IT in Industry, Vol. 9, No.2, 2021 Published Online 08-April-2021

Network Anomaly Detection for NSL-KDD Dataset Using Deep Learning

[1]Kavitha S, [2]Dr. Uma Maheswari N, [3]Dr.R.Venkatesh

[1]Assistant Professor, Department of Computer Science and Engineering, Velammal College of Engineering and Technology,Madurai ,Tamil Nadu ,India.
[2]Professor, Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu ,India.
[3]Professor, Department of Information Technology, PSNA College of Engineering and Technology, Dindigul,, Tamil Nadu ,India.

Abstract-

Deep learning based intrusion detection cyber security methods gained increased popularity. The essential element to provide protection to the ICT infrastructure is the intrusion detection systems (IDSs). Intelligent solutions are necessary to control the complexity and increase in the new attack types. The intelligent system (DL/ML) has been widely used with its benefits to effectively deal with complex and great dimensional data. The IDS has various attack types like known, unknown, zero day attacks are attractive to and detected using unsupervised machine learning techniques. A novel methodology has been proposed that combines the benefits of Isolation forest (One Class) Support Vector Machine (OCSVM) with active learning method to detect threats without any prior knowledge. The NSL-KDD dataset has been used to evaluate the various DL methods with active learning method. The results show that this method performs better than other techniques. The design methodology inspires the efforts to emerging anomaly detection.

Keywords- **Deep learning, Machine learning, Cyber Security, Intrusion Detection Systems, Isolation forest, Support Vector Machine.**

1. INTRODUCTION

The cyber-attack has become one of the severe problem with the increasing usage of mobile devices and Internet of Things (IOT). A report incident that devices employed like compromised IOT to make attacks like DDOS [1]. The key problem in different computer technology domain is the information security. Various efforts for security solutions like fire wall and Intrusion Detection System (IDS) has been established. The application layer communication packets are not examined by network layers firewall and IDSs.

With the tremendous growth of Internet, the cyber threats on computers and networks have expeditiously increased. To prevent these attacks, Intrusion Detection Systems (IDS) are employed in networking devices. IDSs has an increased significance in taking measures against network attacks, the IDSs based on payload has the issue of lack in scalability because of networks high speed and traffic. A deep packet inspection mechanism in flow based IDSs are favored over IDSs traditional methods for two main reasons- 1. Lesser quantities of data are processed. 2. The data flow is easily noted from forwarding devices that use standard protocols in the network of each computer devices [1].

Compared with the machine learning technique, a newer technique has emerged in the scene is the Deep learning. The Deep learning involves set of techniques of progressing algorithms that are based on knowledge learning. The Deep learning has higher potential of adaptability in the network due to the capability to learn and process the features of data on its own.

For the past few decades, the machine learning techniques has been used as the conventional method in the network to detect network anomaly. To propose solutions to the anomaly detection, various techniques like supervised, unsupervised and semi-supervised learning algorithms has been employed.

The supervised learning has the anomaly detection as a classification problem. The labeled data are used to train detection of anomaly models in supervised learning. In this training process the test data are classified as anomalous or normal based on the feature vectors. The unsupervised learning uses unlabeled data to proceed with the learning task. The popular method of unsupervised learning is the clustering [2] that searches the dataset for similarities in the instances to create clusters. Instances of similar characteristics are treated as alike and grouped in the

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

same type of cluster. The supervised and unsupervised method of learning combined to perform Semi-Supervised Learning (SSL) method. The semi supervised method of learning uses both labeled and untagged or unlabeled data [3]. The Semi-Supervised Learning method learns association of feature label from labeled data and allocates the labels to the unlabeled examples having related features of labeled example based on the associations learned from feature label.

The section II describes the literature survey, section III describes about the proposed methodology, section IV shows the evaluation and section V concludes the conclusion of the proposed technique.

2. LITERATURE SURVEY

The prevailing anomaly detection model classified as three types, the general probability (statistical) model, the machine learning model and the neural network model. The neural networking model achieves the deep learning model, as compared to machine learning model. The neural network model captures deep and much more characteristics of network traffic. Though the neural networking model is one among machine learning model, but it truly different from conventional model of machine learning that learns only shallow features [4].

Over the years the work has been involved on detection of active anomaly. The solution to the detection of rare category problem is by using active learning to the skewed distributions of datasets [5]. In [6], the active learning to problem of reduced classification are solved using the artificially generated instances that tries to reduce outlier detection to classification and applies sampling selective mechanism.

In [7], the author describes a Semi supervised anomaly detection method created on support vector data description [8]. In [9], the author proposes an active method of approach that involves the combination of supervised and unsupervised learning technique to label the selected instances by the expert. In [10], the active learning model is used to identify the needed anomalies. The new features are created to improve their model based on expert choices. In [11], (i) the algorithm proposed can be deployed top of any ensemble techniques based on random projections, (ii) [12], the isolation forest works in active environment.

One of the classification methods is SVM that transforms n dimensional input data into classes of vector spaces. The SVM technique is one of the intrusion detection research fields that afford results in lower false positive rates and the accuracy is high [13]. In [14], an intrusion detection system based on inductive network proposed uses OCSVMs method for analysis that functions on network flow. In [15], a detection method for anomaly has been used to process huge volume of netflow data record based on SVM. A technique used to handle quantifiable and relative netflow data to feed into the function of kernel and forwarded the calculated result to an OCSVM. In [16], to handle netflow data a two stage model of intrusion detection technique proposed to use OCSVM to identify malicious flow of data efficiently and then malicious traffic forwarded to the detection model of second phase to perform malicious flow analysis.

3. PROPOSED METHODOLOGY:

The proposed methodology involves unsupervised anomaly detection-based cluster using Isolation forest (One Class) Support Vector Machine (OCSVM) with active learning method. The unsupervised approach uses clustering method to group data allowing similarity measure. The clustering goal is to achieve high -intra -cluster similarity (i.e., clustered data are similar data) and low –inter –cluster similarity (i.e., different clustered data are dissimilar data). The clustering method has some approaches to cluster the input data, the well-known K-means and DBSCAN technique.

A sphere like cluster is produced as partition in clustering algorithm of K means. The dataset of medium and large set data uses K-mean algorithm as it is efficient one. The model tries to minimize the distance of intra-cluster and maximize the inter-clustered data. The drawback of K-mean cluster is that there must be pre specified number of k clusters. The K choice is uncertain and dependent highly on the shape and scale of distribution point in the dataset.

The DBSCAN is based on density clustering algorithm produces cluster of arbitrarily shaped one. The density is the specified radius within the defined number of points. It is useful in dealing with spatial clusters or when the dataset contains noise. DBSCAN has two parameters as radius and minimum points. The DBSCAN can find a different cluster that surrounds a cluster and is robust to the outliers. It is

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

better than K mean algorithm since it does not require the number of clusters as in K mean algorithm.

A. Isolation forest SVM (OCSVM) method:

The present technique of clustering usually lacks robustness. The clustering algorithm results be based on the type of algorithm and influenced by the parameters, initialization of the algorithm.
The paper proposes an intrusion detection algorithm to detect unsupervised anomaly and the technique is Isolation forest SVM (OCSVM) [17, 18, 19]. The isolation forest clustering is similar to sub space clustering (SSC). SSC is the technique of traditional clustering. The clusters are grouped from different small sub-spaces of original dataset

The clusters are produced from small subspaces of different original dataset $X \in R^{nxm}$, n is the number of records and m is the number of attributes or features. The Nsubspaces $X_i \in X(i \in \{1,2..,N\})$ is selected and produced by q features from the m attributes. The N number of sub-spaces corresponds to $({}^{m}_{n})$. The value of q is set, the closure property is taken in downward and implies the collected samples in X, it is the subspaces of X in low dimension. The small value of q is faster and efficient [17]. The low dimensional improved result are given by DBSCAN [20]. The value for q is set as 2 in SSC, that gives N=mx(m-1)/2.

The supervised learning model SVM analyzes and recognizes data pattern. The SVM extension method is OCSVM and is suited for unlabeled data [19]. The SVM model in OCSVM is trained with the data of one class(normal class). The data mapped to the feature space of the corresponding kernel that separates from origin of maximum margin [19].

The technique of isolation forest OCSVM algorithm has the steps as follows,

(1) **Initialization**:. Set D, a null dissimilarity vector and divide X as feature space into Ndifferent sub-spaces $X_i \in X(i \in \{1,2..,N\})$.
(2) **Clustering andLearning**:. Each X_i subspace applied with OCSVM and P_i partitions produced.
(3) **Evidence accumulation**:. Update D dissimilarity vector based on each P_i partition. The distance of different outliers found in subspace X_i accumulated in Vector D (EA clustering) [21].
(4) **Anomaly detection**:. Rank and obtain the Vector D ranked. If the dissimilarity value of Drank is greater than threshold value predefined, then the selected sample is an anomaly.

The flowchart of the proposed algorithm is illustrated in Figure 1.

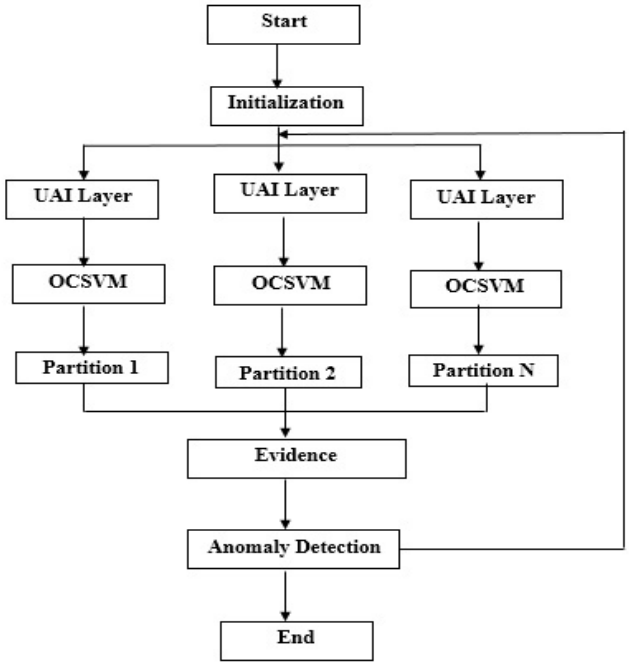


Fig. 1. Flowchart of isolation forest OCSVM algorithm.

B. Measure

Various metrics have been used to evaluate the machine learning/deep learning techniques how efficient in detecting attacks. To evaluate the detection method there are some common measures as follows:-

Confusion matrix or Error matrix:- The matrix is used to compare the result of actual and predicted one. The supervised learning technique uses this to predict the classifier accuracy. The confusion matrix has been shown in table 1, each row relates to the actual results, each column relates to the predicted ones. True positive (TP) refers to actual class Y that was classified correctly as class Y, False positive (FP) refers to the actual class Y' that was classified incorrectly as Class Y, False negative (FN) refers to the actual class Y that was marked incorrectly as class Y' and True Negative (TN) refers to the actual class Y' that was classified correctly as class Y'.

True Positive Rate (TPR):- It can be also known as Recall or Sensitivity or Detection rate(DR) or

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

probability of detection. It is the proportion or ratio of positive samples that are classified correctly as such,

$$TPR=TP/(TP+FN)$$

False Positive Rate(FPR) or False Alarm Rate (FAR):- It is the proportion or ratio of samples that are identified incorrectly as anomalies,

$$FPR=FP/(FP+TN)$$

Receiver Operating Characteristic (ROC) curve:- It is a method to visualize the TPR against the FPR for various parameter settings. It shows the relative tradeoffs between TPR on the y axis and FPR on the x axis. [22]

Table I
Confusion Matrix

Actual Class	Predicted Class	
	Y	Y'
Y	TP	FN
Y'	FP	TN

C. The ACTIVE-LEARNING Technique:

The unsupervised anomaly detection strategy is to train parameterized model $p_\theta(x)$ to capture full data distribution $p_{full}(x)$. The small constant is λ, It is assumed to be $p_{full}(x) \approx p_{normal}(x)$.
To say, the low value $p_{full}(x)$ is said as anomalous by using $s(x) \alpha 1/p_\theta(x)$ [23].
This technique has 3 main issues:

- If anomalies are common than expected, p_{full} be poor approximation of p_{normal}
- If in some ways the anomalies are clustered tightly, the high region probability are identified and learned by high end techniques.
- If anomalies are rare, and has access to only p_{full} ,there is no information regarding probability distribution p_{anom}

Arguments(parameters) for Active Learning:.

For anomaly detection, the said questions claim in favor of active learning, which also include auditor expert in loop training. Thus anomaly finding is based on benefits and feedback from it. The active learning is the one of the choice that can be adopted for the techniques handling unbalanced data set (__0) [24],[25]. The active learning has the capability to seek less labeled data than the supervised technique [26]-[28].

D. The UAI Layer

The most of the practical states of unsupervised anomaly detection shows slight accuracy, and the instances are ranked to be evaluated by human professionals later.

Here the task is given with a dataset $D=\{x|x \sim p_{full}(x)\}$, in which the data points of anomaly are ranked and sent to human professionals to be audited. Rather to select and rank once the instances, it can be iterated as small groups (each of k instance) to experts. The number of anomaly can be increased in the labeled instances.

In the active learning technique, it can be iterated with expert. At each step ,k<< labeled instances(b) of data points, the anomalous are sent to the expert audit and the new training process takes place after the return of feedback from the expert. At each steps, the most likely positive selection takes place in this strategy by selecting the top k elements. It is one of the approach for informative instance selection from datasets of imbalanced highly [29],[30], and the recent work of active anomaly detection is followed [31]-[33].

The Unsupervised to Active Inference (UAI) layer is developed by keeping this in mind. The technique followed in anomaly detection model is that the UAI layer is incorporated on top of the any unsupervised deep learning that provide anomalous score to rank anomalies (any). It takes input as layer latent representation (l(x)) and the output anomaly score (s(x)) created by the model and it is passed to the classifier to find the anomaly scores item. It is formally said as:.

$$p'(y|x) \alpha s_{uai}(x)=classifier([l(x);s(x)])$$

where $p'(y|x)$ is the empirical estimate of the probability of point being anomalous x. The work states that the learned representations have the statistical structure simple [25], this makes the modeling task manifold and detect unnatural points in simpler way [26].

In this work the model UAI layer uses any classifier;
The classifier is given as :.

$$p'(y|x) \alpha s_{uai}(x)= \sigma(W_{act}[l(x);s(x)] + b_{act})$$

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

where, the linear transformation is W_{act} , the bias term is b_{act}, and $\sigma(.)$ is the sigmoid function. The value of W and b are obtained by using back propagation with the cross entropy loss function, where the actively labeled instances are the targets. We allow gradients to flow through *l*, but not via *s*, where *s* is the non-differentiable. There after the networks with UAI layer is said to be UAI nets.

IV EVALUATION

In this section, the experiment carried out on public dataset:NSL KDD dataset[36],[37]. Then the performance analyze has been done on various deep learning –UAI and Deep learning models and compared the performance of deep learning model with this state of the artworks.

A. BENCHMARK DATASETS

The anomaly detection network traffic final result closely related to the benchmark dataset. The dataset used is the improved version of KDD cup 1999 dataset[38],[39], used in the intrusion detection methods.

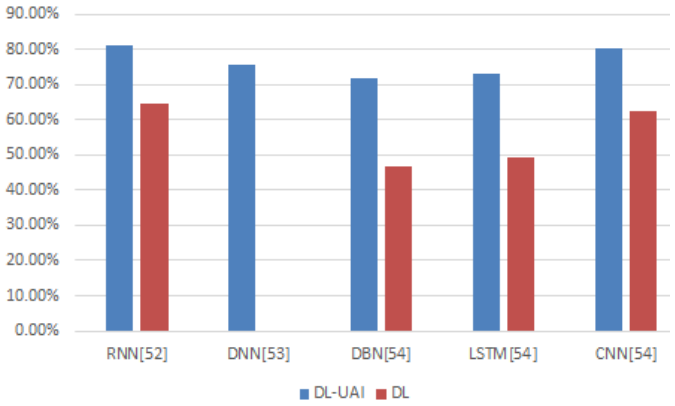
The NSLKDD dataset not only solve effectively the inherent redundant record problem of KDD cup1999 dataset and makes reasonable number of records in the training-dataset and testing-dataset. The NSLKDD dataset composed of KDD training dataset,KDD testing dataset and that can make reasonable comparison with different deep learning models.The NSL KDD-dataset have various normal records and different types of four abnormal records as shown in table 2.

The network traffic data is collected at fixed time intervals. The network traffic data is composed of multiple data packets. The data packet consists of sequence of traffic bytes. The different data packet contains 41 features and every data packet contains one class label. It is the form of x=(b0,....,bi,….). bi – ith feature in the data packet, x-data packets continuous features. The dataset includes the basic feature(1 – 10), content features (11 – 22) and traffic features (23 – 41) [40]. Based on the characteristics the attack types are of four in the dataset:- DoS (Denial of Service attacks), R2L (Root to Local attacks), U2R (User to Root attack), and Probe (Probing attacks).

TABLE 2. Different classifications in the NSL-KDD dataset

	Total	Normal	Dos	Probe	R2L	U2L
KDDTrain+	125973	67343	45927	11656	995	52
KDDTest+	22544	9711	7458	2421	2754	200

The comparison result of the performance analyze has been done on various deep learning –UAI and Deep learning models and compared the performance of deep learning model with this state of the artworks and the graph as shown:



	RNN[52]	DNN[53]	DBN[54]	LSTM[54]	CNN[54]
DL-UAI	81.29%	75.75%	71.91%	73.18%	80.13%
DL	64.67%	0	46.73%	49.38%	62.32%

Figure 2.Performance of Deep Learning –UAI and other Deep Learning models

V.CONCLUSIONS AND FUTURE WORK

The work shows how efficiently unsupervised anomaly detection can be detected using an UAI layer over the top of any deep learning techniques. The isolation forest is one of the classifier(one class learner) used to separate abnormal data from normaldata. The NSL-KDD dataset has been used to evaluate the various ML/DL methods with active learning method.The model shows it achieves similar results like other models and in common, deep learning models have improved performance. For future work, an extension of the method for other deep learning methods and different data streams can be considered.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

REFERENCES

[1] *DDoS Attack Snarls Friday Morning Internet Traf_c*. Accessed: Jul. 29, 2018. [Online]. Available: ttp://www.eweek.com/security/ddos-attack-snarls-friday-morning-internet-traf_c.html

[2] M. Luo, L. Wang, H. Zhang, and J. Chen, ``A research on intrusion detection based on unsupervised clustering and support vector machine," in Proc. 5th Int. Conf. Inf. Commun. Secur. (ICICS), Hohhot, China, S. Qing, D. Gollmann, and J. Zhou, Eds. Berlin, Germany: Springer, Oct. 2003, pp. 325_336, doi: 10.1007/978-3-540-39927-8_30.

[3] X. Zhu and A. B. Goldberg, ``Introduction to semi-supervised learning," Synth. Lect. Artif. Intell. Mach. Learn., vol. 3, no. 1, pp. 1_130, 2009. [Online]. Available:http://www.morganclaypool.com/doi/abs/10.2200/S00196ED1V01Y200906AIM006

[4] N. Moustafa, J. Hu, and J. Slay, ``A holistic review of network anomaly detection systems: A comprehensive survey," J. Netw. Comput. Appl., vol. 128, pp. 33_55, Feb. 2019. doi: 10.1016/j.jnca.2018.12.006.

[5] D. Pelleg and A. W. Moore, "Active learning for anomaly and rarecategory detection," in NeurIPS, 2005, pp. 1073–1080.

[6] N. Abe, B. Zadrozny, and J. Langford, "Outlier detection by active learning," in ACM SIGKDD Conf. ACM, 2006, pp. 504–509.

[7] N. G¨ornitz, M. Kloft, K. Rieck, and U. Brefeld, "Toward supervised anomaly detection," Journal of Artificial Intelligence Research, vol. 46,pp. 235–262, 2013.

[8] D. M. Tax and R. P. Duin, "Support vector data description," Machine learning, vol. 54, no. 1, pp. 45–66, 2004.

[9] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, "Aiˆ 2: training a big data machine to defend," in Big Data Sec. Conf. IEEE, 2016, pp. 49–54.

[10] M. Sharma, K. Das, M. Bilgic, B. Matthews, D. Nielsen, and N. Oza, "Active learning with rationales for identifying operationally significant anomalies in aviation," in Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, 2016,pp. 209–225.

[11] S. Das, W.-K. Wong, T. Dietterich, A. Fern, and A. Emmott, "Incorporating expert feedback into active anomaly discovery," in ICDM. IEEE, 2016, pp. 853–858.

[12] S. Das, W.-K. Wong, A. Fern, T. Dietterich, and M. Siddiqui, "Incorporating feedback into tree-based anomaly detection," Workshop on Interactive Data Exploration and Analytics (IDEA), 2017.

[13] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, ``Intrusion detection system: A comprehensive review," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16_24, 2013, doi: 10.1016/j.jnca.2012.09.004.

[14] P. Winter, E. Hermann, and M. Zeilinger, ``Inductive intrusion detection in _ow-based network data using one-class support vector machines," in Proc. 4th IFIP Int. Conf. New Technol., Mobility Secur., Feb. 2011, pp. 1_5, doi: 10.1109/NTMS.2011.5720582.

[15] C.Wagner, J. Franáois, R. State, and T. Engel, ``Machine learning approach for IP-_ow record anomaly detection," Lecture Notes Comput. Sci., vol. 6640, no. 1, pp. 28_39, 2011, doi: 10.1007/978-3-642-20757-0_3.

[16] M. F. Umer, M. Sher, and Y. Bi, ``A two-stage _ow-based intrusion detection model for next-generation networks," PLoS ONE, vol. 13, no. 1, Jan. 2018, Art. no. e0180945, doi: 10.1371/journal.pone.0180945.

[17] P. Casas, J. Mazel, and P. Owezarski, Unsupervised network intrusion detection systems: Detecting the unknown without knowledge, Computer Communications, vol. 35, no. 7, pp.772–783, 2012.

[18] L. Parsons, E. Haque, and H. Liu, Subspace clustering for high dimensional data: A review, SIGKDD Explor. Newsl., vol. 6, no. 1, pp. 90–105, 2004.

[19] B. Sch¨olkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, Estimating the support of a highdimensional distribution, Neural Computation, vol. 13, no. 7, pp. 1443–1471, 2001.

[20] A. K. Jain, Data clustering: 50 years beyond K-means, Pattern Recognition Letters, vol. 31, no. 8, pp. 651–666, 2010.

[21] A. L. N. Fred and A. K. Jain, Combining multiple clusterings using evidence accumulation, IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 27, no. 6, pp. 835–850, 2005.

[22] T. Fawcett, An introduction to ROC analysis, Pattern Recognition Letters, vol. 27, no. 8, pp. 861–874, 2006.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[23] [23] C. Zhou and R. C. Paffenroth, “Anomaly detection with robust deep autoencoders,” in ACM SIGKDD Conf. ACM, 2017, pp. 665–674.

[24] R. Silva, M. Gonc¸alves, and A. Veloso, “A two-stage active learning method for learning to rank,” J. Assoc. Inf. Sci. Technol., vol. 65, no. 1, pp. 109–128, 2014.

[25] R. Silva, M. Goncalves, and A. Veloso, “Rule-based active sampling for learning to rank,” in ECML PKDD Conf., 2011, pp. 240–255.

[26] B. Settles, “Active learning,” Synthesis Lectures on Artificial Intelligence and Machine Learning, vol. 6, no. 1, pp. 1–114, 2012

[27] A. Ferreira, R. Silva, M. Gonc¸alves, A. Veloso, and A. H. F. Laender, “Active associative sampling for author name disambiguation,” in JCDL Conf., 2012, pp. 175–184.

[28] M. Moreira, J. dos Santos, and A. Veloso, “Learning to rank similar apparel styles with economically-efficient rule-based active learning,” in ACM ICMR Conf., 2014, pp. 361–370.

[29] M. Sharma, K. Das, M. Bilgic, B. Matthews, D. Nielsen, and N. Oza, “Active learning with rationales for identifying operationally significant anomalies in aviation,” in Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, 2016, pp. 209–225.

[30] M. Bilgic and P. N. Bennett, “Active query selection for learning rankers,” in Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval. ACM, 2012, pp. 1033–1034.

[31] K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, “Aiˆ 2: training a big data machine to defend,” in Big Data Sec. Conf. IEEE, 2016, pp. 49–54.

[32] S. Das, W.-K. Wong, T. Dietterich, A. Fern, and A. Emmott, “Incorporating expert feedback into active anomaly discovery,” in ICDM. IEEE, 2016, pp. 853–858.

[33] S. Das, W.-K. Wong, A. Fern, T. Dietterich, and M. Siddiqui, “Incorporating feedback into tree-based anomaly detection,” Workshop on Interactive Data Exploration and Analytics (IDEA), 2017.

[34] Y. Bengio, G. Mesnil, Y. Dauphin, and S. Rifai, “Better mixing via deep representations,” in ICML, 2013, pp. 552–560.

[35] A. Lamb, J. Binas, A. Goyal, D. Serdyuk, S. Subramanian, I. Mitliagkas, and Y. Bengio, “Fortified networks: Improving the robustness of deep networks by modeling the manifold of hidden representations,” arXivpreprint arXiv:1804.02485, 2018.

[36] S. Revathi and A. Malathi, ‘‘A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection,’’ Int. J. Eng. Res. Technol., vol. 2, no. 12, pp. 1848–1853, 2013.

[37] D. H. Deshmukh, T. Ghorpade, and P. Padiya, ‘‘Improving classification using preprocessing and machine learning algorithms on NSL-KDD dataset,’’ in Proc. Int. Conf. Commun., Inf. Comput. Technol. (ICCICT), Jan. 2015, pp. 1–6.

[38] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, ‘‘A detailed analysis of the KDD CUP 99 data set,’’ in Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl., Jul. 2009, pp. 1–6.

[39] V. Engen, J. Vincent, and K. Phalp, ‘‘Exploring discrepancies in findings obtained with the KDD Cup ‘99 data set,’’’ Intell. Data Anal., vol. 15, no. 2, pp. 251–276, Mar. 2011.

[40] L. Dhanabal and S. P. Shantharajah, ‘‘A study on NSL-KDD dataset for intrusion detection system based on classification algorithms,’’ vol. 4, no. 6, pp. 446–452,201

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731