International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 5, Issue 2 (April '2019)

REVIEW ON SECURITY BASED DATA MINING IN WIRELESS SENSOR NETWORK'S SYSTEM

P.Kanagavalli,
Research Scholar,
Periyar University,
Salem, Tamilnadu,India.

Dr.V.Karthikeyani,
Assistant Professor,
Department of Computer Science,
Government Arts and Science College,
Komarapalayam,Tamilnadu,India.

Abstract: Website security is about keeping strangers out but also enabling controlled access to a network. Nowadays security on the wireless Internet is a crucial issue, so the Intrusion Identification System (IDS) is one of the solutions used to detect harmful attacks that threaten Internet security. The two main types of IDS are Misuse based Intrusion Detection Systems and Anomaly based Intrusion Detection Systems. In Misuse detection, the IDS analyzes the information it gathers and compares it to extensive databases of known attacks. While anomaly detection monitors the behaviour of the network, profile the normal behaviour and look for any anomalies. Data mining methods has been generally applied in the network intrusion detection system by extracting useful knowledge from vast number of network data and furthermore detect the intrusions. This paper gives an overview of existing strategies utilized for intrusion detection.

Keywords: Wireless Sensor Network, Intrusion Detection System, Classification, Clustering, Key management and authentication

I. INTRODUCTION

A Wireless Sensor Network is a network of simple sensing devices; these are capable of sensing changes in the events/parameters and communicate with various devices, over a specific geographic domain for some specific purposes, such as target tracking, surveillance, environmental monitoring and so forth. Processing ability, storage capacity and energy sensitivity, routing and data synchronization in WSN are challenging because the sensor nodes are tightly constrained. Network Intrusion Detection System (IDS) plays significant role in security framework. There are numerous techniques to reinforce the system security right now, for example, encryption, VPN, firewall, etc., but these techniques provide security in a static manner. However, dynamic intrusion detection system can give dynamic protection to the network, security, which is another form of intrusion detection system. Intrusion Detection is the issue of identifying unauthorized utilization, exploitation, and misuse of computer systems by both system insiders and outside attackers. An exploit is a general term used by hackers to create vulnerability in an application or a system so that they can have access to it. There are two basic types of exploits: known and unknown. Known exploits may help relieve any threats. However, unknown exploits are not yet been reported and they therefore exhibit a serious threat, especially if utilized at companies or governments. Based on the location in a network, IDS can be classified into two groups. One is host based IDS and the other one is network based IDS. Host-based IDS are installed in a host, which are capable of monitoring the traffic that is created by the host and arriving in that host only. In the event that there are attacks in some other part of the network, they won't be identified by the host-based IDS.Network-based IDS are strategically situated in a network to identify any attack on the hosts of that network. Since a Network-based IDS need to screen every one of the information going through the network, it should be quick to investigate the traffic. In order to capture all the data passing through the network, IDS should be position at the entry and exit point of the data in the network.

Intrusion Detection strategies fall into two classes [2] Signature-based IDS, Anomaly-based IDS. In Signature-based IDS, any suspicious activities are discovered and compare it with a set of predefined signatures. In intrusion detection system, the meaning of 'signature' is recorded confirmation of an attack or intrusion. It is also called knowledge-based IDS. The main drawback of this IDS has failed to identify new attacks that someone has created. Anomaly-based IDS monitors the network traffic, and if any doubtful behavior is found in the network, it compares against established baseline for normal use and classifying it as either normal or anomalies. If any suspicious activity or vulnerability is identified, it alerts the administrator or user. It is also named as behavior-based IDS. It is more responsive to new dangers or threats than the signature-based IDS yet hard to execute [3, 4]. Data mining procedures is a rising field of data security particularly in the issue of intrusion detection. Data mining is the procedure of consequently searching vast volumes of information for patterns utilizing association rules. It is also called Knowledge-Discovery.

It is much of the time used to designate the process of extracting useful information from huge databases. Data mining techniques can be significantly used in intrusion detection, each having its own specific advantages. The techniques used and the purposes for them are listed here.

Machine Learning: Machine learning is a category of algorithm that provides systems the ability to automatically learn and become more accurate in predicting outcomes

IJCRCST © 2019 | All Rights Reserved

without being explicitly programmed. The essential commence of machine learning is to construct algorithms that can get input data and utilize statistical analysis to predict an output while updating outputs as new data becomes available. When contrasted with statistical procedures, machine learning methods are appropriate to learning patterns. Classification and Clustering are most commonly used machine learning algorithms.

Classification: Classification is a data mining function that is used to classify each item in a set of data into one of a predefined set of classes or categories. The purpose of classification is that each data should reach its correct target class. Classification scheme makes use of mathematical techniques such as decision trees, linear programming, neural network and statistics. This procedure has been well known to identify individual attacks. However, it should be applied with some of the more advanced technologies to minimize high false positives rate.

Clustering: Clustering is the method of organizing a set of objects into groups related in some way or another. A cluster is thus a group of objects which are "similar" among them are placed in one class and "disparate" objects are placed in different class. Clustering is an unsupervised machine learning algorithms and no predefined classes. However, it investigates the information and may draw inferences from datasets to depict hidden structures from unlabelled data. Clustering algorithms are utilized in intrusion detection systems for isolating typical activities from anomalous activities. Clustering techniques provides some important benefits than the classification techniques.

Feature Selection: Feature selection is a procedure usually utilized and could be a essential part of machine learning. Several unimportant attributes might be present in data and many mining algorithms don't perform well with a lot of features. In this way, they should be expelled before any sort of mining algorithm is applied. The main objective of Feature selection is reducing the inputs for process and analysis, or of finding the most significant sources of information.

Association and Correlation Analysis: Association Rule Mining is a technique that finds frequently occurring patterns, correlations, or associations from large sets of data items found in different sorts of databases such as relational databases, transactional databases or other forms of data stores. This helps to discover hidden patterns and includes a wide variety of applications in business and analysis. Association rules can be used to select isolating attributes that are important for intrusion detection and guides the IDS to produce the better rules for finding various attacks.

Regression: Regression is a statistical technique used in data mining and it is a type of predictive modelling procedure which examines the relationship between a dependent (target value) and independent variable (s) (predictor). There are two types of regression normally used in data mining techniques. They are Linear and Logistic Regression. Linear regression is easier to use, more straightforward to interpret and designed for numeric dependent variables.. It is used to find the mathematical relationship between variables. If the result is straight line then it is considered as linear model and if it is curved line, at that point it is considered as a non linear model. Logistic regression is designed for categorical dependent variables. It is regularly used for prediction of output which is binary (2 classes), it may be utilized for categorical dependent variables with excess of 2 classes. For this situation, it is called Multinomial Logistic Regression. Logistic regression is one of the most commonly used regression methods in the business which is widely applied across fraud detection, credit card scoring and clinical trials.

Stream Data Analysis: Streaming Data is the ability to continuously explore the data to get the crucial information. It is changeable depending on the time, and its value is renewable. Data streams play an important role in the intrusion detection system by finding a sensation that an event may have occurred. It helps to track the sequences of frequently encountered events and to recognize the attacks by finding sequential patterns. The streaming data investigation may be in the form of mathematical calculations, statistical analysis, packet inspection, image processing, and so on.

Key management and authentication: Key management and authentication have been utilized to shield WSNs from various attacks.The primary security measures for protecting WSN [5] are encryption and authentication. But cryptography supported secret key management are not enough to safeguard the WSN, because many attacks might extract sensitive data and utilize them for malicious reasons, in the first level of security. After the failure of the cryptographic techniques [6], Detection-based approaches are proposed as a second line of defense, to protect WSNs from intrusion and attacks. Intrusion detection system (IDS) monitors and analyzes the events to find the maximum security issues generated in the network system. IDSs are utilized to screen the network to notice something uncommon [7].Intrusion detection concept was initially proposed by Anderson [8] and there are several range of ID techniques utilizing data mining techniques. As a result, the motivation behind this paper is to review related papers of using data mining for intrusion detection

II. LITERATURE REVIEW

2018, Nabeela Ashraf, et al. [9] In this exploration, Naive Bayes, J48 and Random Forest classifiers are compared to work out the detection rate and accuracy of IDS.For tests, the KDD_NSL dataset is utilized and therefore the classification performances of Naive Bayes, J48 and Random Forest are compared on 20% KDD_NSL dataset. From the outcomes, Random Forest works better than Naive Thomas Bayes and J48 in terms of accuracy and detection rate. All the three classifiers accomplished up to 90% outcomes in both exactness and review.

2018, Kinam Park, et al. [10] The forest algorithm utilized by this research is an efficient supervising machine learning algorithm for IDS. By utilizing this algorithm, it analyzes a class-specific detection of Kyoto 2006 + datasets. This

examination initially refined the first 3 classes (i.e., normal, known attack unknown attack) into 6 classes (i.e., normal, unknown, shellcode, IDS+shellcode, malware, IDS). One test dataset and two training datasets varies in size have been built for evaluating the performance of detecting various types of attacks. Although this research gained high overall detection efficiency when trained with the first training set (0.99 of precision, recall, F1-score, and F2-score). Hence, this research developed the second training set by means of random under-sampling to set the size of all the class equivalent to the quantity of instances of the smallest class (i.e., shellcode).This analysis resulted in lesser performances for all categories, that was unsatisfying. So that the dimensions of data was not adequate, and training with a similar size class may not be suitable for the machine learning approaches. In this analysis additionally note that the unknown attack category still proves a decent performance. F1-score of zero.90, that proposes that there is a definite pattern for the unknown attack.

2017, Elham Ariafar, et al. [11] Proposed a system in view of improvements of the K-means clustering and decision tree (DT) classification algorithms, effort were made in this investigation to identify network interruption with higher accuracy. This proposed system uses a genetic algorithm (GA) to improve the parameters such as number of clusters (K), max_runs, and confidence. One of the most critical characteristics of the recommended system is its relevance to both supervised and unsupervised strategies. The simulation results on the NSL-KDD 2009 dataset is that this method has proved an improvement on detection rate (TR) and incorrect alert rate (FAR) compared to the new Cluster Clerical (NEC) method.

2017, Dr. Shashikant Dugad, et al. [12] presented a technique known as Seashore ship intrusion detection system which is utilized in surveillance of coastal areas from intrusions of unauthorized marine vessels in a extremely dynamic surroundings. This system uses a mixture of both Image processing and SVM machine learning procedure, reduce the setbacks such as expensive setups, inaccurate detection and algorithmic error of the prevailing system. Finally, experimental results showed that SVM can be utilized as a machine learning process to train the framework by exposing it to various seashore situations. As a result, it can be utilized as a real time security framework at coastal areas.

2017,LI Miao, et al. [13] This research analyzes the use of the CART decision tree combined with PCA algorithm in network intrusion detection. This study makes clear that the use of ID3 and C4.5 algorithms is negligible in the intrusion detection application. KDD CUP 1999 data set is employed in this research to investigate the Scikit-learn machine learning platform which is used to verify the legitimacy of the model. Furthermore, the experimental results on backup datasets demonstrated that the model can effectively identify and enhance the prediction accuracy of network attack behaviour

2017, Mohammad Almseidin, et al. [14] In this analysis, many experiments were performed and tested to evaluate the efficiency and also the performance of the following machine learning classifiers: J48, Random Forest, Random Tree, Decision Table, MLP, Naive Bayes, and Bayes Network. KDD intrusion dataset is used in this model for all the tests. The rate of various form of the attacks in the KDD dataset are around 79% of DOS attacks, 19% of normal packets and 2% of different kinds of attacks. In this investigation 148753 instances of records have been selected as training data to construct the training models for the preferred machine learning classifiers. The testing part is executed based on 60000 random events. Several performance metrics such as accuracy rate, precision, false negative, false positive, true negative and true positive are computed. The experimental results have exhibited that there is no single machine learning mechanism that may effectively handle every kind of attacks. The decision table (rules base classifiers) accomplished the least false negative value of (0.002).At the same time, it is far behind in finding the highest accuracy rate detection. On the other hand, Bayes network classifier has highest rate of identifying the typical packets accurately. On the other hand, Bayes network classifier has the highest rate of accurate identification of typical packets. Random forest classifier enrolled the best accuracy rate 93.77%, with the smallest RMSE value and false positive rate. It appears that the random forest classifier presents acceptable execution parameters with the exception of the false negative parameter. On the contrary, all the chosen machine-learning classifiers, except MLP were able to generate their training models in an acceptable timeframe. In addition, to save the availability and the privacy of the network resources, the true positive and the average accuracy rates alone are not adequate to identify the intrusion. Further attention should be paid on finding false negative and false positive measurements.

2017, Hongbing Wang, et al. [15] designed a system named as (SP-PCA-SVM), a parallel principal component analysis (PCA) combined with support vector machine (SVM) algorithm based on spark platform.PCA is utilized to lessen the sample data and parallelize SVMs. Then, the model is implemented on spark platform. The experimental outcomes show that the proposed system can cut down the classification time of the classifier under the condition that the accuracy rate is not considerably reduced. The PCA dimensional reduction parameter selection is still in the temporary phase, and the classification accuracy is reduced when the parameter is incorrectly set.

2017, Tuncay Soylu, et al. [16] proposed a scheme using Simple CART machine learning algorithm for hardware-based traffic classification. The existing process used the discretization pre-process in order to improve the accuracy of the algorithm. However, the various sizes of nodes of Simple CART decision tree created by discretization pre-process have directly mapped onto the hardware. As a result, memory and resource inefficiency issues appeared. To resolve these issues, they proposed to represent Simple CART decision tree in two phase hybrid data structure (Extended-Simple CART).This extended structure contains different range of trees in phase 1 and a Simple CART decision tree nodes improved with bitmaps in phase 2. To obtain high throughput the suggested system is implemented on hardware utilizing

Field Programmable Gate Arrays (FPGAs). The testing result proves that Extended Simple CART scheme outperforms the existing methodologies in terms of accuracy and delay. In addition, it is less responsive to the type of the dataset applied.

2016, Divyatmika, et al. [17] proposed a completely unique design for intrusion detection system using neural networks and data mining. The recommended framework has 2 layers of architecture and it helps to extend the data security, because data needs to go through two classifiers. In the first phase data has classified through KNN classification which separates the regular traffic patterns from an unseen /new data. The system is built as bottom-up approach with the help of Hierarchical agglomerative clustering algorithm. Furthermore, multilayer perception algorithm is used in this model to detect any threats faster and more accurately.KNN classification reduces cost-overheads and Reinforcement learning decreases the false alarm rate. Thus, this framework gives an abnormal state of security by giving high TP and low false positive rate

2016, Kajal Rai M, et al. [18]. In this recommended work, the C4.5 decision tree approach is used to construct a decision tree algorithm. This research has seeks to address two important issues, such as the feature selection and split value. This proposed algorithm, calculate split value by taking the average of the values within the domain of a selected attribute at every node and gives uniform weight-age to all the values in the domain. It offers taking limited number of attributes and provides reasonable accuracy with reasonable timing. An Experimental result on NSL-KDD datasets, the proposed algorithm, is more efficient in detecting attacks on the network with a limited number of features and requires less time to build the model. The formula utilized to calculate the gain ratio in Decision Tree Split can even be utilized in attribute selection for feature reduction

2016, Dikshant Gupta, et al. [19] This research automatically creates rules for categorizing network functions using various data mining algorithms, including Linear Regression and K-Means Clustering. In this proposed scheme, intrusion has been detected by comparative analysis of these data mining technique and the patterns of attacks are known by using the NSL-KDD dataset. NSL-KDD dataset was pre-processed utilizing mean normalisation technique. The experimental results proved that the linear regression technique could be very helpful in finding network attacks with an amazing 80% accuracy and K-Means Clustering approach showed 67.5 % accuracy.

2016, Ajinkya Wankhade, et al. [20] This proposed work, uses distributed intrusion detection system (DIDS) to collect data across the network and to use the hybrid model to describe network behaviour as normal or unusual. To detect intrusion this hybrid model combines machine learning algorithms such as Support Vector Machine (SVM) and Ant Colony Optimization (ACO) techniques. Since, these hybrid modes provide a high level of detection rate and faster running time that is incredibly helpful in real-time environments. Experiments are carried out in three algorithms such as pure SVM, pure ACO and the hybrid method. The results showed that the intrusion detection rate of hybrid method significantly increased compared to pure SVM and pure ACO.

2016, R.Ravinder Reddy, et al. [21] introduced a new concept known as SVM discriminant function which is used for classify the intrusions. The Effective discriminant function perfectly identifies the intrusion and abnormality of the data. In this method rough set theory is applied for feature selection and it reduces the dimensionality of the dataset as well as reduces the detection time. Scaling the dataset improves the discriminant function execution. The overall performance of the proposed intrusion detection system has been enhanced by combining the scaling and rough set feature selection.

2016, K. Saravananathan, **et al. [22]** to discover the optimal solution for Diabetes, this research work analyzes frequently used classification techniques such as J48, CART, SVMs, and kNN on the medical dataset. For the given dataset specificity, sensitivity, precision, error rate are calculated as performance indicators. Based on these performance indicators, the above said four algorithms are analyzed. Experimental results showed that the performance of J48 technique is significantly higher than the other three techniques such as CART, SVMs, and kNN in determining accuracy. However, the performance of the KNN algorithm showed the minimum accuracy. Data normalization function improved the performance of J48 technique.

2015, Motaz M. et al. [23] This research focused on predicting terrorist attacks by comparing various classifiers such as standard, ensemble, hybrid, and hybrid ensemble machine learning methods. It is mainly focused on supervised machine learning (SVM) classification. Analyses were done utilizing real world dataset produced by Global terrorism Database (GTD) from National Consortium for the study of terrorism and Responses of Terrorism (START). During the experiment, 18 classification algorithms were analyzed to make comparative analysis. They are classified into four main categories; Standard classification protocols, hybrid classifiers, ensemble, and hybrid ensemble classification. Three distinct tests have been performed in the dataset and Litwise deletion method used to handle missing data. In the first experiment the whole dataset is consider as training data. Whereas in the second experiment the whole dataset splited into 66% training data set and 34% testing data set and the last experiment investigate the classifiers using 10 fold cross-validation. Test results showed that hybrid machine learning classifiers exhibit smart and proven improvement in predictive accuracy over some standard comprehensible and ensemble techniques. Furthermore, the ability to predict the attacks ensemble methods are more accurate compared to hybrid ensemble methods

2015, Yousef El Mourabit, et al. [24] This proposed work compared and evaluated data mining techniques such as clustering approach, Support Vector Machine (SVM) Classifier, Naïve Bayes Classifier and Random Forest Classifier, which are used to detect intrusions in wireless

IJCRCST © 2019 | All Rights Reserved

sensor network (WSN). To measure the performance of detection this recommended model organized the data set into five steps, based on standard KDDCup'99 intrusion detection dataset in order to normalize the dataset. The experimental outcomes exhibit that the random forest strategies give high detection rate and lessen false alarm rate. According to the experimental results, it is greatly suggested that data mining techniques effectively find intrusions and attacks in WSN.

2015, Jaina Patel, et al. [25] This recommended scheme used hybrid model in which it combines Anomaly based Intrusion detection technique with Signature based Intrusion detection technique. This system consists of two step mechanism. During the first step, signature based IDS SNORT is employed to create alerts for anomaly data and in the second step "k-means + CART" is employed for categorize usual and unusual activities. Experiments were carried out on KDD Cup Dataset and test results showed that CART algorithm performed well than C4.5 algorithm for intrusion detection. Moreover, this proposed system not only increases the effectiveness of identifying attacks, but also has a high accuracy rate and low false warning rate.

2014, Alaa F., et al. [26] this research implemented three models, such as decision tree based C4.5 algorithm, Multi-Layer Perceptron and Support Vector Machine, to solve the intrusion detection problem. The numbers of attacks are categorized using three techniques. A set of features are selected by utilizing best first search and genetic search methods in order to improve the performance of the proposed model. The test results show that the proposed models are capable of reducing the complexity while maintaining the acceptable detection accuracy. Furthermore, the decision tree based C4.5 algorithm shows the very best classification accuracy compared to other search techniques.

III. CONCLUSION

Intrusion detection system (IDS) is one of the essential mechanisms against harmful attacks that threaten the Internet security. This paper describes the various existing data mining techniques used for intrusion detection and explains how the techniques are implemented and evaluated by the researchers. According to this survey, data mining techniques are being improved in network IDS, making it possible to find intrusions and attacks in high accuracy rate.

IV. REFERENCES

[1]. Bhavsar, Yogita B., and Kalyani C. Waghmare. "Intrusion detection system using data mining technique: Support vector machine." International Journal of Emerging Technology and Advanced Engineering 3.3 (2013): 581-586.

[2]. Siddiqui, Mohammad Khubeb, and Shams Naahid. "Analysis of KDD CUP 99 dataset using Clustering based Data Mining." International Journal of Database Theory and Application 6.5 (2013): 23-34.

[3]. Ektefa M., Memar S., "Intrusion Detection Using Data Mining Techniques",IEEE Trans., 2010.

[4]. Theodoros Lappas and KonstantinosPelechrinis, "Data Mining Techniques for (Network) Intrusion Detection Systems".

[5]. E.Kesavulu Reddy, Member IAENG, V.Naveen Reddy, P.GovindaRajulu, "A Study of Intrusion Detection in Data Mining" Proceedings of the World Congress on Engineering 2011 Vol III WCE 2011,pp London, U.K. July 6 - 8, 2011

[6]. Dokas, P., Ertoz, L., Kumar, V., Lazarevic, A., Srivastava, A.J., and Tan, P.N. "Data Mining for Network Intrusion Detection." Denning, D.E. "An Intrusion Detection Model, IEEE Trans-actions on Software Engineering." SE-13:222-232, 1987.

[7]. Depren, O., Topallar, M., Anarim, E., Ciliz, M.K. "An intelligent intrusion detection system (IDS) for ano-maly and misuse detection in computer networks." Expert System with Applications 29, 713-222.

[8]. Didaci,L.,Giacinto,G.and Roli, F. "Ensemble Learning for Intrusion Detection in Computer Networks"(2002), Proc. of AIIA, Siena, Italy, Friedman, J.H. "Multivariate adaptive regression spines." Anal Stat, 19:1–141. (1991)

[9]. Nabeela Ashraf, Waqar Ahmad and Rehan Ashraf," A Comparative Study of Data Mining Algorithms for High Detection Rate in Intrusion Detection System", Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018

[10]. Kinam Park, Youngrok Song, Yun-Gyung Cheong," Classification of Attack Types for Intrusion Detection Systems using a Machine Learning Algorithm", 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications.

[11]. Elham Ariafar, Rasoul Kiani," Intrusion Detection System Using an Optimized Framework Based on Datamining Techniques", 2017, IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI).

[12]. Dr. Shashikant Dugad, Vijayalakshmi Puliyadi, Heet Palod, Nidhi Johnson, Simran Rajput, Swapna Johnny," Ship Intrusion Detection Security System Using Image Processing & SVM",IEEE, 2017 International Conference on Nascent Technologies in the Engineering Field (ICNTE-2017)

[13]. LI Miao, "Application of CART Decision Tree Combined with PCA Algorithm in Intrusion Detection",IEEE,2017.

[14]. Mohammad Almseidin, Maen Alzubi, Szilveszter Kovacs and Mouhammd Alkasassbeh," Evaluation of Machine Learning Algorithms for Intrusion Detection System", SISY 2017 • IEEE 15th International Symposium on Intelligent Systems and Informatics • September 14-16, 2017 • Subotica, Serbia.

[15]. Hongbing Wang, Youan Xiao and Yihong Long," Research of Intrusion Detection Algorithm Based on Parallel SVM on Spark", National Science & Technology Pillar Program ,2017 IEEE.

[16]. Tuncay Soylu, Oguzhan Erdem, Aydın Carus, Edip S. Guner," Simple CART Based Real-Time Traffic Classification Engine on FPGAs," 2017 IEEE

[17]. Divyatmika, Manasa Sreekesh," A Two-tier Network based Intrusion Detection System Architecture using Machine Learning Approach",IEEE, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.
[18]. Kajal Rai, M. Syamala Devi, Ajay Guleria," Decision Tree Based Algorithm for Intrusion Detection", Int. J. Advanced Networking and Applications Volume: 07 Issue: 04 ,(2016) ISSN: 0975-0290.
[19]. DikshantGupta, SuhaniSinghal, Shamita Malik, Archana Singh," Network Intrusion Detection System Using various data mining techniques", International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016)
[20]. Ajinkya Wankhade, K. Chandrasekaran," Distributed-Intrusion Detection System using combination of Ant Colony Optimization (ACO) and Support Vector Machine (SVM)", IEEE, 2016 International Conference on Micro-Electronics and Telecommunication Engineering
[21]. R.Ravinder Reddy, Dr.Y Ramadevi ,Dr.K.V.N Sunitha," Effective Discriminant Function for Intrusion Detection Using SVM",IEEE, 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India
[22]. K. Saravananathan, and T. Velmurugan," Analyzing Diabetic Data using Classification Algorithms in Data Mining", Indian Journal of Science and Technology, Vol 9(43), November 2016
[23]. Motaz M. H. Khorshid , Tarek H. M. Abou-El-Enien , Ghada M. A. Soliman," A Comparison among Support Vector Machine and other Machine Learning Classification Algorithms", IPASJ International Journal of Computer Science (IIJCS), Volume 3, Issue 5, May 2015.
[24]. YOUSEF EL MOURABIT, AHMED TOUMANARI , ANOUAR BOUIRDEN , NADYA EL MOUSSAID," Intrusion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms: Comparative Evaluation Based on Attacks Detection", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, 2015.
[25]. Jaina Patel, Mr. Krunal Panchal," Effective Intrusion Detection System using Data Mining Technique", June 2015, Volume 2, Issue 6 JETIR (ISSN-2349-5162)
[26]. Alaa F. Sheta1, Amneh Alamleh2," A Professional Comparison of C4.5, MLP, SVM for Network Intrusion Detection based Feature Analysis",ICGST,2014.

IJCRCST © 2019 | All Rights Reserved