International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 556 – 558

A Review of Intrusion Detection System

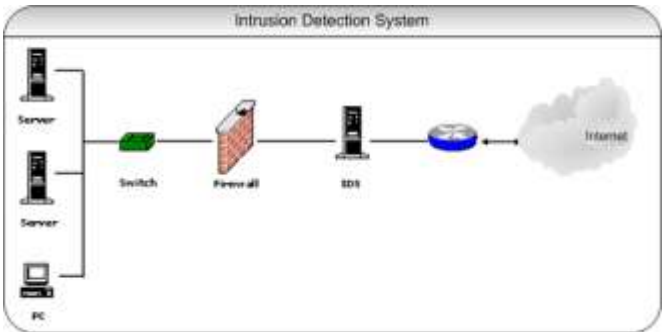
Mr. Utpal Shrivastava
Department of Computer Science Engineering, Amity University, Gurgaon ,Haryana, India
Email: ushrivastava@ggn.amity.edu, utpalshrivastava@gmail.com

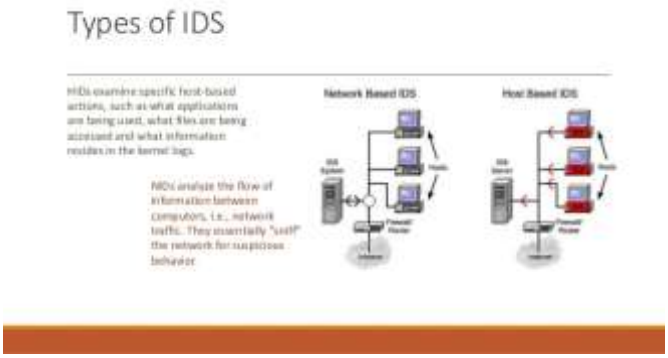
***Abstract*:** Intrusion detection systems are systems that can detect any kind of malicious attacks, corrupted data or any kind of intrusion that can pose threat to our systems. In this paper a study of various types of intrusion detection system is done along with the aid of many research papers which have employed machine learning , DNA sequence ,pattern matching ,data mining as a technique for learning attacks and taking preventive actions when similar types of attacks are encountered in the future. Study of these papers have given a deep insight to further explore the related techniques in the field of Intrusion Detection Systems.

*****

I. INTRODUCTION

An **intrusion detection system** (**IDS**) is a device or software application that monitors a network or systems for malicious activity or policy violations. The most common classifications are **network intrusion detection systems** (**NIDS**) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an **intrusion prevention system**. [WikiPedia and https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799





II. RELATED WORK

A Two-tier Network based Intrusion Detection System Architecture using Machine Learning Approach[4]

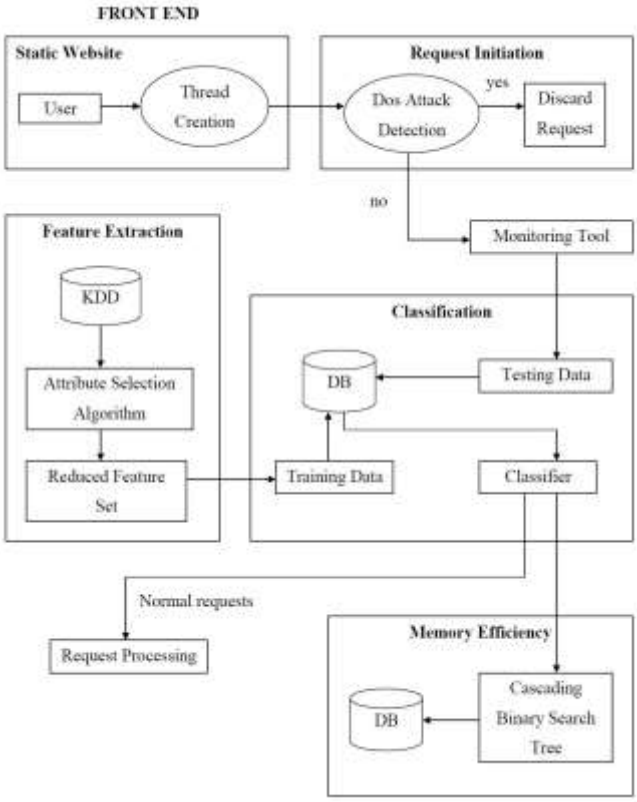
In this paper the authors have proposed a two-tier architecture to detect intrusions on network level. Network behavior can be classified as misuse detection and anomaly detection. As per their analysis they considered data packets of TCP/IP as their input data. After, pre-processing the data by parameter filtering, they build a autonomous model on training set using hierarchical agglomerative clustering. Further, data gets classified as regular traffic pattern or intrusions using KNN classification. This reduces cost-overheads. Misuse detection is conducted using MLP algorithm. Anomaly detection is conducted usingReinforcement algorithm where network agents learn from the environment and take decisions accordingly. The TP rate of our architecture is 0.99 and false positive rate is 0.01. Thus, our architecture provides a high level of security by providing high TP and low false positive rate. And, it also analyzes the usual network patterns and learns incrementally (to build autonomous system) to separate normal data and threats.

A Unique Approach to Design an Intrusion DetectionSystem using an Innovative String SearchingAlgorithm and DNA Sequence [5]

In this paper authors have proposed a novel string searching algorithmand an Intrusion Detection System using this algorithm. Inaddition, they have explored few exact-pattern searchingalgorithms and their comparative analysis as our backgroundstudy. A dataset of five thousands records (a subset from KDDCup dataset) with forty one features is taken for evaluating theefficacy of the proposed IDS. The corresponding globalnucleotide sequences of all the features of the dataset helped us toimplement our IDS.In this paper thye have proposed an innovative stringmatching algorithm which helped us to design an IDS. For thispurpose they have used DNA encoding methodology where all
the features of each record is being translated into nucleotidesequence.

Memory Efficacious Pattern Matching Intrusion Detection System [6]

In this paper authors have proposed a system that could detect and ferret out the novel attacks. Since any number of users can use a web page,maintaining the availability of the resources and allocating themto the active users as per their need is very essential. The multithreadconcept is used to share the resources that each client canuse. Attribute Selection Algorithm is used as the featureextraction algorithm in weka, to yield those relevant featurespertaining to the user's request and helps in achieving a moreaccurate result. Memory efficiency is brought in with the cascading binary search tree. The patterns are efficiently storedand hence the search for the presence of an attack isaccomplished effectively. An Intrusion Detection System which ismemory efficient and effective enough in detecting attacks andreducing the false positives is thus proposed.



Network Intrusion Detection System Model Based onData Mining [7]

In this paper the authors have proposed a network intrusiondetection model based on data mining technology, which candetect known intrusion effectively and has a good capacity torecognize unknown data schema which can't be detectedeffectively in traditional IDS. The paper mainly does the followingwork: by analyzing the intrusion deeply, extract the propertieswhich can reflect intrusion characteristics effectively; combinemisuse detection, anomaly detection and human intervention,establish rule library based on C.45 decision tree algorithm anduse the optimal pattern matching so as to improve detection rate;the hosts are clustered to be IP group based on visit number by k means clustering algorithm, the audit data are divided into partsunder the IP group's direction, and the classifiers are built up bydivided audit data respectively, then the detected Data applydifferent rules according to their own IP group, thereby reducefalse positives. The experiments proved that the method iseffective to detect intrusion such as scanning and Deny of Service.

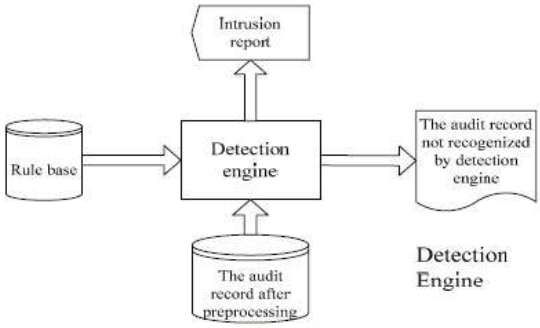


Fig. 6. Detection engine structure

Network Intrusion Detection SystemUsing various data mining techniques[8]

A Network Intrusion Detection System (NIDS)is a software application that monitors the network orsystem activities for malicious activities andunauthorized access to devices. The goal of designingNIDS is to protect the data's confidentiality andintegrity. Authors project focuses on these issues with thehelp of Data Mining. The research paper includes theimplementation of different data mining algorithmsincluding Linear regression and K-Means Clustering toautomatically generate the rules for classify networkactivities. A comparative analysis of these techniques todetect intrusions has also been made. To learn thepatterns of the attacks, NSL-KDD dataset has beenused.

Improving Performance of Intrusion Detection System byApplying a NewMachine Learning Strategy[9]

The most acute problem for misuse detection method is itsinability to detect new kinds of attacks. A better detection method,which uses a new learning strategy, is proposed to solve thisproblem. A Concept Hierarchy Generation for attack Labels(CHGL) applying relevant feature subset codes clustering, makescommon machine learning algorithms learn attack profiles onhigh concept levels. And that will enable the system detect moreattack instances. Experimental results show the advantage of thisnew method. To detect more attack instances including those belonging to newattack types with the help of a data-oriented classification, whichoutputs a concept hierarchy. Experimental results have shown theimprovement of the system performance. Another advantage ofthis method is that attack types are automatically classified bycomputer, not by human.

Fast Filtering for Intrusion Detection Systems withthe Shift-Or Algorithm[10]
Intrusion Detection Systems (IDS) play an importantrole in network security. The main challenge is how to findoccurrences of patterns defined in the rule set which describethe signature of malicious activities. In this paper, authors proposedan efficient exact pattern matching algorithm based on the bit parallel approach. Experimental results show that our algorithm outperforms the traditional Aho-Corasick automaton at the costof a small number of false positives.They showed a bit-parallel filtering algorithm for IDS. It runsfaster than the traditional Aho-Corasick automata. Althoughit yields a small number of false positive answers, it can betolerated as we do regular expression matching afterwards.

III. CONCLUSION

The growing threat of intrusion detection is crippling the networking community and various organization. The paper has discussed and analyzed some of the best techniques as proposed by the various researchers in this field. This study has really helped in proposing in my own research work and come out with something unique.

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] I. Lee, "Fast Filtering for Intrusion Detection Systems with the Shift-Or Algorithm," pp. 869–870, 2012.

[6] C. Science and K. Mangalore, "A Two-tier Network based Intrusion Detection System Architecture using Machine Learning Approach," pp. 42–47, 2016.

[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.

[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 Comput. as Transdiscipl. Sci. Technol. - CSTST '08*, p. 51, 2008.