Detection of intrusions using self-trained support vector machine

Danish Akhtar[#1], Narendra Parmar[*2], Gagan Sharma[#3]

Department of Computer Science & Engineering
Sri Satya Sai College of Engineering, Bhopal, India

[1]danishakhtar.010@gmail.com
[2]narendrarkdf.ac@gmail.com
[3]gagansharma.cs@gmail.com

Abstract— with the rapid increase of technology and exposure to the internet and cyberspace there is a vast increase in cyber-attacks and attempts of data theft. Almost all the private information of people is now on public domain, so it becomes very important to secure that information from fraudsters and intruders. Thus Intrusion Detection systems become very necessary to protect and safeguard our computer systems and networks from hackers and unknown attackers as they might steal the system's highly confidential and important data and misuse them for their own interest. The conventional methods of protection like the firewalls and the virtual private networks are not sufficient enough to protect the systems. So new and advanced techniques and methods are required for detection of potential threats and protecting the network from such threats and attacks. The objective of this paper is to discuss Intrusion Detection System using a data mining approach i.e. a self-trained Support Vector machine.

Keywords — ***Support Vector Machine, Intrusion Detection, IDS, Self-training SVM***

I. Introduction

Intrusion in general terms is often said to be an attack on a system or a network for any unsocial activity. In a research report from Carnegie Mellon University [1], Julia, et Al. defined an attack as "*An attach is an action taken by some un social people to get access to others' computer or network to use their information and data for the fulfilment of their needs. Their needs may be the data or the information or it may be financial needs. The attackers may ask for ransom against the data they have accessed.*

By the above definition it is quite clear that an attack by an intruder is harmful for the victim in different ways. Many a times an attack may be successful or it may not be successful depending upon different perspective. For example an attack which is not successful with respect to the intruder can be considered as a successful attack with respect to the victim. The intruder might not have gained what he was expecting but the victim has lost much of its data or information in this attack. So it is always good to follow the perspective of the victim while investing the intrusion detection for a successful result.

Thus we found that detection of intrusion becomes very vital aspect for any system or organization because the intruder can harm the integrity and safety of the system by stealing the confidential information from the system and using it for any illegal purpose of his interest and leisure.

II. Intrusion Detection System Architecture

The architecture of Intrusion detection system is as follows.

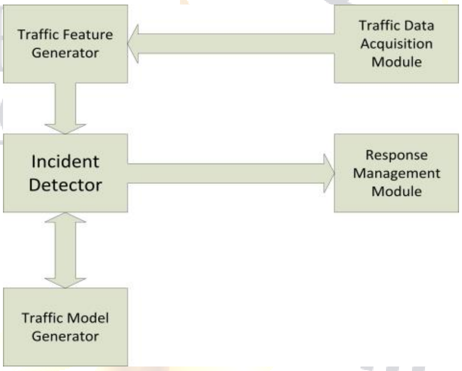
Traffic Feature Generator
Traffic Data Acquisition Module
Incident Detector
Response Management Module
Traffic Model Generator

Figure 1. Architecture of IDS

Data Acquisition: In this step we have to acquire data from several companies and organization for creating our model. Several companies are willing to provide such data for research and development purpose. Using such amount of vast data our model for detection can be created which can help in the identification of the intrusion and thus its elimination is possible.

Feature Generator: In This section the collected data is then processed and a feature generation process is carried out to obtain features of the intrusion detection system.

Incident Detector: This is very crucial component of IDS system as it detects the incident that has happened due to the attempt of the intrusion or unauthorized attempt of access to the system or the resources of the network. This component immediately helps in alarming that an unauthorized attempt is being carried out. Any attack that has taken place does have some or the other effect.

Traffic Model Generator: This component helps us to identify the amount of variation in data before and after the incident happened as a result of intrusion. This helps us to analyse the loss of data, if any happened due to the attack or the unauthorized access to the system. A model is then created for maintaining the traffic and assuring continuous sharing of the resources and data in the network.

Response Management: This phase of the architecture deals with the response of the warning that is generated by the other previous components of the model. The responses may be different with different types of warnings and alarms. Sometimes same kind of responses may be applied for different alarms just like same medication for different illness works many a times. This phase is very important because if the warnings are ignored the intruder may get the clue that this system does not have any anti intrusion policy and he may launch further attacks one after another which will be very danger for our system.

III. Classification of IDS

The Intrusion Detection Systems are primarily classified depending upon the methodology of detection.

1) Signature Based Intrusion Detection:

Signature based Detection system or the Misuse Detection system are the most common type of intrusion detection system using which if there happens any misuse of the system or the resource the incident detector detects is and starts alarming. Also if any signature is not in accordance with the signature registered in the system, an alarm is set by the incident detector.

2) Anomaly Based Intrusion Detection:

This method is based on the comparison of the different traffic profiles of different times. Anomaly is the false value that is present in the system which often creates a false impression and false scenario. So it is very important to remove any anomaly present in the system for the smooth working of the system. This detection system has a very potential mechanism of identifying any attacks.

3) Stateful Protocol Analysis Based System:

This is a method which uses the state of the system to predict or identify any intrusion or attack on the system. It continuously measures the state of the system. The state means in what position a system is. Is it idle or working or in hibernation. If a system abruptly changes its state against the predetermined timing slots, it suspects an intrusion and alarm the incident detector for further actions to be taken.

4) Hybrid:

This is a hybrid type of Intrusion detection system in which a combination of different types of IDSs is used to detect or identify any intrusion. The signature based detection, Stateful protocol or the other types of detection system are often used simultaneously thus making it a robust system of detection and prediction of intrusion.

IV. Literature Review

Chen, et al [2] and Eskin, et al [3] have discussed various used of Support Vector Machines and the Artificial Neural Network for the purpose of detection of intrusions. An IDS does not include prevention of the intrusion to happen. It only detects and reports the intrusion to the system Administrator. Various problems related to intrusion detection and reporting have been discussed by Catania, et al [4].

An intrusion detection system monitors the activities of a given system or a network or a working environment and makes a judgment whether the activities going on there are legitimate or illegitimate or suspicious or malicious based on the integrity, security, confidentiality and availability of the information resources.

A very simple and useful review of detection of intrusion has also been done by Liao, et al [5].

Information is very crucial and vital in the respect of organizations security and integrity. Information theft is considered a criminal offense. Network monitoring techniques can increase performance of networks by 5 to 20 precent compared to audit based systems. Patcha, et al [6] have discussed about the process of analysing audit trails which increases the performance degradation of the system.

V. Motivation

The motivation for this research work lies in the problem that is being faced by so many software users each and every day. The intruders are continuously attacking their systems to steal vital information and data. These days cyber security is one of the greatest challenges for the software industry. Because international cyber criminals are also very active to get access to our confidential data of the military and nuclear power plant to endanger our safety and integrity of the country.

So for maintaining a healthy programming environment it is very essential to keep the environment safe and intruder free by not allowing any intruder to launch any attack to the system. If already attacked by malware or spyware the system should be capable enough to fight with them to keep all our code safe.

VI. Problem Definition

The significant reduction of obtaining normal protocol is a new normal. Every time a new protocol is launched it becomes difficult to cope with the protocol for that system. It must be understood that when there is a change in protocol the whole system and its architecture needs to be changed. The requirement to do this is dependent on the demand of the client. The proposed methodology for this work depends upon the structure and scenario of data mining and association rule mining. Any anomaly must be detected and reported to the administrator as early as possible.

VII. PROPOSED WORK

Support Vector Machine:

The Support Vector Machines which are often also called as the SVM's are very robust and powerful tools for data mining purposes. Support Vectors are data points that are closer to the hyperplane and influence the position and orientation of the hyperplane. An SVM is a supervised machine learning methodology which uses algorithms of classification for classification problems.

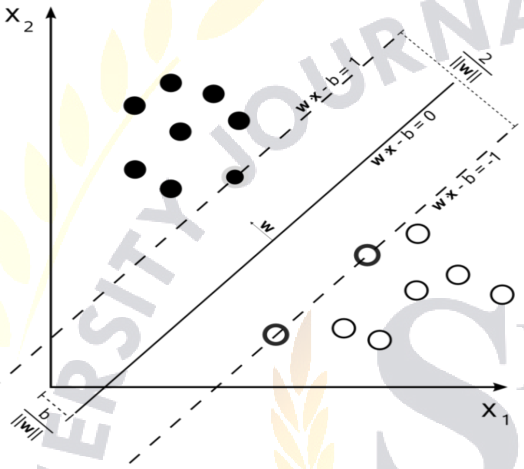

Fig. 2. Decision hyperplanes of SVM

Self-Training: A semi supervised learning technique

Conventionally there have been many machine learning methods available for data mining tasks. They function on the assumption that attacks are different form normal activity and can therefore be detected by systems that identify these differences [7].

Supervised learning uses previous experiences and results as a teacher to train the data set and arrive at the results. The key disadvantage of pattern recognition is the ineffectiveness in reducing the collaborative or extended methodologies. If attack characteristics do not match one which has been coded into the system, the intrusion may not be detected. Various methods of clustering and classification may be used for this purpose of pattern identification and recognition.

Semi-Supervised learning is blend to two different technologies. One is the supervised learning and other is the UN supervised learning used together to create Semi Supervised learning method. In this methodology the data set may be or may not be trained according to the needs. A label is often put to the trained data set which is helpful in detection of the anomalies and intrusion. This process lets the administrator understand what the exact position of the environment is whether the working environment is effected or not. The second general approach to intrusion detection is the misuse detection. If the system resources are misused by any unauthorized person an alarm is set immediately to notify the administrator. While anomaly detection typically utilized threshold monitoring to indicate when a certain established metric has been reached, misuse detection techniques frequently utilize a rule based approach.

Intrusion Detection Using Self-training SVM

An SVM which is trained by itself by learning and experiencing is known as a Self-trained SVM. The Training of SVM is being used for various purposes like recognition of Transcription start sites [8], Sensing from remote place [9] and computer interface speller system based on EEG brain [10]. Self-trained SVM is quite helpful and it is often used by various industry experts and it is highly recommended.

Algorithm

An algorithm is a set of steps to be taken to get any task done. The algorithm that is developed for our research process is also a series of steps to be executed in a sequential way. The proposed algorithm is as follows.

Input: S_1, S_t and S_0

$S_1 =$ A set of labelled training examples.
$S_t =$ Training examples with unknown labels
$S_0 =$ Convergence threshold

Output: A support vector machine i.e. trained

```
1.  Train a Support Vector machine by using $S_1$ and $S_t$
2.  P=2
3.  While true do
4.  $S_n=S_1+S_t$
5.  Now Train a different Support Vector machine with
        $S_n$ and $S_t$
6.  Evaluate objective function f(w(k);   (k)) = ½ $|w^k|^2$ +
        $C\sum^{M1+M2}{}_{j=1}$
7.  If $f(w(k)) – f(w)^{k-1} < S_0$
8.  Break
9.  Else
10. k++
11. end while
```

VIII. RESULT ANALYSIS

The results of our experiment are very impressive and outstanding in respect of their accuracy. This is achieved because of the diverse data sets that we have used which we received from various distinct sources of different nature. This is important because the result should be robust in nature so different types of input and data sets should definitely be used to arrive at the final conclusion. [11]

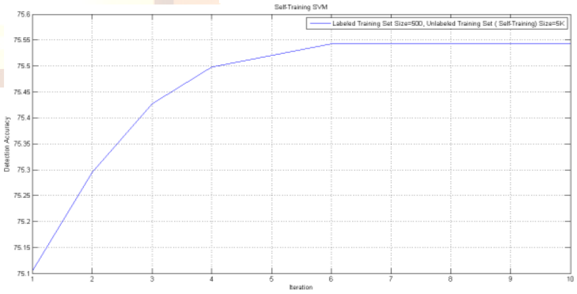

Figure 3. Intrusion detection accuracy of Support Vector Machine using Self-training of the data sets for different number of records.

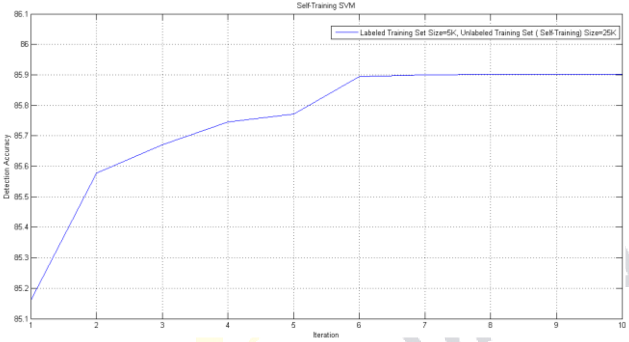

Figure 4: Intrusion detection accuracy of Support Vector Machine using Self-training of the data sets for labelled data sets.

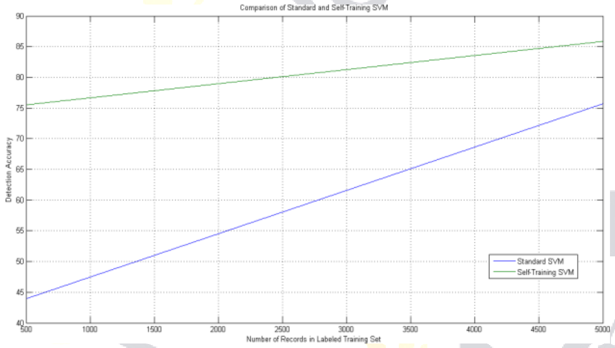

Figure 5: Comparison of Intrusion Detection Accuracy for Self-trained SVM and Standard SVM

IX. Conclusion and Future Scope

In this extensive research work we have given a new approach of intrusion detection by using the support of vector machines by giving them self-training and also applying various data mining algorithms for classification and categorization of the intrusions. The approach is found to be very effective and suitable for a moderate size of the system and quite satisfactory results have been received. The accuracy and preciseness, the efficiency and correctness of our approach is far better than the previous methods that we have studied. This method can be applied to a number of problems and situations where there is a treat of intrusion or any risk of unauthorized access to the system’s confidentiality or integrity.

The performance of this new method may also be compared to various other unsupervised and supervised learning methods and it can also be improvised for very huge number of data records and big data sets with variety, velocity and veracity. Additionally the method may also be combined or blended with other technologies and methods to create more strong methodology for intrusion detection and correction

References

[1] [1] Julia Allen, Alan Christie, William Fithen John McHugh, Jed Pickel, and Ed Stoner. State of the practice of Intrusion detection technologies. Technical report, Carnegie Mellon University, 2001.

[2] Wun-Hwa Chen, Sheng-Hsun Hsu, and Hwang-Pin Shen. Application of svm and ann for intrusion detection. Computers and Operations Research, 2005.

[3] [4] Eleazar Eskin, Andrew Arnold, Michael Prerau, Leoniod Portnoy, and Sal Stolfo. A geometric framework for unsupervised anomaly detection detecting intrusions in unlabeled data. Advances in information security, 2002.

[4] Carlos A. Catania and Carlos Garcia Garino. Automatic network intrusion detection – current techniques and open issues. Computers and Electrical Engineering, 2012.

[5] Hung-Jen Liao, Kuang-Yuan Tung, Chun-Hung Richard Lin, and Ying-Chih Lin. Intrusion detection system - a comprehensive review. Journal of Network and Computer Applications, 2013.

[6] Animesh Patcha and Jung-Min Park. An overview of anomaly detection techniques- existing solutions and latest technological trends. Computer Networks, 2007.

[7] Olivier Chapelle, Bernhard Scholkopf, and Alexander Zien, editors. Semi-Supervised Learning, chapter Introduction to Semi-Supervised Learning. MIT Press, 2006. [10] Jun Cai Huang, Feng Bi Wang, Huan Zhang Mao, and Ming Tian Zhou. A self-training semi- supervised support vector machine method for recognizing transcription start sites. Interna- tional Conference on Apperceiving Computing and Intelligence Analysis (ICACIA), 2010.

[8] Jun Cai Huang, Feng Bi Wang, Huan Zhang Mao, and Ming Tian Zhou. A self-training semi- supervised support vector machine method for recognizing transcription start sites. Interna- tional Conference on Apperceiving Computing and Intelligence Analysis (ICACIA), 2010.

[9] Ujjwal Maulik and Debasis Chakraborty. A self-trained ensemble with semisupervised svm – an application to pixel classi_cation of remote sensing imagery Pattern Recognition Letters, 2011

[10] Yuanqing Li, Cuntai Guan, Huiqi Li, and Zhengyang Chin. A self-training semi-supervised svm algorithm and its application in an eeg-based brain computer interface speller system. Pattern Recognition Letters, 2008.

[11] Yuanqing Li, Cuntai Guan, Huiqi Li, and Zhengyang Chin. A self-training semi-supervised svm algorithm and its application in an eeg-based brain computer interface speller system. Pattern Recognition Letters, 2008.