Sindh Univ. Res. Jour. (Sci. Ser.) Vol. 51 (2) 259-270 (2019)

http://doi.org/10.26692/sujo/2019.6.43

SINDHUNIVERSITY RESEARCH JOURNAL (SCIENCESERIES)

Intrusion Detection: Tools, Techniques and Trends

H. NASIR, MAHAWISH*, S. S. ZIA**, M. NASEEM**, I. MALA***

Department of Computer Science, NED University of Engineering & Technology, Karachi

Received 15th December 2018 and Revised 16th April 2019

Abstract: With rapid growth of internet applications and communication technologies, more users/devices are entering into the network. The security of these devices and networks is a major concern. An intrusion detection system is a software or hardware tool, which monitors the packet for malicious activity. Various tools and techniques are used for Intrusion detection. This paper presents classification of different IDS, the efforts has been made to put forward a review and comparison of Intrusion detection tools and techniques that are in use today, then bibliometric analysis is performed to locate the trends of IDS tools in the research community in the end a generic framework for developing a hybrid network intrusion detection system is proposed.

Keywords: Intrusion Detection System, Bibliometric Analysis, Machine Learning.

1. INTRODUCTION

The preliminary concept of securing data by monitoring malicious user activities was first coined by Jim Anderson in 1980. The idea is to protect the system from information leakage by internal or external unauthorized access, privilege escalation and exploiting other vulnerabilities (Ashara, *et al.,* 2012). This was the basis of development of Host Intrusion Detection Systems (HIDS). Since then the intrusion detection became the popular topic of research. As increasing number of organizations and users are connected to internet, research has been made to devise sophisticated algorithms and techniques to make intrusion detection more powerful and robust to fulfill industrial demands. The paper is structured as follows. Section II presents a brief review of intrusion detection and its classification. Various intrusion detection tools are discussed in section III. Section IV gives brief about various intrusion detection models and its comparison. Bibliometric analysis and trends of Intrusion detection tools are discussed in Section V. Section VIpresents a generic framework for developing a hybrid network intrusion detection system. Last section contains general conclusions and future work.

Section -II

2.1 Intrusion Detection Systems An intrusion detection system (IDS) is a software or hardware tool whose major task is to detect malicious activities & behaviors of users and systems as well as violation of security policies in a host or network (Ashara, *et al.,* 2012). (Aleksandar, and Marco 2015). This violation is usually reported in the form of alerts, to a security administrator directly or through a central management software know as security information and event management (SIEM) system (Kai-Oliver (2015). Typical activities of intrusion detection systems are:

- Detection of Intrusion
- Alerting &Reporting
- Logging
- Recognizing a security policy violation
- Identifying a network security problem

A typical intrusion detection system is like a CCTV camera installed at home or office building, it only reports about any malicious activity such as an unknown person is coming inside. It does not stop that person to come inside. However an advance version of intrusion detection is active in nature. It is like a security personnel, it not only monitors but also stops unknown person from coming inside. This type of active intrusion detection system is known as intrusion prevention systems (Akash 2016).

++ Corresponding Author: Saood_zia@hotmail.com

*Department of Software Engineering, Bahria University (Karachi Campus) Karachi

**Department of Software Engineering, Sir Syed University of Engineering & Technology, Karachi

***Department of Electrical Engineering, Usman Institute of Technology, Karachi Imala@uit.edu

2.2 Classification Of Intrusion Detection Systems

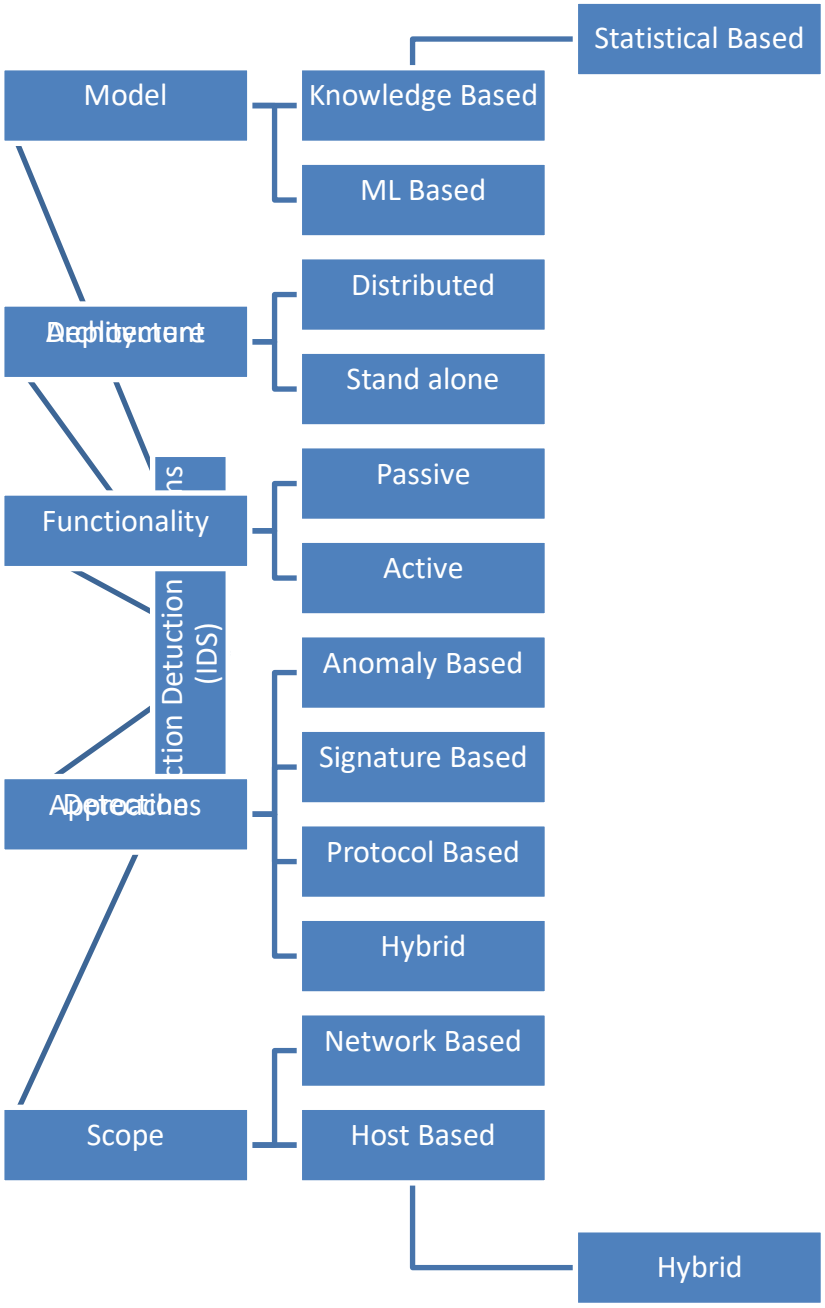


Fig. 1: Classification of Intrusion Detection System

The **(Fig. 1)** shows a typical classification of IDS with respect to different perspectives. The intrusion detection systems can be classified according to their scope i.e. Network Based (NIDS), Host Based (HIDS) or combination of both (Hybrid) IDS or by detection approaches like Anomaly based, misuse/rule/signature based (Aumreesh and Saxena, 2017), protocol based and application protocol based. It can also be classified based on its functionality that weather it only generates alert upon detection of any malicious activity (Passive IDS) or it blocks or performs remedial actions after detection (Active IDS). Deployment architecture

(Distributed or Standalone) is also a criteria to classify IDS (Aleksandar, and Marco 2015).

Network Based Intrusion Detection System (NIDS)

A Network based intrusion detection system captures packet from a network segment looking for attack patterns. It can identify a vast variety of attacks such as DOS, DDOS attacks if a huge set of related packet stream of specific pattern is found, it can also spot unauthorized share access or a port scan. A NIDS is installed at a specific place, as shown in figure, in a network segment where it can have a glance over all ongoing traffic. Bro, Snort and Suricata are the examples of NIDS (Dhanashri and. Bhosale, 2015).(Muhammad and.. Asif, 2013).

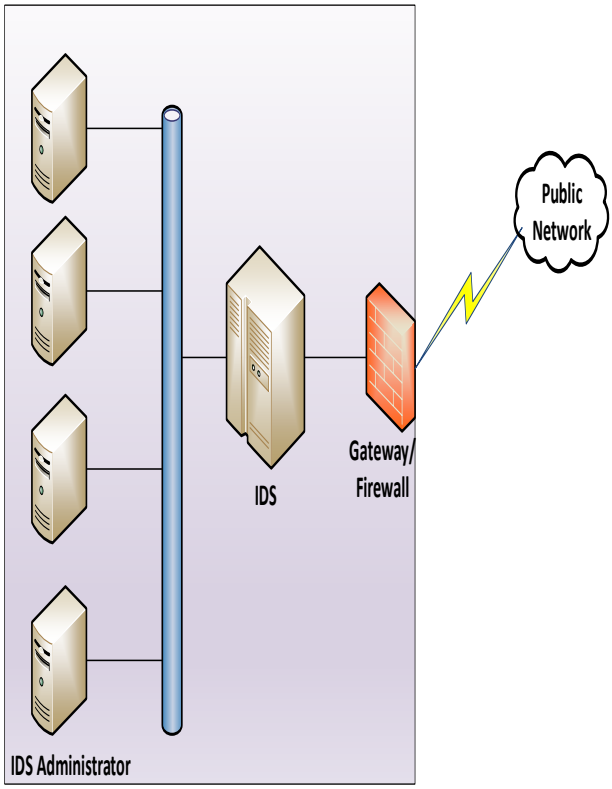


Fig. 2: Network Based IDS (NIDS)

2.3 Host Based Intrusion Detection System (HIDS)

The scope of the HIDS is limited to particular host or server where it resides and looks for unauthorized operating system level changes such as creation, modification or deletion of system files and generates an alert for IDS administrator of SIEM.OSSEC, Sagan and Splunk are the examples of HIDS

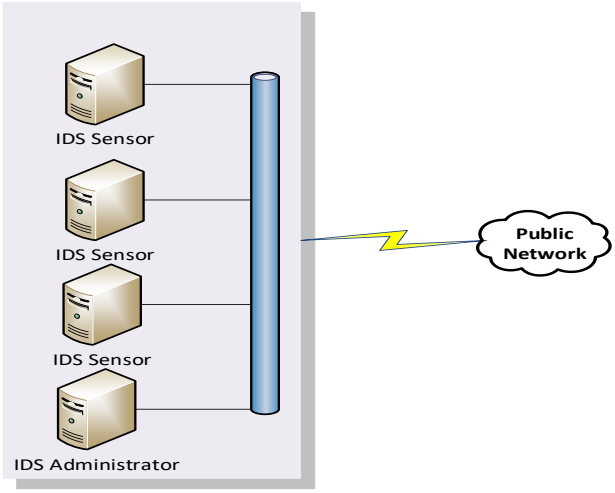


Fig. 3: A Typical Host Based Intrusion Detection System Scenario

2.4 Hybrid IDS

A Hybrid Intrusion detection system contains the features of both Network based and Host based Intrusion detection systems. The model presented in (Akash 2016). is the example of Hybrid IDS.(Prachi *et al.*, 2014).

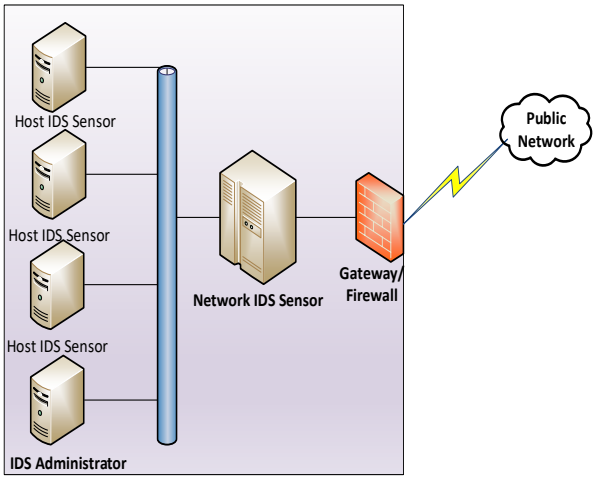


Fig4: A Typical Hybrid Intrusion Detection Scenario

2.5 Anomaly Based Detection Technique

Anomaly based detection technique is a methodology to detect Host and network malicious activities that falls out of normal system operation based on some rules, such as baseline profile of a system of network, rather than signatures. The advantages of this type of detection includes (but not limited to) detection of zero day attacks and the ability to spot privilege escalation of the user (Rafath 2017).(Mohdand. Raffie 2016).

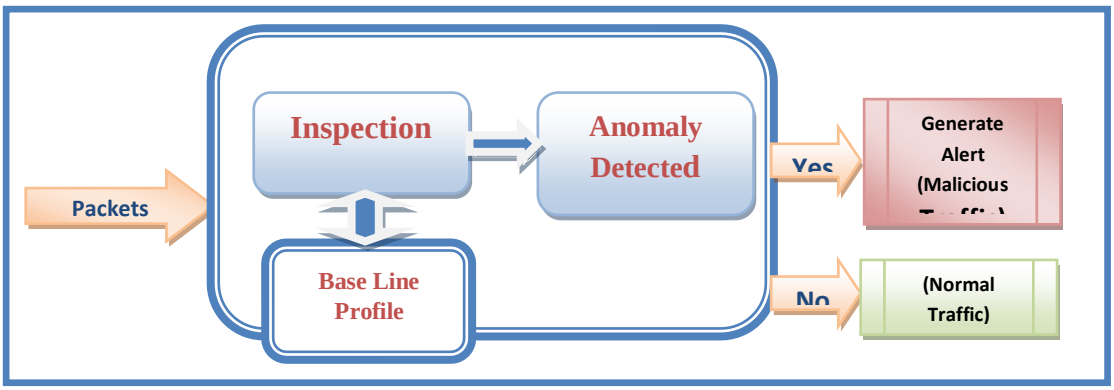


Fig. 5: Anomaly based IDS

2.6 Signature Based

Signature based detection technique also known as misuse based detection is a methodology to detect Host and network malicious activities based on known malicious patterns or sequence. It maintains the pattern database for known attacks like an antivirus software.

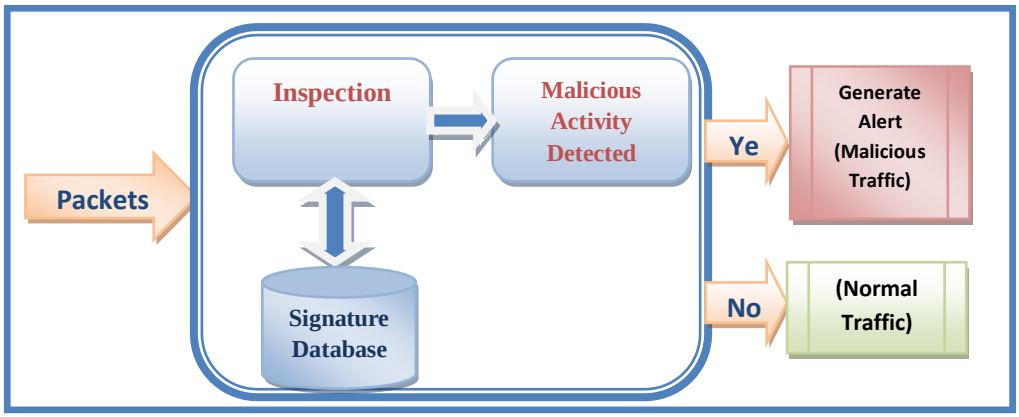


Fig.6: Signature Based IDS

The main advantage is that detection of known attack is very fast, on the other hand the main disadvantage is it is unable to identify novel (zero day) attacks (Abdullah and. Almutairi,2017). .

2.7 Hybrid Detection Technique

Hybrid detection technique combines both the anomaly and signature based methodologies. The idea is to first detect malicious activities of known patterns maintain in a database then look for unknown malicious patterns, this will significantly increase the detection percentage. The advantage is that it can detect known, unknown as well as novel zero day attacks but the computational cost of detection will increase(Patel, 2013). are the examples of hybrid detection techniques.

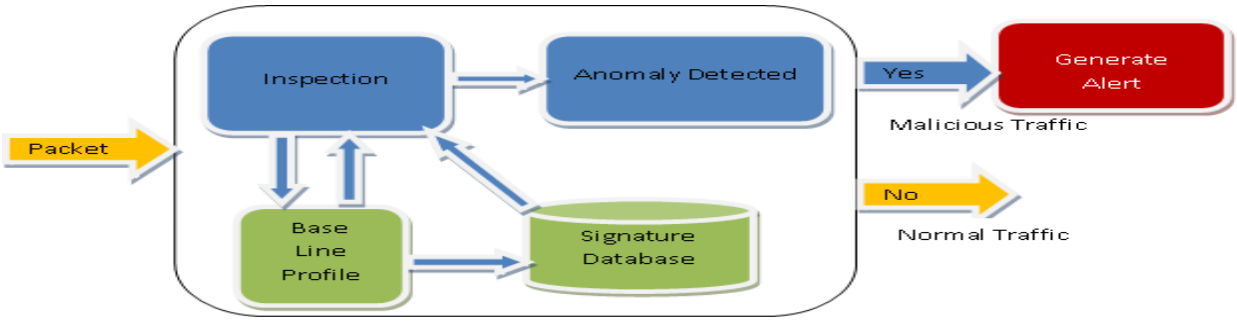


Fig. 7: Hybrid IDS

2.8 Protocol Based

Protocol based Intrusion detection technique is a methodology to monitor protocols used by a system by conducting the state and dynamic behaviour analysis and enforce the legal use of protocol. This is done by an IDS sensor node which typically resides in the server and monitors the communication between internal & external devices .The Protocol based IDS can be configured to identify acceptable behaviour of the protocol and therefore can easily detect malicious behavior (Akash 2016).

.

2.9 Passive Intrusion Detection System

Passive intrusion detection systems only have an alert generating mechanism and required IDS administrator to take decisions to either allow or block malicious host/traffic manually. It can only generateanalert or log alerts in a file upon identification of an anomaly (Aumreeshand Saxena, 2017). (Roshan 2018).

2.10 Active Intrusion Detection System

Active intrusion detection systems can be configured to protect the host or network by applying policy measures such as blocking malicious host/traffic or shutting down the suspicious network interface. Active IDS is also known as Intrusion prevention system (IPS). (Rifqi and Pratama, 2018). (http//www.snort.org. (Visited page on Jan 2019).(Hui Li, 2010) are the example of an IPS.

2.11 Single Mode/Non-Distributed Intrusion Detection System

Non distributed IDS are deployed separately in standalone mode and all the devices/applications does not communicate with each other. These IDS can only detect intrusions in a single host or network segment.

2.12 Distributed Intrusion Detection System

A distributed Intrusion Detection System comprises of multiple instances (Sensors) of co operative IDS which are configured and controlled by a centralized IDS server. The IDS server administrating team has a broader view of inbound and host generated traffic which helps to analyze internal/external malicious behaviors, patterns, attacks and overall network operations of multiple network segments spread over distinct geographical locations (Akash 2016). (Yaping 2017)

2.13 Statistical Based Intrusion Detection Model

In statistical-based Intrusion detection systems, the stochastic behavior based profile from the network activity is created. The metrics such as the traffic rate, total packets for every protocol, the connection's rate, the total quantity of IP addresses, are used in building a profile. In this type of models prior knowledge of normal network traffic activity is not required. Examples of statistical models are uni/multi-variate models and time series models
(https://suricata-ids.org).

2.14 Knowledge based Intrusion Detection Model

The knowledge based model also known as expert system framework is one of the most widely used IDS schemes. These expert systems are used to classify the data with respect to some preset rules. It consists of three major steps, first identification of various attributes and classed from training data. Then a set of rules to classify an intrusion, different attributes and classes are identified from the training data. Second, a set of classification rules are made, thirdly, the classification of data auditing is made. Examples of Knowledge based models are Bayesian Networks and finite state machines
(https://suricata-ids.org).

2.15 Machine Learning Based Intrusion Detection Model

The Machine learning based models are based on categorization of analyzed patterns. A singular characteristic of this type of models is the requirement of labeled training data set for behavioral modeling. Examples of machine learning based models are neural networks, Bayesian and decision tree classification (https://suricata-ids.org).(Hebatallah and Anwer2018).

Section -III

3. INTRUSION DETECTION TOOLS

This section describes various intrusion detection tools available in the market. A comparison based on their functionalities is also discussed.

3.1 SNORT

SNORT is an open source network based IDS/IPS system designed by Martin Rosesch in late 90's. It is a light weight, high speed system with cross-platform support and uses protocol & Signature based detection methodologies. SNORT contains signature database which consists of definition of thousands of exploits, worms, network scans and other network vulnerabilities which can identify malicious activities and attacks with high speed (Rifqi and Pratama, 2018). (Mohd and Raffie 2016).

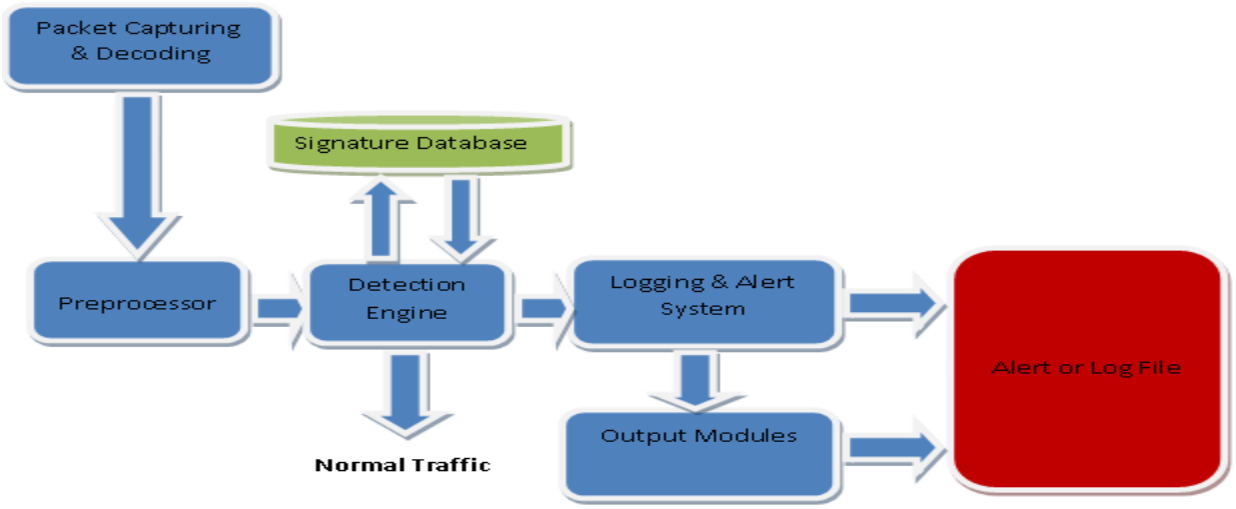


Fig. 8: Functions of SNORT

Typical functions of the SNORT is illustrated in **(Fig. 8),** it captures packets from networks segment and send it to preprocessor which performs decoding defragmentation of data stream. Then the packet is forwarded to the detection engine which matches the stream with the definitions stored in the database if a match is found the logging and alerting system sends it to output module to either log it in a file or generates alert for the IDS administrator.

3.2 OSSEC (Open Source Security)

Open source security or OSSEC is a hybrid open-source HIDS which uses both misuse based and profile based anomaly detection methodologies. It is capable of doing operating system's log analysis, integrity checking, monitoring of Windows registry, detection of root kit, active response and time-based alerting. It support various operating systems, like windows, Linux, BSD, Solaris, and OS X. OSSEC allow multi-systems monitoring because of its centralized and cross-platform architecture. The IDS log analysis engine is capable of correlating and log analysis from multiple hosts (Yaping, 2017)

3.3 BRO

Bro, now zeek, is most commonly used open source network traffic analysis and classification engine which uses behavioral analysis to detect a network anomaly. Bro enables network administrators to perform incident response, forensic analysis, file extraction, and hashing. It is an advance tool that captures metadata about network activities then provide an interpreter for understanding the activity (Kai, 2012). (Xiaohong Qu, 2009).

Suricata

Suricata is also an open source, network intrusion detection and prevention system. It has extensive rule-set, signature language and Lua script support of identification of complex threats. Suricata can easily interact with SIEM solutions lie Kibana, Splunk etc. Suricata is a community based development which focuses on security, usability and efficiency (httpswww.ossec.net).

3.4 Sagan

Sagan is a cross platform, open source Intrusion detection system written in C language. It uses a multi threaded architecture for event and log monitoring which allows the use of all cores of the processor. Sagan rules are compatible with other IDSs like Snort and suricata. Sagan can work with various SEIM solution like Sguil, Snorby, BASE and Prelude IDS. Sharing of data between various processes is done with intra process communication. It also use Redis to share data between various sagan instances in a network segment (httpswww.ossec.net).

3.5 IDS Tools Comparison

The **(Table 1)** shows comparison between different IDS tools based on different classification discussed in previous sections:

Table 1: Comparison of IDS Tools

Tools	Supported Platforms	Detection Approaches	Scope	Deployment Type
Bro	Linux/Mac OS	Anomaly based	NIDS	Both
Snort	Windows/Linux	Signature based	NIDS	Non distributed
Suricata	Cross Platform	Signature based	NIDS	Non distributed
Sagan	Linux	Signature based	HIDS	Non distributed
OSSEC	Windows/Linux	Anomaly based	HIDS	Distributed

Section-IV

4. RELATED WORK

In the year 2000 a group named Intrusion Detection Working Group within IEEE defines the generic architecture of intrusion detection system, since then various frameworks and models are being proposed. In (Made 2017). developed a model using multi-layer perceptron and back propagation learning for detecting shell code patterns within the data to reduce false positives which usually generated by benign binary and image files. This novel approach enhances the utility of intrusion detection by reducing the false positive rates up to 2% in repetitive 10-fold cross validation.

(Made 2017) presented a distributed Machine learning based IDS in(httpswww.zeek.org.)which resides on cloud's edge routers and monitors inbound network traffic. The inbound traffic of each router is forwarded to anomaly detection module using Naive Bays Classifier which is forwarded to a centralized server. The classification and detection of attack is done by using Random forest algorithm. The model is implemented on google cloud and tested on CIDDS-001 public dataset. The model reaches overall average accuracy of 97% in detecting attacks like DOS, Brute-force Port & Ping scans.

The paper mainly combines the methodologies of signature based intrusion detection using snort & signature apriori algorithm and anomaly based detection with the help of different classifiers (Bayesian, Associative, and decision tree) and a score function to improve the accuracy and efficiency to detect known, unknown as well as distributed attacks in traditional and cloud networks. In Signature based detection phase the packets are processed through snort and signature apriori to detect known and derivative of known attacks and the output is sent to score function. The other normal packets are then applied to three classifiers after removing redundant information for anomaly detection. The classifiers individually detects class label (Intrusion or not) and sends a 1 (intrusion detected) or 0 (normal packet) to score function which calculates the average of weighted sum of all three classifiers and compares it with a threshold to determine that the packet is an intrusion and saves it to a central log. It also checks that if many sensors are sending same alert to central log then it considers it as distribution attack and should be blocked from entire cloud otherwise intrusion only for relevant host.

The paper (https://quadrantsec.com/sagan) represents a model based on an advance version of Support vector machine called core vector machines classification which is based on the concept of minimum enclosing ball. Training and testing is done sing KDDCup'99 dataset which includes: DOS, Probe, privilege escalation (U2R) and R2L attacks. In this approach attack points from the dataset are selected as core set, a circle that encloses every point in the data set is found. Now the radius is increased to locate similar attack points which may have left outside. This process continues until no attack points are left outside the circle.

In (PGarcı´a-Teodoro, 2009). a feature selection framework using filer and wrapper method then naive bayes and j48 classifiers are used to identify attacks on UNSW-NB15 dataset. This framework aims to use minimum number of features with high accuracy. The tests on UNSW-NB15 data set results in 88% accuracy by using j48 and 18 features, moreover 82% accuracy is achieved using 5 feature set.

(Alex 2018). implemented an improved model of Adaptive Boost RBF support vector machine for wireless sensor networks and simulated in Network Simulator 2 using AODV protocol the average detection rate comes out to be more than 95 % with reduced end-to-end delay and energy consumption.

(Mohamed 2018)proposed a framework which uses Average on dependence Estimators (AODE) which is an enhancement in the traditional naïve based technique. The model has been tested using NSL-KDD dataset to detect four types of attacks (DOS, Probe, User to root & R2L) and compared with Naïve based detection model. The results showed the improved performance as compared with Traditional naïve based model.

Table 2: Comparison of Different work related to Intrusion detection

Comparison of Different work related to Intrusion detection					
Author/year	**Intrusion Detection type**	**Proposed method**	**Technique**	**Detection approach**	**Accuracy**
Alex Shenfield et al/2018	NIDS	Reducing False Positives using Multi-Layer Perceptron and back propagation learning	ANN	Anomaly based	98%
Mohammad Idhammad et al/2018	NIDS	ensemble learning classification/Random Forest Algorithm	Machine Learning	Anomaly Based	97%
ChiragModi et al / 2013	Hybrid-NIDS	Snort Along with Associative, Bayesian and decision tree Classification	Machine Learning	Hybrid	-
Divyasree et al/2018	NIDS	Core Vector Machine classification	Data Mining	Anomaly Based	99% with 27% False positive rate
HebatallahMostafaAnwer/2018	NIDS	J48, Naive Bays Algorithm	Machine Learning	Anomaly Based	88%
Dai Jianjian/2018	NIDS	Adaptive boost, RBF Support Vector Machine	Machine Learning	Anomaly Based	95.72%
Amreen Sultana/2016	NIDS	Average one dependence estimator (AODE)	Data Mining	Anomaly Based	96-97 %

Section-V

5. BIBLIOMETRIC ANALYSIS

Bibliometric analysis is essential in analyzing past research by examining the relationship between different variables such as fields, individual papers, journal, annual scientific productions etc. to make progressions in a particular field. Year-wise publication provides a broad way to devise a conclusion on trend analysis in the intrusion detection tools over the last few years. Annual scientific production presents a mean to observe variation in the scientific contributions from the year 2010-2019. Analysis shows that the global publication trend for overall IDS tools touched its peak during the year 2017.

The **(Fig, 9)** shows trend of intrusion detection tools from 2010 to 2018, result of query run in web of science for getting top intrusion detection tools used in literature. Bro comes out to be leading tools, which is used in literature having impact of 46%, then the Linux/windows based Snort has 21% share and suricata has 15% share.

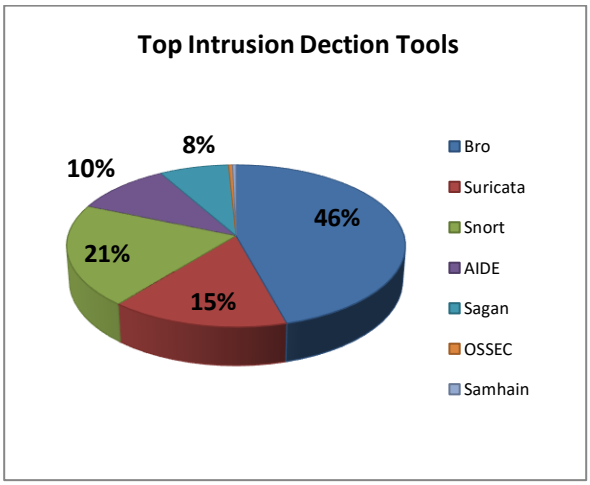
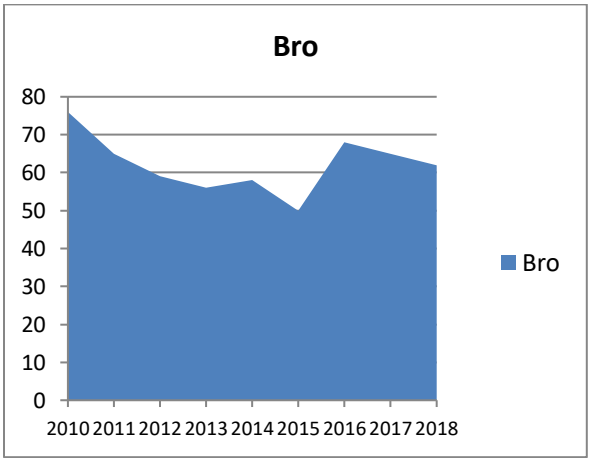
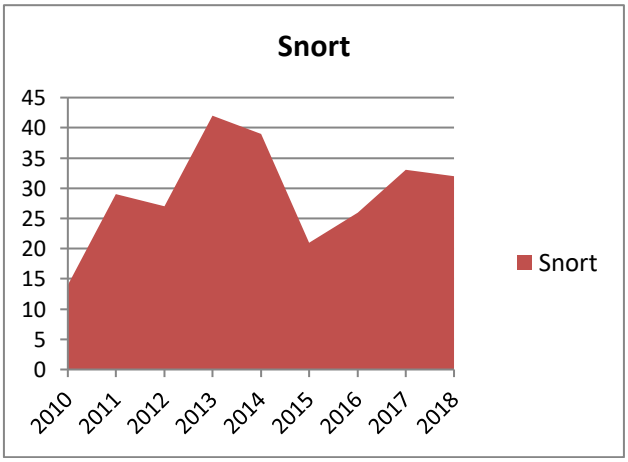


Fig. 9: Top Intrusion Detection Tools





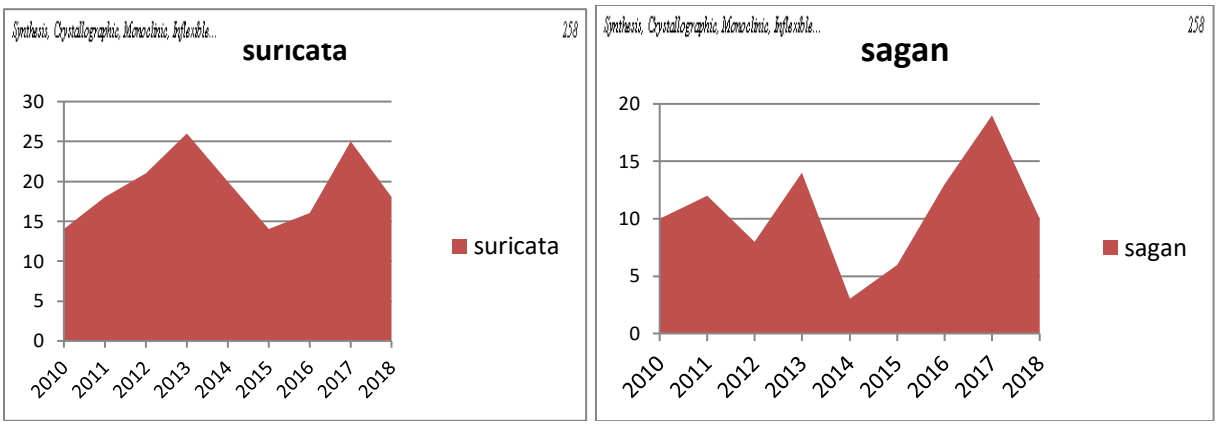


Fig. 10: Trend Analysis of different IDS (B/w 2010 to 2018)

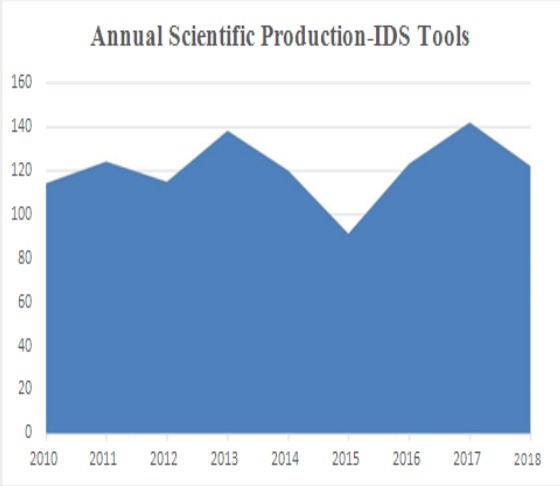


Fig. 11: Annual Scientific Production

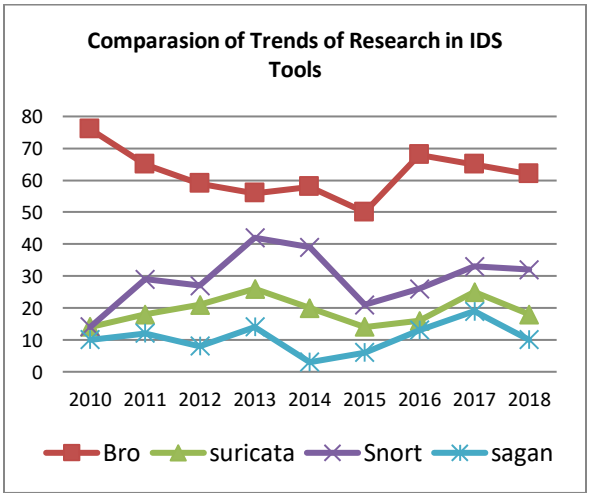


Fig. 12: Comparison of ASP of Different ID Tools

(Fig. 10) shows the individual trend analysis in terms of number of publications per year for top four IDS tools and **(Fig. 11)** shows overall scientific production of ID tools, **(Fig 12)** shows a comparison between them. The results of the comparison shows that the Bro is the tool which is consistently being used/referred in the literature the snort IDS is the second most used tool Suricata and Sagan has less share as compared to other two IDS.

Section VI

6. PROPOSED FRAMEWORK

A simplified Hybrid network based framework is proposed which combines the advantages of signature based as well as anomaly based detection. The model consists of four phases, Management phase, Signature Detection phase, Anomaly Detection phase and decision &Alerting phase. Consider I_P as the input packet, S_{DB} is the signature database ACi are the anomaly classifiers which can be based on statistical, expert system or machine learning, R is the resultant of all classifiers and D is the decision. The management engine controls overall IDS activities, it first captures packet from network performs operation like defragmentation, removes duplicate packets etc, then applies the input packet (I_P) to signature detection phase which compares it the definitions stored in signature database (S_{DB}) if a match found the result with $S_{DB=1}$ (yes) along with intrusion details is forwarded to management engine. If no match is found in signature database ($S_{DB=0)}$ then the same input Packet (I_P) is applied to anomaly detection phase which consists of n number of classifiers. The input is applied to each anomaly classifier (AC_i) which further detects intrusion. Now we have:

R= $\sum_{i=1}^{n} IpACi$ =0no Intrusion>=T Intrusion detected,

(where T is the threshold which determines minimum number of classifiers detects an intrusion).

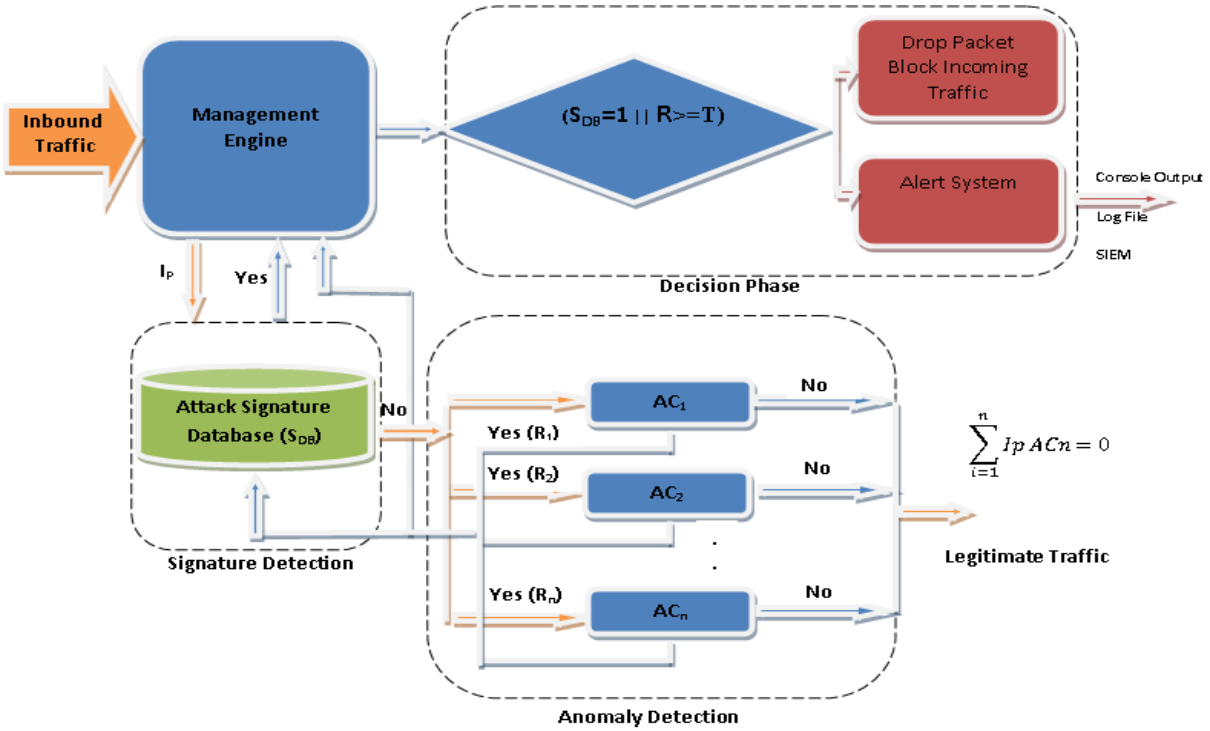


Fig.13 : Proposed Framework for NIDS

If the output of all anomaly classifiers is zero, it means no intrusion is detected and the traffic is treated as legitimate traffic on the other hand, the output >=1 shows that one or more classifiers detected an intrusion. The output ($\sum Rn$) is then sent to decision phase where decision is based on two main conditions

a) If output of SDB is 1
b) If cumulative output of I_P&ACi>=T,

Now the Decision D comes out to be 1 if

(S_{DB}=1 || R>=T) , where R=$\sum_{i=1}^{n} IpACi$

If any of the condition is true then the decision phase either drop packet or block the interface from which the data is coming based on pre-defined rules and/or generates an alert in the form of output to console, log file or send it to SIEM for further analysis. The false positive of the classifiers is also stored in S_{DB} which enables faster detection of same attacks in the future.

7. CONCLUSIONS

In this paper we present the classification of intrusion detection systems. Survey of various intrusion detection techniques show that the machine learning algorithms are widely used for classification of anomaly-based attack. The comparative study of different intrusion detection models is also discussed. We have also performed trend analysis results show that bro is the most widely used tool in the literature and consists of 46% of share. In the end a generic framework is proposed for Hybrid Network Based IDS.

REFERENCES:

Ashara, B. M., B. I.Norbik, andS. Bharanidharan, (2012). A Brief Introduction to Intrusion Detection System. *International Conference on Intelligent Robotics, Automation, and Manufacturing.* Verlag Berlin Heidelberg: Springer.

Amreen S. M. (2016). Intelligent Network Intrusion Detection System using Data Mining Techniques. IEEE.

Aleksandar, M and V. Marco. (2015). Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices. ACM Computing Surveys,V. 48, 1.

Aumreesh K.,andD. S.Saxena, (2017) General Study of Intrusion Detection System and Survey of Agent Based Intrusion Detection System. International Conference on Computing, Communication and Automation (ICCCA2017).

Akash Garg, P. M. (2016). A Hybrid Intrusion Detection System: A Review. *10th International*

Conference on Intelligent Systems and Control (ISCO). IEEE.

Abdullah H. and. D. N Almutairi,. (2017). Innovative Signature Based Intrusion Detection System Parallel Processing and Minimized Database. 978-1-5386-3148-5/17/$31.00 © 2017 IEEE.

Akash Garg, P. M. (2016). Performance Analysis of Snort-based Intrusion Detection System. 3rd International Conference on Advanced Computing and Communication Systems (ICACCS -2016).

Alex S, (2018). Intelligent intrusion detection systems using artificial neural networks. *ICT Express 4 The Korean Institute of Communications and Information Sciences (KICS).* Elsevier.

Dhanashri A., and V. M. Bhosale, (2015). Comparative Study and Analysis of Network Intrusion Detection Tools. *International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).* IEEE.

Divyasree T. H.. (2018). Network Intrusion Detection System Based On Ensemble CVM Using Efficient Feature Selection Approach. *8th International Conference on Advances in Computing and Communication (ICACC-2018).* Elsevier.

Dai J., (2018) A Novel Intrusion Detection System based on IABRBFSVM for Wireless Sensor Networks. *8th International Congress of Information and Communication Technology (ICICT-2018).* Elsevier.

httpswww.ossec.net.

httpswww.zeek.org.
http//www.snort.org. (Visited page on Jan 2019).

https://suricata-ids.org.

https://quadrantsec.com/sagan_log_analysis_engine/.

Hui Li, D. L. (2010) Research on Intelligent Intrusion Prevention System Based on Snort..

Hebatallah M. M. and F.H. Anwer, (2018). A Framework for Efficient Network Anomaly Intrusion Detection with Features Selection. *9th International Conference on Information and Communication Systems (ICICS).* IEEE.

Kai-Oliver D., (2015). SIEM Approach for a Higher Level of IT. Warsaw, Poland: The 8thIEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications.

International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE).

Kai, Z. (2012). Research and design of the distributed intrusion detection system based on Snort. *International Conference on Computer Science and Electronics Engineering.* IEEE.

Muhammad K. T. and. A. Asif, (2013). Network Intrusion Detection and its Strategic Importance. *IEEE Business Engineering and Industrial Applications Colloquium (BEIAC).*

MohdZ. A., and. M. F. Raffie (2016). Anomaly-Based NIDS: A Review of Machine Learning Methods on Malware Detection. Kuala Lumpur, Malaysia: International Conference on Information and Communication Technology (ICICTM), IEEE.

Made D., and S. M. Suryadinata, (2017). ANALYSIS Security Metric On Bro Ips Based On Cvss And Vea-Bility Metric. *International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC).* IEEE.

Mohamed I., (2018). Distributed Intrusion Detection System for Cloud Environments based on Data Mining techniques. *The First International Conference On Intelligent Computing in Data Sciences (Procedia Computer Science).* Elsevier.

Prachi D., S. C. Sharma, and. S. K. Peddoju, (2014). HIDS: A host based intrusion detection system for cloud computing environment. Int J Syst Assur Eng Manag, Springer.

Patel, C. M. (2013). A novel hybrid-network intrusion detection system (H-NIDS) in cloud computing. In Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security.

Pgarcı´a-Teodoro, J. D. V. F. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security 28*. Elsevier.

Rafath Samrin, D. V. (2017). Review on Anomaly based Network Intrusion Detection System. International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), IEEE.

Roshan K. (2018). HyINT: Signature-Anomaly Intrusion Detection System. 9th ICCCNT.

Rifqi F., and N. A. Pratama, (2018). Design and Implementation Adaptive Intrusion Prevention System (IPS) for Attack Prevention in Software-Defined Network (SDN) Architecture. 6th International Conference on Information and Communication Technology (ICoICT).

Rpatel, E. (2018). Protocol Specific Multithreaded NIDS for DOS/DDOS setection in cloud. th ICCNT.

Xiaohong Qu, Z. L. (2009). Research on Distributed Intrusion Detection System Based on Protocol Analysis. *3rd International Conference on Anti-Counterfeiting, Security, and Identification in Communication.* IEEE.

Yaping Chi, T. J. (2017) Design and Implementation of Cloud Platform Intrusion Prevention System based on SDN. 978-1-5090-3619-6/17/$31.00 ©2017 IEEE.

Zhijian Y., and Z. A Wang, (2017) Centralized HIDS Framework For Private Cloud. Kanazawa, Japan: 978-1-5090-5504-3/17/$31.00 ©2017 IEEE Computer Society.