International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072

Genetic Algorithm Based Intrusion Detection-Survey

Aswathy T[1], Misha Ravi[2]

[1]*M. Tech. Student, Computer Science and Engineering, Sree Buddha College of Engineering, Kerala, India.*
[2]*Assistant Professor, Computer Science and Engineering, Sree Buddha College of Engineering, Kerala, India.*

Abstract - *Network attack detection is one of the most important problem in network information security. An intrusion detection system is a network security countermeasure that monitors a network for suspicious activity. By analyzing the packets from the network, an intrusion detection system detects abnormal behaviors and blocks malicious network connections from attackers or intruders. The main objective of the framework is to develop an application that can process incoming network connection and identify the risk of intrusion. The framework that aggregates different classifiers and find the normal and abnormal network connections. To improve detection performance and reduce bias towards frequent attacks, a two-step hybrid method based on binary classification and k-NN algorithm. Several binary classifiers used in step 1 and in step 2, k-NN technique is used for further classification of network data. One aggregation module to effectively detect the exact class labels of network connections.*

Key Words: **Intrusion detection, Network data, Hybrid approach, Binary classifiers, K-NN algorithm**

1. INTRODUCTION

In recent years to maintain network security is a crucial task. The network is attacked by the unauthorized users. There are many methods to increase the security of the network. Intrusion detection system is a software application which analyzes the network activities and finds if there is any malicious activity or vulnerabilities occur. The goal of intrusion detection is to provide an outline of a malicious or real attack. Many of the intrusion approaches, methods and algorithms help to detect those malicious activities. An intrusion detection can provide advance knowledge of attacks or intrusion attempts by monitoring an intruder's activity. Intrusion detection can be classified on where detection takes place and the detection method that employed. According to, where detection takes place intrusion detection systems are either network – based or host – based. A network based intrusion detection system is used to analyze network traffic to protect a system from threats or vulnerabilities. This type of intrusion detection systems operates on network data flows. Host based intrusion detection systems operate on a host to detect malicious activity. It focuses on detecting attack log files that are created and stored on that host. This type of intrusion detection system also has the ability to monitor key system files and any effort to overwrite these files. In host-based intrusion detection system, which monitors the characteristics of a single host and the events occurring within that host for malicious activity. In intrusion prevention, performing intrusion detection and attempting to stop detected possible abnormal behaviors. Most of the network intrusion detection systems are easy to deploy on a network and can often view traffic at once from many systems. It is necessary that the intrusion detection systems react and to be able to block the detected network attacks. Intrusion detection system has three main functions such as monitoring, detecting and respond to unauthorised activities. Existing intrusion detection systems only determine the occurrence of attacks, but do not provide their type and also have low detection performance. Then a genetic algorithm based intrusion detection system is to develop an application that can process incoming network connection and monitor the risk of intrusion. In this framework that aggregates different classifiers and identify the risk of intrusion.

2. LITERATURE SURVEY

There are various approaches being utilized in intrusion detections. Some of them are discussed below.

2.1 Anomaly and misuse based intrusion detection in computer networks

Ozgur Depren et al. [1] proposed an intrusion detection for anomaly and misuse based detection approaches. The developed intrusion detection contains mainly three modules such as anomaly detection, misuse detection, decision support system. The anomaly detection module is responsible for malicious activity based on the trained normal behavior and the normal behavior model is built by using self-organizing map. The decision support system combines the result of both anomaly and misuse detection modules.

A) Anomaly detection modules

The anomaly detection approaches are based on the normal behavior model. Anomaly detection approach contains three sub modules such as pre-processing module, anomaly analyzer modules and communication module. In this each network connection record is examined and the traffic features are extracted. After pre-processing, the anomaly analyzer module uses the self-organizing map algorithm for training. The self-organizing map algorithm used to build profiles of normal behavior.

B) Misuse detection module

A misuse based detection system monitors an intrusion by matching it with predefined attack signatures. A rule based approach is utilized by misuse detection systems The rules are generated from the decision tree, and these rules are used classification of attacks.

C) Decision support system

The decision support system is combining the result of both anomaly and misuse detection approaches. In this work, decision support system is the final module. If any attack detects, then the decision support system reports to the system administrator.

2.2 FC-ANN based intrusion detection system

Gang Wang et al. [2] introduced artificial neural networks and fuzzy clustering (FC-ANN) based intrusion detection approach. For low frequent attacks and detection stability, the FC-ANN enhance the detection precision. The developed FC-ANN contains three modules such as fuzzy clustering, ANN modules and fuzzy aggregation module.

A) Fuzzy clustering module

The fuzzy cluster module is used to partition a given set of data into clusters. In this module, the training set is clustered into different subsets. Using fuzzy clustering technique, FC-ANN divides the heterogeneous training data into homogeneous subsets. Based on cluster centers, the membership function of each subset is calculated and a new ANN combines to get final results.

B) ANN module

The goal of ANN module is to learn every subset pattern. In this work, classic feed- forward neural networks trained with the back propagation algorithm to predict intrusion.

C) Fuzzy aggregation module

Fuzzy aggregation module is a meta-learner. It is used to learn again and aggregate the result of different ANN. Finally, each sub training sets complexity is reduced and the detection performance is improved.

2.3 PCA filtering and probabilistic SOM for network intrusion detection

Eduardo DelaHoz et al. [3] suggests PCA filtering and probabilistic SOM for network intrusion detection. For anomaly detection, the statistical techniques and self-organizing map combine to form a classification approach. The principal component analysis and fisher discriminant ratio techniques are used for feature selection and noise removal. By addressing feature space modelling, for distinguishing normal and abnormal connections. In order to remove noise, principal component analysis is used to generate a new set of non-correlated features. According to discriminative capability, the new features are selected. The new feature space is generated by using eigenvectors. The Bayesian self-organizing map is used for classification. The activation probability of each unit is measured by a fuzzy version of the classical self-organizing map. The output of the probabilistic self-organizing map is given to Gaussian Mixture Model(GMM). The aim of the Gaussian mixture model is to train the map only once. The classification result can have improved by using the activation probabilities of the self-organizing map. During the training stage, the activation probabilities are computed. In order to identify normal and abnormal patterns activation level is used.

2.4 Network traffic profiling and online sequential extreme learning machine

Raman Singh et al. [4] investigates an intrusion detection system using network traffic profiling and online sequential extreme learning machine. The online sequential extreme learning machine is a fast and accurate single hidden layer feed forward neural network which can process network traffic instances. This technique uses alpha profiling and beta profiling reduce time complexity and size of the training dataset while irrelevant features are discarded using an ensemble of filtering, correlation and consistency based feature selection techniques. The proposed methodology for intrusion detection have been performed three experiments such as Alpha-Full Features, Alpha–FST and Alpha-FST-Beta respectively. Pre-processing, cross-validation, alpha profiling and beta profiling are the various stages of these experiments. In alpha profiling, the training connections are categorized on the basis of protocol and service features and in beta profiling, duplicate and similar connections are grouped together and center of these groups is beta profiles. In pre-processing, all the categorical features are represented into continuous using 1 of k coding. In beta profiling, density- based spatial clustering of applications noise is used as beta profile. In result aggregation, the collected result of each experiment are analyzed.

2.5 Cuttlefish Optimization Algorithm for Intrusion Detection Systems

Adel Sabry et al. [5] developed a feature selection approach based on the cuttlefish optimization algorithm. The intrusion detection system deals with large volumes of data. One of the crucial task of intrusion detection systems is to keep better quality features from the dataset. The cuttlefish algorithm is used as a search strategy, to ascertain the optimal subset of features. For classification process, decision tree classifier is used. In this framework, cuttlefish algorithm is used as a feature selection tool. The decision tree is used as a classifier to improve the quality of the produced subset of features. In general, whenever the number of features is decreased, the accuracy rate and detection rate are increased. For constructing a decision tree, ID3 algorithm is used. The cuttlefish feature selection algorithm starts with a population. Each population deals with two subsets such as selected features and unselected

features. In every population, each selected features are evaluated by a decision tree classifier. Based on the fitness value, sorting the population in descending order to generate new subsets. Using reflection set and visibility set, the new set is generated from each subset.

2.6 A multi-level intrusion detection method for abnormal network behaviors

Soo-Yeon et al. [6] investigates a multi-level intrusion detection method for abnormal network behaviors. This work contains three steps. The first step is understanding hidden underlying patterns of network traffic data by creating reliable rules to network abnormality. The next step is generating a predictive model to determine exact attack categories and the last step is integrating visual analytics tool to conduct an interactive visual analysis and validate the identified intrusions. Based on the interactive visual analysis, a significant difference between the attack categories was discovered by visually representing attacks in separate clusters. The multi-level detection method is used for monitoring hidden underlying patterns and attacks by representing the relationship among the features of network traffic data. The first step of proposed the approach is generating rules to detect normal and abnormal behavior. First, the input data is divided into two subsets such as categorical or nominal data and numerical data. The nominal variables are used to generate rules. An iterative visual analysis, conducting to provide transparent reasons. Classification and regression tree is used to design a rule based model. The rules were statistically significant to detect intrusions.

2.7 Cluster center and nearest neighbor based intrusion detection approach

Wei-Chao Lin et.al [7] developed a feature representation method for efficient intrusion detection based on cluster centers and nearest neighbors. The k-means clustering algorithm is used to extract cluster centers of each pre-defined attack category. Then, the nearest neighbor of each data sample in the same cluster is identified in the proposed approach. Next, the sum of the distance between a specific data sample in the data set and the cluster centers and the distance between this data and its nearest neighbor is calculated. This result in a new distance based feature that represents the data in the given dataset. The clustering and nearest neighbors are based on two distances which are used to determine the new features, between a specific data point and cluster center and nearest neighbor respectively. In this system, it mainly consists of three steps. The first step is clustering technique. In this technique, the cluster centers are extracted. The second step is to measure and sum the distance between all data of the given dataset and the cluster centers and the distance between each data point and its nearest neighbor in the same cluster. The proposed approach first transforms the original feature representation of a given dataset into one – dimensional distance based feature. Then this new dataset is used to train and test the K-NN classifier for classification.

2.8 Time varying chaos particle swarm optimization method for intrusion detection

Huadong wang et. al [8] presents a time varying particle swarm optimization method for intrusion detection. Based on time-varying chaos particle swarm optimization (TVCPSO) combined with multiple criteria linear programming (MCLP) and support vector machine (SVM) an effective intrusion detection framework proposed. TVCPSO-MCLP and TVCPSO-SVM is to provide an adaptive, robust, precise methodology to detect intrusions. A weighted objective function is proposed to simultaneously take into account the detection rate along with the false alarm rate and also the number of features to maximize the effectiveness of proposed methods. By adopting the time-varying inertia weight factor (TVIW) and time-varying acceleration coefficients (TVAC), namely TVCPSO, modified chaos particle swarm optimization have been proposed to make it faster in searching for the optimum and avoid the search being trapped into local optimum. An extended version of multiple criteria linear programing, namely MCLP, has been adopted to increase the performance of this classifier in dealing with the unbalance intrusion detection dataset.

2.9 An intrusion detection with weighted signature generation

Kai Hwang et. al [9] presents an intrusion detection with weighted signature generation over anomalous internet episodes. The proposed intrusion detection is built with a SNORT and an anomaly detection subsystem. A weighted signature generation algorithm to characterize anomalous attacks and extract their signatures. By mining anomalous traffic episodes from Internet connections, build an anomaly detection system that detects anomalies. A weighted signature generation scheme is developed by combining anomaly detection system with SNORT. The episode rule mining engine consists of two phases such as training and detection phase. The training phase is used to generate the normal traffic database without attacks. Attacks may have monitored in the detection phase. The anomaly is identified once the episode rule describing the network traffic connections cannot detect any match with the normal connection rules in the database. To reduce the episode rule space, three pruning techniques are developed. In this system, the signatures are extracted from an anomaly detection system and adds them into SNORT for accurate intrusion detection.

2.10 Network intrusion detection on cloud based robotic system

Ying Gao et al. [10] developed a novel semi supervised learning approach for network intrusion detection on cloud based robotic system. The variance in the classifier output

is reduced by the ensemble-based system. Due to the good generalization ability of ensemble learning, an ensemble system constructed for training the labeled data. The classification and regression tree as the basic learner of the ensemble system. In order to integrate the outputs of classification and regression trees, a 3-layers neural network is applied to decide their weight. The fuzziness-based method to mine the hidden structure of unlabeled data. The method extracts the useful information and removes the redundant term. The backpropagation method is used for training. The FSSL-EL uses the principle of bagging algorithm to build the classification model. It mainly consists of two parts: the supervised and the unsupervised part. For the supervised part, an ensemble learning approach based on CART. The fuzziness-based method makes the unlabeled data available for classification. In this system, combines the ensemble learning method and the fuzziness-based method for intrusion detection.

2.11 Convolutional neural network based intrusion detection model

Kehe wu et al. [11] proposed a novel intrusion detection model for massive network using convolutional neural network. In the proposed approach, a method to convert the raw traffic vector format into the image data format. The image format can reduce the number of computation parameters. From the raw data set, convolutional neural network is used to select traffic features automatically, and to solve the imbalanced data set problem.Based on the convolutional neural network, the novel intrusion detection model includes four steps. The first step is data pre-processing. This step adjusts the initial data format and normalizes the data values. In order to improve the performance of convolutional neural network model, it needs to convert normalized data into an image data format. In step two, training is performed to improve the convolutional neural network model performance through constant tuning of the parameters. Testing is the third step. In this step, the test data should be used to check the accuracy rate of the convolutional neural network model. The final step is evaluation. This step is used to evaluate the model performance.

2.12 Neural network ensemble classifier for effective intrusion detection

Mohammad Amini et. al [12] suggests a neural network ensemble classifier for effective intrusion detection using fuzzy clustering and radial basis function networks. A new ensemble classifier is developed for intrusion detection, which divides the problem space by fuzzy clustering and then utilizes the different subspaces for training similar artificial neural network. The proposed approach contains three components. First, a fuzzy clustering module partition the total training set into smaller subsets. Second, the ensemble members include radial basis function neural networks. Third, the classification accuracy is improved by a hybrid model for smaller classes and the model can act more consistently. An ensemble system consists of three major modules such as fuzzy clustering and subdivision module, neural network base classifiers, and combination module. In order to establish the ensemble system, first divide the original training dataset into several subsets using a fuzzy clustering technique. Then train a radial basis function network using each of the different produced subsets. For the fuzzy clustering module, fuzzy c-means algorithm is used. From unlabeled data with fuzzy membership grades, fuzzy c-means algorithm creates clusters. The combination module uses the predictions of the base classifiers, integrated them with an efficient method and delivers the results as the final prediction of the ensemble.

2.13 AdaBoost algorithm for network intrusion detection

Weiming Hu et al. [13] developed a AdaBoost-based algorithm for network intrusion detection. In the algorithm, decision stumps are serve as weak classifiers. Both the categorical and continuous features, the decision rules are provided. To improve the performance of the AdaBoost-algorithm, adaptable initial weights and a simple strategy for avoiding overfitting are used. The AdaBoost algorithm corrects the misclassifications made by weak classifiers, and it is less susceptible to overfitting than most learning algorithms. The framework consists of the following four modules such as feature extraction, data labeling, design of the weak classifiers, and construction of the strong classifier. For each network connection, three major groups of features for detecting intrusions are extracted, they are, basic features of individual Transmission Control Protocol connections, content features within a connection suggested by domain knowledge, and traffic features. In data labelling, a set of data has to be labeled for training. This labelled data set should contain both normal samples labeled as “+1” and attack samples labeled as “−1.” By combining the weak classifiers, a strong classifier is obtained. The strong classifier has higher classification accuracy than each of the weak classifier.

2.14 Semi - supervised learning approach for intrusion detection system

Rana Aamir Raza Ashfaq et al. [14] presents Fuzziness based semi-supervised learning approach for intrusion detection system. In this system, the unlabelled samples assisted with supervised learning algorithm to improve the classifier’s performance for the intrusion detection systems. A single hidden layer feed-forward neural network is trained to form a fuzzy membership vector, and the sample categorization on unlabelled samples is performed using the fuzzy quantity. After incorporating each category separately into the original training set, the classifier is retrained. The neural network with random weights as a base classifier. The fuzziness unclears the boundary between two linguistic terms and is based on the membership function of fuzzy sets. The probability measure of an event to a fuzzy event and to interpret the uncertainty

associated with a fuzzy event, entropy in information theory is used. In this system, fuzziness as a type of cognitive uncertainty. Coming from the transition of uncertainty from one linguistic term to another. Based on divide- and-conquer methodology, a SSL algorithm is designed for intrusion detection.

2.15 Random forests based network intrusion detection

Jiong Zhang et al. [15] presents the random forests based network intrusion detection. In this framework, the random forests algorithm is used for network intrusion detection. To improve the performance of the intrusion detection system, apply sampling techniques and feature selection algorithm in misuse detection. The feature selection technique improves the overall intrusion detection performance. To address the problems of rule-based systems, the random forests algorithm to use build patterns of intrusions. The proposed misuse detection framework has two phases such as an offline phase and an online phase. The system builds patterns of intrusions in the offline phase and detects intrusions in the online phase. In the offline phase, feed a training dataset into the pattern builder module that can build the patterns of intrusions. To handle imbalanced intrusions, the module employs the feature selection algorithm, and builds the patterns by the random forests algorithm with optimal parameters. After mining the intrusion patterns, the module outputs the patterns as the input of the detector module. In the online phase, the system captures the packets from network traffic. For each connection, the features are constructed by the pre-processors from the captured network traffic. Then, the detector module classifies the connections as intrusions or normal traffic using the patterns built in the offline phase. Finally, when it identifies any intrusion pattern, then the system raises an alert to the system administrator.

2.16 Field programmable gate arrays based network intrusion detection architecture

David et. al [16] designed a field programmable gate arrays based network intrusion detection architecture. In this work, first develop a feature extraction module which aims to summarize network behavior. It also incorporates an anomaly detection mechanism using principal component analysis as the outlier detection method. Both these modules are implemented on reconfigurable hardware and can manage the gigabit throughput demands by modern networks. Extraction of packet headers cannot provide an accurate description of the network behavior. Depending on the application utilizing this information different properties, such as connection duration, the number of flags sent, etc. should be monitored. In the first phase, the network header data are separated from the packets fed into the system. The feature extraction module utilizes these headers to removal the temporal and connection-based characteristics of the network. This module extracts more information than conventional techniques that only identify a small amount of features from network packets. A feature extraction module consists of a feature controller, hash functions, feature sketch, and a data aggregate. All these components are integrated to give a fast, scalable, and accurate platform.

2.17 Distributed graph-based statistical approach for intrusion detection

Hamidreza Sadreazami et al. [17] introduced distributed graph-based statistical approach for intrusion detection in cyber physical systems. The graph affinity matrix used in the proposed scheme is constructed based on both the sensors measured data and the proximity of the sensors. In this system, modeling sensor measurements as the target graph-signal and utilizing the statistical properties of the graph-signal for intrusion detection. The Gaussian Markov random field is used as an underlying probabilistic model for the graph signals in the context of detecting any deviation from the normal behavior of the network. This scheme establishes a temporal analysis of the network behavior by computing the Bhattacharyya distance between the measurement distributions at consecutive time instants. The Bhattacharyya distance measures the identical of two discrete or continuous probability distribution. This framework uses a statistical properties of the target graph signal. The network is supposed to be composed of a number of distributed sensors having spatial dependencies with irregular data measurements as signals on nodes of a weighted graph. The proposed approach is capable of detecting the existence of any deviation from the normal behavior profile.

2.18 An intrusion detection approach for visual sensor networks

Kaixing Huang et al. [18] presents an efficient intrusion detection approach for visual sensor networks based on traffic pattern learning. A traffic model is developed to describe the dynamic characteristics of network traffic in visual sensor networks. Based on this traffic model, the optimal feature set for traffic pattern learning can be extracted. Then a hierarchical self-organizing map is employed to learn traffic patterns and detect intrusions. A light-weight active learning method is designed for training self-organizing map on big and imbalanced datasets by actively selecting a small number of representative instances from the training set. According to the correlated *N*-Burst model, traffic features can be categorized into two groups such as node-level features and network-level features. The node-level features are used to describe the activities of specific sensor nodes, while the network-level features present the overall network condition of the whole system. In the intrusion detection process, by extracting features from network traffic in a short period of time, an input vector is fed into the hierarchical self-organizing map for pattern classification.

2.19 Intrusion detection by using data mining and forensic techniques

Fang-Yie Leu et al. [19] proposed to detect insider attacks at the system call level by using data mining and forensic techniques. The internal intrusion detection system creates users' personal profiles to keep track of users' usage habits as their forensic features and identify whether a valid login user is the account holder or not by comparing his/her current computer usage behaviors with the patterns mined in the account holder's personal profile. To identify a user's forensic feature by analyzing the corresponding system calls to enhance the accuracy of attack detection and able to port the internal intrusion detection systems to a parallel system. The proposed framework consists of a system call monitor and filter, a mining server, a detection server, a local computational grid, and three repositories, including user log files, user profiles, and an attacker profile. The system calls monitor and filter, as a loadable module embedded in the kernel of the system being considered, collect those system calls submitted to the kernel. Both the detection server and the mining server are running on the local computational grid to accelerate the internal intrusion detection and protection system online detection and mining speeds and enhance its detection and mining capability.

2.20 Online intrusion alert aggregation

Alexander Hofmann et al. [20] suggests online intrusion alert aggregation with generative data stream modeling. Alert aggregation is an important subtask of intrusion detection. This framework is a generative modeling approach using probabilistic methods. The proposed approach is a data stream approach. Each observed alert from the intrusion detection system is processed only a few times. Then it can be applied online and under harsh timing constraints. The framework is the layered architecture of an intrusion detection agent. It consists of four layers such as sensor layer, detection layer, alert processing layer and reaction layer. The sensor layer acts as the interface to the network and the host on which the agent resides. Sensors acquire network traffic data from both the network and the host. At the detection layer, different detectors, that is the classifiers trained with machine learning techniques. If any attack occurs, they create alerts which are then forwarded to the alert processing layer. At the alert processing layer, to combine the alerts by the alert aggregation module that are assumed to belong to a specific attack instance. Thus, so called meta-alerts are generated. The task of the reaction layer is reporting. The goal of the framework is to identify and to cluster different alerts.

To overcome all the difficulties of the existing methods, develop a novel framework for intrusion detection. It is a hybrid model combining various classifiers. The contributions of this system are present a two-step hybrid framework of intrusion detection system based on various classifiers. The two-step hybrid intrusion detection approach consists of binary classification and k-NN technique. For the network connections whose classes are uncertain after step 1, which is further classifies class label in step 2 using the k-NN algorithm. The combination of two steps makes an effective intrusion detection technique.

3. CONCLUSION

The literature survey could fetch a number of existing intrusion detection systems. These intrusion detection has drawbacks. Most of the existing intrusion detection systems only determine the occurrence of attacks, but do not provide their type and also have low detection performance. Another limitation is too many parameters in certain intrusion detection system. That is, some intrusion detection models, have many parameters. Setting values for those parameters is not easy. Due to these limitations genetic algorithm based intrusion detection system is proposed.

REFERENCES

[1] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, ''An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks,'' Expert Syst. Appl., vol.29, no.4, pp.713–722,2005.

[2] G. Wang, J. Hao, J. Ma, and L. Huang, ''A new approach to intrusion detection using artificial neural networks and fuzzy clustering,'' Expert Syst. Appl., vol. 37, no. 9, pp. 6225–6232, 2010.

[3] E. De la Hoz, E. De La Hoz, A. Ortiz, J. Ortega, and B. Prieto,''PCA filtering and probabilistic SOM for network intrusion detection,'' Neuro computing, vol. 164, pp. 71–81, Sep. 2015.

[4] R.Singh, H.Kumar, and R.K.Singla, ''An intrusion detection system using network traffic profiling and online sequential extreme learning machine,'' Expert Syst. Appl., vol. 42, no. 22, pp. 8609–8624, 2015.

[5] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, ''A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems,''Expert Syst. Appl., vol.42, no.5, pp.2670–2679,2015.

[6] S.-Y. Ji, B.-K. Jeong, S. Choi, and D. H. Jeong, ''A multi-level intrusion detection method for abnormal network behaviors,'' J. Netw. Comput. Appl., vol. 62, pp. 9–17, Feb. 2016.

[7] W.-C. Lin, S.-W. Ke, and C.-F. Tsai, ''CANN: An intrusion detection system based on combining cluster centers and nearest neighbors,'' Knowl.Based Syst., vol. 78, pp. 13–21, Apr. 2015.

[8] S. M. H. Bamakan, H. Wang, T. Yingjie, and Y. Shi, ''An effective intrusion detection framework based on MCLP/SVM optimized by time varying chaos particle

swarm optimization,'' Neuro computing, vol. 199, pp. 90–102, Jul. 2016.

[9] K. Hwang, M. Cai, Y. Chen, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes," Vol. 4, pp. 41 – 55, Feb. 2007.

[10] Y.Gao, Y. Jin, J. Chen, and H. Wu, " A Novel Semi-Supervised Learning Approach for Network Intrusion Detection on Cloud-Based Robotic System," Vol. 6, pp. 50927 – 50938, Sep.2018.

[11] K. Wu, Z. Chen, and W. Li, "A Novel Intrusion Detection Model for a Massive Network Using Convolutional Neural Networks," Vol. 6, pp. 50850 – 50859, Sep.2018.

[12] M. Amini, J. Rezaeenour A and E. Hadavandi, "A Neural Network Ensemble Classifier for Effective Intrusion Detection Using Fuzzy Clustering and Radial Basis Function Networks," Vol. 25, Apr 2016.

[13] W. Hu, Wei Hu and Steve Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," Vol. 38, pp. 577- 583, Apr. 2008.

[14] R. Amir,X. Zhao Wang and H. Abbas, "Fuzziness based semi-supervised learning approach for intrusion detection system," Vol. 6,pp. 484- 497,Apr.2016.

[15] J. Zhang, M. Zulkernine, and A. Haque, "Random-Forests-Based Network Intrusion Detection Systems," Vol. 38, pp. 649 – 659, Sep. 2008.

[16] A. Das, D. Nguyen, and J. Zambreno, "An FPGA-Based Network Intrusion Detection Architecture," Vol. 3, pp. 316 – 317, Mar.2008.

[17] H. Sadreazami, A. Mohammadi and A. Asif, "Distributed Graph-based Statistical Approach for Intrusion Detection in Cyber-Physical Systems," Vol. 4 pp. 137-147, Sep.2017.

[18] K. Huang, Q. Zhang, C. Zhou and N. Xiong, "An Efficient Intrusion Detection Approach for Visual Sensor Networks Based on Traffic Pattern Learning," Vol. 47, pp. 2704 – 2713, May. 2017.

[19] F. Yie Leu, K.Lin Tsai, and Y. Ting Hsiao, "An Internal Intrusion Detection and Protection System by Using Data Mining and Forensic Techniques," Vol. 11,pp. 427 – 438, Apr.2015.

[20] A. Hofmann and B. Sick, "Online Intrusion Alert Aggregation with Generative Data Stream Modeling," Vol.8, pp. 282 - 294 Aug.2009.

BIOGRAPHIES

Aswathy T, she is currently pursing Master's Degree in Computer Science and Engineering in Sree Buddha College of Engineering, Elavumthitta, Kerala, India. Her research area of interest includes the field of data mining, internet security and technologies.

Misha Ravi received the master's degree in Software Engineering from Cochin University of Science and Technology, Kerala. She is an Assistant Professor in Department of Computer Science and Engineering, at Sree Buddha College of Engineering.