International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

Augment Method for Intrusion Detection around KDD Cup 99 Dataset

Ajay Prakash Sahu[1], Amit Saxena[2], Kaptan Singh[3]

[1]*PG Scholar Truba institute of Engineering and Information Technology, Bhopal (M.P.) India*
[2]*Head CSE Dept Truba institute of Engineering and Information Technology, Bhopal (M.P.) India*
[3]*CSE Dept Truba institute of Engineering and Information Technology, Bhopal (M.P.) India*

Abstract - *The Intrusion Detection Systems (IDS) can be used extensively for protecting network. Intrusion detection systems (idss) are mostly deployed along with other defending security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. Now a day's most users use ids and password as login pattern for the authenticate users. However They making patterns is weakest point of computer security as so many user share the login pattern with the co-workers for the completed co-task, inside attacker is attacked internally and it will be valid attacker of system, As using intrusion detection systems and firewalls identify and isolate harmful behaviours generated from the outside world they can find out internal attacker of the system only. Lot of pcs confirm client ID and covert word before clients can login there frameworks. On the off likelihood that there is a legitimate client of a framework who assaults the framework inside is difficult to recognize. . The KDD cup 99 dataset is a well- remembered standard in the research of Intrusion Detection Techniques. Various efforts is going on for the enhancement of and testing the detection model is consistently of prime concern since improved data superiority could advance offline intrusion detection. In this work the investigation is carried out with respect to two important evaluation metrics, Precision/Accuracy and True Positive (TP)/Recall for an Intrusion Detection System (IDS) in KDD cup 99 dataset. As a outcome of this experiential investigation on the KDD cup 99 dataset, the contribution of every of four assault classes of attributes on Recall and Precision is illustrate which can assist to improve the correctness of KDD cup 99 dataset which attain highest accuracy with lowest false positive (FP).*

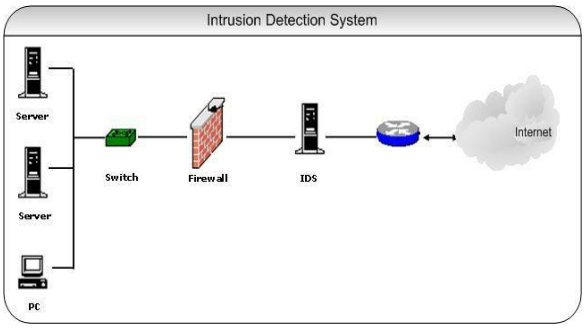
Keywords: Intrusion Detection, Machine Learning, Classifiers, WEKA tool, Precision, Recall.

1. INTRODUCTION

Internet plays needful role in today's universe. It is used in shopping, education, social networking, business etc. This has gain a risk of computer systems linked to the internet becoming targets of intrusions by cyber criminals. Cyber criminals attack systems to gain unlawful access to information, misuse information or to reduce the availability of information to authorized users. This result in massive financial losses to companies besides losing their goodwill to consumer. Intrusion avoidance techniques such as user authentication (e.g. using biometrics or password), information protection (e.g. Encryption), sidestep programming errors and firewalls have been used to secure computer systems. But, regrettably these intrusion prevention techniques alone are not sufficient. There will always be unknown exploitable deficiency in the system due to design and programming flaws in application programs, protocols and operating systems. Therefore, we need technique to detect intrusions as soon as possible and take appropriate actions [1]. The processes for secure software development comprise similar concepts as provable security. Developers identify the potential enemy and the risk is analyzed based on the value of the data and the estimated capabilities of the adversary. Use cases are developed to help developers create and authenticate security. Even with security requirements, use cases, code walkthroughs, and vulnerability testing, anonymous vulnerabilities still make it into systems. Controls such as IDS, firewalls and local access controls are used to improve the security posture of a system [2]. Firewall systems are customarily implemented to everywhere computer networks. They act as a measure of control, enforcing the relevant segment of the security policy. A firewall can be a number of different segments such as a router or a collection of host machines. However, the basic function of a firewall is to protect the integrity of the network which is firewall controlled is firewall controlled. There are various types of freewill that can be enforcing, with the choice of firewall being reliant upon the security policy and the level of formation in the system [3]. For known accomplishment, intrusion detection systems can quickly classify and eschew attacks. Systems that only have the assets to use intrusion detection systems that rely on pre-existing knowledge of particular exploits are vulnerable to novel exploits until security professional can manually create classifiers for those exploits. Automated signature generation (ASG) is used to fill the gap until security professional can analyze novel exploits [4]. Automated signature generate (ASG) refers to the progress of dynamically generate rules for detecting network. intrusions. The stern definition of automated system formation should only include signature based intrusion detection systems; anyhow modeling for anomaly-based

detection is usually associated with ASG. In the last few years there has been considerable analysis on this topic. Automated signature generation support assuage the limitation signature based intrusion detection systems have with organize novel exploits. Up until the appearance of automated signature generation systems the best solution to alert a against novel attacks was to employ anomaly detection agents on the network and on critical hosts. Signatures are alone able to detect accomplishment against known vulnerabilities [5]

1.1ARCHITECTURE OF INTRUSION DETECTION SYSTEM



1.2 HISTORIES OF IDS

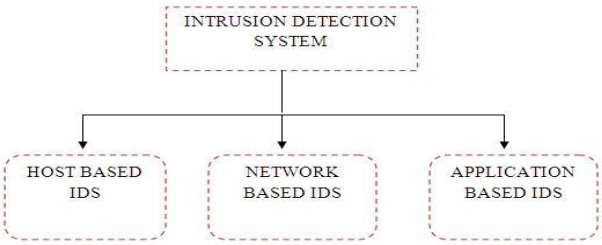
Intrusion detection concept was universalizing in early 1980's after the progression of internet with surveillance end monitoring the threat [7]. There was a sudden rise in reputation and incorporation in security structure. Since then, several incidents in IDS technology have progressive intrusion detection to its current state. James Anderson's wrote a paper for a government organization and imported an approach that audit trails consist of important information that could be beneficial in tracking misuse and sympathetic of user behavior .Then the detection appeared and audit data and its priority led to terrific improvements in the sub systems of operating system [6]. IDS and Host Based Intrusion Detection System (HIDS) were first time defined. In 1983, SRI International and Dorothy Denning began alive on a government project that introduces a new effort into intrusion detection system development. Around 1990s the revenues are engendered and intrusion detection market has been constructing. Real secure is an intrusion detection network developed by ISS. After a year, Cisco recognized the priority for network intrusion detection and the deal in Wheel Group for attaining the security solutions [7].

1.3 OVERVIEW OF ID

An intrusion detection system (IDS) is a type of security software layout to automatically alert bureaucrat when someone or something is irritating to compromise information system through venomous activities or through security policy misdemeanor. An IDS works by observe system activity through investigate vulnerabilities in the system, the integrity of files and regulate an analysis of patterns based on previously known attacks. It also automatically monitors the Internet to analysis for any of the current threats which could result in a future attack. An intrusion detection system (IDS) is a elemental of the computer and information security structure. Its main goal is to differentiate between natural activities of the system and behavior that can be classified Mistrustful or intrusive [8]. IDS‟s are vital. Because of the huge number of incidents reported increases whole year and the attack techniques are always develop. IDS approaches can be branched into two main categories: misuse detection or anomaly detection [8]. Intrusion detection system (IDS) inspects all outbound and inbound network process and find out the indecisive patterns that may point to a network or system intrusion or attack from someone trying to crack into or conciliation a system. IDS gather and observed information from different areas inside a network of systems to find out credible safety breaches, which contain well-adjusted called intrusions (attacks external from the association) and misuse (attacks from inner the association). IDS use susceptibility appraisal, it is an expertise which is layout and developed to assess the security of a network [9]. Mainly security is concerned with the ensuing aspects in a computer system [10].

- Confidentiality – information is to be gain only by permissible persons.
- Integrity – information must remain guileless by destructive or malicious attempts.
- Availability – computer is culpable to function without downgrading of access and equip resources to legal users when they require it

1.4 COMPONENTS



There are three primary components of IDS:

- Network Intrusion Detection System (NIDS):

This does analysis for traffic on a whole subnet and will make a match to the traffic passing by to the attacks already known in a library of known attacks.

- Network Node Intrusion Detection System (NNIDS):

This is similar to NIDS, but the traffic is only monitored on a single host, not a whole subnet.

- Host Intrusion Detection System (HIDS):

This takes a "picture" of an entire system's file set and compares it to a previous picture. If there are significant differences, such as missing files, it alerts the administrator.

1.5 IDS PROVIDE

IDS provide the following:

- Monitoring and analysis of user and system activity.
- Checking and comparing vulnerabilities.
- Availability of critical data files.
- Statistical analysis of activity patterns based on the matching to known attacks.
- Abnormal behavior analysis.
- Operating system analysis and comparison with stable state.

1.6 TYPES OF IDS'S

HOST BASED INTRUSION DETECTION SYSTEM (HIDS): A (HIDS) monitors the activities of an particular host or computer system. The initial focus of host based intrusion detection system is on the operating system presentation and events. However, in network systems also, HIDS finds its leading values in finding the flow of information and detecting the attacks over the network based on the events appear within the network.[11]

NETWORK INTRUSION DETECTION SYSTEM (NIDS): A (NIDS) is used to monitor and activities network traffic to protect a system from network-based hazard where the data is traffic across the network. A NIDS tries to detect mischievous activities alike as denial-of-service (Dos) attacks, port scans and monitoring the network traffic attacks. NIDS consist of a number of sensors to monitors packet traffic, one or also than servers for NIDS management functions, and one or also management relieves for the human interface [12]

.

APPLICATION-BASED INTRUSION DETECTION SYSTEM: Is an exclusive subset of Host-Based IDS (HIDS) that analyzes the events arise within a software application. The most common information origin for Application-Based intrusion detection system is the application's transaction log file. The ability to interface with applications directly allows Application-Based intrusion detection system to detect suspicious behavior such as users exceeding their security authorization. Application-Based intrusion detection system monitors the interaction between user and application, which traces activity to individual users.

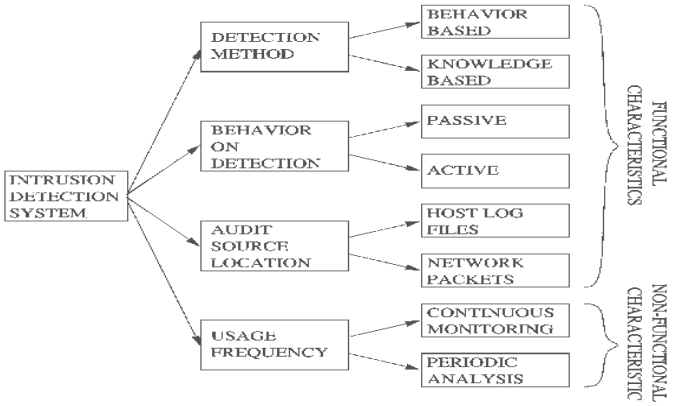
1.7COMPONENTS OF INTRUSION DETECTION SYSTEM

The two main classification through which network can be analyzed for the detection of intrusion are Misuse detection and Anomaly detection.

MISUSE/SIGNATURE-BASED DETECTION: This kind of detection engine detects intrusions that follow illustrious patterns of attacks (or signatures) that exploit illustrious software vulnerabilities. The main limitation of this access is that it only looks for the known deficiency and may not care about detecting unknown future intrusions [13] Misuse detection is an access where the detection of intrusions is based on pattern matching. Here the atypical system behaviour is defined at first by collecting the patterns of attack, and then characterize any other behaviour, as normal behaviour by matching them against the once recorded attacks.

ANOMALY/STATISTICAL-BASED DETECTION: IDS that look at network traffic and examine data that is not credible, incorrect or generally abnormal is say anomaly-based detection. This method is effective for detecting redundant traffic that is not specifically known. For instance, anomaly-based IDS will detect that an Internet protocol (IP) packet is

abnormal. It does not detect that it is abnormal in a specific way, but indicates that it is anomalous [14].



Functional Characteristics and non Functional Characteristics IDS

2. DATA MINING IN INTRUSION DETECTION SYSTEM

Data mining is the non-trivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data. In prevail years, data mining techniques employed in intrusion detection have proved to be successful. Data mining is the search for valuable information within large volumes of data by systematically exploring underlying patterns, trends, and relationships hidden in available data [15]. Data Mining-based Misuse Detection each data record is hush-hush and labeled as normal or anomalous activity. This process is the support for a learning algorithm able to detect known attacks and new ones if they are cataloged accordingly under a statistical process. The basic eminent as discovery outliers, matches an aberrant behavior crosswise an attack patterns knowledge base that capture behavioral patterns of intrusion and commonplace activity. To do this, it is vital to compute each measure with random variables implying more updating achievement as more audit records are analyzed but more accuracy with more mined data. Although the activity needs to be scrutinize individually, complementary visualization and data mining techniques can be used to improved performance and reduce the computational requirements. Some researches focused on this topic are Java Agents for Metal earning (JAM), Mining Audit Data for Automated Models for Intrusion Detection (MADAM ID) and Automated Discovery and Concise On the other hand [16]

2.1 MACHINE LEARNING

Machine Learning is the study of computer algorithms that improve automatically through experience. Applications range from data mining programs that discover general rules in large data sets, to information filtering systems that automatically learn users' interests. Probably the two most popular machine learning problems. Techniques that address both of these problems has been applied to idss .They are two types of Techniques [17].

2.2 CLASSIFICATION TECHNIQUES

In a classification task in machine learning, the task is to take each instance of a dataset and assign it to a particular class. A classification based IDS attempts to classify all traffic as either normal or malicious [17].

NEURAL NETWORKS: Neural networks for intrusion detection were first introduced as an alternative to statistical techniques in the IDES intrusion detection expert system to model.

FUZZY LOGIC: Fuzzy logic is derived from fuzzy set theory dealing with reasoning that is approximate rather than precisely deduced from classical predicate logic.

GENETIC ALGORITHM: Genetic algorithms were originally introduced in the field of computational biology.

SUPPORT VECTOR MACHINE: Support vector machines (svms) are a set of related supervised learning methods used for classification and regression.

2.3 CLUSTERING TECHNIQUES

Data clustering is a essential technique for statistical data investigation, which is used in many area, including machine learning, data mining, pattern recognition, image analysis and bioinformatics. Machine learning consistently regards data clustering as a form of unsupervised learning. Clustering is advantageous in intrusion detection as malicious activity should cluster together, separating itself from non-malicious activity [17]. Of new patterns from large volume of training data that are collected from Knowledge Discovery in Data Mining (KDD) CUP 1999 benchmark dataset in order to execute hybrid intrusion detection in host as well as in network. Moreover, intrusion detection has been carried out using classification and clustering algorithms integrated with feature selection [18].

2.4KDD CUP 99 DATASET

The KDD99 dataset is now the criterion for training, testing and interpret learning IDS, so it is basic for IDS developers. The competition task was to structure network intrusion radar, a predictive model or a classifier that cantle what are "bad'' connections, called intrusions or attacks. Normal connections are organize to profile that natural in a military network and attacks fall into one of four division as follows.

DENIAL OF SERVICE ATTACK (DOS): DOS type of attack where the attacker makes an hunt to make a source unavailable for owned intended users.

USER TO ROOT ATTACK (U TO R): This is one of the almost dreaded cyber-attacks in the traffic. Here the attacker ascent access to an end user's account and try to admittance root access to the absolute information system.

REMOTE TO LOCAL ATTACK (R TO L): occurs when an attacker who has the capability to send packets to a machine over a network but who does not have an account on that machine accomplishment some vulnerability to earnings local access as a user of that machine.

PROBING: Probing is a class of attacks in which an attacker examine a network of computers to gather information or find known vulnerabilities. An attacker with a design of machines and services that are accessible on a network can use this information to look for exploits TCP stance for "Transmission Control Protocol". TCP is a significant protocol of the Internet Protocol Suite at the Transport Layer which is the fourth layer of the OSI model. TCP symbolic connection-oriented protocol which implies that data sent from one side is guaranteed to reach the destination in the same order. In 1999, the authentic TCP dump files were pre possessed for utilization in the Intrusion Detection System yardstick of the International Knowledge Discovery and Data Mining Tools Competition. visage are grouped into four categories as given below.

Basic Features: Basic features can be derived from packet headers without investigate the payload.
Content Features: Domain knowledge is used to assess the payload of the authentic TCP packets. This includes features such as the number of failure login attempts.
Time-based Traffic Features: This stand of features is creating mentally to capture properties that mature over a 2.0 second impermanent window.
Host-based Traffic Features: Utilize a historical window estimated over the 100 number of connections instead of time.

The KDD CUP 1999 intrusion detection benchmark dataset consists of three components, which are detailed in Table 1.1. In the Data Mining Tools and International Knowledge Discovery antagonism, only "10% KDD" dataset is employed for the purpose of training. This dataset contains 22 attack categories and is a more succinct version of the "Whole KDD" dataset.

3. PROPOSED WORK

In this paper a "Strengthen Intrusion Detection Method Using Machine Learning for KDD Cup 99 Dataset" is proposed to enhance the efficiency of intrusion detection using KDD cup Intrusion dataset. We utilized Naïve Bayes, J48 and Random forest classifiers for the classification. Classifiers are appraising based on recall, Precision, f-measures and ROC Curve area performance criteria's. A WEKA 3.7.1 workbench is used for experimental study. It is recognized that random forest is the best classifier among all used methods. Following algorithm is used to implement proposed method on Linux OS (Ubuntu 14.04)

INPUT: KDD Cup99 Dataset **OUTPUT:** clandestine dataset in ARFF format

Step 1: Create Temp file for processing

Step 2: pre pares input dataset

Step 3: Remove outliers // trim the dataset

Step 4: Replace all attacks by their parent category

Step 5: create WEKA compatible file of classified attacks // ARFF file.

Step 6: check the accuracy of classification of proposed method on WEKA by applying different classifiers (for instance we used Naive Bayes, J48 and Random forest classifiers.

Table 1: Characteristics of the KDD CUP 99 Intrusions Detection Dataset

Dataset	DoS	Probe	U2R	R2L	Normal
10% KDD	391458	4107	52	1126	97277
Corrected KDD	229853	4166	70	16347	60593
Whole KDD	3883370	41102	52	1126	972780

Used WEKA Classifiers: - Processed dataset is applied to the Naive Bayes, J48, and Random forest classifiers. Brief description of each classifier is given here.

NAIVE BAYES CLASSIFIER: - A naive Bayes classifier is a simple probabilistic classifier physique on implement Baye‟s theorem with strong (naive) independence assumptions. In simple terms, a naive Bayes classifier presume that the presence (or absence) of a precise feature of a class is unrelated to the presence (or absence) of any other feature, given the class variable. Naïve Bayes classifier presumes that the impact of the value of a predictor (X) on a given class (C) is independent of the values of other predictors. This expectation is called class provisional independence.

J48 CLASSIFIER: J48 classifier is a uncomplicated C4.5 decision tree for classification. It brings about a binary tree. The decision tree approach is most useful in classification complication. With this technique, a tree is constructed to model the classification process

RANDOM FORESTS CLASSIFIER:-Random forests are an ensemble learning technique for classification, regression and extra tasks, that operate by constructing a large number of decision trees at training time and outputting the category that's the mode of the categories (classification) or mean prediction (regression) of the individual trees.

4. RESULT

RESULT ANALYSIS: Experiment is carried out on the system having Intel Core i3 Processors, 8 GB RAM, 1TB HDD, UBUNTU 14.10 Operating System and WEKA Machine V 3.6.11 Learning Workbench matured by university of Waikato is appropriate for the classification task. WEKA [17]. It can be extended by the user to execute new algorithms. Classification Models are evaluation based on following criteria's.

TRUE POSITIVE OR TP: Recall in this context is defined as the number of true positives divided by the total number of elements that actually belong to the positive class

$$\text{Recall} = \frac{TP}{TP + FN}$$

FALSE POSITIVE OR FP: It is the proportion of negative cases that were wrongly classified as positive, as calculated using the equation.

$$FP = \frac{FP}{TN + FP}$$

TRUE NEGATIVE OR TN: It defined as the proportion of negatives cases that were classified correctly, as calculated using the equation.

$$TN = \frac{TN}{TN + FP}$$

FALSE NEGATIVE OR FN: It is the dimension of positive cases that were unjustifiably classified as negative, as calculated accept the equation.

$$FN = \frac{FN}{FN + TP}$$

PRECISION: - Precision for a class is the number of true positives divided by the total number of elements labeled as belonging to the positive class Accuracy is the proportion of the total number of attacks that are correctly detected. It is decisive using the equation:

$$\text{Accuracy} = \text{Precision} = \frac{TP}{TP + FP}$$

F- MEASURE: - A measure that consolidates precision and recall is the symphonic mean of precision and recall, the traditional F-measure or balanced F-score. F- Measure that mixes precision and recall is the symphonic mean of precision and recall is known as F-measure. This is also prominent as the F1 measure, as a result of recall and precision are evenly weighted. [19]

$$F - \text{measure} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

Receiver operating characteristics (ROC) graphs are efficient for create classifiers and envision their performance. Receiver Operating Characteristic (ROC) contrariwise ROC curve, is a graphical prototype that delineate the performance of a binary classifier system as its discrimination threshold is varied. The curve is invented by plotting the true positive rate in opposition to the false positive rate at various threshold settings. Receiver Operator Characteristics (ROC) lay out the trade-off between sensitivity and singularity. ROC curves maneuver the true positive rate v/s. the false positive rate, at fluctuate threshold cut-offs. The ROC is also known as a analogous operating characteristic curve, as a result of it is a comparison of two operating characteristics (TPR and FPR) as the criterion changes.

The conclusion of naïve bayes, J48 and random forest Classifier is shown in Table 2, 3 & 4. As can be seen the

realization of Naive Bayes Classifier is below par. For U2R and R2L attack is it‟s below 41% mark. The reason for this is as a result of the expectation of Naive Bayes access that all parameters are independent. Recognition this is not invariably the case. Many security parameters are interdependent to one another. As a result Naive Bayes Classifier, though takes less memory and is rapid faster in computation is ward off because of poor results To improve beginning with Naive Bayes Classifier we have used J48 and Random Forrest classifier in WEKA. These two classifiers have shown significant enhancement in detection rate and accuracy. As can be observed in Figure 1 that average TP rate for J48 and Random Forrest classifier is above 98% which is perfectly higher as correlate to naive Bayes whose weighted average is 78.1%. Almost all the attacks have precision of exceeding 81% in J48 and Random Forrest classifier except for R2L attack. We have compared our contribution with the work with [30] and it‟s given in table 5. In [19] the authors have used C4.5 and SVM for classification. We have used Naive Bayes, J48 and Random Forrest for classification. The table IX shows the precision under various classifiers used. Though the effectiveness of detection of probing attack have been reduced, the improvement in DoS, U2R, R2L have been significant. The use of naive bayes outcome in poor results after all naive bayes assumes all parameters to be independent.

Table 2: Results of Naive Bayes Classifier

	TP-Rate	FP-Rate	Precision	Recall	F-Measure	MCC	ROC-Area	PRC-Area	Class
	0.793	0.01	0.995	0.793	0.883	0.609	0.987	0.994	dos
	0.732	0.003	0.13	0.732	0.22	0.307	0.141	0.141	a2r
	0.984	0.139	0.087	0.984	0.161	0.272	0.994	0.794	probe
	0.966	0.076	0.411	0.966	0.576	0.603	0.976	0.718	r2l
	0.674	0.005	0.97	0.674	0.796	0.775	0.977	0.925	normal
Weighted-Avg	0.782	0.014	0.948	0.0.281	0.84	0.703	0.985	0.964	

Table 3: Results of J48 Classifier

	TP-Rate	FP-Rate	Precision	Recall	MeasureMCC		ROC-Area	PRC-Area	Class
	1	0.001	1	1	1	0.999	0.999	1	dos
	0.761	0	0.857	0.761	0.806	0.934	0.934	0.773	u2r
	0.976	0	0.985	0.978	0.981	0.994	0.994	0.976	probe
	0.83	0.011	0.81	0.83	0.82	0.994	0.994	0.931	r2l
	0.947	0.011	0.953	0.947	0.95	0.997	0.997	0.991	normal
Weighted-Avg0	0.98	0.003	0.981	0.981	0.981	0.998	0.998	0.993	

Table 4: Results of Random Forrest Classifier

	TP-Rate	FP-Rate	Precision	Recall	F-Measure	MCC	Column2	ROC-Area	PRC-Area	Class
	1	0.001	1	1	1		0.999	1	1	dos
	0.915	0	0.956	0.915	0.935		0.935	986	0.951	u2r
	0.989	0	0.996	0.989	0.993		0.992	0.999	0.997	probe
	0.82	0.01	0.816	0.82	0.808		0.808	0.995	0.921	r2l
	0.95	0.012	0.952	0.95	0.939		0.939	0.999	0.993	normal
Wighted Avg	0.981	0.003	0.981	0.981	0.979		0.978	0.999	0.996	

Table 5: Comparison of Proposed Work with Previous Methods

	C4.5	SVM	Naïve Bayes	J48	Random Forrest
dos	93.88	93.84	99.56	100	100
u2r	95.38	89.09	13	85.75	95.6
probe	33.33	66.67	8	98.56	99.6
r2l	16.45	15.91	41	81	81.61

5. CONCLUSION

In this paper we are providing solution on the existing intrusion detection techniques through speedup and meticulous anomaly network intrusion detection system. In this work, the prospective method of machine learning for intrusion detection system is presented the proposed method is evaluated on KDD Cup 99 dataset and training of 66% is done. The performances of WEKA classifies are measured in terms of True Positive (TP)/Recall and Precision/Accuracy and false positives. The performance of the all method is compared with other standard machine learning techniques. The experimental results show that the implied machine learning technique hand over highest classification accuracy of 99.679 %.

REFERENCES

[1]] Lee, W., & Stolfo, S. (1998), “Data mining approaches for intrusion detection,” In Paper presented at the proceedings of the seventh USENIX security symposium (SECURITY’98). San Antonio, TX.

[2] Stewart, J. Michael. Network Security, Firewalls and VPNs. Jones & Bartlett Publishers, 2013.

[3] Mr. Suresh kashyap, Ms. Pooja Agrawal, Mr.Vikas Chandra Pandey, Mr. Suraj Prasad Keshri”Importance of Intrusion Detection System with its Different approaches” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 5, May 2013

[4] Wang, Lanjia, Zhichun Li, Yan Chen, Zhi Fu, and Xing Li. "Thwarting zero-day polymorphic worms with network-level length-based signature generation." IEEE/ACM Transactions on Networking (TON) 18, no. 1 (2010): 53-66.

[5] SSL Automated Signatures William Wilson and Jugal Kalita Department of Computer Science University of Colorado Springs ,CO 80920 USA wjwilson057@gmail.com and kalita@eas.uccs.edu

[6] Asmaa Shaker Ashoor, Prof. Sharad Gore – “Importance of Intrusion Detection System”-International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011.

[7] Paul Innella- “The Evolution of Intrusion Detection Systems“-Tetrad Digital Integrity, LLC.

[8] Wang Pu and Wang Jun-qing “Intrusion Detection System with the Data Mining Technologies” IEEE 2011.K. Elissa, “Title of paper if known,” unpublished.

[9] E. J. Derrick, R. W. Tibbs and L. L. Reynolds, "Investigating New Approaches to Data Collection, Management and Analysis for Network Intrusion Detection", ACMSE, Winston-Salem, N. Carolina, USA, **(2007)** March 23-24, pp. 283-287.

[10] Vivek Nandan Tiwari, Prof. Satyendra Rathore, Prof. Kailash Patidar "Enhanced Method for Intrusion Detection over KDD Cup 99 Dataset" International Journal of Current Trends in Engineering & Technology ISSN: 2395-3152 Volume: 02, Issue: 02 (MAR-APR, 2016).

[11] Harvinder Pal Singh Sasan and Meenakshi Sharma'' INTRUSION DETECTION USING FEATURE SELECTION AND MACHINE LEARNING ALGORITHM WITH MISUSE DETECTION'' International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 1, February 2016.

[12] V. Jaiganesh, S. Mangayarkarasi, Dr. P. Sumathi ''Intrusion Detection Systems: A Survey and Analysis of Classification Techniques'' International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2013.

[13] Priya U. Kadam, Prof.Manjusha Deshmukh "Various Approaches for Intrusion Detection System: An Overview" ISSN (Online): 2320-9801, Vol. 2, Issue 11, November 2014.

[14] B.Santos Kumar, T.Chandra Sekhara Phani Raju, M.Ratnakar, Sk.Dawood Baba, N.Sudhakar " Intrusion Detection System- Types and Prevention" International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 77 – 82.

[15] Inadyuti Dutt, Dr. Samarjeet Borah "Some Studies in Intrusion Detection using Data Mining Techniques" International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 7, July 2015.

[16] Sathish.S.N "Sathish.S.N "Using Data Mining Techniques for Intrusion Detection" International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 6, June 2015.

[17] Ms.R.S.Landge, Mr.A.P.Wadhe "Review of Various Intrusion Detection Techniques based on Data mining approach" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622

[18] Luo, L., Ye, L., Luo, M., Huang, D., Peng, H. and Yang, F"Methods of Forward Feature Selection Based on the Aggregation of Classifiers Generated by Single Attribute", Computers in Biology and Medicine, Vol. 41, No. 7, pp. 435-441, 2011.

[19]]Ektefa, Mohammadreza, Sara Memar, Fatimah Sidi, and Lilly Suriani Affendey. "Intrusion detection using data mining techniques." In Information Retrieval & Knowledge Management, (CAMP), 2010 International Conference on, pp. 200-203. IEEE, 2010.

BIOGRAPHIES

AJAY PRAKASH SAHU
Qualification-B.E (CSE)
PG Scholar Truba institute of Engineering and Information Technology.
Email-
sahuajayprakash113@gmail.com

Prof. AMIT SAXENA
Associate Professor & HoD (truba)
Qualification-B.E(CSE) ,M.TECH , PhD(MANIT) Bhopal
Publication-18 international & 05 National Paper
Email-amitsaxena78@gmail.com

Prof. KAPTAN SINGH
Qualification-B.E(CSE) ,M.TECH , PhD*(MANIT) Bhopal
Publication-01 international & 01 National Paper
Email-kaptan2007@gmail.com