used deep learning concepts for the detection of attacks. Even though DL demonstrates excellent suitability for cyber security applications, day-to-day cyber-attacks are increasing with more sophistication and also hackers started to use the deep learning (DL) model rapidly to build suspicious data, etc [13]. In order to conquer this

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8846

issue, the work has developed Semi Supervised anomaly detection in the cloud computing using IRLS-cGAN detection technique.

The rest of the paper is organized as Section 2 reviews various attack detection frameworks, section 3 illustrates the proposed methodology for detecting an attack, section 4 discusses the obtained result for the proposed work and section 5 concludes the work.

2. LITERATURE SURVEY

Sahil Garg et al. [14] developed a hybrid data processing model for network anomaly detection that leveraged Grey Wolf Optimization (GWO) and Convolutional Neural Network (CNN). It worked in two phases for efficient network anomaly detection. In the first phase, ImGWO was used for feature selection in order to obtain an optimal trade-off between two objectives, i.e., reduced error rate and feature-set minimization, and then fed to CNN for detection of an anomaly. The results demonstrated that the cloud-based anomaly detection model was superior in comparison to the other state-of-the-art models (used for network anomaly detection), in terms of accuracy, detection rate, false-positive rate, and F-score. The approach was highly vulnerable to evasive as well as causative attacks.

Shalini Batra et al. [15] illustrated an Ensemble Artificial Bee Colony-based Anomaly Detection Scheme (En-ABC) for multi-class datasets in a cloud environment. En-ABC performed certain step-by-step processes: i) feature selection and optimization ii) data clustering, and iii) identification of the anomalous behavior of nodes. Experimental results on the benchmark (NSL-KDD, NAB, and IBRL) and synthetic datasets validated the effectiveness of the scheme. The approach was unable to detect uncertain attacks, which made the model inefficient.

Shalini Batra et al. [16] developed a Fuzzified Cuckoo-based Clustering Technique (F-CBCT) anomaly detection technique, which operated in two phases: training and detection. The training phase was supported with a Decision Tree followed by an algorithm based on hybridization of Cuckoo Search Optimization and K-means clustering. Experimental results in terms of detection rate (96.86%), false-positive rate (1.297%), accuracy (97.77%), and F-Measure (98.30%) proved the effectiveness of the developed model, but the approach was not reliable.

Mahmoud Abdelsalam et al. [17] introduced a novel online malware detection approach in the cloud that leveraged one of its unique characteristics—auto-scaling. Auto-scaling in the cloud maintained an optimal number of running VMs based on the load that dynamically adds or terminates the VMs. The detection system was online and it detected malicious behavior while the system was running. Malware detection was performed that utilized process-level performance metrics to model a Convolutional Neural Network (CNN). The 2d CNN approach reaches an accuracy of 90% for malware detection, but the adversarial attacks were unable to detect or prevent.

3. PROPOSED SEMI SUPERVISED FRAMEWORK FOR ANOMALY DETECTION IN CLOUD COMPUTING

Cloud concepts such as resource sharing, outsourcing, and multi-tenancy create significant challenges to the security community. Also, trusted third party and web technologies-based cloud service provisioning arises new security threats in the cloud environment. The detection of anomalies in data has become a vital research area within cyber security. Despite various IDS-based models had been developed, the fact is that the existing cloud security research still faces shortcomings in improving the detection accuracy and detecting the new or unknown attacks in the cloud. To address the constraints above the work has developed semi supervised anomaly detection in the cloud computing using IRLS-cGAN detection technique as illustrated in figure 1.

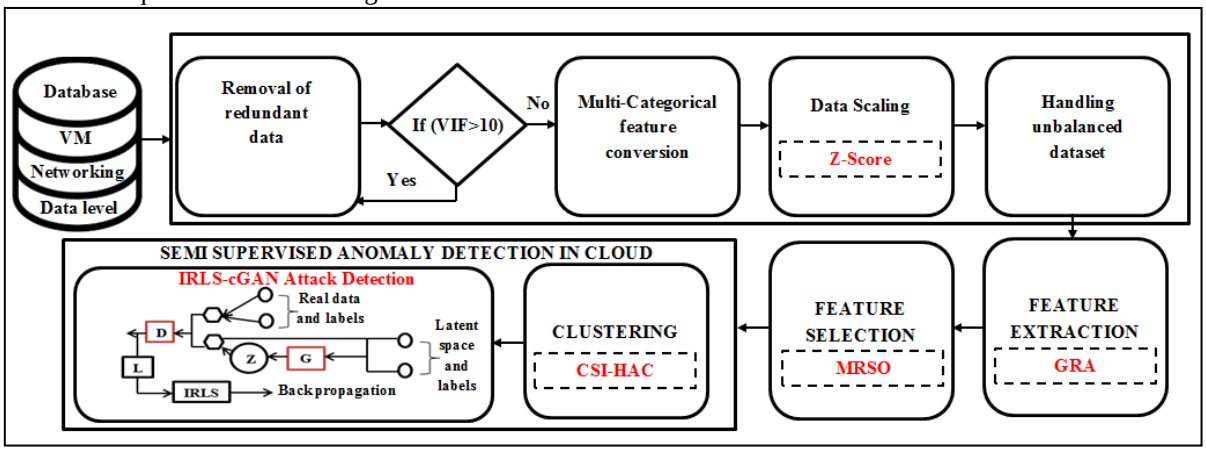

Figure 1: Proposed Semi Supervised framework for semi supervised anomaly detection in cloud computing

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8846

3.1. PREPROCESSING

Preprocessing improves the structure of data in order to avoid the chances of error for detecting anomalies or attacks. The Preprocessing phase involves the removal of redundant data, categorical feature conversion, data scaling, and balancing the data.

3.1.1. Removal of Redundant Data

The features are evaluated under Multicollinearity that finds out the features that are highly correlated with one or more independent features and remove the correlated features in order to reduce the complexity as well as computational time. Sometimes, the correlated features may lead to undermining the significant data present in the dataset.

$$\Re_{VIF} = \frac{1}{1-\Im_i^2(\Gamma_{i,j})} \tag{1}$$

Where, $\Re_{VIF}$ denotes the variance inflation factor which evaluates the Multicollinearity for the input feature $\Gamma_{i,j}$ at the row and column, $\Im_i^2$ denotes the R-Squared value.

3.1.2. Categorical feature conversion

Categorical features constrain informative data needed for detecting an attack, but without considering the categorical feature may reduce the accuracy of improving an attack. In order to avoid that, the work uses KDD orange multi-categorical variable conversion into numeric data, so that the model can make the decision over the categorical data. The conversion performs multi variable categorical conversion by taking the top 10 frequent labels and performs the one-hot encoding for the 10 labels.

$$\Re_{cat} = C_{KDD}^{10}(frq(\Gamma_{i,j})) \tag{2}$$

3.1.3. Data Scaling

Data scaling provides to standardize the features into one scaling or one unit. Data scaling helps to process the data quickly, it also contributes to a fast convergence rate. The work adapts Z-score standardization to scale down the features.

$$\Re_{Scaling} = \frac{\Gamma - \overline{\Gamma}}{\sigma} \tag{3}$$

Where, $\overline{\Gamma}$ and σ denotes the mean and standard deviation of the features.

3.1.4. Handling Unbalanced data

Unbalanced data leads to a high false prediction of attack, which may collapse the entire working network. In order to conquer this, the data are initially counted. If it is balanced then no need for any computation but, if it is unbalanced then Random Over Sampler is used to handle the dataset and makes them into balance form.

$$\Re_{UB} = RandomOverSampler(\Gamma_{i,j}) \tag{4}$$

3.2. FEATURE EXTRACTION

Feature extraction helps to get the most relevant informative data from the dataset to outcome the accurate result of detecting the attack. Feature extraction extracts the relevant features by analyzing the relation between the independent variables and dependent variables. The features are analyzed based on a Grey relation analysis that finds out the correlation among the features and sorts it down based on the rankings.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8846

$$G\left[\left(\Gamma_{i,j}^{0},\Gamma_{i,j}^{1}\right)\right]=\frac{\Delta\min+Q\Delta\max}{s.d+Q\Delta\max},\ 0<G\left[\left(\Gamma_{i,j}^{0},\Gamma_{i,j}^{1}\right)\right]\leq 1 \tag{5}$$

$$G\left[\left(\Gamma_{i,j}^{0},\Gamma_{i,j}^{1}\right)\right]=\sum_{i=1}^{n}\sum_{j=1}^{m}\chi_{k}G\left[\left(\Gamma_{i,j}^{0},\Gamma_{i,j}^{1}\right)\right] \tag{6}$$

The equation 6 states that the grey relational grade (GRR) represents the level of correlation between the dependent and independent variables. If GRR is equal to 1 then, the two feature series are identical to each other. GRR also shows the level of influence applied to the dependent and independent variables.

3.3. FEATURE SELECTION

Feature selection provides with selecting the best set of attributes to build a useful classification model. Feature selection helps in reducing the computation time, and at the same time, improves the accuracy of the model. The work has developed a Mutated Rat swarm optimization (MRSO), which works based on the objective of ranked features.

The feature selection algorithm is initiated by initializing the best search agent rat or features which have the location of the prey. Now, based on the best search agent, the following rat's updates their position using:

$$\vec{\Phi}=\mathrm{A}\vec{\Phi}_{i}(\Gamma_{i,j})+\mathrm{E}\left(\vec{\Phi}_{r}(\Gamma_{i,j})-\vec{\Phi}_{i}(\Gamma_{i,j})\right) \tag{7}$$

$$\mathrm{A}=\eta-x\times\left(\frac{rand}{I_{\max}}\right)$$
$$\mathrm{E}=2.rand() \tag{8}$$

Where, $\vec{\Phi}_{i}(\Gamma_{i,j})$ defines the positions of rats and $\vec{\Phi}_{r}(\Gamma_{i,j})$ represents the best optimal solution, R and C are random numbers between [1, 5] and [0, 2], respectively. The parameters A and C are responsible for better exploration and exploitation over the course of iterations.

Now, the mutation is performed for obtaining a global best solution:

$$\vec{\Phi}_{i}(\Gamma_{i,j})=\begin{cases}\Gamma_{gbest,j}+\gamma\left(\Gamma_{p,h}-\Gamma_{q,h}\right) & rand_{i,j}<\mathrm{M}\\ \Gamma_{i,j} & else;\end{cases}$$
$$\mathrm{M}=0.05\vec{\Phi}_{i}(\Gamma_{i,j})$$
$$where,\ p,q\in\{1,2,.....,i-1,i+1,....K\},\gamma\in[0,1] \tag{9}$$

Based on the mutation, the updation of the position of the rat is evaluated using:

$$\vec{\Phi}_{i}(\Gamma_{i,j}+1)=\left(\vec{\Phi}_{r}(\Gamma_{i,j})-\vec{\Phi}_{i}\right) \tag{10}$$

Where, $\vec{\Phi}_{i}(\Gamma_{i,j}+1)$ defines the updated next position of the rat. It saves the best solution and updates the positions of other search agents with respect to the best search agent.

3.4. ANOMALY DETECTION IN CLOUD COMPUTING

Anomaly detection helps the cloud platform administrators by analyzing the cloud behavior pattern and improves the reliability of the cloud services from malicious attacks. The work has developed a semi-supervised anomaly or attack detection framework. Initially, the selected features get learned by Cauchy Schwartz inequality-based Hierarchical Agglomerative Clustering (CSI-HAC) which is able to handle uncertain data attacks and able to recognize it without any

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8846

training and also cluster the various behavior of the cloud, VM, Networking. Thereafter, the developed cGAN detects the attacks based on the conditions generated.

3.4.1. Clustering

The CSI-HAC Clustering forms the clusters of the data points until all data points get merged into one cluster point. Initially, a distance matrix is formed for each data point using Euclidean distance based on Cauchy Schwartz inequality, which is used to improve the performance of the clustering. The method specifies how geometrically well separated the clusters should be

$$ED_{i,j} = \left(\sum_{i,j=0}^{n} \left(\Gamma_{i,j} \Gamma_{i,j}^{\phi} \right)^2 - \left(\sum_{i,j=0}^{n} \Gamma_{i,j} \right)^2 \left(\sum_{i,j=0}^{n} \Gamma_{i,j}^{\phi} \right)^2 \right) \tag{11}$$

$$\Phi_{i,j}^{+} = \begin{bmatrix} \Gamma_{1\times1} & \Gamma_{1\times2} & \cdots & \Gamma_{1\times n} \\ \Gamma_{2\times1} & \Gamma_{2\times2} & \cdots & \Gamma_{2\times n} \\ \vdots & \vdots & \cdots & \vdots \\ \Gamma_{n\times1} & \Gamma_{n\times2} & \cdots & \Gamma_{n\times n} \end{bmatrix} \tag{12}$$

Where, $\Gamma_{i,j}$ and $\Gamma_{i,j}^{\phi}$ represents the two different data points. Now, each feature within the matrix is grouped into the cluster using a single linkage minimum distance $\left(\Phi_{i,j}^{+} \in \Theta_i \right)$. For the matrix, the minimum distance of the features is computed by using

$$D(\Phi_{i,j}^{+}) = \min imum\{ED_{i,j} R\left(\Phi_{i,j}^{+}\right) + C\left(\Phi_{i,j}^{+}\right) : R, C \in Rows\ and\ columns\} \tag{13}$$

The region that has the minimum distance is formulated into the cluster $\left(\Theta_j\right)$ and now the change in the cluster is given by:

$$\Theta_j = \Theta\left\{\Theta_n^{\Phi}\right\} \tag{14}$$

The iteration continues until the distance value becomes negative and all the features get into one cluster point. The outcome of the clustering will constrain different information or behavior regarding the cloud, VM, networking, attacks, etc.

3.4.2. Attack Detection

Attack detection is carried out based on the clustered data to train the model. The work has developed an Iteratively Reweighted Least-Squares-Based Conditional Generative Adversarial Network (IRLS-cGAN). The approach consists of discriminator $\left(\Omega\right)$ and generator models $\left(\Psi\right)$ which are conditioned on some extra class labels $\left(\Theta_j\right)$. The generative model is capable of generating attack data $\left(\Psi\left(z^*\right)\right)$by adding up some noises $\left(z^*\right)$ from the trained real data $\left(\Theta_j\right)$. Its role is to generate an adversarial data sample over real sampled clusters. On the other hand, Discriminator gets trained with the real sampled clusters $\left(\Theta_j\right)$and returns the probability saying that the data is real and it is from real sample points rather than generated by the generator. The ultimate aim of the cGAN is that the generator maximizes the probability $\left(P_{\Psi}\right)$ by saying Ψ is not real data and for the Discriminator is to do the opposite. The generator and discriminator play a two-player min-max game and at one point, they come to the conclusion with a unique solution. The value function is computed as:

$$\min_{\Psi} \max_{\Omega} \nu(\Omega, \Psi) = \forall_{x\sim Pdata(x)} \left[\log \Omega(\Theta_j)\right] + \forall_{Z^*\sim P_Z(Z^*)} \left[\log(1 - \Omega(\Psi(\Theta_j \mid z^*)))\right] \tag{15}$$

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8846

Now, the work has initiated with iteratively reweighted least squares (IRLS) to achieve the optimum solution, which is

$$loss = \arg\min_{v} \sum_{i=1}^{n} \left| \zeta_i - f_i(v) \right|^2$$
$$v^{t+1} = \arg\min_{v} \sum_{i=1}^{n} w_i\left(v^t\right) \left| \zeta_i - f_i(v) \right|^2 \quad (16)$$

Where, ζ_i denotes the dependent variables, $f_i(v)$ denotes the predicted value w_i represents the weight matrix and v^{t+1} denotes the updated predicted value

The IRLS obtains maximum likelihood solutions and avoids computational complexity and is capable of detecting the attacks with great accuracy.

4. RESULTS AND DISCUSSION

The proposed Semi supervised framework for anomaly detection in cloud computing is validated experimentally based on various performance metrics and compared with existing methodologies to observe the efficiency of the framework. The work is carried out based on NSL-KDDCUP99, CIDDS-001 dataset's in the working platform of python.

4.1. Evaluation of Proposed IRLS-cGAN based on various metrics

The proposed IRLS-cGAN is analyzed based on Accuracy, Specificity, Sensitivity, Precision, F-Measure, FPR, FNR, and MCC metrics and compared with artificial neural network (ANN), Adaptive Neuro-Fuzzy Interface System (ANFIS), Convolutional neural network (CNN), and Ensemble Learning (EL). The evaluation is tabulated in table 1.

Table 1: Evaluation of proposed IRLS-cGAN based on Accuracy, Specificity, Sensitivity, and Precision

Performance metrics/techniques	ANN	ANFIS	CNN	EL	Proposed IRLS-Conditional GAN
Accuracy	85.69	85.65	88.95	87.85	92.31
Specificity	85.99	84.99	85.65	86.65	92.56
Sensitivity	86.47	85.45	84.56	87.88	92.99
Precision	87.45	84.56	85.66	88.92	93.65

Table 1 illustrates the validation value obtained for various metrics which are formulated based on the true negative (TN), true positive (TP), false negative (FN), and false positive (FP). For a model to perform well, it should be capable of obtaining a high accuracy, specificity, sensitivity, and precision value. According to that, the proposed technique tends to obtain an accuracy of 92.31%, specificity of 92.56%, the sensitivity of 92.99%, and precision of 93.65% whereas the existing methods achieve metrics ranging between 84.99 % and 88.92 %, which is comparatively low compared to the proposed approach. The proposed IRLS-cGAN method achieves a better metrics value and is capable of detecting an adversarial attack, dynamic attacks, and proved to be efficient as compared to the existing methods. In order to analyze the proposed method's reliability and misclassification rate, the method is graphically validated based on F-measure, FPR, FNR, and MCC in figure 2.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8846

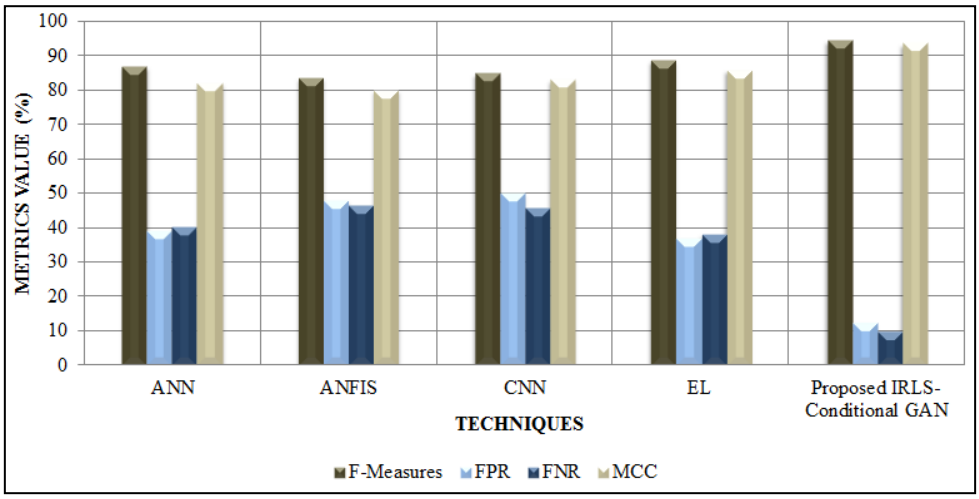

Figure 2: Graphical Analysis of proposed IRLS-cGAN based on Various Metrics

The reliability of the approach in order to handle various datasets under dynamic circumstances is very much important to maintain cyber security. Considering the reliability of the metrics MCC, F-measure is evaluated for the proposed classification techniques. The proposed method achieves an F-Measure and MCC value of 94.56%, and 93.65%, respectively whereas the existing method tends to achieve a low F-Measure and MCC value that ranges between 80.11%-88.74%, which represents a highly non-reliable model. In addition to that, the proposed IRLS-cGAN is evaluated based on FPR and FNR metrics for validating the misclassification of the attacks. According to that, the proposed methods achieve an FPR of 12.32% and FNR of 10.01%, whereas the existing techniques tend to achieve a high misclassification which decreases the model efficiency.

4.2. Evaluation of Proposed IRLS-cGAN based on Attack Detection Rate

Attack detection rate illustrates how accurately the IRLS-cGAN detects various attacks according to the training given. The graphical representation of the attack detection rate is illustrated in figure 3.

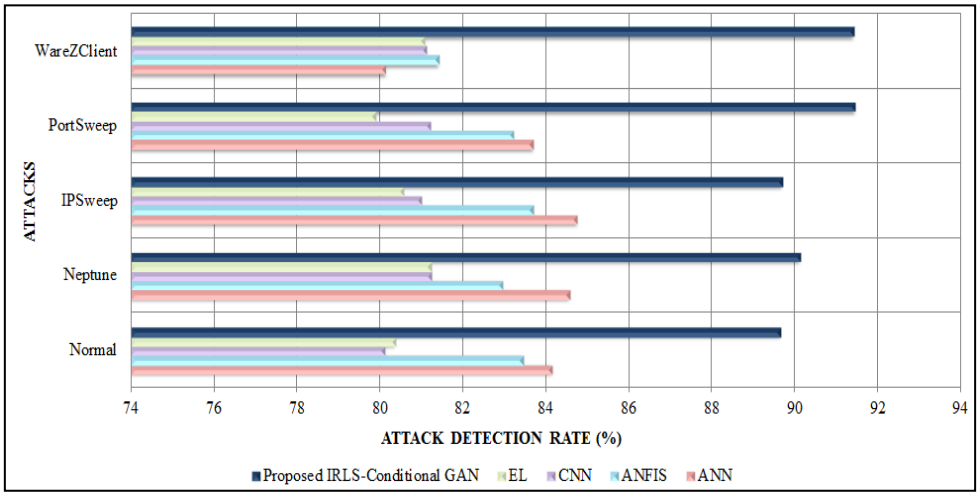

Figure 3: Graphical Analysis of proposed IRLS-cGAN based on ADR

The analysis is carried based on the attacks such as Neptune, PortSweep, IPSweep, WareZClient, and normal. Based on the attacks, the proposed IRLS-cGAN detects each attack accurately that ranges between 96.52% -99.88%, whereas the existing EL, CNN, ANFIS, and ANN achieve an attack detection rate ranging between 79.89% to 84.75%, which is comparatively lower than the proposed technique. Thus, the proposed approach achieves a better detection of an attack and is capable of detecting uncertain attacks.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.8846

5. CONCLUSION

The work provides a novel semi supervised framework for anomaly detection in cloud computing using the benchmark dataset available publically. The work suits best for avoiding most of the uncertain attacks, adversarial attacks, and various online attacks and maintains confidential integrity and availability of data. The framework traps all the back doors for attackers by performing a robust structuration of data that includes: redundant data removal, handling categorical variables, scaling of data, and handling the unbalanced data. The informative information from the data is extracted by using the GRA technique and the relevant feature is selected using the MRSO technique so as to reduce the data congestion and to improve the accuracy of the model. Thereafter, various behavior of the networking, cloud, VM, etc is clustered using CSI-HAC technique and then the clustered data is trained to the IRLS-cGAN, which detects various vulnerabilities of attacks. The approach handles various random attacks and also secures the cloud environment from being attacked. The experimental outcome showed that the model tends to be superior to the existing methodology that achieves an accuracy of 92.31%, and an average attack detection rate of 90.46%. It also avoids mis-predictions of attacks by obtaining an FPR of 12.32% and an FNR of 10.01%.

REFERENCES

1. Chenquan Gan, Qingdong Feng, Xulong Zhang, Zufan Zhang and Qingyi Zhu, “Dynamical propagation model of malware for cloud computing security”, IEEE Access, vol. 8, pp. 20325-20333, 2020.
2. Michele De Donno, Alberto Giaretta, Nicola Dragoni, Antonio Bucchiarone and Manuel Mazzara, “Cyber-storms come from clouds security of cloud computing in the iot era”, Future Internet, vol. 11, no. 6, pp. 1-30, 2019.
3. Deval Bhamare, Maede Zolanvari, Aiman Erbad, Raj Jain, Khaled Khan and Nader Meskin, “Cybersecurity for industrial control systems a survey”, computers & Security, 2020, DOI:10.1016/j.cose.2019.101677.
4. Md Tanzim Khorshed, ABM Shawkat Ali and Saleh A. Wasimi, “Trust issues that create threats for cyber attacks in cloud computing”, In 2011 IEEE 17th international conference on parallel and distributed systems, IEEE, 7-9 Dec. 2011, Tainan, Taiwan, 2011.
5. Charles Kamhoua, Andrew Martin, Deepak K. Tosh, Kevin A. Kwiat, Chad Heitzenrater and Shamik Sengupta, “Cyber-threats information sharing in cloud computing a game theoretic approach”, In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, IEEE, 3-5 Nov. 2015, New York, NY, USA, 2015.
6. Kakkad, Vishruti, Hitarth Shah, Reema Patel, and Nishant Doshi, “A Comparative study of applications of Game Theory in Cyber Security and Cloud Computing”, Procedia Computer Science, vol. 155, pp. 680-685, 2019.
7. Olusola Akinrolabu, Jason RC Nurse, Andrew Martin and Steve New, “Cyber risk assessment in cloud provider environments current models and future needs”, Computers & Security, vol. 87, pp. 1-18, 2019.
8. Saurabh Dey, Qiang Ye and Srinivas Sampalli, “A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks”, Information Fusion, vol. 49, pp. 205-215, 2019.
9. Abebe Abeshu and Naveen Chilamkurti, “Deep learning the frontier for distributed attack detection in fog-to-things computing”, IEEE Communications Magazine, vol. 56, no. 2, pp. 169-175, 2018.
10. Rafał Kozik, Michał Choraś, Massimo Ficco and Francesco Palmieri, “A scalable distributed machine learning approach for attack detection in edge computing environments”, Journal of Parallel and Distributed Computing, vol. 119, pp. 18-26, 2018.
11. Mahdi Rabbani, Yong Li Wang, Reza Khoshkangini, Hamed Jelodar, Ruxin Zhao and Peng Hu, “A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing”, Journal of Network and Computer Applications, vol. 151, pp. 1-13, 2020.
12. Hyunjoo Kim, Jonghyun Kim, Youngsoo Kim, Ikkyun Kim and Kuinam J. Kim, “Design of network threat detection and classification based on machine learning on cloud computing”, Cluster Computing, vol. 22, no. 1, pp. 2341-2350, 2019.
13. Ram Mahesh Yadav, “Effective analysis of malware detection in cloud computing”, Computers & Security, vol. 83, pp. 14-21, 2019.
14. Sahil Garg, Kuljeet Kaur, Neeraj Kumar, Georges Kaddoum, Albert Y. Zomaya and Rajiv Ranjan, “A hybrid deep learning-based model for anomaly detection in cloud datacenter networks”, IEEE Transactions on Network and Service Management, vol. 16, no. 3, pp. 924-935, 2019.
15. Sahil Garg, Kuljeet Kaur, Shalini Batra, Gagangeet Singh Aujla, Graham Morgan, Neeraj Kumar, Albert Y. Zomaya and Rajiv Ranjan, “En-ABC an ensemble artificial bee colony based anomaly detection scheme for cloud environment”, Journal of Parallel and Distributed Computing, vol. 135, pp. 219-233, 2020.
16. Sahil Garg and Shalini Batra, “Fuzzified cuckoo based clustering technique for network anomaly detection”, Computers & Electrical Engineering, vol. 71, pp. 798-817, 2018.
17. Mahmoud Abdelsalam, Ram Krishnan and Ravi Sandhu, “Online malware detection in cloud auto-scaling systems using shallow convolutional neural networks”, IFIP International Federation for Information Processing, 2019, Doi: 10.1007/978-3-030-22479-0_20.
18. Gladia Angeline P; Jagadesh S; Jeba Christina D; Nevetha G; Poornima L. "Efficient and Enhanced Data Encryption in Cloud Computing". International Research Journal on Advanced Science Hub, 2, 3, 2020, 1-4. doi: 10.47392/irjash.2020.16
19. Mohd Akbar; Irshad Ahmad; Thirupathi Regula. "Study and improved data storage in cloud computing using cryptography". International Research Journal on Advanced Science Hub, 3, Special Issue ICOST 2S, 2021, 94-99. doi: 10.47392/irjash.2021.046
20. Karthikraj H; Savitha V; Pavithra M; Mohammed Fayyaz K M; Sangeetha K. "Doctor Appointment System Using Cloud". International Research Journal on Advanced Science Hub, 3, Special Issue ICARD-2021 3S, 2021, 13-17. doi: 10.47392/irjash.2021.053
21. Babitha M N; Siddappa M. "A Review on Data protection and privacy in Fog Computing Network". International Research Journal on Advanced Science Hub, 3, Special Issue ICIES-2021 4S, 2021, 1-5. doi: 10.47392/irjash.2021.101
22. Dharshika S; Nagaraj G Cholli. "Green Cloud Computing: Redefining the future of Cloud Computing". International Research Journal on Advanced Science Hub, 3, Special Issue 7S, 2021, 12-19.

