Volume 8, Issue 6
December 2019

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Comparative Analysis of Decentralized Real Time Anomaly Detection Mechanisms for IoT

[1]Mr. Sanjith S L and [2]Dr. E George Dharma Prakash Raj

[1] Indian Institute of Management Tiruchirappalli, Tamilnadu, India

[2] Bharathidasan University, Tiruchirappalli, Tamilnadu, India

E-mail: [1]sanjithsl@gmail.com, [2]georgeprakashraj@yahoo.com

ABSTRACT

Anomaly detection is a major requirement of the current Internet of Things (IoT) and inter-networked communication environment. This research work analyzes recent and prominent contributions in the domain of Anomaly detection. This research is performed especially in domains related to real time operations and IoT environment. The review is performed and results from most prominent models as well as the three models developed during my research are considered for the final analysis. This research concentrates on the working mechanisms and solutions for the major issues in Anomaly detection such as data imbalance, concept drift, centralized mechanisms and noise particularly in IoT domain. The methods used to handle the above issues and its advantages are thoroughly analyzed in this paper.

Keywords: *Intrusion Detection, IoT, Ensemble Models, Anomaly Detection, Decentralized security, Real-time security*

I. INTRODUCTION

Intrusion detection in networks is a challenging process, mainly due to huge amount of data and the imbalanced nature of the data. Intrusion detection has become a major need for the current networked environment due to the high usage levels and the mandatory security that are needed, as sensitive information are shared in the network. Detecting intrusions has become a mandatory service in IoT environments due to the power and resource constrained nature of the networks. However, there are several intrinsic issues persists in the network data that complicates the detection process.

Anomaly Detection System is the process of analyzing the network traffic and identifying if an anomaly has occurred. These models are mainly categorized into two; anomaly-based systems and misuse-based systems [1, 2]. Misuse based models are classifiers built using anomalous data for training the model. It has its major focus towards detecting anomalous traffic. The rules are determined using anomalous signatures. These models flag any network data matching these signatures. The major downside of these models is that anomalous traffic is dynamic and varies over time. Hence, models trained with past signatures cannot cope with variations in the traffic. Anomaly based systems are built using normal traffic as their base data. Data showing variations from the normal instances are anomalous. However, it should be noted that the normal data is huge and hence the trained model should be capable of utilizing a large amount of data for model building phase.

The ever-changing transmission patterns introduces concept drift, which also exhibits a huge challenge. Decentralization has to be incorporated to accelerate the anomaly detection process, as there would be huge volume of data passing through the gateway considering ‘big data’ and IoT applications. Real-time detection mechanisms are also required due to the high velocity of data flow that could be expected in the domain.

Machine learning algorithms are widely used for anomaly detection. Both supervised and unsupervised models can be effectively used for the prediction process. Further, with the increase in the complexity levels of anomalies, a single algorithm might not be suitable for complex predictions. Hence, the current literatures witness a large usage level of ensemble-based models for Anomaly detection. Ensembles are models built using multiple and sometimes varied models for prediction. Final predictions are obtained by aggregating the results of all the models. Such models are widely used due to the increasing complexities and reducing distinctions between normal and anomalous traffic [3, 4].

Since the inception of networks and communication technologies, research has been progressing for the anomaly detection and correction mechanisms. Due to the augmented practice of such technologies, several research articles on anomaly detection and avoidance mechanisms have been already available. Though it is a bequest topic, it is always a warm topic of research because of the ever-varying anomaly signatures and the reducing dissimilarity between the normal and anomaly traffic in the network. Three models are developed after analyzing all the positive and negative factors of five distinct, latest and best projecting models as references. These reference models are ensemble based Semi-Supervised Multi-Layered Clustering (SMLC) [5] model, SVM based model / Feature Augmentation based models - LMDRT SVM, LMDRT SVM2 [7], RampLoss K-SVCR[6] and Extreme Learning Machine (ELM) based Clustering model [8].

Anomaly detection has been carried out in all the three ensemble based proposed models that are Reinforcement based Heterogeneous Ensemble Model (RHEM) [11], Decentralized Bagged Stacking Ensemble Model (DBSEM)[12], Decentralized Time-window based Real-time Anomaly Detection mechanism (DTRAD) [10]. Same NSS. All these proposed ensemble architectures are created using Python. The NSL-KDD data, which is a standard benchmark intrusion detection data that is used to determine the effectiveness of these proposed models. Analysis is performed based on Precision, False Positive Rate and Accuracy.

The rest of this paper is organized as given below;

i) Section II presents the analysis of the existing models.
ii) Section III explains about the problems and challenges in Intrusion Detection System,
iii) Section IV explains the performance of the proposed machine learning models
iv) Section V presents the results and discussion of the proposed models using NSL-KDD data for analysis, and
v) Section V presents the conclusion part of this paper.

II. ANALYSIS OF THE EXISTING MODELS:

Well before starting the development of the new models, the pros and cons of five distinct, latest and best projecting models were evaluated. These models are ensemble based Semi-Supervised Multi-Layered Clustering (SMLC) [5] model, SVM based model/ Feature Augmentation based models - LMDRT SVM and LMDRT SVM2 [7], RampLoss K-SVCR and Extreme Learning Machine (ELM) based Clustering model [8]. The performance of these models had been compared by using NSL-KDD database as input, the result had been verified and the comparative analysis had been made in terms of performance and the same is given in Table-1 below:

Models	**Accuracy**	**FPR**	**Precision**
RampLoss K-SVCR	**0.986**	**0.008**	**0.98**
SMLC	**0.99**	**0.003**	**0.995**
LMDRT-SVM	**0.993**	0.6	**0.992**
LMDRT-SVM2	**0.992**	0.61	**0.991**
ELM	0.808	0.03	0.84

Table 1 : Comparison chart

It can be observed from Table-1 that RampLoss K-SVCR model and SMLC models have given best result in terms of over all performance. RampLoss K-SVCR model was used as reference model for the development of the new models. The result of the newly developed models have been compared with the RampLoss K-SVCR model for evaluating the performance.

III. PROBLEMS AND CHALLENGES IN INTRUSION DETECTION SYSTEM.

Anomaly detection system can be verbalized as binary classification or multi-class classification model. The multi-class classification model considers normal traffic as a class and each type of anomalous traffic is indicated as a new class, while binary classification model considers normal traffic as the negative class and all the other classes as positive class. Both considerations have their own pros and cons and are used depending on the result requirements. The domain however has several intrinsic properties associated with it, which also poses challenges, irrespective of the type of classification used. They are, data imbalance, noise, outliers and data hugeness.

a. Data Imbalance

Data imbalance is the property of a dataset to contain a large number of instances pertaining to one class and very low instances pertaining to another class. Network generated data is laden with a large number of normal instances, while the anomalous or attack traffic tends to be very low, hence indicating the presence of imbalance [13]. The major issue in using a data with data imbalance is that the imbalance levels tends to create a biased classifier model, where the model is over trained with the majority class and undertrained with the minority class [14].

b. Presence of Noise and Outliers

The network data, being machine generated, records all the generated packets, leading to noise and outliers [15,16]. The presence of noise and outlies tend to heavily affect the generalization capabilities of the classifier models [13]. Noise is considered as a variation in the regular data, while outliers are exaggerated noise levels exhibiting very high variations, positioning themselves as belonging to a different class. This usually occurs due to variations in the distribution levels of the data. Classifiers, when operated upon noisy data and outliers, interprets them as a different class. However, when the training data is labelled, such instances disrupt the decision rules, reducing the prediction efficiency of classifier models [17].

c. Big Data and IoT

The upsurge in the usage of interconnected devices has caused the generation of enormous amounts of information. Processing such huge amounts of information requires Big Data environments for effective processing. However, large number of instances alone is not the major issue; instead, an increase in the dimensionality levels of the data was also observed in the current network data. This leads to the curse of dimensionality, where the learning models get computationally intensive, which successively influence the performance of the classifier models.

d. Centralized approach

Centralized approach is the conventional way for detecting intrusion in a network, which would not be a suitable approach in the present scenario due to heavy traffic and the usage of big data and IoT applications. Hence, there should be a decentralized mechanism for the effective and faster detection of anomalies. In our models, we have incorporated the decentralized anomaly detection mechanism without affecting the performance. Rather, we had proved that DTRAD [10] has given significantly better performance and accuracy compared to the existing centralized models like RampLoss K-SVCR model.

e. Concept drift

The database has to be updated according to the changes that are happening in the development of applications that are using network for the data transfer. According to the evolutions that happens on such applications, the nature of data and it's behavior will be changed. This would create more and more anomalies in a timely manner. Over a period such unknown anomalies will start ruling and spoiling the network traffic which will end up with many complications and threats in the network. This is called concept drift. We could overcome this issue only with the constant updation of training data. As and when the latest anomalies are arrived, the system should be trained to detect those anomalies without manually updating the database. It is required to train the anomaly detection system using the real-time data for the effective solution for concept drift. This is made possible by the inclusion of the reinforcement based iterative training module in RHEM model [11], where every wrong prediction is corrected, hence leading to effective handling of concept drift.

IV. PERFORMANCE OF THE PROPOSED MACHINE LEARNING MODELS

Three models have been developed and analyzed for finding out the suitability of these models as well as the advantages and drawbacks of these models. The effectiveness of these models have been evaluated and necessary testing strategies have been applied on these models. The details regarding these intrusion detection models is described below:

a. Reinforcement based Heterogeneous Ensemble Model (RHEM)

Reinforcement based Heterogeneous Ensemble Model (RHEM) [11] presents a heterogeneous ensemble based prediction model to detect anomalies in the network environment, which was named as Reinforcement, based Heterogeneous Ensemble Mechanism for Anomaly Detection in Streaming Environment (RHEM). The major goal of the model is to provide faster, more efficient real-time predictions and to enhance the reliability of the model by providing an iterative mechanism to handle concept drifts. The ensemble is created using three varied base learners and the results are aggregated using a voting combiner to provide results. Decision Tree, Random Forest, and Gradient Boosting Trees are used as the base learners. The varied nature of the learners enables effective performances in models. Further, a reinforcement and an iterative training component is introduced into the model to handle concept drift. Experiments were performed on benchmark intrusion detection data and the results indicate the high performing nature of the model. Comparisons were performed with recent state-of-the-art models in literature and they indicate improved performances of the proposed model, indicating the high performing nature of the proposed ensemble model.

b. Decentralized Bagged Stacking Ensemble Model (DBSEM)

Decentralized Bagged Stacking Ensemble Model (DBSEM)[12] presents an ensemble based intrusion detection model to handle data imbalance and noise for Anomaly detection. Further, the entire approach has been decentralized to enable parallelized detection. The proposed model utilizes a BAgged Stacking Ensemble as the detection model. The ensemble architecture initially creates data bags, enabling distributed processing. The input training data is divided into multiple training data bags, where each data bag is composed of 60% of the entire training data. Multiple heterogeneous base learners process the bags. Prediction results from the base learners are passed to a stacked classifier for final predictions. This ensemble model is distributed over the network to enable decentralized processing. Experiments were performed on the NSL-KDD data and the results were compared with recent models. Comparisons with state-of-the-art models indicate the effectiveness of the proposed model.

c. Decentralized Time-window based Real time Anomaly Detection mechanism in IoT (DTRAD)

Our third and final model presents a Decentralized Time-Window based Anomaly Detection model for cost and time effective intrusion detection in IoT environments, which was named as Decentralized Time-window, based Real time Anomaly Detection mechanism in IoT (DTRAD) [10]. In this work, the features that lacks in the previous works have been incorporated. The proposed model is composed of time window based training data selection module, which enables better detection and reduced bias. Training data are selected based on their temporal significance and the bag creation process is also temporally performed such that data with similar temporal signatures are grouped into same bags. The ensemble model is created and weighted voting is performed to enable better results. The data reinforcement module enables new data to be appended to the training data, hence maintaining the recency of the data. Further, the entire process is decentralized, hence enabling data processing at appropriate nodes. This keeps the size of the training data low, hence reducing the computational complexity of the model to a large extent. Experiments were performed with benchmark data and comparisons were performed with recent models. Results indicate high performance of the proposed models.

V. RESULTS AND DISCUSSION

Analysis were performed using the NSL-KDD dataset. The NSL-KDD dataset has been derived from the KDD CUP 99 dataset [18], which is the benchmark dataset for intrusion detection. The KDD CUP 99 dataset however has several issues like duplicated records, leading to bias in the classifier training process. The NSL-KDD dataset is constructed by eliminating all the duplicates to provide a cleaner and compact dataset [19]. Features of the NSL-KDD dataset is shown in table 2 below:

Class	Feature	Data Type
Basic features	duration	continuous
	protocol_type	nominal
	service	nominal
	src_bytes	continuous
	dst_bytes	continuous
	flag	nominal
	land	nominal
	wrong _fragment	continuous
	urgent	continuous
Content – based features	hot	continuous
	num_failed_logins	continuous
	logged_in	nominal
	num_compromised	continuous
	root_shell	nominal
	su_attempted	nominal
	num_root	continuous
	num_file_creation	continuous
	num_shells	continuous
	num_access_file	continuous
	num_outbound_cmds	continuous
	is_hot_login	nominal
	is_guest_login	nominal
Time – based traffic features	count	continuous
	serror_rate	continuous
	rerror_rate	continuous
	same_srv_rate	continuous
	diff_srv_rate	continuous
	srv_count	continuous
	srv_serror_rate	continuous
	srv_ rerror_rate	continuous
	srv_diff_host_rate	continuous
Host – based traffic features	dst_host_count	continuous
	dst_host_srv_count	continuous
	dst_host_same_srv_rate	continuous
	dst_host_diff_srv_rate	continuous
	dst_host_same_src_ port_rate	continuous
	dst_host_srv_diff_host_ rate	continuous
	dst_host_serror_rate	continuous
	dst_host_srv_serror_rate	continuous
	dst_host_rerror_rate	continuous
	dst_host_srv_rerror_rate	continuous

Table - 2

NSL-KDD is a multi-class classification dataset, composed of five entries; normal and four attack classes. Normal class instances are the majority class instances with highest frequency, while all the others are minority class instances, with U2R exhibiting very high imbalance levels. The detailed descriptions are shown in table 3.

Sl. No	**Type of Traffic / Attack**	**Full NSL – KDD training set**	
		Number of records	**Frequency of occurrence**
1	Normal	67,341	53.46
2	DOS	45,927	36.43
3	Probe	11,656	9.25
4	R2L	995	0.79
5	U2R	52	0.04
Total records		125,971	

Table-3

The ensemble architectures are created using Python. The NSL-KDD data is used to determine the effectiveness of the proposed model. NSL-KDD is a standard benchmark intrusion detection data.

The ROC curves representing the prediction efficiency of all the three proposed models/mechanisms are shown in figure 1. It could be observed that all the proposed models exhibit a very high TPR level and very low FPR levels. This is attributed to the high generalizing nature and the low bias and variance exhibited by the proposed ensemble. It could also be observed that DTRAD model shows best results among all the models.

Similar to the ROC curve, PR curve (Precision Recall Curve) are also used to represent the performance level of a classifier models. PR Curve of all the three proposed models are shown in figure 2 below. PR curve is constructed by plotting the recall in x-axis and precision in y-axis. Higher values for both precision and recall indicates high performance of the classifier model. It could be observed from the figures that the proposed models exhibits very high values of both precision and recall. Hence exhibiting higher performance of these models.

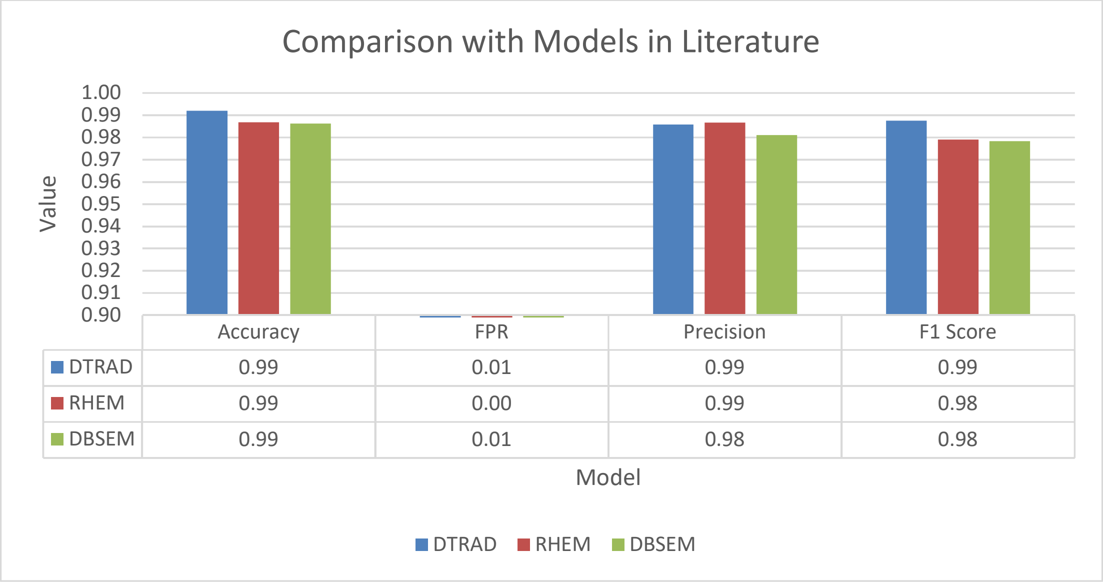
A comparison of the DTRAD model was performed with RHEM and the DBSEM models and the result is shown in figure-3. Comparisons were performed based on accuracy, FPR, Precision and F1 Score. It could be observed that the proposed DTRAD model exhibits the highest performance compared to all the other models, exhibiting the high efficiency of the proposed model.

Reinforcement based Heterogeneous Ensemble for Anomaly Detection (RHEM) in Streaming Environment has made it possible by the inclusion of the reinforcement based iterative training module, where every wrong prediction is corrected, hence leading to effective handling of concept drift.This has resulted in the model fine-tuning itself towards the data, hence enabling better predictions. This mechanism also results in learning new patterns contained in the data, hence leading to better handling of concept drift.

Decentralized Bagged Stacking Ensemble Model (DBSEM) proposes an effective intrusion detection model that has been developed in a decentralized fashion to enable faster and more effective detection of anomalies. The Bagged Stacking Ensemble architecture has been designed to provide faster and more accurate predictions in a decentralized manner. The bag creation phase is a process of data sampling results in random distribution of data to each of the heterogeneous learners, and at the same time, results in some similarity in the data patterns between the various base learners. The proposed architecture has been found to be highly scalable and tends well to parallelization.

The major advantage of the proposed Decentralized Time-window based Real time Anomaly Detection mechanism in IoT (DTRAD) model arises from the fact that the model operates on only a part of the data, while all the other models operate on the entire training data. This results in reduced time requirements, in-turn leading to faster results. This property serves as the base for IoT devices. This exhibits the capability of the proposed model in operating on devices with low compute resources and still provide effective performances.

The comparison of the results obtained through all the three models are given in Figure 1 below:



	Accuracy	FPR	Precision	F1 Score
🟦 DTRAD	0.99	0.01	0.99	0.99
🟥 RHEM	0.99	0.00	0.99	0.98
🟩 DBSEM	0.99	0.01	0.98	0.98

Figure-1

The values obtained during the result analysis using NSL KDD data from all the three developed models is given separately with 6 decimal points in the following table (Table-4)

Parameters	Proposed models		
	DTRAD	RHEM	DBSEM
Accuracy	0.992014	0.986771	0.986218
FPR	0.006723	0.004326	0.008826
Precision	0.985841	0.986611	0.981143
F1 Score	0.987589	0.979100	0.978407

Table-4

As per the above comparison graphs and values, it could be observed that DTRAD model gives best result among all the three models. Ideally, FPR value should be as minimum as possible for a better model because the model should not consider an anomaly as a normal data. We could achieve this requirement in all our models. As the values are less than 0.01, it is not visible in the graph. Accuracy, Precision and F1 Score needs to be high for a good anomaly detection model. All our models have given better values in terms of Accuracy, Precision and F1 Score. Since RHEM is a centralized model, it has given slightly better precision than the other two models (Difference between RHEM and DTRAM is 0.001). However, we have improved the precision in the DTRAD model though it was a decentralized model. From the graph, it is clear that our system has given good over all results. It could also be observed that all the three models have shown more effectiveness compared to the existing models as well. From the above experiments, it is obvious that the DTRAD model would be the best model compared to all the existing and proposed models for the decentralized real time anomaly detection process.

V. CONCLUSION

This work presents an analysis of three models in literature and also considered few recent and prominent intrusion detection models as reference during the comparison process. The DTRD model developed in this research is less compute intensive compared to other two algorithms. The major advantage of this model is that it filters the training data and utilizes only the recent data for the machine learning process. This results in faster model creation with low computational levels. Further, every node processes its own information and also shares the knowledge about the anomaly signatures. Hence every model is updated, leading to low error levels. The major advantage of the DTRAD model arises from the fact that the model operates on only a part of the data, while all the other models operate on the entire training data. This results in reduced time requirements, in-turn leading to faster results. This property serves as the base for IoT devices. This exhibits the capability of the proposed model in operating on devices with low compute resources and still provide effective performances. Limitations of the proposed model is that it exhibits a FNR level of 6%. This is due to the usage of time constrained data, leading to elimination of older anomalous signatures. Future enhancements of this model can be based on modifying the existing architecture to maintain the anomalous signatures irrespective of their temporal occurrence which can effectively reduce the FNR levels.

ACKNOWLEDGMENT

We are indebted to Bharathidasan University, IIM Tiruchirappalli and our colleagues for the kind support provided to us during this research.

REFERENCES

[1] Hoque, Mohammad Sazzadul, Md Mukit, Md Bikas, and Abu Naser. "An implementation of intrusion detection system using genetic algorithm." arXiv preprint arXiv:1204.1336, 2012.

[2] Piyush Pareta, Manish Rai, Mohit Gangwar, "An Integrated approach for effective Intrusion Detection with Elasticsearch", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.3, pp.13-17, 2018

[3] S. Abt, H. Baier, "A plea for utilising synthetic data when performing machine learning based cyber-security experiments", in: Proceedings of the 2014 Workshop on Artificial Intelligent and Security Workshop, ACM, pp.37–45, 2014.

[4] Ramchandar Durgam and R.V.Krishnaiah, "Online Intrusion Alert Aggregation with Generative Data Stream Modeling", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.5, pp.23-23, 2013

[5] Al-Jarrah, O.Y., Al-Hammdi, Y., Yoo, P.D., Muhaidat, S. and Al-Qutayri, M. "Semi-supervised Multi-Layered Clustering Model for Intrusion Detection". Digital Communications and Networks. 2017

[6] S.M.H. Bamakan, H. Wang, and Y. Shi. "Ramp loss K-Support Vector Classification-Regression; a robust and sparse multi-class approach to the intrusion detection problem". Knowledge-Based Systems, Vol.126, pp.113-126, 2017.

[7] H. Wang, J. Gu, and S. Wang. "An effective intrusion detection framework based on SVM with feature augmentation". Knowledge-Based Systems, Vol.136, pp.130-139, 2017.

[8] S. Roshan, Y. Miche, A. Akusok, and A. Lendasse. "Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines". Journal of the Franklin Institute, Vol.355, Issue.4, pp.1752-1779, 2018.

[9] Sanjith S L, E George Dharma Prakash Raj "A Comprehensive Analysis of Machine Learning Models for Real Time Anomaly Detection in Internet of Things ", International Journal of Computer Sciences and Engineering, Vol.6, Issue.11, pp.932-937, Nov 2018.

[10] Sanjith S L, E George Dharma Prakash Raj "Decentralized Time-window based Real-time Anomaly Detection mechanism in IoT ", International Journal of Recent Technology and Engineering, Vol.8 Issue.2, July 2019

[11] Sanjith S L, E George Dharma Prakash Raj "Reinforcement based Heterogeneous Ensemble for Anomaly Detection in Streaming Environment ", International Journal of Intelligent Enterprise, (DOI: 10.1504/IJIE.2019.10022335)

[12] Sanjith S L, E George Dharma Prakash Raj " Decentralized Bagged Stacking Ensemble Model (DBSEM) for Anomaly Detection ", Lecture Notes in Networks and Systems, (In communication)

[13] S.M.H. Bamakan , H. Wang , T. Yingjie , Y. Shi , "An effective intrusion detec- tion framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization", Neurocomputing, Vol.199, pp.90–102, 2016.

[14] S. Akila, and U.S. Reddy. "Data Imbalance: Effects and Solutions for Classification of Large and Highly Imbalanced Data". Proceedings of ICRECT, Vol.16, pp.28-34, 2016.

[15] J. McHugh , "Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln laboratory", ACM Trans. Inf. Syst. Secur. Vol.3, Issue. 4, pp.262–294, 2000 .

[16] P. Rutravigneshwaran, "A Study of Intrusion Detection System using Efficient Data Mining Techniques", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.6, pp.5-8, 2017

[17] A. Somasundaram, and U.S. Reddy. "Modelling a stable classifier for handling large scale data with noise and imbalance". In Computational Intelligence in Data Science (ICCIDS), IEEE International Conference, pp. 1-6, 2017.

[18] KDD Cup'99 intrusion detection data set, Available on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, October 2007.

[19] M. Tavallaee, E. Bagheri, W. Lu, and A.A. Ghorbani,. "A detailed analysis of the KDD CUP 99 data set". In Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium, pp. 1-6, July, 2009

AUTHOR PROFILES

Mr. Sanjith S L has completed his Master's degree from Manonmanium Sundaranar University, Tirunelveli in Computer and Information Technology in the year 2012 and Bachelor's degree in Electronics Engineering from Cochin University of Science and Technology in the year 1999. He has more than 19 years of experience in the Planning, Designing, Implementation and Management of ICT Infrastructure of reputed organizations out of which 14 + years in academic organizations. Currently he is working as Systems Administrator at Indian Institute of Management Tiruchirappalli (IIM Trichy). Before joining IIM Trichy, he was working as Senior System Manager at PAACET, Trivandrum. He also worked as part-time consultant in few organizations for the implementation of ERP. His experience includes Managed LAN (OFC & Ethernet), Servers with VMs, ERP implementation, Controller based WiFi network, IP Telephony system, IP Surveillance system and Automated Audio visual solutions.

Dr. E. George Dharma Prakash Raj completed his Master's Degree in Computer Science and Master of Philosophy in Computer Science in the years 1990 and 1998. He has also completed his Doctorate in Computer Science in the year 2008. He has around twenty-seven years of Academic experience and nineteen years of Research experience in the field of Computer Science. Currently he is working as a Faculty in the School of Computer Science, Engineering and Applications at Bharathidasan University, Trichy, India. He has published several papers in International Journals and Conferences related to Computer Science and has been an Editorial Board Member, Reviewer and International Programme Committee Member in many International Journals and Conferences. He has convened many National and International Conferences related to Computer Science.