International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7433
***Article Received**: 14 May 2023 **Revised:** 30 June 2023 **Accepted:** 30 July 2023*

A Hybridized- Logistic Regression and Deep Learning-based Approaches for Precise Anomaly Detection in Cloud

Banavathu Rajarao[1], Meruva Sreenivasulu[2]
[1]Research Scholar, Department of Computer Science and Engineering
Jawaharlal Nehru Technological University Anantapur
Ananthapuramu-515002, India
b.rajarao1207@gmail.com
[2]Department of Computer Science and Engineering, Professor K.S.R.M College of Engineering, Kadapa
Affiliated to Jawaharlal Nehru Technological University Anantapur
Ananthapuramu-515002, India
mesrinu@rediffmail.com

Abstract—Anomaly Detection plays a pivot role in determining the abnormal behaviour in the cloud domain. The objective of the manuscript is to present two approaches for Precise Anomaly Detection Approaches by hybridizing RBM with LR and SVM models. The various phases in the present approach are (a) Data collection (b) Pre-processing and normalization; OneHot Encoder for converting categorical values to numerical values followed by encoding the binary features through normalization (c) training the data (d) Building the Feedforward Deep Belief Network (EDBN) using hybridizing Restricted Boltzmann Machine (RBM) with Logistic Regression (LR) and Support Vector Machine (SVM); In the first approach, RBM model is trained through unsupervised pre-training followed by fine-tuning using LR model. In the later approach, RBM model is trained through unsupervised pre-training followed by fine-tuning using SVM model; both the approaches adopt unsupervised pre-training followed by supervised-fine-tuning operations (e) Model Evaluation using the significant parameters such as Precision, Recall, Accuracy, F1-score and Confusion Matrix. The experimental evaluations concluded the effective anomaly detection techniques by integrating the RBM with LR and SVM for capturing the intricate patterns and complex relationships among the data. The proposed approaches paves a path to improved anomaly detection technique, thereby enhancing the security features and anomaly monitoring systems across distinct domains.

Keywords-Deep Belief Network, RBN, SVM, Logistic Regression, OneHot Encoding

I. INTRODUCTION

Cloud computing is an inevitable advancement in modern computing technology providing access to utilise the computing resources on-demand. Due to incrementalscale and complexity in cloud environment, the security in cloud is challenging eventually landing up in detection of anomalies. Accordingly, to detect anomalies in cloud, a Hybridized-Logistic Regression and Deep Learning based approach is put forth.

Cloud computing a trending paradigm in information technology reformed the routineof businesses and individuals in leveraging the computing resources.As shown in Figure 1 and Figure 2, cloud computing allows sharing of computing resources from the pool of networks, servers, applications, storage data though internet; thus cutting the costs for organizations such as local resources and maintenance costs. With high scalability, flexibility, and low cost organizations prefer cloud computing rather than complex IT technologies or infrastructures as the resources can be accessed and utilised on-demand. Thus, embracing of cloud computing in organisations increases the significance of security in cloud domain.

Anomaly detection guarantees security and stability in cloud environment. Anomalies indicate abnormal behaviour that arise due to software or hardware failures, network traffic, security breaches or malicious attacks. The timely detection and remediation of anomalies eradicate service hindrances, data or financial loss and damage of resources for both service providers and users of several areas as shown in Figure 3. When anomalies are addressed promptly, organizations ensure stability and reliability thus improvising the system performance. For anomaly detection to be effective, detection techniques need to be pro-active and robust. Undoubtedly, pro-activeness in detection and remediation of anomalies, benefits the service providers to deliver uninterrupted service at minimal cost and time with optimum resources. Ultimately, the users access cloud services without hurdles and security

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7433
***Article Received**: 14 May 2023 **Revised:** 30 June 2023 **Accepted:** 30 July 2023*

breaches at minimal cost. Moreover, anomaly detection smoothens planning of resource allotment and fetching relevant data and patterns from data pool in cloud at optimum time. Consequently, more pro-active the anomaly detection technique better the user experience.

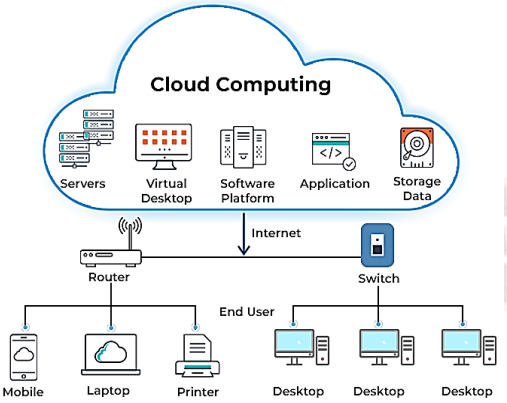

Figure 1. Cloud Computing Architecture (Courtesy: Source [11])

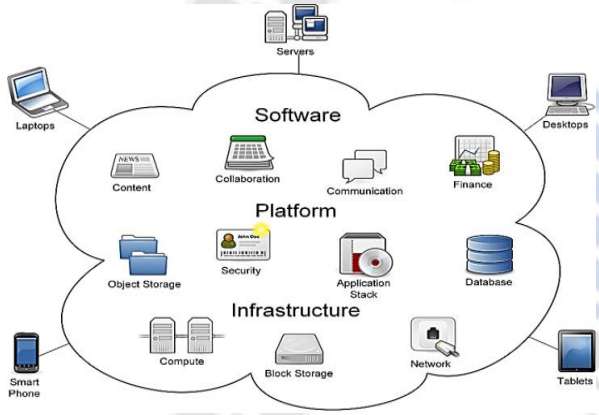

Figure 2. Work-Flow of Cloud Domainsummarized from [12] (Courtesy: Source [12])

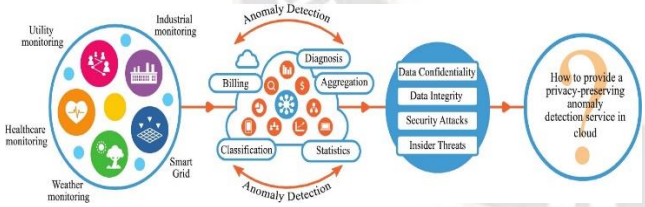

Figure 3. Anomaly Detection (Courtesy: Source [13])

Machine Learning (ML) techniques are promising to detect anomalies in cloud environment. ML is capable to analyse huge volume and complex data and has the capacity to capture relative patterns. The train and test data of ML models can differentiate the odd data from the normal one. Unlike the traditional rule based models, ML models identify even minor deviations in patterns. ML based anomaly detection techniques afford automation, adaptability, scalability and reliability for cloud computing.

In this proposed work, Hybridized Logistic Regression is combined with Deep Learning (DL) approaches to detect the anomalies in Cloud. The classic statistical model Logistic Regression performs well in binary classification. In anomaly detection, the decision making and probabilistic techniques are utilized to interpret if the features fed are normal or anomalous.

DL techniques leverage artificial neural networks, deep neural networks and convolution neural networks in studying hierarchical data representation, natural language processing (NLP),anomaly detection. DL models analyse intricate complex patterns, dependencies and non-linear relationships amicably influencing accuracy and efficiency of the investigating model. Moreover, DL models handle large scale datasets in various domain efficiently which is pre-requisite for anomaly detection where multiple sectors are handled by and large.

Thus in this proposal, the strengths of Hybridized Logistic Regression in interpreting the anomaly and DL models' feature extraction capacities are applied to build an amicable, efficient and effective model to detect anomalies.

II. SUMMARY OF EXISTING METHODS

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

The following section summarizes the salient features of existing methods regarding the anomaly detection in Cloud Domain.

Gao and Zhu [1] formulated a fault detection technique in cloud computing through Deep Learning (DL). The Depth Learning based fault detection method detected abnormality in cloud apart from determining the faults. The Depth Learning model involve an auto encoder wherein a parallel network was constructed through sparse denoising. For the verification purpose, four different fault types were considered namely process, network, resources and normal status with the sample size of 200, 200, 200 and 100. The metrics True Positive Rate (TPR) and Subsequence False Positive Rate (SFPR) were evaluated for the three networks Auto-Encoder, Sparse Auto-Encoder and Sparse Denoising Auto encoder in addition to the traditional algorithms BP, SVM and Depth Auto-Encoder Networks - Series and Parallel. Comparative results exhibit depth auto-encoder with sparse denoising accurate fault detection capacity in cloud.

Garg and his research team [2] proposed hybrid DL anomaly detection model in cloud. The Grey Wolf

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7433
***Article Received**: 14 May 2023 **Revised:** 30 June 2023 **Accepted:** 30 July 2023*

Optimization (GWO) and Convolution Neural Network (CNN) were enhanced to improve the exploration, exploitation capacity as well as the dropout functionality. The Improved GWO (ImGWO) extracted features with the objective to reduce error rate and minimize feature set; and additionally Improved CNN (ImCNN) classified the network anomaly. Upon investigation on DARPA'98,KDD'99 and synthetic datasets for efficacy, the performance metrics vis-à-vis detection rate, accuracy and false positives exhibited a large improvement of 8.25%, 3.62% and 4.08% respectively.

Rai, Saxena and Manoria[3] designed a Machine Learning (ML) framework for intrusion based Anomaly Detection System (ADS) in cloud that can withstand high traffic, excess load, larger resources and users. The framework was evaluated on the basis of certain parameters namely Recall, Precision, Accuracy, True positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). Each parameter indicated the performance of IDS: TP-Prediction correctness of Attack; TN-Prediction correctness of Normal Behaviour; FP-System capacity to Detect intrusion; FN-System susceptibility to intrusion. The framework was experimented on KDD and NSSKDL dataset for high TP and TN to exhibit the superiority of the present work. Moreover, the framework was experimented on different approaches, IDS, and datasets respectively. The comparative result proved superiority with the value of Precision-99%, Accuracy-98%, and Recall Rate-97% approximately.

Nedelkoski, Cardoso and Kao [4] implemented Distributed tracing and DL based anomaly detection and classification technique. The entire technique involved time series preprocessing where data was cleaned, normalized, and noise removed; model training comprising layers such as input layer, First hidden GRU layer, sampling layer, Repeat layer and output layer where response time acts as base; test-time prediction and faulty pattern classification. When experimented, the present work exhibited more than 90% accuracy with less than 10ms and rapid classification.

Kim [5] proposed a model for anomaly detection based on reinforcement learning for load balancing. The proposed work used an agent DetectBot which identified and processed anomalies for load balancing on the basis of reinforcement technique. Moreover, during the process the model used Deep Belief Network (DBN) to attain load balancing. The DetectBot model involved phases like measurement of network load, structural map configuration, load prediction using neural algorithm and finally balancing the load. The phases when handled successfully aided at efficient load balancing in networks.

Kimmell, Abdelsalam, and Gupta [6] investigated ML approaches to detect online malwares in cloud environment. The author's detected online malwares based on the performance metrics and analysed the efficacy on base line ML algorithms such as Random Forest Classifier, Support Vector classifier, K-Nearest Neighbour classifier, Gradient Boosted classifier, Naïve Bayes Classifier and CNN. The comparative study of the proposed work with the investigation on related work in terms of features, domain, model utilised in the related work gave a detailed insight about the superiority of proposed work. Moreover, based on performance metrics, among the ML algorithms CNN performed optimally when experimented on 40,680 samples.

Mule and their team [7] reviewed auto encoder and SVM based Network Intrusion Detection System (NIDS) in cloud environment utilising KDDCUP dataset. Moreover, the model included DL classification built through feature extraction techniques where the network traffic was analysed thoroughly. The model attained improved accuracy, Recall, and Precision with minimal time.

Ahmad and team [8] designed anomaly detection technique for IoT using Deep Neural Network (DNN) algorithm. The model was tested on IoT-Botnet 2020 dataset which involved two phases such as Data capturing and preparation followed by DNN based anomaly detection stage. Moreover the comparative study with other DL algorithms such as CNN, Long Short Term Memory (LSTM), Recurrent Neural Network (RNN), and Gated Recurrent Unit (GRU) on the basis of performance metrics – Recall, Accuracy, Precision, and F1 score and Confusion Matrix exhibited superiority of the proposed DNN with utmost 99.01% and 99.30% accuracy and precision values respectively.

Malik and co-authors [9] formulated an improvised DBN based IDS IoT Network for handling traffic. ML and DL based DBN algorithms effectively detect attacks. The proposed improved DBN pre-processed the data from TON-IOT termed as Data preparation which involved data shuffling, Sampling, Label Encoder, and MinMax scalar. After segregation of train and test data, the train classified data was processed by the DBN model. The performance metrics were evaluated; further the comparative performance of other models like NB, SVM, KNN, Classification and Regression Tree (CART), Random Forest (RF), LDA with the same TON-IOT dataset were evaluated; additionally DNN was experimented on Google code Jam; LSTM+CNN was tested on CICIDS; while DNN3 was experimented on KDD dataset. The proposed DBN model was superior to other prevailing algorithms with the average accuracy of 86.3%.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7433
***Article Received**: 14 May 2023 **Revised:** 30 June 2023 **Accepted:** 30 July 2023*

Cai and research team [10] implemented a Hybrid Parallel-DL-IDS Model (HPM) based on metric learning. The initial phase of HPM consisted Data pre-processing comprising flow splitting, traffic clean and traffic tailor followed by metric learning. The CICDS 2017 and ICSX 2012 dataset were experimented on HPM. The study used CNN, CNN based LSTM, Double_BiLSTM. Moreover to prove the rapidity, and generality HPM was improved as HPMSL, HPMEM where CosMargin function was used to improve the validation accuracy[11]. The results were compared HPM + SoftMax values.The experimental results were evaluated based on metrics Precision, Recall, Macro-f1, Weighted –f1 and FAR. The comparative results reveal embedded metric learning HPM was rapid on different datasets with high classification performance and low consuming time.

Table 1 summarizes the significance of the existing approaches regarding the methods adopted, dataset along with the observation.

TABLE I. SUMMARY OF EXISTING METHODS

Ref. No.	*Method adopted*	*Dataset*	*Methods Compared with*	*Observation*
[1]	Depth Learning based Model	200, 200, 200 and 100	Auto-Encoder, Sparse Auto-Encoder and Sparse Denoising Auto encoder in addition to the traditional algorithms BP, SVM and Depth Auto-Encoder Networks – Series and Parallel	Depth auto-encoder with sparse denoising detected faults based on TPR, SFPR
[2]	ImGWO and ImCNN	DARPA'98, KDD'99 and synthetic datasets		Improved metrics: Detection rate 8.25%,accuracy 3.62% and false positives 4.08%
[3]	Machine Learning techniques	KDD and NSSKDL	Performance metrics and confusion matrix values for different IDS, approaches and datasets	Precision - 99%, Accuracy-98%, and Recall rate-97%
[4]	Distributed tracing and DL based anomaly detection and classification technique	-	-	Accuracy->90%; Processing time < 10ms
[5]	Reinforcement learning using DetectBot agent	-	-	Attained effective load balancing
[6]	Machine Learning approaches	40680 samples	RF, SVM, KNN, Gradient Boosted, NB and CNN	CNN exhibited superiority
[7]	Auto encoder and SVM based NIDS	KDDCUP	-	Improved accuracy, Recall, and Precision with minimal time.
[8]	DNN	IoT-Botnet 2020	CNN, LSTM, RNN, GRU	99.01% - accuracy and 99.30% - precision
[9]	Improvised DBN based IDS IoT Network	TON-IOT Google code Jam CICIDS KDD	NB, SVM, KNN, Classification and Regression Tree (CART), Random Forest (RF), LDA with (i); DNN with (ii); LSTM+CNN with(iii); DNN3 with (iv)	Accuracy of improved DBN-86.3%
[10]	Hybrid Parallel DL IDS model	CICDS 2017 ICSX 2012	CNN, CNN based LSTM, Double_BiLSTM	Embedded Metric Learning HPM is superior than other methods

III. PROPOSED METHOD

The following section depicts the work-flow of the present method in two approaches.

A. Approach 1: Feature extraction+DL based classification model

Figure 4 illustrates the architecture of the proposed work's Approach 1.

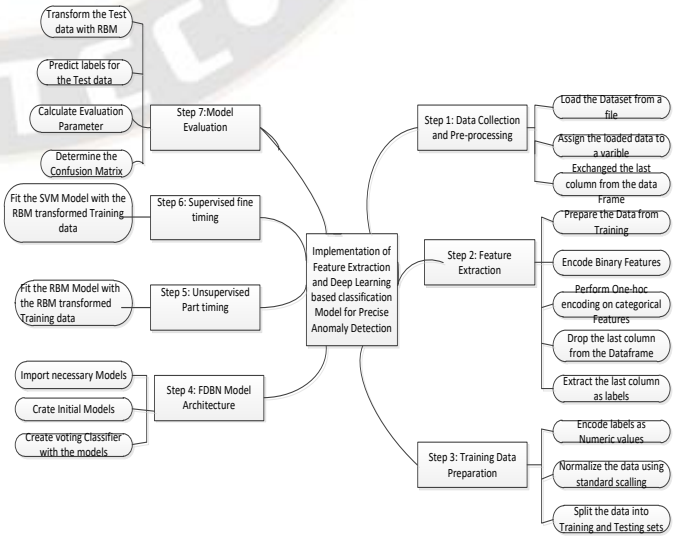

Figure 4. Architecture of the Proposed Work's (Approach 1)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7433
***Article Received**: 14 May 2023 **Revised:** 30 June 2023 **Accepted:** 30 July 2023*

The step-by-step Anomaly Detection process involve a fusion of Feature Extraction and DL based Classification techniques in the following phases.

- Data Collection and Pre-processing: The entire process begins with data collection from "KDDTrain+.txt". The .txt file is converted into pandas DataFramewithout header. Such data is assigned to variable data.
- Feature Extraction: The code performs feature extraction on the pre-processed data. Whilst extraction, the class columns are removed from the featuresand then extracted for labels. Consequently, the categorical columns are extracted through OneHotEncoder which is assigned to categorical data; further such data is fitted and transformed using the encoder function to form one_hot_encoded_data. Finally the encoded data is concatenated with remaining features.
- Training Data Preparation: This step prepares the data for model training. The code created by LabelEncoder iterates over the binary columns and encodes. Further the labels are converted to numerical values and assigned to labels. Using StandardScalerthe labelsare normalized. Such normalised data is split into test and train data further processing.
- FDBN Model architecture: In this phase, necessary models SVC and the voting classifiers are imported from scikit-learn. Subsequently, individual models are created using Bernoulli Restricted BoltzmanMachine (RBM). Further, voting classifiers were created with both the models RBM and SVM.
- Unsupervised Pre-training: The code fits RBM model with training data.
- Supervised Fine-tuning: This phase fits SVM model with RBM transformed training data.
- Model evaluation: This phase predicts the labels of the RBM transformed data using SVM model for the test data. Subsequently, the performance metrics F1 score, recall, precision and accuracy were evaluated followed by confusion matrix computation.

B. Approach 2: Integrating RBM and Logistic Regression for Precise Anomaly Detection

Architecture of the proposed work's Approach 2 is illustrated in Figure 5.This anomaly detection approach is a hybridization of RBM and Logistic Regression. The summary of the process is as mentioned below after importing the pre-requisite packages like scikit-learn modules, pandas and more for manipulating and processing the data.

Figure 5. Architecture of the Proposed Work's (Approach 2)

This anomaly detection approach is a hybridization of RBM and Logistic Regression. The summary of the process is as mentioned below after importing the pre-requisite packages like scikit-learn modules, pandas and more for manipulating and processing the data.

- Data collection and Pre-processing: The process begins by reading the CSV data in KDDTrain dataset.
- Feature Extraction: The labels from the last column were extracted and then stored as variable thus removing the last column from the frame.
- One-hot Encoding for categorical features: Upon using OneHotEncoder class from scikit module the categorical features were extracted and transformed into binary vectors. Finally the encoded data is concatenated with balance features.
- Encoding binary features: The binary features in the dataset are determined from the list of column; the scikit module through LabelEncoder class encodes the binary features to numerical format.
- Training Data Preparation: Consequently, the features in the dataset are normalised by using classes in scikit learn module – LabelEncoder, StandardScaler respectively. For the purpose of investigation, the normalised data is split into test and train data.
- FDBN Model Architecture: Through scikitneural and linear modules both Bernoulli RBM and Logistic Regression (LR) objects are initiated respectively.
- Unsupervised Pre-training: A pipeline is created by the scikit module for RBM and LR that fits to the training data.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7433
***Article Received**: 14 May 2023 **Revised:** 30 June 2023 **Accepted:** 30 July 2023*

- Supervised Fine Tuning: This process fits LR model to train data.
- Model Evaluation: The trained LR model predicts the labels of the test data and evaluates the metrics such as accuracy, F1 score, precision and recall. Next, after computing the confusion matrix both performance metrics and matrix values are determined.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed methods are evaluated on the public dataset titled "NSL-KDD" compiled from the Kaggle Website [1]. The proposed model is evaluated on the two datasets namely, "KDDTrain+" and "KDDTest+" respectively. There are 43 attributes in the dataset; few significant attributes are as follows: duration( ), protocol_type (such as 'tep', 'icmp', 'ndp'), service, source and destination types, logged-in status, wrong fragment, host or guestlogin, urgent and class ('normal' and 'anomaly'). There are 1,25,973 records and 22,544 in the 'KDDTrain' and 'KDDTest' datasets,respectively. The last column in the dataset defines the service as 'normal' or 'anomaly'. In the initial step, during the feature extraction step, the 'class' column and its values are removed. Later one-hot encoding is adopted to transform the "categorical values" to "binary vectors". As the "Logistic Regression (LR) algorithm expects the numerical value, the categorical values namely (a) protocol type (b) service and (c) flag are converted into numerical values. Henceforth, the processing by LR approach is feasible with numerical values. The OneHot Encoding ensures representation of categorical values into corresponding numerical values. During data preparation phase, encoded data are normalized for further processing. The major advantage of adopting the Forced Deep Belief Network (FDBN) which integrates RBN and LR functionalities through pipeline architecture ensures learning the complex patterns and results in more effective predictions. The pipelined architecture of RBN (promotes unsupervised pre-training) and LR (performs supervised-fine- tuning) of RBN's output and adjusts the weights depending on the labelled-training data. This kind of integration that is supervised and unsupervised learning makes the FDBN architecture to learn complex patterns very effectively and make predictions accurately. Finally the model evaluation phase, where the evaluation metrics are determined for the proposed model. The various parameters are as follows (a) Prediction which is used to predict labels for the test instances (b) Accuracy (A) defined as the ratio of correctly predicted influences to the total number of instances; further, it projects the overall correctness of the prediction (c) Precision (P) a metric used to measure the ratio of correctly predicted positive instances to the total positive predicted instances. In the present method, Weighted Average Method (WAM) is adopted (d) Recall (R)also referred as True Positive Rate (TPR) defined as the ratio of perfectly predicted positive instances from the existing positive instances; it deals with both True Positive and False Negative. Further, it used WAM for determining recall parameter (R), (e) F1-score (F1) it is determined as harmonic mean of precision and recall parameter; additionally, WAM is adopted to determine F1-score (f) and lastly Confusion Matrix is used to summarize the present model's predictions against the actual values. Table 2 summarizes the determined A, P, R and F1 parameters for the present model.

The second approach is the implementation of Feature Extraction and DL-based Classification model for Precise Anomaly Detection. In this approach, the initial steps are similar to earlier model namely, Data collection, pre-processing and training the input data. With respect to designing the model, RBM (with 100 components) and SVM (with default values) are created individually. Later, these models are integrated to form a Voting Classifier (VC). By enabling the "hard" parameter during the "Voting" process, ensures that the final prediction is based on constituent models. Later stage deals with the transformation of original feature data into RBM's transformed data; thus capturing the high-level abstraction and patterns from the input data through the unsupervised pre-training method. Subsequently the SVM model is employed to train the RBM-transferred training data. Thus the Supervised-Fine-Tuning of RBM features is done. Henceforth, the complex patterns and relationships in data are captured through the RBM's unsupervised pre-training approach and the resultant is fine-tuned by Supervised Model using SVM model. The parameters, namely, A, P, R and F1 are used to evaluate the present model. Table 2 summarizes the determined evaluation parameters.

TABLE II. TABLE 2 EVALUATION PARAMETERS

Parameters	***Proposed Approach 1(%)***	***Proposed Approach 2 (%)***
Accuracy (A)	98.38	87.87
Precision (P)	98.32	78.80
Recall (R)	98.38	87.87
F1 – Score (F1)	98.33	83.05

V. CONCLUSION

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7433
***Article Received**: 14 May 2023 **Revised:** 30 June 2023 **Accepted:** 30 July 2023*

The manuscript presents two approaches for Precise Anomaly Detection using hybridized LR and Deep Learning based approaches.

Approach 1 focussed on the integration of RBM and LR for better anomaly detection. The initial steps, such as dataset collection from Kaggle domain, pre-processing and normalization are common for Approaches 1 and 2 respectively. Consecutively, FDBM architecture was implemented by integrating RBM and LR objects, then be forming the pipelined architecture. The unsupervised pre-training step with RBM was fine-tuned using the supervised LR model's fine-tuning step.

Approach 2 focussed on the fusion of RBM and SVM for effective anomaly detection. The process initiates with collecting the dataset from Kaggle domain and follows the pre-processing stage, where the categorical data are transformed into numerical values using One-Hot Encoder approach followed by integrating the RBM and SVM models to form a Voting Classifier. Here, fine-tuning of RBM's extracted data was performed using SVM model.

Both the approaches performance were determined using the parameters namely P, R, A and F1-score and confusion matrix respectively. To conclude, both approaches demonstrated the effective anomaly detection though integrating RBM with LR (approach 1) and RBM with SVM (approach 2) by capturing complex patterns and determining the relationships in the data; thereby paving a path for improved accuracy in anomaly detection. Overall, these approaches offered an effective technique for accurate anomaly detection in the cloud domain.

REFERENCES

[1] Weipeng Gao, Youchan Zhu, "A Cloud Computing Fault Detection Method Based on Deep Learning," Journal of Computer and Communications, vol. 05, no. 12, pp. 24-34, 2017, DOI: 10.4236/jcc.2017.512003.

[2] S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A. Y. Zomaya, and R. 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, DOI: 10.1109/TNSM.2019.2927886.

[3] Anurag Rai, Amit Saxena, Manish Manoria, "Cloud based Security Framework for Anomaly Based Intrusion Detection using Machine Learning Techniques," International Journal of Engineering Research & Technology, (NCRIETS-2019 Conference Proceedings), vol. 7, no. 12, pp. 1-5, 2019.

[4] SashoNedelkoski, Jorge Cardoso, and Odej Kao, "Anomaly detection and classification using distributed tracing and deep learning," Proceedings of 19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID-2019), pp. 241-250, 2019, DOI: 10.1109/CCGRID.2019.00038.

[5] Hye-Young Kim, "A scheme of anomalous detection based on reinforcement learning for load balancing," IOP Conf. Series: Materials Science and Engineering, vol. 790, no. 1, pp. 1-7, 2020, DOI: 10.1088/1757-899X/790/1/012035.

[6] JeffreyCKimmel, MahmoudAbdelsalam, and MaanakGupta, "Analyzing machine learning approaches for online malware detection in cloud," in Proceedings of 2021 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 189-196, 2021, DOI: 10.1109/SMARTCOMP52413.2021.00046.

[7] SangitaBaban Mule, MohiniDilipChikane, BankarArti Sunil, Sunil SudamKhatal, "Advanced and secure incursion detection system using auto-encoder and support vector machine in cloud computing: A Review," International Journal of Advance Scientific Research & ET, vol. 4, no. 12, pp. 35-39, 2021

[8] Kumar Pramanik, K. K., Neha, R. ., Limkar, S. ., Sule, B. ., Qureshi, A., & Kumar, K. S. . (2023). Accurate Classifier Based Face Recognition using Deep Learning Architectures by Noise Filtration with Classification. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 179–183. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2558

[9] Zeeshan Ahmad, Adnan Shahid Khan, KashifNisar, IramHaider, Rosilah Hassan,Muhammad ReazulHaque, SeleviawatiTarmizi and Joel J. P. C. Rodrigues, "Anomaly detection using deep neural network for IoT architecture," Applied Sciences, vol. 11, no. 15, pp. 1-19, 2021, DOI: 10.3390/app11157050.

[10] Rayeesa Malik, Yashwant Singh, Zakir Ahmad Sheikh, Pooja Anand,Pradeep Kumar Singh, and TewabeChekoleWorkneh, "An improved deep belief network IDS on IoT-based network for traffic systems," Journal of Advanced Transportation, vol. 2022, pp. 1-17, 2022, DOI: 10.1155/2022/7892130.

[11] ShaokangCai, Dezhi Han, Xinming Yin, Dun Li and Chin-Chen Chang, "A Hybrid parallel deep learning model for efficient intrusion detection based on metric learning," Connection Science, vol. 34, no. 1, pp. 551-577, 2022, DOI: 10.1080/09540091.2021.2024509.

[12] Banavathu, Rajarao, and Sreenivasulu Meruva. "Efficient secure data storage based on novel blockchain model over IoT-based smart computing systems." Measurement: Sensors 27(2023):100741. DOI: https://doi.org/10.1016/j.measen.2023.100741

[13] Cloud Architecture, Available online: https://pimages.toolbox.com/wp-content/uploads/2021/07/09134159/38-3.png

[14] Kartika S. (2016). Analysis of "SystemC" design flow for FPGA implementation. International Journal of New Practices in Management and Engineering, 5(01), 01 - 07. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/41

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7433
***Article Received**: 14 May 2023 **Revised:** 30 June 2023 **Accepted:** 30 July 2023*

[15] Martin Duggan, The Application of Machine Learning to Optimise Live Migration in Cloud Data Centres, Ph.D., Thesis, 2019, DOI: 10.13140/RG.2.2.33506.27848

[16] AbdulatifAlabdulatif, HeshanKumarage, Ibrahim Khalil, Xun Yi, Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption, Journal of Computer and System Sciences, vol. 90, p. 28-45,2017, DOI: https://doi.org/10.1016/j.jcss.2017.03.001