International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

Anomaly Based Intrusion Detection Using ANN and PSO

Govind Narayan[1], Anil Kumar Pandey[2], Abhishek Kumar Dewangan[3]
[1]*M.Tech Scholar GD-RCET, Bhilai, Chhattisgarh, India*
[2]*Assistant Professor GD-RCET, Bhilai, Chhattisgarh, India*

Abstract: ***Sequence mining calculations can be ordered into essentially four ways, viz, apriori-based calculation, pattern matching and pattern growth, pruning and last yet not for fear that the mix any of these. These calculations can be identifying the abnormal patterns in day by day schedules of the cloud utilizes with great level of precision. According to current status of the condition of craftsmanship around there, it was discovered that blend of pattern growth with most recent factor are most appropriate for distinguishing proof of insider attack in cloud. According to current work we have discovered that combination of pattern growth with most recent factor are most appropriate for ID of insider attack in cloud. This is obvious from the outcomes from the arrangement of investigations. This execution fundamentally helped in building an ideally estimated information structure portrayals of the arrangement database that requires the need of recent parameters joining in attack recognition calculations. It was discovered that our proposed calculation is better as far as memory use and exactness in finding the abnormal arrangements for identifying the attacks.***

Keywords: Intrusion Detection Systems, Data Mining, Clustering, Security, Anomaly based Intrusion Detection System.

I. INTRODUCTION

Intrusion Detection System needs to process expansive measure of information in one go. Over the long haul the accomplishes require larger amounts of accessibility and adaptability of handling capacities. Such outline decisions commonly show a tradeoff in which information freshness is yielded for decreased access latencies. There are numerous conceivable methodologies for productively taking care of the recourses so that to strike a fine harmony between both the nature of administration (QoS) and nature of information (QoD) [1] to be utilized for examination in distinguishing noxious exercises in cloud biological community. The cloud systems [2] information stream originate from time shifting procedures happening at various cloud end focuses , it isn't sufficient to ensure value of the information for finding noxious exercises with blend of old and new information ; we likewise should guarantee every exchange under perception is crisp, so continuous reaction chain can be manufacture. Casually, information freshness suggests that the information is later, and it guarantees that no foe replayed old messages.

An intrusion detection framework is utilized to recognize a wide range of malicious network traffic and PC use that can't be identified by an ordinary firewall. An intrusion detection framework is a gadget normally an assigned PC framework that persistently screens movement to distinguish vindictive cautions. A solitary intrusion in a network can be the reason of data spillage and can perform data adjustments that are exceptionally hurtful to an association [9].

II. INTRUSION DETECTION SYSTEM (IDS)

Intrusion detection is characterized as the way toward observing the occasions happening in a PC framework or network and examining them for indications of intrusions, characterized as endeavors to bargain the secrecy, trustworthiness accessibility or to bypass the security instrument of PC or network [10]. The fundamental segments of IDS are appeared in Fig.1.

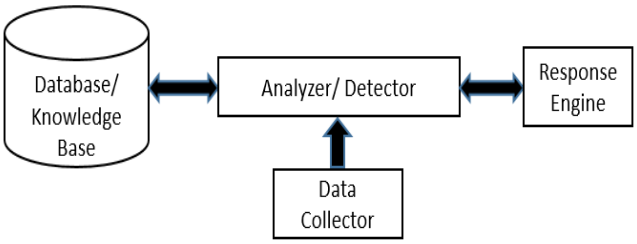

Fig. 1. IDS with its Components

III. COMPONENTS OF IDS

A. Data Collection/Preprocessor

Data collection segment is in charge of gathering and giving the review data that will be utilized by next part to decide. Data utilized for identifying intrusion ranges from user get to example to network parcel level highlights [10].

B. Analyzer (Intrusion Detector)

The analyzer or the intrusion detector is the center part which examines the review examples to identify attacks. This is a basic part and a standout amongst the most looked into. Different procedures are utilized as intrusion indicators [8]

C. System profile (database or Knowledge Base)

The framework profile is utilized to describe the typical and anomalous behavior. It is the knowledge base for attacks, setup data about the present condition of the framework and review data portraying the occasions that are going on the framework.

D. Response Engine

The response engine controls the response component and decides how to react. The framework may raise an alert and answer to overseer or may block the source of attack [7].

IV. LITERATURE SURVEY

In this segment, we survey the existing literature on IDS frameworks.

M. E. L. Ajjouri et al. [1], the advancement of data frameworks requires the usage of an abnormal state of security to limit the issues related with these frameworks. Intrusion Detection Systems (IDS) plays a critical part in the security of systems by identifying when an attack is going on, yet most current IDS are by and large brought together and experience the ill effects of noteworthy constraints.

L. M. L. de Campos et al. [2], the point of this examination is to simulate a system movement analyzer that is a piece of an Intrusion Detection System - IDS, the primary concentration of research is information digging and for this sort of use the means that go before the information mining : information arrangement (conceivably including cleaning information, information transformations, choosing subsets of records, information standardization) are viewed as major for a decent execution of the classifiers amid the information mining stage. In this specific circumstance, this paper talks about and exhibits as a commitment not just the classifiers that were utilized as a part of the issue of intrusion location, yet in addition the underlying phase of information planning.

S. Dhivya et al. [3], in the present web-empowered world, the interchanges occurring over the system is strengthening at a vast rate. Not all interchanges are valid and malpractice can emerge anywhere, anytime. In the event that the ordinary movement is marginally changed to misdirect the intrusion location framework, at that point the customary frameworks won't not have the capacity to perceive the same successfully. Hence, a framework that could recognize and uncover the novel attacks has been proposed. Since any number of clients can utilize a page, keeping up the accessibility of the resources and dispensing them to the dynamic clients according to their need is exceptionally fundamental.

Y. Gao et al. [4], in this paper, the authors have proposed a two-tier design to identify intrusions on network level. System conduct can be delegated abuse identification and abnormality recognition. According to their investigation they considered information packets of TCP/IP as their information. After, pre-handling the information by parameter filtering, they assemble a self-ruling model on preparing set utilizing various leveled agglomerative clustering. Further, information gets delegated customary activity example or intrusions utilizing KNN classification. This decreases cost overheads.

I. Lee et al. [5], in this paper, authors have proposed a novel string looking algorithm and an Intrusion Detection System utilizing this algorithm. What's more, they have investigated few correct example searching algorithms and their similar examination as our background study. A dataset of five thousand records (a subset of KDD Cup dataset) with forty-one highlights is taken for assessing the adequacy of the proposed IDS. The comparing worldwide nucleotide arrangements of the considerable number of highlights of the dataset helped us to execute our IDS.

C. Science et al. [6], in this paper, authors have proposed a framework that could identify and uncover the novel attacks. Since any number of clients can utilize a page, keeping up the accessibility of the resources and designating them to the dynamic clients according to their need is extremely fundamental. The multithread idea is utilized to share the resources that every customer can utilize. Quality Selection Algorithm is utilized as the element extraction algorithm in weka, to yield those significant features pertaining to the client's demand and aides in accomplishing a more accurate result. Memory productivity is gotten by the falling paired inquiry tree.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

V. METHODOLOGY

In this section we present the proposed system architecture. Fig. 1. Shows the workflow.

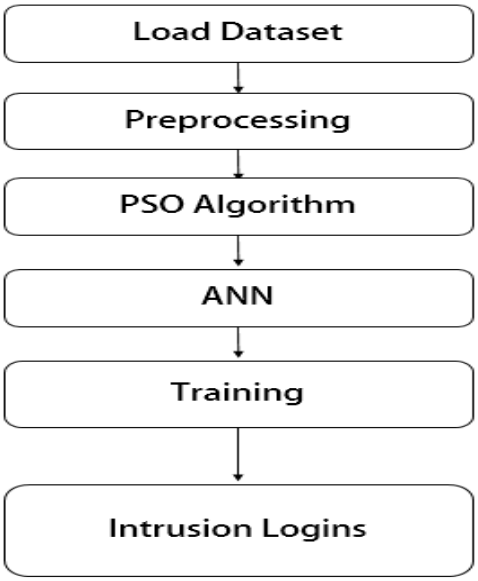

Fig. 1. Proposed System Architecture

The proposed method is described below
The dataset are loaded and prepared for processing.
The irrelevant information are filtered in pre-processing step.
PSO and Artificial Neural Network Algorithm are applied to the network related datasets.
The intrusion or unauthorized persons are detected.

A. Load Dataset

KDD dataset are used for analysis. The dataset is divided into 2 parts. First, the training set and another is test set. Training set is larger than test set.

B. Preprocessing

In this phase, the dataset are processed and remove the irrelevant features.

C. PSO and ANN Algorithm

PSO is used for initializing the weights and ANN is used for training the datasets. The algorithm is presented below:

```
{    PROPAGATE FORWARDS                                    }
 for i := 1 to num_hidden do
  begin
   hidden_net[i] := 0;{clear net for hidden unit}
   for j := 1 to num_input do  {sum inputs to hidden unit}
    begin
     hidden_net[i] := hidden_net[i] +
     (input_act[j]*input_to_hidden_wt[j,i]);
    end;
   hidden_act[i] := 1/(1 + exp(-1 * hidden_net[i]));
   {apply transfer function to get activation of hidden unit}
  end;
```

Fig. 2. Back propagation Algorithm

VI. RESULT

KDD dataset are used for analysis. The dataset is divided into 2 parts. First, the training set and another is test set. Training set is larger than test set. The test dataset are used which are unseen to the classifier.

We performed experiments with ANN classification algorithm. The input consists of sequence of logins of users as shown in fig. 3.

```
0,tcp,ftp_data,SF,491,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,2,2,0.00,0.00,0.00,0.00,1.00,0.00,0.00,150,25,0.
17,0.03,0.17,0.00,0.00,0.00,0.05,0.00,normal
0,udp,other,SF,146,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,13,1,0.00,0.00,0.00,0.00,0.08,0.15,0.00,255,1,0.00,
0.60,0.88,0.00,0.00,0.00,0.00,0.00,normal
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,123,6,1.00,1.00,0.00,0.00,0.05,0.07,0.00,255,26,0.1
0,0.05,0.00,0.00,1.00,1.00,0.00,0.00,anomaly
```

Fig. 3. Input KDD Dataset

After classification, the results are presented in fig. 4.

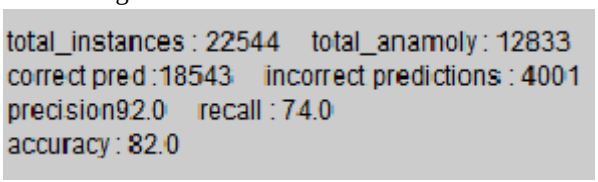

Fig. 4. Output of Backpropagation Network

VII. CONCLUSION

We have performed experiment using ANN and PSO. The combination of both algorithm performs well with the KDD dataset. The experimental results shows that the output of classifier is 82% with 92% precision.

The KDD dataset consists of 22544 instances out of which 12833 are detected as anomaly. The result shows that huge number of anomaly detected.

REFERENCES

[1] M. E. L. Ajjouri, “New Model of Intrusion Detection Based On Multi Agent Systems and CBR Paradigm,” pp. 133–138, 2016.
[2] L. M. L. de Campos, R. C. L. de Oliveira, and M. Roisenberg, “Network Intrusion Detection System Using Data Mining,” vol. 311, pp. 104–113, 2012.
[3] S. Dhivya, D. Dhakchianandan, A. Gowtham, P. K. Sujatha, and A. Kannan, “Memory efficacious pattern matching intrusion detection system,” 2013 Int. Conf. Recent Trends Inf. Technol. ICRTIT 2013, pp. 652–656, 2013
[4] Y. Gao, J. Z. Huang, D. Gu, and H. Rong, “Learning Classifier System Ensemble for Data Mining,” Gecco’05, pp. 63–66, 2005
[5] Sung-Il Oh, Inbok Lee and Min Sik Kim, "Fast filtering for intrusion detection systems with the shift-or algorithm," 2012 18th Asia-Pacific Conference on Communications (APCC), Jeju Island, 2012 IEEE, pp. 869-870
[6] Divyatmika and M. Sreekesh, "A two-tier network based intrusion detection system architecture using machine learning approach," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016 IEEE, pp. 42-47
[7] N. Sharma and S. Mukherjee, “Layered approach for intrusion detection using naïve Bayes classifier,” Proc. Int. Conf. Adv. Comput. Commun. Informatics – ICACCI ’12, p. 639, 2012.
[8] N. Sheikh, K. Mustafi and I. Mukhopadhyay, "A unique approach to design an intrusion detection system using an innovative string searching algorithm and DNA sequence," 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, 2016, pp. 1-9.
[9] Z. Yanbin, “Network Intrusion Detection System Model Based On Artificial Immune,” vol. 9, no. 9, pp. 359–370, 2015.
[10] T. Zou, Y. Cui, M. Huang, and C. Zhang, “Improving performance of intrusion detection system by applying a new machine learning strategy,” Proc. 5th Int. Conf. Soft.