Journal of Statistics, Computing and Interdisciplinary Research
ISSN (P): 2707-7101

J. Stat. Comp. & Interdis. Rese.
Volume 3(2) (2021), 189 -223
http://scir.wum.edu.pk/index.php/ojs

Systematic Literature Review over IDPS, Classification and Application in its Different Areas

Shehroz Afzal[1*] and Jamil Asim[2]
Faculty of Computer Science & IT, Universiti Malaysia Sarawak (UNIMAS), Malaysia
Department of Criminology, University of Okara, Pakistan
[*]Corresponding Author: *shehrozafzal347@gmail.com*

Abstract

Cyber-attacks are becoming more sophisticated and thereby presenting increasing challenges in accurately detecting intrusions. Failure to prevent the intrusions could degrade the credibility of security services, e.g. data confidentiality, integrity, and availability. Numerous intrusion detection methods have been proposed in the literature to tackle computer security threats, which can be broadly classified into Signature-based Intrusion Detection Systems (SIDS) and Anomaly-based Intrusion Detection Systems (AIDS). Network security is vital for any organization connected to the Internet. Rock solid network security is a major challenge that can be overcome by strengthening the network against threats such as hackers, malware, botnets, data thieves, etc. Firewalls, antivirus, and intrusion detection systems are used to protect the network. The firewall can control network traffic, but reliance on this type of security alone is not enough. Attackers use open ports such as port 80 of the web server (http) and port 110 of the POP server to infiltrate networks. The Intrusion Detection System (IDS) minimizes security breaches and improves network security by scanning network packets to filter out malicious packets. Real-time detection with prevention using Intrusion Detection and Prevention Systems (IDPS) has elevated network security to an advanced level by strengthening the network against malicious activities. In this Survey paper focuses on Classifying various kinds of IDS with the major types of attacks based on intrusion methods. Presenting a classification of network anomaly IDS evaluation metrics and discussion on the importance of the feature selection. Evaluation of available IDS datasets discussing the challenges of evasion techniques.

Keywords: Intrusion Detection Systems, Signature-based Intrusion Detection Systems, Anomaly-based Intrusion Detection Systems, Host-based Intrusion Detection Systems.

Introduction

The evolution of malicious software (malware) poses a critical challenge to the design of intrusion detection systems (IDS). Malicious attacks have become more sophisticated and the foremost challenge is to identify un-known and obfuscated malware, as the malware authors use different evasion techniques for information concealing to prevent detection by an IDS (Khraisat, et al., 2019). In addition, there has been an increase in security threats such as zero-day attacks designed to target internet users. Therefore, secure transactions must be provided using firewalls, intrusion detection systems (IDS), encryption, authentication, and other hardware and software solutions. IDS are designed to reliably detect probe, DoS, U2R, R2L and data attacks on Solaris, Sun OS, Linux and Windows NT operating systems with low false alarm rates. However, due to the complexity of the system, configuration and administration errors and misuse by authorized users, most systems cannot be completely prevented from attacking. An IDS has far more knowledge and many tricky detection features than ordinary firewalls. The firewall only allows the desired IP addresses and ports to pass traffic, but cannot detect whether the traffic is normal or harmful. Therefore, the firewall has some obvious advantages, but it does not have the ability to detect attacks. The intrusion detection system, on the other hand, detects threats and attacks by monitoring network traffic. When intrusion activity occurs on a network, IDS generates an alert asking the network administrator to activate and act to block or mitigate the attack (Ahmed et al., 2014). We generally have three groups of threats in any system. Threats are classified as Internal Penetrations, External penetrations and Misfeasance. External threats are those who try to break in system security for some illegal attempts, second category include of those who are internal members and try to access system outside their legal actions. There are three main approaches to intrusion prevention: Secure engineering: creation of systems without vulnerability, taking perfect corrective measures to detect and correct vulnerabilities, and detection and blocking of the operation Try before a crash (Bace, 1999). serious damage. In this paper I will focus on detailed Analysis of IDPS, Working of IDPS its methodologies and techniques used my IDPS. Late I will evaluate different methodologies, working principals and tools used by IDPS.

Literature Review

Barghi has stated that when the Intrusion Detection System shields the network from the network attack, it produces a large number of false, redundant or irrelevant alerts. It is a downside of it. An online approach was presented using DARPA 1999 dataset and Shahid Rajaee Port Complex dataset. The results showed that the system reduce the number of alerts by 94.32%. In some cases, it had high detection rate and also a very high false alarm rate too (Barghi et al., 2015).

A technique to find out if a web page is harmful or benign. First, the static content of web pages that use a self-developed JAVA program is used to process signatures with regular expressions to speed up the parsing process, then a honeypot system for navigating web pages, and finally ends with the type of Web page (Koo et al., 2013).

Friedberg confirmed that Advanced Persistent Threat (APT) uses different attack methods to access the unauthorized system in initial stage and then slowly spread throughout the network. This proposed approach is designed to extend any" packet -level" IDS systems to improve their results. The model is built with Search-Patterns (P), Event Classes(C), Hypothesis(H) and Rules (R) (Friedberg et al., 2015).

Salama suggested that the web anomaly misuse intrusion detection framework (WAMID) works with the combination of abuse and anomaly detection algorithms to detect SQL injection attacks. First, in the training phase, a profile is created for the legitimate behavior of the database extracted from the association rules application in an XML file that contains SQL queries sent by the application to the database.

In reference to Chen Botnet it is a collection of hosts (bots) and is controlled by a master bot through a command and control channel (C&C). Therefore, this detection mechanism detects the attack during the C&C phase, that is, before the attack on the botnet. IRC traffic patterns on an organization network were taken into account for testing. The similarity measure and the periodic characteristics were observed. This system can detect malicious network traffic from normal IRC clients (Chen et al., 2015).

SQL injection attack technique that involves stealing confidential information from the main database, such as credit card numbers. They proposed IDS-SQL IDDS (SQL injection detection through query transformation and document similarity) to detect different types of SQL injection attacks. Only the requests portion after the WHERE keyword was considered. For testing, five Honeypot web applications were developed using PHP and MySQL (Kar et al., 2015).

According to Showmanship Honeypot is nothing more than a fake server that provides emulated services similar to real services running on the real server. Therefore, every time the attacker tries to attack the real server, the attacker is redirected to this fake server and ends up trapped. Honeypot then gives precious information about the intruders. This document suggested a new honey pot system. The components of the system are: i) Event auditor: to supervise the exchange of data between the nodes and send them to IDS. ii) IDS service with two components, namely the analyzer and the alert system (Somwanshi et al., 2016).

Kaur, J. stated that whenever users use a web application, all user activities are automatically added to the web log files. This system essentially focused on these journal entries and suggested a preventive technique to protect them. The most common attacks, namely denial of service and brute force attacks. And it provides a secure platform for file sharing. This system is capable of distinguishing between malicious and non-malicious users (Kaur et al., 2015).

Cross-Site Scripting attack (XSS) is a code injection attack carried out to exploit existing vulnerabilities in the web application by injecting html tag / java script functions. They featured different types of XSS attacks. This system works in two steps: the first is to track cross-site

scripting vulnerabilities in the web application. A php website, hosted on the local host (XAMPP server), has just been created and experiments have been performed on modern browsers (Google Chrome49, IE11, Opera15 and Firefox44.0.2) to exploit XSS vulnerabilities. The second step is to mitigate the attack (Kour et al., 2016).

Seeber (2018) have suggested a new approach to form an IDS with multiple IDSs to detect network attacks by processing data from the main components of the network using the properties of OpenFlow in an SDN environment. OpenFlow is capable of triggering an event or updating a flow counter at the arrival time of a packet based on a match or a mismatch with an existing or non-existent flow. If there are multiple Intrusion Detection Systems (IDS), traffic redirection is primarily based on subnets or IP addresses (Seeber et al., 2015).

Intrusion

Intrusions are actions that attempt to bypass security mechanisms of computer systems. So they are any set of actions that threatens the integrity, availability, or confidentiality of a network resource. These properties have the following explanations:

1. Confidentiality – means that information is not made available or disclosed to unauthorized individuals, entities or processes;
2. Integrity – means that data has not been altered or destroyed in an unauthorized manner;
3. Availability – means that a system or a system resource that ensures that it is accessible and usable upon demand by an authorized system user. Availability is one of the core characteristics of a secure system.
4. Occasionally intrusions are caused by:
    - Attackers accessing the system from Internet;
    - Insider attackers − authorized users attempting to gain and misuse non-authorized privileges.

Examples of Intrusions

There are a number of attacks summary of attacks are given in a table below.

Table 1: Classes of computer attacks and Intrusions

Type of Attacks	Explanation	Examples
Buffer Overflow	Attacks the buffer's boundaries and overwrites memory area.	Long URL strings are a common input. Cowan,
worm	Reproduces itself on the local host or through the network.	SQL Slammer, Mydoom, CodeRed Nimda.
Trojan	Programs appear attractive and genuine, but have malicious code embedded inside them.	Zeus, Spy Eye

DOS	A security event to disrupt the network services. It is started by forcing reseton the target computers. The users can no longer connect to the system because of unavailability of service.	Buffer overflow, Ping of death (PoD), TCP SYN, smurf
Common Gateway Interface Scripts	The attacker takes advantage of CGI scripts to create an attack by sending illegitimate inputs to the web server.	Phishing email
Traffic Flooding	Attacks the limited size of NIDS to handle huge traffic loads and to investigate for possible intrusions. If a cybercriminal can cause congestion in the networks, then NIDS will be busy in analyzing the traffic.	Denial of Service (Dos) or Distributed Denial of Service (DDoS)
Physical Attacks	Aims to attack the physical mechanisms of the computer system.	Cold boot, evil maid
Password Attack	Aims to break the password within a small time, and is noticed by a sequence of failures login.	A dictionary attack, Rainbow attack
Information Gathering	Gathers information or finds weaknesses in computers or networks by sniffing or searching.	System scan, port scan
User to Root attack	The cybercriminal accesses as a normal user in the beginning and then Attackupgrades to a super-user which may lead to exploitation of several vulnerabilities of the system.	Intercept packets, rainbow attack, social engineering Rootkit, load module
Remote to Local	The cybercriminal sends	Warezclient, ftp write,

Attack	packets to a remote system by connecting to the network without having an account on the system.	multihop,phf, spy, warezmaster, imap
Probe	Identifying the valid IP addresses by scanning the network to gather host data packets.	Sweep, portsweep

Intrusion Detection

Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, like unauthorized entrance, activity, or file modification. There are three steps in the process of intrusion detection which are:

- Monitoring and analyzing traffic.
- Identifying abnormal activities.
- Assessing severity and raising alarm.

Intrusion Detection and Prevention System

Intrusion detection and prevention systems are a combination of intrusion detection systems and intrusion prevention systems. Intrusion detection and prevention systems (IDPS) have become a precious tool for the security of information systems. IDPS are security tools used to monitor, analyze and respond to potential security breaches against computers and network systems. These violations may result from a failure of attempts by unauthorized external intruders to compromise the system or from privileged internal users who do not use their credentials. Intrusion Detection System (IDS) is software that automates the intrusion detection process and detects possible intrusions. Intrusion Detection Systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. An IDS is composed of several components:

- Sensors which generate security events;
- Console to monitor events and alerts and control the sensors;
- Central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received

In many simple IDS implementations, these three components are combined into a single device or device. In particular, IDS tools aim to detect computer attacks and / or computer abuse and alert the right people after detection. IDS uses directives to define certain events that issue a warning when they are detected. In other words, if a particular event is considered a security incident, a warning is issued if that event is detected. Some IDSs can send alerts so that the IDS administrator receives a page, email, or SNMP trap notification of a potential security incident. Many IDSs not only recognize a specific incident and issue a corresponding warning, but also

react automatically to the event. Such a response can include logging off a user, disabling a user account, and starting scripts. IDSs are an integral and necessary part of a comprehensive information security infrastructure that acts as a "logical addition to network firewalls". Simply put, IDS tools allow complete network monitoring regardless of what is being done, so that information is always available to determine the type of security incident and its origin. Ideally, the computer network is separated from the outside world by a well-designed firewall. The outside world includes the host organization of the team.

Firewalls protect a network and try to prevent intruders, while IDS tools detect whether the network is attacked or has actually been breached. IDS tools are therefore an essential element of a complete and complete security system. They do not fully guarantee security, but can significantly improve network security when used with security policies, vulnerability assessments, data encryption, user authentication, access control and firewall. IDS can also be used to monitor network traffic to determine if a system is under attack by a network attack, such as a DoS attack. IDS remains the only proactive way to detect and respond to threats that occur inside and outside of a corporate network. Intrusion detection tools use a variety of techniques to determine what can be called an intrusion compared to normal traffic. Whether a system uses anomaly detection, misuse detection, target monitoring, or stealth probes, they generally fall into one of two categories:

Location Based IDPS

Host-based IDSs (HIDS)

Examine the data on individual computers that act as hosts. The host-based network architecture is based on an agent. This means that there is a software agent on each of the hosts controlled by the system. Host-based principles are similar in principle and purpose to network-based principles, except that a host-based product monitors the properties of a single host and the events that occur on this host, e.g. These include monitoring network traffic (for this host only) and system logs, executing processes, accessing and modifying files, and modifying system and application settings. They often use a combination of attack signatures and knowledge of expected or typical behavior to identify known and unknown attacks on systems. When a host-based product monitors host network traffic, it offers detection capabilities similar to those based on the network. Host-based IDPS is most commonly deployed on critical hosts, such as publicly available sensitive information servers.

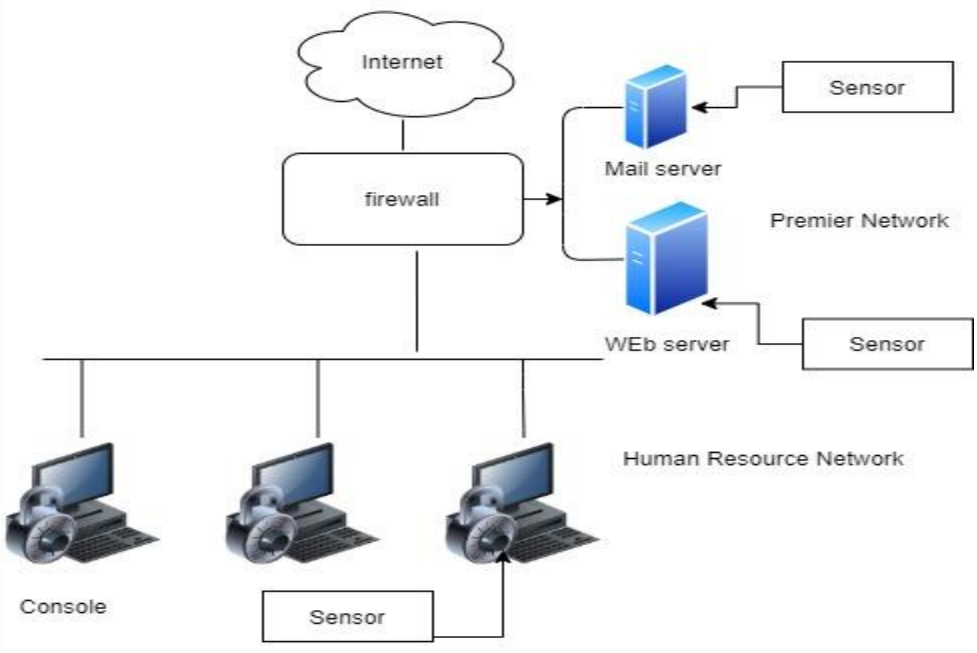

Fig1: Host Based IDS

Network-based IDSs (NIDS)

Examine the data exchanged between computers. The most efficient host-based intrusion detection systems can monitor and capture system audit trails both in real time and on time, thereby distributing and providing CPU usage and overhead of the network. They are usually implemented online. Like a network firewall. They receive packets, analyze them, decide to authorize them and let the acceptable packets pass. Allow certain attacks, such as network service worms, email. Worms and viruses transmitted with easily recognizable characteristics (for example, subject, name of attachment) which must be detected in networks before reaching their intended destinations (for example, mail server, web server). Most products use a combination of attack signatures and application and network protocol analysis. Network-based products can detect and stop unknown threats by analyzing the application log. With certain products, administrators can create and implement attack signatures for many new malware threats in minutes. Although the misspelled signature triggers false positives that block harmless activity, a custom signature can block certain new malware threats hours before antivirus signatures are available. However, web-based products are generally unable to stop malicious mobile code or Trojans.

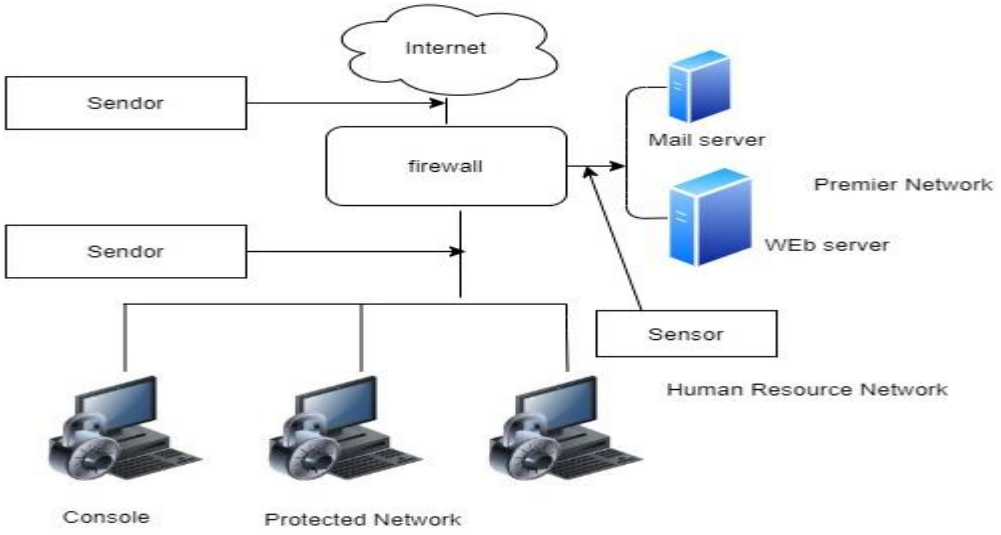

Fig2: Network based IDS NIDS

Technology		Advantages	Disadvantages	Data source
	HIDS	• HIDS can check end-to-end encrypted communication behavior. •No extra hardware required. •Detects intrusions by checking hosts file system calls or network events. •Every packet is reassembled •Looks at the entire item, not streams only	• Delays in reporting attacks • Consumes host resources • Needs to be installed on each host • It can monitor attacks only on the machine where it is installed	• Audits records, log files, Application Program • Interface (API), rule patterns, system calls.
	NIDS	•Detects attacks by checking network packets •Not required to	•Challenge is to identify attacks from encrypted traffic.	•Simple Network Management Protocol

		install on each host •Not required to install on each host •Capable of detecting the broadest ranges of network protocols	•Dedicated hardware is required. •It supports only identification of network attacks. •Difficult to analysis high-speed network •The most serious threat is the insider attack	(SNMP) •Network packets (TCP/UDP/ICMP) •Management Information Base (MIB) •Router Net Flow records

IDPS Methodologies

After examining the two basic types of IDS (HIDS and NIDS) and why they should be used together, we can examine how they do their job. IDPS uses many different methods to detect changes in the systems they monitor. These changes can be external attacks or misuse by internal employees. Four of the many methods stand out and are widely used. These are signature protocol, anomaly, Stateful and hybrid analyzes. Most current IDPS systems use the hybrid method, which combines other methods to provide better detection and prevention functions. All methods use the same general model, and the main difference between them is how they process the information they collect from the monitored environment to determine if there has been a policy violation. Figure 3 shows a broad architecture on which these systems are based. This architecture was developed by the intrusion detection working group and includes four functional blocks, event blocks, which are event tables, which capture events from the monitored system and are analyzed by other blocks. , then the database blocks, which are the database tables in which the events of the event blocks are stored, then the analysis blocks which process the events and send a warning and terminate the response blocks , whose goal is to respond to an intrusion and stop it.

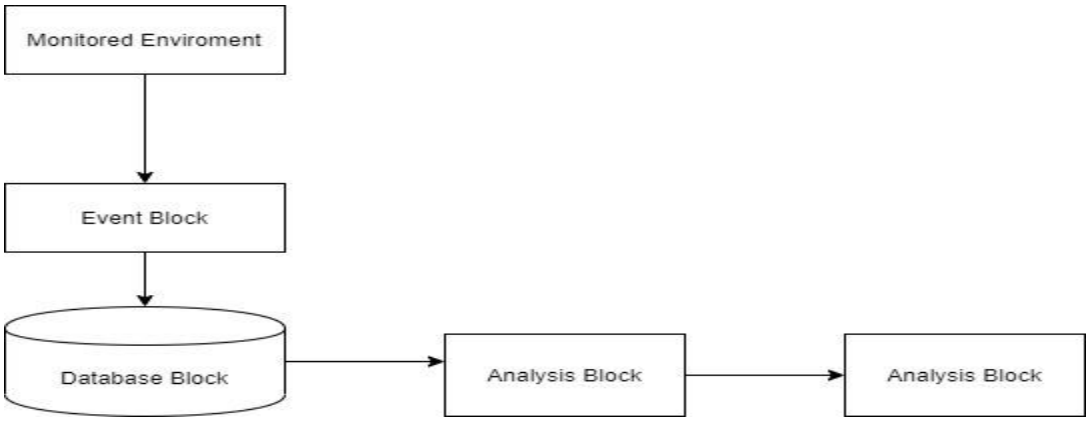

Fig3: General Architecture of IDPS system

Anomaly Based Methodology

The anomaly-based methodology works by comparing the observed activity with a reference profile. The basic profile is the normal learning behavior of the monitored system and develops during the learning phase when IDPS learns the environment and develops a normal profile of the monitored system. This environment can be networks, users, systems, etc.The profile can be fixed or dynamic. A fixed profile does not change once it is set up, while a dynamic profile changes as the monitored systems evolve. A dynamic profile adds additional overhead to the system as IDPS continues to update the profile, which also opens it for avoidance maneuvers. An attacker could dodge IDPS using a dynamic profile by extending the attack over a long period of time. In this way, your attack is part of the profile because IDPS takes into account changes to your profile when the normal system changes. If a predefined threshold is used, any deviation outside the threshold is reported as a violation. A fixed profile is very effective in detecting new attacks because any change in normal behavior is classified as an anomaly.

Anomaly-based methods can detect zero-day attacks on the environment without system updates. The anomaly intrusion detection method uses three general techniques for anomaly detection: statistical anomaly detection, knowledge / data mining and machine learning.

Statistical IDS Technique

Statistical anomaly techniques are used to create the two required profiles, one during the learning phase, which is then used as the base profile, and the current profile, which is compared to the base profile, as well as any differences that are identified by an appropriately labeled anomaly the monitored environmental parameter threshold. The threshold must be tuned according to the requirements and behavior of the environment being monitored for the systems to be effective. Statistical IDS normally use one of the following models.

Univariate: "Uni" means "one", which means that the data has only one variable. This technique is used when creating a normal statistical profile for a single measure of behavior in computer systems. Univariate identifications look for abnormalities in each individual metric.

Multivariate: it is based on the relationships between two or more measures to understand the relationships between the variables. This model would be useful if the experimental data shows that a better classification can be obtained from correlated measures combinations instead of analyzing them separately. Ye et al. To examine a multivariate quality control method to identify intrusions by constructing a long-term profile of normal activities. The main challenge for multivariate statistical identifiers is that it is difficult to estimate distributions for large data.

Knowledge based IDS Technique

Knowledge and data mining technology is used to automate the technical monitor's search for anomalies, and this process pays much attention to the system. The technique produces peak false positive and false negative results due to the high overhead resulting from the complex task of correctly identifying and categorizing the events observed in the system. The machine learning technique works by analyzing the system calls and it is the widely used technique. The main advantage of knowledge-based techniques is the ability to reduce false positive alarms because the system is aware of all normal behaviors. However, in a dynamic and evolving IT environment, this type of IDS needs a regular update of knowledge for expected normal behavior, which is a long task, since gathering information on all normal behaviors is very difficult. Finite State Machine (FSM): FSM is a calculation model used to represent and control the flow of execution. This model could be applied to intrusion detection to produce an intrusion detection system model. Typically, the model is represented as states, transitions, and activities. A report verifies the historical data. For example, any variation in input is noted and based on the transition of the detected variation that occurs. An FSM can represent legitimate system behavior, and any deviation from this FSM is considered an attack.

Description language: The description language defines the syntax of the rules that can be used to specify the characteristics of a defined attack. Rules could be constructed using description languages like N-grammars and UML (Studnia et al., 2018).

Expert system: An expert system includes a series of rules that define attacks. In an expert system, the rules are generally defined manually by a knowledge engineer working in collaboration with an expert in the field (Kenkre et al., 2015).

Signature Analysis: This is the first technique applied in the IDS. It is based on the simple idea of joining chains. In string matching, an incoming packet is inspected, word for word, with a separate signature. If a signature matches, an alert is generated. Otherwise, the traffic information corresponds to the following signature in the signature database.

Machine learning Technique

Machine learning is the process of extracting knowledge from large amounts of data. Machine learning models include a complex set of rules, methods or “transfer functions” that can be applied to find interesting data models, or to recognize or predict behavior (Duque et al., 2015). widely applied in the field of AIDS. Several algorithms and techniques such as clustering, neural

networks, association rules, decision trees, genetic algorithms and nearest neighbor methods have been applied to discover the knowledge of intrusion data sets (Kshetri et al., 2017). The goal of using machine learning techniques is to create SDIs with improved accuracy and less human knowledge. In recent years, the amount of AIDS that has used machine learning methods has increased. A key objective of IDS based on machine learning research is to detect patterns and build an intrusion detection system based on the dataset. In general, there are two types of machine learning methods, supervised and unsupervised.

Supervised Learning in Intrusion Detection System

This section introduces several supervised learning techniques for IDS. Each technique is presented in detail and references to important research publications are presented. IDS techniques based on supervised learning detect intrusions using tagged training data. A supervised learning approach generally involves two steps, namely training and assessment. In the training stage, the relevant characteristics and classes are identified, and then the algorithm learns from these data samples. In IDS supervised learning, each record is a pair, containing a network or host data source and an associated output value (that is, a label), that is, an intrusion or a normal value. Then feature selection can be applied to remove unnecessary features. Using the training data for the selected characteristics, a supervised learning technique is used to train a classifier to learn the inherent relationship between the input data and the labeled output value. A wide variety of supervised learning techniques have been explored in the literature, each with its advantages and disadvantages. In the testing phase, the trained model is used to classify unknown data into intrusion or normal class. The resulting classifier becomes a model that, given a set of entity values, predicts the class to which the input data might belong. There are many classification methods, such as decision trees, rule-based systems, neural networks, support vector machines, naive Bayes, and closest neighbors. Each technique uses a learning method to build a classification model. However, an appropriate classification approach. Not only must you manage your training data, but you must also accurately identify the kind of records you've never seen before. Creating classification models with reliable generalizability is an important task of the learning algorithm.

Decision trees: A decision tree has three basic components. The first component is a decision node, which is used to identify a test attribute. The second is a branch, where each branch represents a possible decision based on the value of the test attribute. The third is a sheet that includes the class to which the instance belongs.

Naïve Bayes: This approach is based on the application of the Bayes principle with solid hypotheses of independence between attributes. Naïve Bayes answers questions such as "what is the probability that a particular type of attack will occur, given the observed system activities?" applying conditional probability formulas. Naive Bayes is based on characteristics that have different probabilities of occurring in attacks and in normal behavior. The Naïve Bayes classification model is one of the most common models in the IDS due to its ease of use and The

efficiency of the calculation, both extracted from its conditional independence hypothesis property. However, the system does not work well if this assumption of independence is invalid, as demonstrated in the KDD'99 intrusion detection data set that has complex attribute dependencies. The results also reveal that the Naïve Bayes model has reduced precision for large data sets. Another study has shown that the more sophisticated Hidden Naïve Bayes (HNB) model can be applied to IDS tasks that involve high dimensionality, highly interdependent attributes, and high-speed networks.

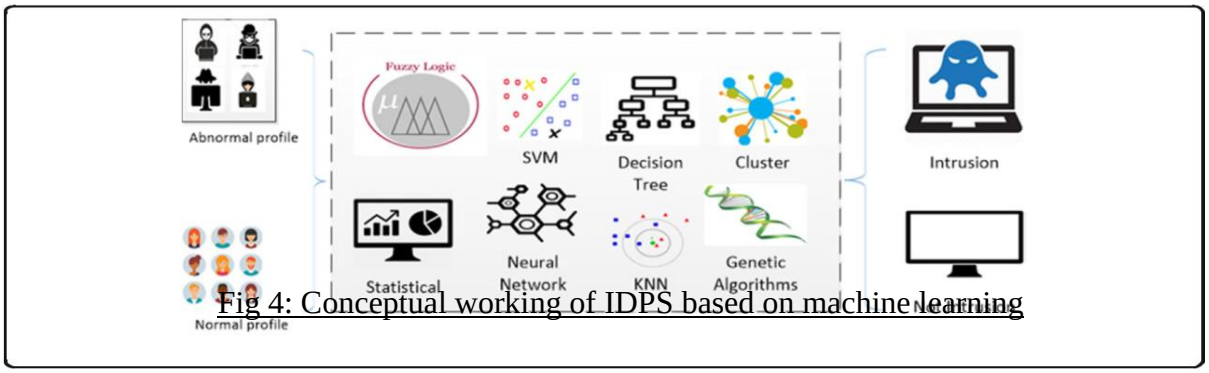

Fig 4: Conceptual working of IDPS based on machine learning

Genetic Algorithms (GA)

Genetic algorithms are a heuristic approach to optimization, based on the principles of evolution. Each possible solution is represented as a series of bits (genes) or chromosomes, and the quality of the solutions improves over time by applying selection and reproduction operators, biased to favor the solutions. adjustment. When a genetic algorithm is applied to the problem of classifying intrusions, there are generally two types of chromosome encoding: one relies on clustering to generate a binary chromosome encoding method; another specifies the center of the group (prototype clustering matrix) for an entire encoding chromosome. Murray et al., Used GA to develop simple rules for network traffic (Murray et al., 2014). Each rule is represented by a genome, and the primary population of genomes is a series of random rules. Each genome is made up of different genes that correspond to characteristics such as the IP source, the IP destination, the port source, the port destination and 1 type of protocol.

Artificial Neural Network (ANN)

ANN is one of the most widely used machine learning methods and has been shown to successfully detect different types of malware. The most widely used learning technique for supervised learning is the backpropagation (PA) algorithm. The BP algorithm evaluates the gradient of the network error with respect to its modifiable weights. However, for ANN-based IDS, detection accuracy, especially for less frequent attacks, and detection accuracy still need to be improved. The training dataset for less frequent attacks is small compared to that for more frequent attacks, making it difficult for the ANN to properly understand the properties of these attacks. As a result, detection accuracy is lower for less frequent attacks. In the area of information security, great damage can occur if low-frequency attacks are not detected. For

example, if user root attacks (U2R) go unnoticed, a cybercriminal can gain authorization privileges from the root user and thus perform malicious activities on the victim's computer systems. Furthermore, less common attacks are usually atypical (Wang et al., 2010). RNA often suffers from local minima, and therefore learning can be time consuming. ANN's strength is that with one or more hidden layers, it is capable of producing highly non-linear models that capture complex relationships between input attributes and classification labels. With the development of many variations, such as recurring and convolutional NNs, ANNs are powerful tools in many classification tasks, including IDS.

Fuzzy Logic

This technique is based on degrees of uncertainty rather than the typical true or false Boolean logic in which contemporary PCs are created. Therefore, it presents a simple way to reach a final conclusion based on unclear, ambiguous, noisy, inaccurate, or missing input data. With a fuzzy domain, fuzzy logic allows an instance to belong, possibly partially, to multiple classes at the same time. Therefore, fuzzy logic is a good classifier for IDS problems as security itself includes lack of clarity and the boundary between normal and abnormal states is not well identified. Also, the intrusion detection problem contains various numerical characteristics in the collected data and various derived statistical measures. The creation of IDS in the digital database with rigid thresholds produces high false alarms. An activity that deviates slightly from a pattern could not be recognized, or a minor change in normal activity could lead to false alarms. With fuzzy logic, it is possible to model this minor anomaly to keep false rates low (Elhag et al., 2015). They have shown that with fuzzy logic, the false alarm rate can be reduced by determining intrusive actions. They described a set of fuzzy rules to describe normal and abnormal activities in a computer system, and a fuzzy inference engine to define intrusions (Elhag et al., 2015).

Support Vector Machines (SVM)

SVM is a discriminatory classifier defined by a division hyperplane. SVMs use a core function to map training data in higher dimensional space so that the intrusion is linearly classified. SVMs are well known for their generalizability and are especially useful when the number of attributes is large and the number of data points is small. Different types of separation hyperplanes can be obtained by applying a nucleus, such as the linear or polynomial radial Gaussian base function (RBF) or the hyperbolic tangent. Many features in IDS data sets are redundant or less influential in separating data points into correct classes. Therefore, feature selection should be considered during SVM training. SVM can also be used for classification into various classes. In the work by Li et al., An SVM classifier with an RBF core was applied to classify the KDD 1999 dataset into predefined classes. From a total of 41 attributes, a subset of characteristics was carefully chosen using the characteristic selection method.

Hidden Markov Model (HMM):

HMM is a statistical Markov model in which the modeled system is assumed to be a Markov process with invisible data. Previous research has shown that HMM analysis can be applied to identify particular types of malware (Annachhatre et al., 2015). In this technique, a hidden Markov model is trained against known malware functionality (e.g., opcode sequence), and after completing the training step, the trained model is applied to record incoming traffic. The score is checked against a predefined threshold, and a score above the threshold indicates malware. Similarly, if the score is below the threshold, the traffic is identified as normal.

K-Nearest Neighbor Classifier (KNN)

The k-Nearest Neighbor (k-NN) technique is a typical non-parametric classifier applied to machine learning (Lin et al., 2015). The idea of these techniques is to name an unlabeled data sample to the class of its k closest neighbors (where k is an integer that defines the number of neighbors to consider). Figure 5 illustrates a K-Nearest Neighbors classifier where k = 5. Point X represents an unlabeled date instance that needs to be classified. Among the five closest neighbors to X, there are three similar models of the Intrusion class and two of the Normal class. A majority vote allows X to be assigned to the Intrusion class. Known behavior for evaluation. Their results revealed that clustering of k-means is a better approach to classify data using unsupervised intrusion detection methods when more than one type of dataset is available. Clustering can be used in IDS to reduce intrusion signatures, generate a high-quality signature, or group a similar intrusion. Hierarchical grouping: This is a grouping technique that aims to create a hierarchy of grouping. Hierarchical grouping approaches are normally classified into two categories:

Bottom-up aggregation techniques where groups have subgroups, which in turn have subgroups and group pairs are combined as one moves up the hierarchy.

Divisor: hierarchical grouping algorithms where the group with the largest diameter in the functional space is iteratively selected and separated into binary subgroups with a lower rank.

Much work has been done in the area of cyber-physical control system (CPCS) with attack detection and reactive attack mitigation using unsupervised learning. For example, Alcara has proposed a resilience approach based on redundancy (Alcaraz et al., 2018). He proposed a dedicated network sublayer that has the ability to manage context by periodically collecting consensus information from controlled pilot nodes in the control network itself and discriminating differences in vision using techniques. data mining such as k-means and k-nearest neighbor. Chao Shen et al. Proposal of fingerprints of hybrid devices increased for IDS in networks of industrial control systems. They used different machine learning techniques to analyze network packets in order to filter anomaly traffic to be detected in intrusions in ICS networks (Shen et al., 2018).

Semi-supervised Learning

Semi-supervised learning is between supervised learning (with fully labeled training data) and unsupervised learning (without categorized training data). The researchers demonstrated that semi-supervised learning could be used in conjunction with a small amount of classifier performance classified data for SDI with less time and cost. This is valuable because for many IDS problems, tagged data may be sparse or occasional (Ashfaq et al., 2017).

Several different techniques have been proposed for semi-supervised learning, such as algorithms based on maximizing expectations (EM) self-training joint training, semi-supervised SVM (Ashfaq et al., 2017), graph based methods, and the strengthening of semi-supervised based learning methods.

Rana et al. (2007) propose a new approach to fuzzy semi-supervised learning by applying unlabeled samples assisted by a supervised learning algorithm to improve classifier performance for IDS. A single hidden-layer direct acting neural network (SLFN) is formed to produce a fuzzy membership vector, and the categorization of samples (low, medium, and high fuzzy categories) into unlabeled samples is performed using the fuzzy quantity (Ashfaq et al., 2017). The classifier is recycled after incorporating each category separately into the original training package. Their experimental results using this semi-supervised intrusion detection in the NSL-KDD dataset show that unlabeled samples belonging to low and high fuzzy groups cause, above all, contributions to improve the precision of IDS as opposed to traditional.

The general architecture of an anomaly based IDPS system is shown in figure 5. The monitored environment is monitored by the detector that examines the observed events against the baseline profile. If the observed events match the baseline, no action is taken, but if it does not match the baseline profile and it is within the acceptable threshold range then the profile is updated. If the observed events do not match the baseline profile and falls outside the threshold range they are marked as an anomaly and alert is issued.

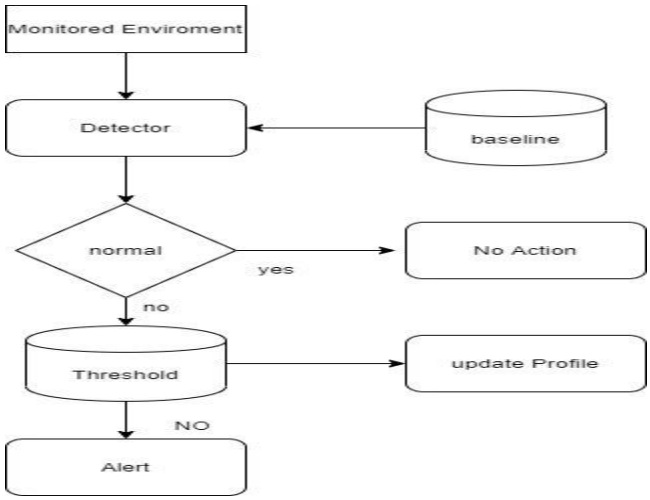

Fig 5: Anomaly based IDPS

Signature Based Methodology

The signature-based method compares the observed signatures with the signatures in the file. This file can be a database or a list of known attack signatures. Any observed signature in the monitored environment that matches the signature in the file is reported as a security policy violation or attack. Signature-based IDPS has a low overhead because not all network activity or data traffic in the monitored environment is checked. Instead, only known signatures in the database or file are searched. In contrast to the anomaly-based methodology, the signature-based methodology system is easy to implement because you do not have to learn the environment. This method works simply by searching, reviewing, and comparing the content of captured network packets for known threat signatures. Behavior signatures are also compared to authorized behavior signatures. The signature-based methodology also analyzes system calls for the payload of known threats. The signature-based method is very effective against known attacks / violations, but cannot detect new attacks until it is updated with new signatures. Signature-based IDPS are easy to circumvent because they are based on known attacks and rely on new signatures that must be applied before new attacks can be detected. Attackers who change known attacks and target systems that have not been updated with new signatures that detect the change can easily bypass signature-based detection systems. The signature-based methodology requires significant resources to handle the infinite number of changes to known threats. The signature-based methodology is easier to change and improve because its performance is mainly based on provided signatures or rules. Signature-based IDS benefits from lower calculation costs, as matching recognized data traffic with a signature is an activity with lower calculation costs The general architecture of a signature-based methodology is shown in Figure 6. This architecture uses the detector to find activity signatures found in the monitored environment and compare them with known signatures in the signature database. If a match is found, a warning is issued, and there is no match, the detector does nothing.

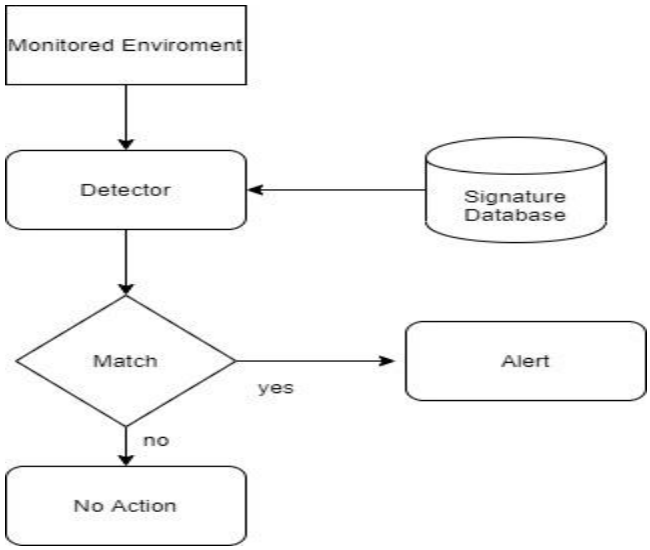

Fig 6: Signature Based IDPS

Table 3: Comparison of Detection methods and strength and weaknesses

Detection Methods		Advantages	Disadvantages
	SIDS	• Very effective in identifying intrusions with minimum false alarms (• Promptly identifies the intrusions. • Superior for detecting known attacks.	• Needs to be updated frequently with a new signature. • SIDS is designed to detect attacks for known signatures. When a previous intrusion has been altered slightly to a new variant, then the system would be unable to identify this new deviation of the similar attack. • Unable to detect the zero-day attack. • Not suitable for detecting multi-step attacks. • Little understanding of the insight of the attacks
	AIDS	• Simple design • Could be used to detect new attacks. • Could be used to create intrusion signature	• AIDS cannot handle encrypted packets, so the attack can stay undetected and can present a threat. • High false positive alarms. • Hard to build a normal profile for a very dynamic computer system. • Unclassified alerts. • Needs initial training.

Stateful Protocol Analysis

The Stateful protocol analysis method works by matching traditional profiles of how protocols should behave against the observed behavior. The established protocol profiles are designed and recognized by vendors. Stateful protocol analysis has a profound understanding of how the protocols and applications should interact/work. This deep understanding/analysis places a very high overhead on the systems (Brugger et al., 2007). Stateful protocol analysis mergers and compliments other IDPS methodologies well which has led to rise of Hybrid methodologies. Stateful protocol analysis's profound understanding of how protocol should behave is used as a base for developing IDPS that understand web traffic behavior and are effective at shielding websites. Although the Stateful protocol analysis has a deep understanding of the monitored protocols, it can be easily avoided by attacks that follow and stay within the acceptable behavior of protocols. Stateful protocol analysis methodologies and techniques have slowly been adapted and integrated into other methodologies over the past decade. This has led to the decline of IDPS

that utilize just Stateful protocol analysis methodology. The majority of the research on IDPS methodologies mainly focusses on anomaly, signature, and hybrid methodologies which further reduce the viability of Stateful protocol analysis as a standalone IDPS methodology. The general architecture of Stateful protocol analysis is shown in fig.7. This architecture is identical to that of the signature based methodology with one exception, instead of the signature database the Stateful protocol analysis has database of acceptable protocol behavior.

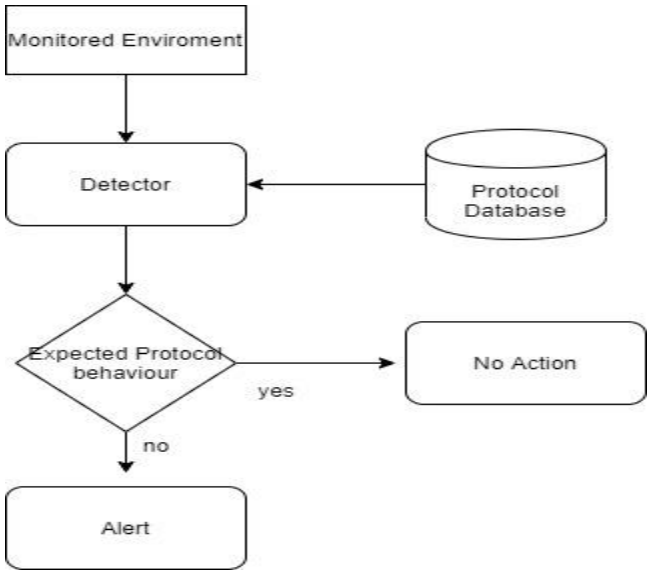

Fig 7: Stateful protocol Analysis

Hybrid Based Methodology

The hybrid-based methodology combines two or more of the other methods. The result is a better methodology that leverages the strengths of the combined methods. A hybrid system [60] combines the advantages and alleviates some of the disadvantages of the two forms of IDS. For the system proposed here, a hybrid IDS is used, which consists of several complementary parts. These include:

1. Signature detection IDS (SDIDS) that helps as a primary filter. Anything that matches or estimates a signature is treated as an intrusion and suitable action is taken. This allows well known attacks to be administered with minimal computational costs. Attacks detected by other components of the IDS can be temporarily or permanently added to the SDIDS to allow repetitive attacks to be dealt with at low computational cost.
2. Abnormal behavior detection IDS (ABDIDS) that detects behavior that significantly differs from normal and expected behavior.
3. Stateful Protocol detection IDS (SPDIDS) that detects the significant absence of expected normal behavior.

Prelude is one of the first hybrid IDS that offered a framework based on the Intrusion Detection Message Exchange Format (IDMEF) an IETF standard that allows different sensors to communicate. Snort is modified by adding an anomaly-based engine to its signature-based engine to achieve better detection. The new hybrid systems are then tested against normal Snort using the same test data. The hybrid system recognized more slumps than the normal system. A hybrid cluster-based wireless sensor network intrusion detection system has been proposed in which the detection is split in half, using an anomaly-based model to filter the data and then using a signature-based model to detect intrusion attempts. Another hybrid method model based on the functioning of the human immune system has been proposed. The proposed system is based "on the framework of the human immune system that uses a hybrid architecture that uses both approaches to detect abnormalities and abuse". An overview of a hybrid-based methodology is shown in Fig. 7, in which three other methods are combined. The monitored environment is analyzed using the first method and moves on to the next and then to the last. This creates a better system.

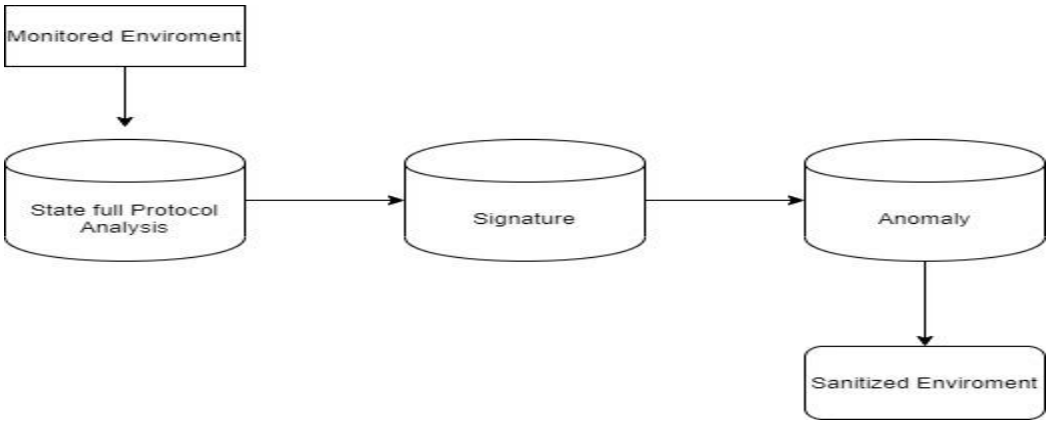

Fig 7: Working model of hybrid IDPS

The hybrid IDS can be placed into several different modes by configuring weightings between the different IDS components. In the most optimistic mode, most weight is placed on the SDIDS, with minimal weight being given to the ABDIDS and MBDIDS. Increasing the weight to either of these components makes the system more responsive to new attacks, but more likely to report false positives, as well.

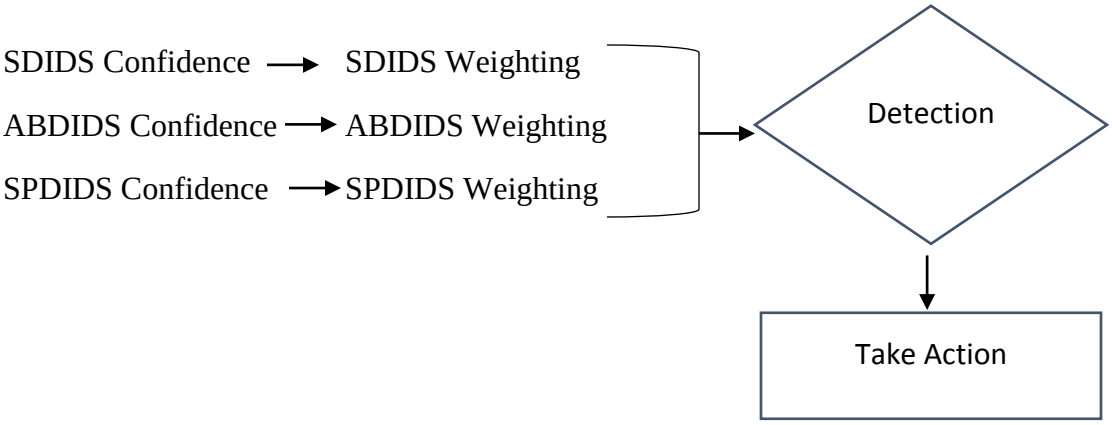

Fig 8: Model for Hybrid IDPS

Evaluation of Methodologies

Table 4: Parameters for Evaluating IDPS methodologies

	Anomaly	**Signature**	**Stateful Protocol Analysis**	**Hybrid**
Resistance to Evasion	Medium	Low	Low	High
High accuracy rate	Medium	Medium	Medium	High
Market Share	Medium	High	Medium	Medium
Scalability	Medium	High	High	Medium
Maturity Level	High	High	High	Medium
Overhead on Monitored System	Medium	Low	Low	Medium
Maintenance	Low	Medium	Medium	Medium
Performance	Medium	High	High	Medium
Easy to Configure	No	Yes	Yes	No
Easy to Use	Medium	Low	Low	Low
Protection against New	High	Low	Medium	High

Attacks				
False Positives	High	Low	Low	Low
False Negatives	High	Medium	Medium	Low

Open Source IDPS

There are Several Open Source IDPS available. Below is the description and comparison of most used IDPS. Snort, Suricata, and Bro.

Snort

Snort is an open Source Network based IDS. Open Source IDS are gradually being used as they offer benefits and ease in the prevention of security issues brought to network and system administrators. They can dynamically examine a network by providing security from intrusions in the open traffic of the Internet. There are several open source Network based IDS such as Snort, Bro, Shadow, M-Ice, Shoki, Spade, Prelude, Firestorm, AAFID etc. Snort is Most widely used open source IDPS and was created by martin Roesch in 1998. Snort has the ability to perform real-time traffic analysis and packet logging over Internet Protocol (IP) networks. Perform protocol analysis, content search, and content matching. The program can also be used to detect probes or attacks, including but not limited to operating system fingerprint attempts, common gateway interface, buffer overflows, server message block probes, and stealthy port scans. There are three main ways Snort can be configured: sniffer, packet recorder, and network intrusion detection. Sniffer modes read network packets and display them to the console in a continuous sequence. Packet recorder mode records network packets to disk. Intrusion detection mode on the network is the most complex mode. Intrusion Detection Mode monitors network traffic and scans it against a set of user-defined rules, then performs a specific action based on what has been identified.

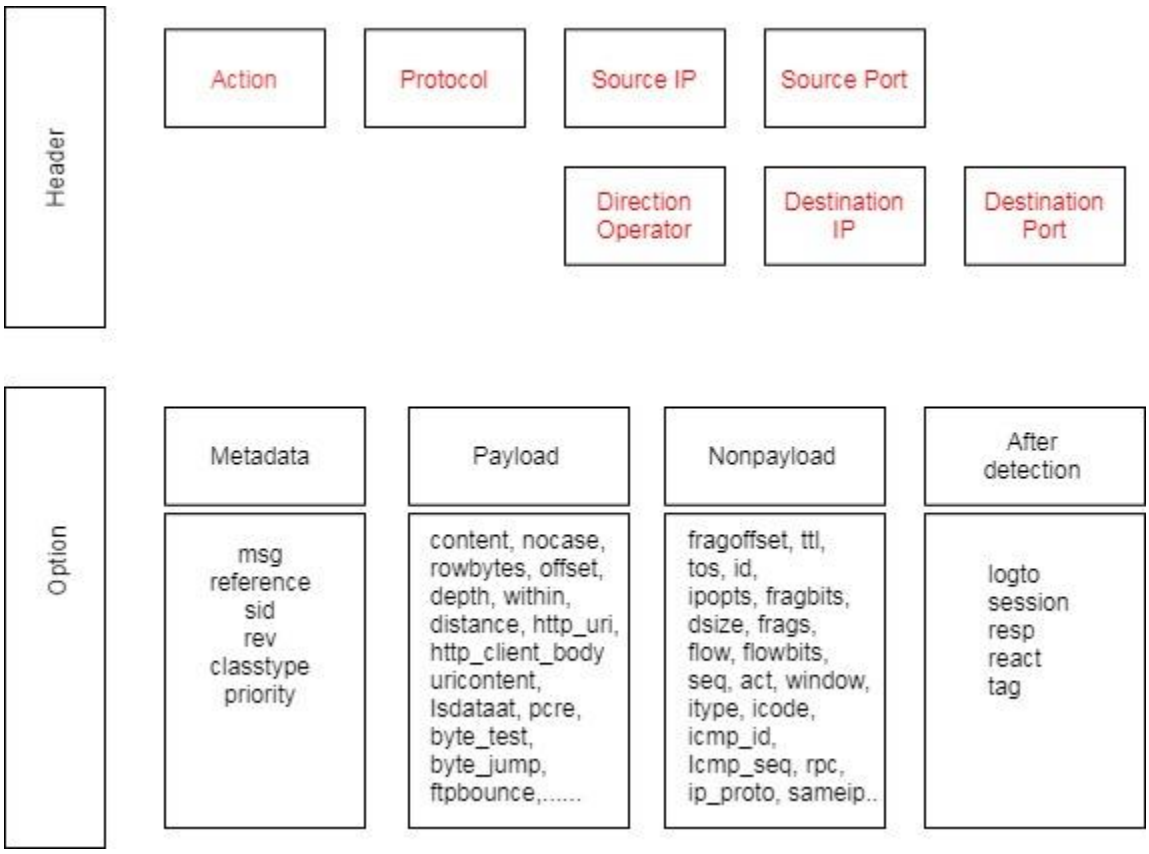

Fig 9: Basic Snort Rule Set

Bro

Bro is an open-source, Unix-based Network IntrusionDetection System (NIDS) that passively monitors network traffic and looks for suspicious activity. Bro was developed by Vern Paxson in the Network Research Group at Lawrence Berkley National Lab, and by the International Computer Science Institute in 1998. BRO has the ability to perform multi-layer analysis, Behavioral monitoring, Policy enforcement, Policy-based intrusion detection and Logging network activity Bro detects intrusions by first parsing network traffic to extract its application-level semantics and then executing event-oriented analyzers that compare the activity with patterns deemed troublesome. Its analysis includes detection of specific attacks (including those defined by signatures, but also those defined in terms of events) and unusual activities (e.g., certain hosts connecting to certain services, or patterns of failed connection attempts) (Bro (n.d.). Retrieved April, 2011 from http://www.ohloh.net/p/bro-ids 2011). Bro analyze the traffic in three phases. First Bro filters the traffic, discarding elements of minimal importance to its analysis. The remaining information is sent to its "event" engine, where Bro interprets the structure of the network packets and abstracts them into higher-level events describing the activity. Finally, Bro executes policy scripts against the stream of events, looking for activity that the rules indicate should generate alerts or actions, such as possible intrusions (Bro intrusion detection system. (n.d.). Retrieved April, 2011 from http://www.bro-ids.org 2011).

Suricata

The Suricata Engine is a next generation open source intrusion prevention and detection engine. IDS / IPS Suricata is a rule-based IDPS engine that uses externally developed rule sets to monitor network traffic and provide alerts to the system administrator when suspicious events occur. Designed to be compatible with existing network security components, Suricata offers unified outbound functionality and pluggable library options to accept calls from other applications. The initial version of Suricata runs on a Linux 2.6 platform that supports passive and online traffic monitoring configuration capable of handling multiple levels of gigabit traffic. Linux 2.4 supports reduced configuration functionality, such as no online options (Lippmann et al., 2000). Available under version 2 of the general public license, Suricata eliminates IDPS engine cost issues while offering a scalable option for the most complex network security architectures.

Comparison of Snort, Bro and Suricata

Table 5: Comparison of Snort, Bro and Suricata

Parameter	Bro	Snort	Suricata
Contextual Signatures	yes	no	yes
Flexible Site Customization	high	medium	yes
High Speed Network capability	high	medium	high
Large User Community	No	yes	yes
Configuration GUI	no	yes	yes
Analysis GUI	A few	A Lot	yes
Installation /deployment	difficult	Easy	
Operating system Compatibility	Unix	Any	Linux
Light and fast/ require extra instances	high	medium	low
Memory and Processor Resources	low	low	high

IDS Application in Various Environment's

Intrusion Detection for Web Application

Web servers are considered an important test environment for intrusion detection. The reason is that due to its importance and the universality of the HTTP protocol and the number of surprising vulnerabilities.While researchers are still exploring the signature and behavior of intrusion detection approaches, many companies are also developing commercial tools to protect web applications using different techniques. For this reason, we will introduce different and specific web IDS according to your detection approach.

Signature Approaches

Most signature-specific web IDSs are application-level host IDSs (HIDS). McHugh and Proctor adopt the principle of this approach, which is based on the use of techniques to learn known attacks and define their signatures. Once the signatures are defined, a regular expression or

pattern match is used to recognize attacks on request waves. It should also be noted that the work of Vigna was part of the intrusion detection scenarios and led to the development of an IDS called Web STAT. In the context of STAT, attacks are initially modeled in high-level language, then automatically compiled to be used as a signature for intrusion detection

Behavioral Approaches

This approach does not use any internal program information. The reference behavior model in these approaches can be defined by the application specifications or by the conclusion of learning to run the application. The approach proposed by (Forest et al., 1996) and (Hofmeyr et al., 1998). It is based on the processing of successive system process calls while executing external information in the program. The result of the experiment showed that short sequences of system calls generate a stable signature to model the normal behavior of a process according to its environment. Network Intrusion Detection Systems - Network Intrusion Detection Systems (NIDS) are placed at one or more tactical points on the network to monitor network traffic. It performs traffic analysis on the entire subnet and maps the traffic that is transmitted through the subnets to the collection of known attacks. If an attack is detected or abnormal behavior is detected, the alert can be sent to the administrator. Example. Smell.

Similarly, a gray box approach is also based on sequences of system calls. Extracts additional information from the process when memory is used. The experience of Gao et al shows that the presence of an attack often occurs during the arguments of the system calls. Based on this proposition, (Kruegel et al., 2004).

Intrusion Detection System in Cloud Environment

In this section, we will introduce different CIDS and classify them into three categories based on the intrusion detection technique used by each system. The categories are based on signatures, anomalies, and hybrids. We study the systems in each category and analyze them to assess whether or not they meet cloud security requirements.

Anomaly Based Detection

Gupta and Kumar proposed an approach to detect malware execution on client virtual machines in a cloud environment, using a new technique to detect the signature of an immediate system call. In this approach, for each unique system call (user program or system program), the list of all immediate system calls that follow it is identified and created from its normal execution logs, and these signatures are stored and then used as a baseline for an abnormal screening program.

Pandeeswari and G. Kumar proposed a system to detect anomalies in the hypervisor layer called the Hypervisor Detector. It uses a hybrid algorithm that is a mixture of the Fuzzy C-Means clustering algorithm and the artificial neural network (FCM-ANN) to improve the precision of the intrusion detection system. The general procedure for The FCMANN approach has the following three phases. In the first phase, a fuzzy grouping technique is used to divide the large data set into small groups or learning subsets.

B. Al-Shadaifatproposed an anomaly intrusion detection model to deal with attacks and security breaches in a cloud environment. The proposed approach consists of an artificial Hopefield net and simulated annealing as an aggregator. The framework of the IDS anomaly is divided into three stages: grouping of data sets, Hopfield artificial neural network (HANN) and annealing simulator.

Hybird Based Detection

P. Ghosh proposed an intrusion detection system to protect the cloud environment from intrusion, based on the collaboration of the Multithreaded Network Intrusion Detection System (NIDS) and the Host Intrusion Detection System (HIDS). The multithreaded NDIS is placed in the cloud bottleneck position, to monitor requests sent by cloud users (Kumar et al., 2016).

Ambikavathi C developed an Intelligent Intrusion Detection System (I-IDS) to improve virtual machine (VM) security, which is the foundation of the cloud computing model. The proposed model works at the virtualization layer, enhances VM security by creating VM profiles, packet flow monitoring, and periodic centralized vulnerability scans for infected VMs (Ambikavathi et al., 2015).

Intrusion Detection in Internet of Things

Tim Bass suggested that a holistic, cross-platform approach to detect unauthorized access through cyberspace should include assessing inferences from multiple perspectives. For this reason, the interaction skills proposed for the first time by Shaiek as a critical parameter in an IDS deployment measure, it was used to classify the level of holistic detection intelligence of the IDS examined. It provides a multi-perspective view of the IDS interaction with the following four levels of network service in the TCP / IP suite: network interface, Internet, transport and application levels. In addition, TCP / IP layers can be assigned to functionally similar WSN ZigBee standards (e.g. physical, MAC 802.15.4, network and application) and as encapsulation or otherwise in 6LoWPAN.

In early 2011, the IDS ideology began to change as the research did not target individual or related components, but the whole IoT. In one of these experiments, Liu et al., They applied the mechanisms of the artificial immune system to IDS3 in IoT.

More recently, computer intelligence (CI) based systems have been proposed that are adaptable and react to new situations by applying reasoning without relying on users. Examples are artificial neural networks, evolutionary calculus, artificial immune systems, swarm intelligence and fuzzy logic. Using a three-tier architecture to monitor, apply cyber intelligence and report intrusions, IDS tracks the IP addresses of the source messages and stores them in its network or in system models.

Another approach used by Kafle et. al., addressed the issue of integrating non-IP networks by assigning unique identifiers to each object. ID-based communication in heterogeneous networks called the identity sublayer has been integrated into the transmission layer for better real-time performance than traditional IDS. More recently, in 2014, Jun et al. developed a complex event processing engine (CEP) for real-time model detection between the various components of the IoT. It was compared to an IDS that first stores and then combines the data with a rule. They found that their approach consumes more CPU resources, but consumes less memory. In fact, it has been shown to work best in real time.

IDS with Lower Interaction Ability Values

The Internet (network) layer is an ideal place for a holistic approach to a rule-based discovery engine because the lower layers are hardware dependent and less abstract. The following is a review of two different IDSs operating at the network layer. The first work uses the traditional TCP / IP suite (Batalla et al., 2014) and the second experiment uses the TCP / IP suite with 6LoWPAN.

Kasinathan Batalla and Krawiec propose a type of service-oriented architecture integrated into the TCP / IP layer of the Internet to allow communication of objects regardless of their hardware or software platforms. An important technique used was registering services and objects to find and provide information about them. Overloading was avoided by using hierarchically designated routers to filter only the necessary information on the main node (Kasinathan et al., 2013).

Another promising DoS detection framework for IoT intrusion detection and built-in security was an open source IDS called Suricatamodified for IPv6 on a low power personal network (6LoWPAN). The 6LoWPAN protocol provides an IPv6 identity to objects that would not otherwise have an IP-based protocol (Kasinathan et al., 2013). Much of this work has been packet analysis that has been integrated into the IEEE 802.15.4 network layer. DoS test showedpromise. A follow-up to the Kasinathan demonstration consisted of modifying the originally open source code to integrate an advanced event monitoring system.

Intrusion Detection in Wireless Sensor Networks (WSN)

In the classification, we do the type of intrusion, the type of intruder, the detection techniques, the source of the collected data, the analysis of the location of the collected data, the frequency of use and this classification is the most complete literature in a network, the intruder type is grouped into two categories. These categories are internal intruders (selfish or malicious knot) and external intruders (an external attacker trying to reach the system) (Jurdak et al., 2011).

Anomaly Detection Approaches in WSN

According to WSN, anomalies can be grouped as network anomalies, node anomalies, data anomalies, and other anomalies. In addition to the types of WSN anomalies, approaches to detect

WSN anomalies are also important. These approaches are used to implement an IDS in WSN as a detection solution and can be combined with each other. These approaches can be classified according to statistics, the artificial immune system, machine learning, data mining, and game theory.

In the A-Game theoretical framework for robust and optimal intrusion detection in wireless sensor networks -2014, it is stated that instead of approaches using heuristic and ad hoc solutions, there is an increase in the use of analytical approaches to problems of security in WSN. Therefore, the authors propose a robust and updated stochastic game framework to analyze the problem of intrusion detection in WSN. The parameters of the game are modeled by the functionality of the WSN and its environment (Coppolino et al., 2013).

In Anomaly detection and localization in UWB wireless sensor networks - 2013, the author proposed an anomaly detection solution specially designed for ultra wideband (UWB) technology. In the document, it is described that UWB is a key solution to serve low power consumption while wireless connectivity. To identify intrusions, a rules-based approach is accepted and the performance of the proposed algorithm is studied by simulations. The algorithm proposed in the article uses a round-based approach (There are particular phases.) Towards the cluster structure and the detection of anomalies based on rules. Test results presented on paper indicate successful detection accuracy.

In Application of data mining techniques to intrusion detection in wireless sensor networks - 2013, it is proposed that the application using data mining approaches for the intrusion detection system in the wireless sensor network and the proposed system can perform both an anomaly detection technique and an abuse detection technique. The IDS consists of a central agent and several local agents, who are placed on the sensors and perform intrusion detection activities. A data mining approach is used on each agent (local agents, central agents). Test results show that high detection accuracy is obtained while maintaining an acceptable, but not negligible, rate of false positives.

Misuse Detection Approaches in WSN

Also called signature-based IDS, it successfully detects known attacks. Its drawback is that it cannot detect new unknown attacks or attacks without predefined rules. Using the abuse detection technique is a complex task for WSN due to WSN restrictions. For example, maintaining attack signatures is very difficult and less effective. In the literature, we see that some studies use an abuse detection technique and propose a surveillance approach and a mobile agent approach.

In detecting intrusions in wireless sensor networks using the watchdog-2013 based clonal selection algorithm, the watchdog approach is used to detect if a node behaves abnormally during data transmission. All WSN nodes are responsible for monitoring neighbors and transferring behavioral information. Bad node behavior negatively affects WSN performance.

Using the watchdog-based clonal selection algorithm, it aims to detect the malicious and selfish nodes of WSN.

Hybrid Detection Approaches in WSN

It is described that some specification-based solutions have been proposed and the main drawback of this solution is that the development of protocol specifications is man-made. WSN security protocols are manually defined by the administrator. The author describes this approach with three techniques and hybrid detection is involved in this classification as the third subtitle.

In the new hybrid intrusion detection system for the clustered wireless sensor network - 2011, the goal is to combine approaches based on anomaly detection and abuse (signature) to obtain a more accurate intrusion detection system. Anomaly detection uses a distributed learning algorithm for the formation of an SVM to solve the problem in two classes (distinguishing between normal and abnormal activities). The purpose of this study is described as energy saving.

Intrusion Detection in Mobile Ad-Hoc Networks (MANET)

J Martin and S. Shanmugavel developed a secure routing approach called Resiliency Oriented Secure (ROS) in 2006 that includes the detection phase in routing to detect the malicious node [105]. To detect the malicious node, they used various update fields in the routing table and set a threshold value for it. Each time a node receives a routing packet that has an update in its routing table, it increments the number of update fields by one. When the count values exceed the threshold values, an alarm signal is triggered. R.Ranjana and M. Rajaram in 2007 proposed a model that does not work any changes to the underlying protocol and used an additional security component to detect manufacturing attack, resource consumption attack, and packet loss attack. Using an extended architecture, IDSX is a cluster based solution and acts as a second line of defense Any IDS solution could be implemented by individual nodes. The IDSX solution is compatible with any IDS solution that serves as the first line of defense. The IDSX produced virtually no false positives based on the simulation results. In fact, it forms a consensus on the responses of the different individual IDS solutions implemented on the nodes. Anomaly-based intrusion detection schemes could be implemented as a first line of defense. IDSX operates within predefined limits. These are quite practical and sufficiently achievable given the nature of ad hoc networks. However, some of them can also be considered limiting restrictions. The proposed two-step approach would also make the task of detecting intrusions costly in terms of energy and resource consumption.

In, a solution called eSOM is described using the concept of unsupervised learning in artificial neural networks using self-organizing maps. The technique used a data structure called a matrix U that is used to represent the data classes. These regions represent malicious information and are marked with the Block-Wise method. Regions representing the benign data class are marked with the Lattice method. When a new attack is launched, it changes the pixel

values. The watermark technique and eSOM can identify together if a pixel has been modified and this makes it very sensitive to intrusion detection. The authors claim that eSOM is SO% efficient and remains constant even with variations in mobility. Using eSOM, IDSs would be trained at regular times. This affects the energy efficiency of the algorithm and incurs additional costs. However, the proposed intrusion detection engine has not been used in various routing protocols for detection of various types of attacks.

Ningrinla marching and Raja Datta have developed "a collaborative technique to detect intrusions in MANET". They proposed two intrusion detection techniques for ad hoc mobile networks, which use the collaborative efforts of nodes in a neighborhood to detect a malicious node in that neighborhood. The first technique is proposed for detecting malicious nodes in a node neighborhood where each pair of nodes in the neighborhood are within radio range of each other and that node neighborhood is known as a click.

Intrusion Detection in Voice Over Internet Protocol (VOIP)

VolP security issues and solutions are increasingly important to the success of VoIP services, particularly in the area of intrusion and intrusion detection. By targeting an effective, flexible and holistic approach to VolP security management. We suggest the use ofan appropriate mobile agent system in an integrated framework that can be applied specifically to VoIP, as well as to modem network management in general

IP transmissions are inherently insecure. As a result, VoIP applications would face security threats inherited from IP networks. In this article, the author classifies attacks on Internet infrastructure into Sour categories: DNS hacking, routing table poisoning, packet abuse, and DoS, and analyzes the impact of this type of intrusion on the Internet.

In addition, the development of the smart network using SS7 (signaling system No. 7) offers greater flexibility to the network thanks to the introduction of new services, but increases its vulnerability to the misuse of these services because certain services allow users to access to information management. Free phone service is an example. Mobile technology also has an impact on telephone security. The previous attacks would also affect VoIP users because VolP networks involve traditional telephone equipment.

VolP relies on various protocols to deal with different aspects of a "call". Protocols related to IP telephony were not initially designed with security as the primary design objective. Although some of these protocols have added security features in their recent versions, the security mechanisms are not secure enough or are not yet practical. This section discusses the security features of the VolP standards currently used in the construction of VolP systems, including SIGTRAN.

Conclusion

Cyber criminals target computer users using sophisticated techniques and social engineering strategies. Some cybercriminals are becoming more sophisticated and motivated. Cyber criminals have demonstrated their ability to conceal their identity, conceal their communication, keep their identity away from illegal profits, and use a compromise resistant infrastructure. As a result, it is increasingly important to protect computer systems using advanced intrusion detection systems capable of detecting modern malware. To design and build such IDS systems, it is necessary to have a complete overview of the strengths and limitations of contemporary IDS research. In this paper, we present in detail a study of the methodologies, types and technologies of intrusion detection systems with their advantages and limitations. Several proposed machine learning techniques to detect zero-day attacks are reviewed. However, such approaches may have the problem of generating and updating information on new attacks and generating high false alarms or poor precision. A computer network is made up of two components, namely hardware and software. These two components can present their own risks and vulnerabilities. In this article, we have studied different types of intrusion detection models in different cases. This article introduces Intrusion Detection Systems (IDS) in various areas. It includes a web application, a cloud environment, the Internet of Things (IoT), an ad hoc mobile network (MANET), a wireless sensor network (WSN), and a Voice over Internet Protocol (VOIP). We have discovered that IDS is an important part of the network security system. The development of IDS capable of overcoming escape techniques remains a major challenge for this area of research. We have summarized the results of recent research and explored contemporary models for improving AIDS performance as a solution to overcome IDS problems. This study also examines four common escape techniques to determine your ability to escape from recent IDSs. An effective IDS should be able to accurately detect different types of attacks, including intrusions and corporate escape techniques.

Acknowledgement

Authors are thankful to the Editorial Team for their constructive support.

References

Ahmed, G., Hussain, M., & Khan, M. N. A. (2014). Characterizing Strengths of Snort-based IDPS. *Research Journal of Recent Sciences 3*(1), 176-182.

Alcaraz, C. (2018). Cloud-assisted dynamic resilience for cyber-physical control systems. *IEEE Wireless Communications, 25*(1), 76-82.

Ambikavathi, C., & Srivatsa, S. K. (2015). Improving virtual machine security through intelligent intrusion detection system. *Indian Journal of Computer Science and Engineering (IJCSE), 6*(2), 39-45.

Annachhatre, C., Austin, T. H., & Stamp, M. (2015). Hidden Markov models for malware classification. *Journal of Computer Virology and Hacking Techniques*, *11*(2), 59-73.

Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H., & He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, *378*(2), 484-497.

Bace, R. (1999). An introduction to intrusion detection and assessment for system and network security management. *ICSA Intrusion Detection Systems Consortium Technical Report*. *14*(1), 138-145.

Barghi, M. N., Hosseinkhani, J., & Keikhaee, S. (2015). An effective web mining-based approach to improve the detection of alerts in intrusion detection systems. *International Journal of Advanced Computer Science and Information Technology (IJACSIT),(ELVEDIT)*, *4*(1), 38-45.

Batalla, J. M., & Krawiec, P. (2014). Conception of ID layer performance at the network level for Internet of Things. *Personal and Ubiquitous Computing*, *18*(2), 465-480.

Brugger, T. (2007). KDD Cup'99 dataset (Network Intrusion) considered harmful. *KDnuggets newsletter*, *7*(18), 15-29.

Chen, C. M., & Lin, H. C. (2015). Detecting botnet by anomalous traffic. *journal of information security and applications*, *21*(3), 42-51.

Coppolino, L., DAntonio, S., Garofalo, A., & Romano, L. (2013, October). Applying data mining techniques to intrusion detection in wireless sensor networks. In *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing* 13(2),247-254

Duque, S., & bin Omar, M. N. (2015). Using data mining algorithms for developing a model for intrusion detection system (IDS). *Procedia Computer Science*, *61*(3), 46-51.

Elhag, S., Fernández, A., Bawakid, A., Alshomrani, S., & Herrera, F. (2015). On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems. *Expert Systems with Applications*, *42*(1), 193-202.

Forrest, S., Hofmeyr, S. A., Somayaji, A., & Longstaff, T. A. (1996, May). A sense of self for unix processes. In *Proceedings 1996 IEEE Symposium on Security and Privacy 25*(1),120-128.

Friedberg, I., Skopik, F., Settanni, G., & Fiedler, R. (2015). Combating advanced persistent threats: From network event correlation to incident detection. *Computers & Security*, *48*(1), 35-57.

Gao, D., Reiter, M. K., & Song, D. (2004, October). Gray-box extraction of execution graphs for anomaly detection. In *Proceedings of the 11th ACM conference on Computer and communications security 15*(6), 318-329.

Hofmeyr, S. A., Forrest, S., & Somayaji, A. (1998). Intrusion detection using sequences of system calls. *Journal of computer security*, *6*(3), 151-180.

Jurdak, R., Wang, X. R., Obst, O., & Valencia, P. (2011). Wireless sensor network anomalies: Diagnosis and detection strategies. In *Intelligence-Based Systems Engineering 25*(6), 309-325.

Kar, D., Panigrahi, S., & Sundararajan, S. (2015, February). SQLiDDS: SQL injection detection using query transformation and document similarity. In *International Conference on Distributed Computing and Internet Technology 22*(4), 377-390).

Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C., & Spirito, M. A. (2013, November). An IDS framework for internet of things empowered by 6LoWPAN. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security 18*(6), 1337-1340.

Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013, October). Denial-of-Service detection in 6LoWPAN based Internet of Things. In *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)* 1*2*(6), 600-607. IEEE.

Kaur, J., Singh, R., & Kaur, P. (2015). Prevention of ddos and brute force attacks on web log files using combination of genetic algorithm and feed forward back propagation neural network. *International Journal of Computer Applications*, *120*(23), 355-382.

Kenkre, P. S., Pai, A., & Colaco, L. (2015). Real time intrusion detection and prevention system. In *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014 34*(6), 405-411.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1-22.

Koo, T. M., Chang, H. C., Hsu, Y. T., & Lin, H. Y. (2013, July). Malicious website detection based on honeypot systems. In *2nd International Conference on Advances in Computer Science and Engineering (CSE 2013) 25*(6), 76-82.

Kour, H., & Sharma, L. S. (2016). Tracing out cross site scripting vulnerabilities in modern scripts. *International Journal of Advanced Networking and Applications*, *7*(5), 2862-2879.

Kshetri, N., & Voas, J. (2017). Hacking power grids: A current problem. *Computer*, *50*(12), 91-95.

Kumar, K. (2016, December). An efficient network intrusion detection system based on fuzzy C-means and support vector machine. In *2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE) 27*(2), 1-6).

Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-based systems*, *78*(1), 13-21.

Lippmann, R. P., Fried, D. J., Graf, I., Haines, J. W., Kendall, K. R., McClung, D., ... & Zissman, M. A. (2000, January). Evaluating intrusion detection systems: The 1998 DARPA off-

line intrusion detection evaluation. In *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00 25*(2), 12-26.

Rath, P. S., Barpanda, N. K., Singh, R. P., & Panda, S. (2017). A prototype Multiview approach for reduction of false alarm rate in network intrusion detection system. *International Journal of Computer Networks and Communications Security*, *5*(3), 49-63.

Sadreazami, H., Mohammadi, A., Asif, A., & Plataniotis, K. N. (2017). Distributed-graph-based statistical approach for intrusion detection in cyber-physical systems. *IEEE Transactions on Signal and Information Processing over Networks*, *4*(1), 137-147.

Seeber, S., & Rodosek, G. D. (2015, June). Towards an adaptive and effective IDS using OpenFlow. In *IFIP International Conference on Autonomous Infrastructure, Management and Security*, *21*(2),134-139.

Shen, C., Liu, C., Tan, H., Wang, Z., Xu, D., & Su, X. (2018). Hybrid-augmented device fingerprinting for intrusion detection in industrial control system networks. *IEEE Wireless Communications*, *25*(6), 26-31.

Somwanshi, A. A., & Joshi, S. A. (2016). Implementation of honeypots for server security. *International Research Journal of Engineering and Technology (IRJET)*, *3*(03), 285-288.

Studnia, I., Alata, E., Nicomette, V., Kaâniche, M., & Laarouchi, Y. (2018). A language-based intrusion detection approach for automotive embedded networks. *International Journal of Embedded Systems*, *10*(1), 1-12.