I.J. Computer Network and Information Security, 2014, 8, 56-70
Published Online July 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.08.08

A New Classification Scheme for Intrusion Detection Systems

Bilal Maqbool Beigh
Department of Computer Science, University of Kashmir, Srinagar, India
Email: bilal.beigh@gmail.com

Abstract—In today's world, overall global mostly depend on technologies for their information storage and transactions. But this frequent use of online technologies make the data stored exposed to the risk of attacks towards the data in the form of intrusion. In order to save our data from these attacks, the researchers had implemented a concept called intrusion detection system, with the help of detection technology the users can prevent their critical data from different kind of attacks. As we know that there are lots of intrusion detection system in market which are either open source and some of them are commercial. Although the number is very high but there is no such classification available in research literature which will help user or security professionals. In this paper we will present a good and elaborated classification based on various parameters which will help the researchers and security professional to understand the category. The paper will also provide a brief detail of those categories which will give idea of representing the intrusion detection techniques.

Index Terms—Network, Intrusion Detection, techniques, Security, attacks, hackers, classification.

I. Introduction

Communication technologies and trends have changed very drastically over last two decades. These days, every organization (either big or small) is maintaining an online profile thus sharing the important as well as non-important resources over the globe [1]. Due to this online profiling, the digital data over the networks have increased marginally. According to the report prepared by Computer Emergency Readiness Team Group (CERT)] [2], the digital data have increased by 200 % during the years and made it more difficult to handle [3]. Thus gives an opportunity to the attackers or hacker to Mis-use or destroy the information available. As we know that every computer is at risk but with sensitive and private information, they are at higher risk. In information security, Intrusion Detection is a key technique which will hunt down the attackers and secures the network systems. Intrusion Detection is the system which observes and analyzes the events generated in a computer or network system to identify maximum security problems. The Intrusion Detection system (IDS) is used to monitor the network assets to detect any thing un-usual [4] [5].Intrusion Detection System monitors the operations of firewalls, routers, management servers and files critical to other security mechanisms. Intrusion Detection System can make the security management of system by non-expert staff possible by providing user friendly interface [6]. The concept of intrusion detection has been for nearly two decades, but it attains attention very recently and that too very huge because of increasing number of attacks on network data. The concept of intrusion detection system starts in 1980 with the James Anderson's paper [7] "Computer Security Threat Monitoring and Surveillance" which discusses the concept of monitoring the data over the local network by using some predefined profiles. With the publication of this paper, the concept of intrusion and audit data came into lime light. This beautiful concept made lot of improvement in auditing subsystems. This paper officially laid the foundation of design and development of intrusion detection systems [6]. The paper describes the basic layout for containing audit trails, which was very much useful in understanding the behaviour of users. His concept makes an impressive impact on the world of security systems. Later In 1984, The Company named SRI International hired Dr. Dorothy Denning and Peter Neumann to work on a government project. This project adds a new passion in the intrusion detection development. The main aim of the project was to conduct an audit trails for government mainframe computers by creating users profile based on their daily activities. In approximately one year, Dr. Denning helps the SRI international to develop the first model for intrusion detection system "Intrusion Detection Expert System (IDES)" **[7].** Also SRI developed a method of hunting and analyzing the data used by the people over real internet called APRNET for authentication information of the users. These concepts laid down possibility track for today's commercial Intrusion detection systems. In 1989, a developer group formed a commercial company namely "Haystack Labs" which releases the first ever commercial intrusion detection system known as "Stalker "in 1990 [8]. According to documentation available, the stalker was a host based, pattern matching system that have a robust search mechanism to query the audit data using both mechanisms i.e. manually as well as automatically. During the period, in which the Haystack were busy in developing their product for intrusion detection, simultaneously, the company SAIC was also busy in developing a host based intrusion detection system called as "Computer Misuse Detection System (CMDS)". Also simultaneously, the Air Force crypto support system developed the system called as “Automated Security Measurement System (ASIM)”. The main aim of the system was to monitor the traffic on the US Air Force’s Network [9] [10]. The ASIM was the first system to incorporate both hardware and software solution to the intrusion detection. The project ASIM is still in existing mode and is running and maintained by Air Force's Computer Emergency Response Team (AFCERT). Soon after completion of the project at Air Force, Soon after the completion of the project at US air Force, in 1994 the developer from US Air Force formed their own commercial company namely “Wheel Group” and their first commercial product “Net Ranger” was released. In around 1997, the security market leader at that time, ISSI developed intrusion detection system namely “Real Secure”. A year after, in 1998, Cisco feels the need of security of their products, they decide to purchase the company Wheel Group in order to provide a combined security solution to their customers. Similarly the formation of company called “Centrex Corporation” came into existence with the merging of two companies i.e. CMDS and SAIC [11] [12].This was the era form where the boost in the design and development of intrusion detection came. Also on December 22, 1998, Marty Roesch released first the first version of SNORT [Marty Roesch reference]. At that time SNORT was only available for UNIX platform and was limited, but was capable of performing real-time packet analysis and logging.

Later in 1999, Lawrence Berkeley National Laboratory made announcement of release of Bro intrusion detection system [13]. The system uses lipcap data for capturing data and has their own rules for analysis of intrusion detection system [14]. In the same year, a packet sniffer was developed by the name of APE [15], but was later renamed as SNORT after one month and is one of the most famous intrusion detection system with over 3000,000 active users. During last one decade the intrusion detection has made very rapid growth and has adopted many techniques from distinguished fields for the purpose of detection of intrusion. The road map of intrusion begins to attain different methodologies from different fields like as biology etc.

Here in this paper the section II will provide some elaboration about the need for classification of existing techniques, section III will provide the details about the existing classification scheme, section IV will provide a new classification scheme and then section V provides conclusion and future scope.

II. Need for Classification

Classification has delivered important meanings in our life. In general, classification can be defined as a means of grouping the similar things together having common qualities or characteristics. Classification has essential part to play especially in assisting in the search and selection process. By classifying things into different segments it enables us to retrieve things or information that we needed to look for, without the risk of too much time consuming in retrieving that particular things or information. When we want to search a particular specified thing or information in departmental store, for example we want to look for “T-Shirt”, we will automatically look for “clothing section” from departmental store because T-shirt is classified as a cloth and the term is broad generalized of classification of T-Shirt. Thus Classification can be used as a tool for very simple yet infinitely crucial purpose. Its purpose is to secure an order which will be useful to users and to those who seek information with the smallest complication of search, also known as a technique designed to expedite the full use of the knowledge stored in books and other material housed in the collection.

The security is very important aspect for an organization. The organization needs to implement a security solution or procedure. As there are many security solutions available in the market thus an organization needs a better classification scheme to fulfill the criteria based on their requirements and needs. Although some authors have given a classification schema but does not fulfill all the cardinalities which an organization requires in its requirement lists, thus a better and full-fledged classification schema needs to be drafted and developed which will make it easy for an organization to choose an intrusion detection systems according to their needs and requirements.

III. Existing Classification schema

Up to the current situation, different researchers have proposed different classification schema. In paper authored by “V. Jaiganesh, S. Mangayarkarasi and Dr. P. Sumathi” **[5],** where they mentioned that the intrusion detection system can be divided in two broad categories: host-based (HIDS) and network-based (NIDS). Also in another paper authored by “Asmaa Shaker Ashoor and Sharad Gore” [6] stated that the intrusion detection systems can be classified into three types:

- Anomaly based.
- Signiture based.
- Hybrid detection.

Other paper drafted by “Suhair H. Amer, and John A. Hamilton, Jr.” [16], were the author stated that the intrusion detection can be categorized into the following groups:

i. Rule Based
ii. Artificial Intelligence (AI)
iii. Data Analysis
iv. Computational Methods

Again the researcher namely “Jaime Daniel Mejía Castro, Jorge Maestre Vidal, Ana Lucila Sandoval Orozco, Luis Javier García Villalba” [17] have put forward another classification shown as under:

i. Statistical Based
ii. Knowledge based
iii. Machine Learning

Peng Ning & Sushil Jajodia, [18] in his paper has provided classification of the intrusion detection based on the position of deployment of the intrusion detection system. The classifications are as under:

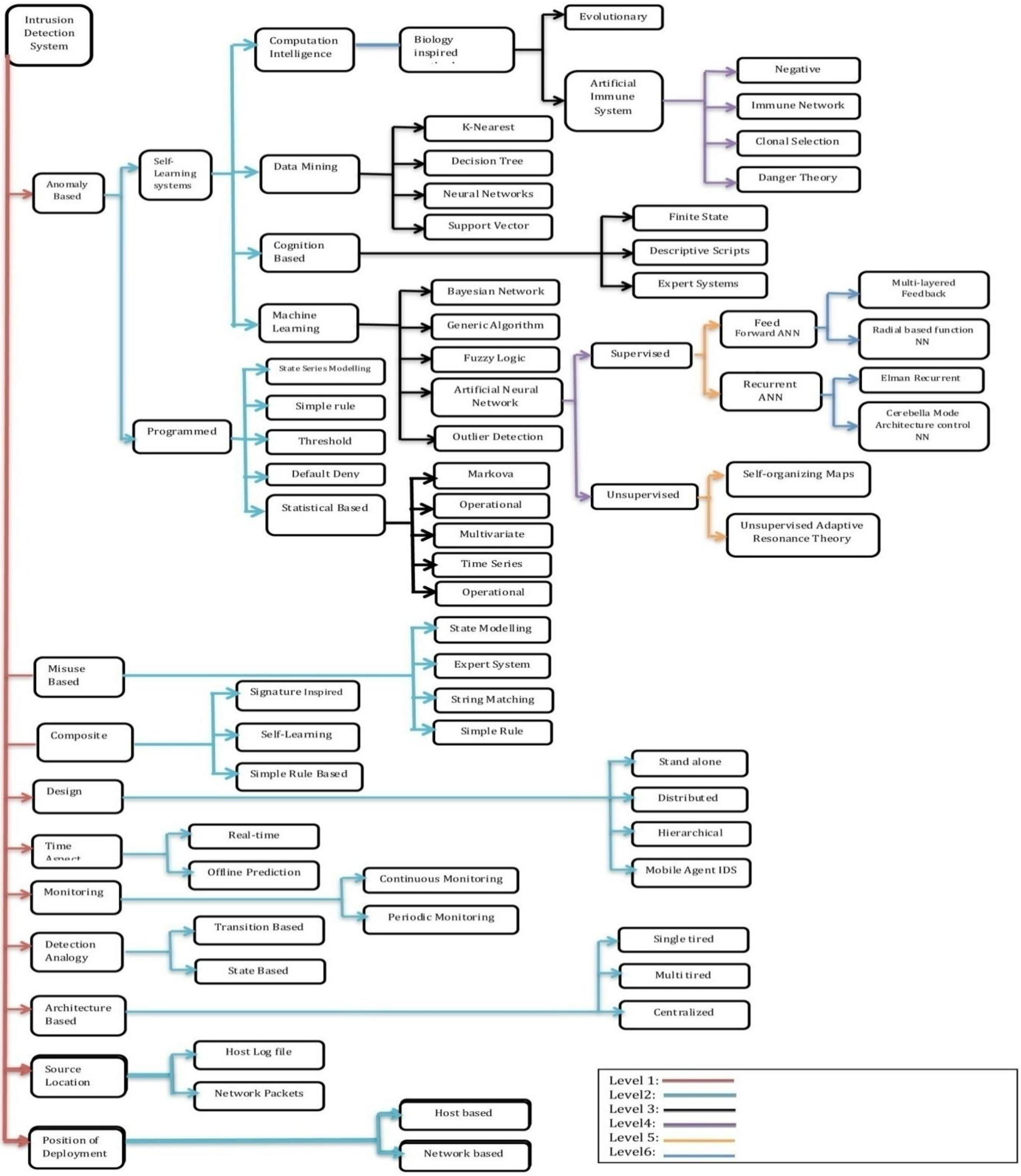

Fig. 1: classification of Intrusion detction system

1. Host Based intrusion detection system
2. Network Based intrusion detection system.
3. Hybrid intrusion detection system.

As surveyed from many papers, intrusion detection system classification is in fuzz and need proper attention towards a better classification. So we have proposed a new classification based on previous classification, literature survey and knowledge gained. The proposed classification will be followed in next section.

IV. Proposed classification Schema

As also mentioned in previous sections, different classifications have been proposed but none of them was fully accountable. I.e. none of the schema has made the suitable position for all the existing intrusion detection system. In order to understand the nature and working mechanisms, we are in need of a better classification schema. So here in this research thesis, we have proposed a better classification schema, which will classify all the existing intrusion detection system very minutely. The proposed classification schema is shown in Figure 1. In the figure we have classify the existing intrusion detection system up to six levels of classification. The levels are differentiated by colours. Each level is being developed after the surveying the proper literature available on that particular technique. The proposed technique has been developed to keeping in view all the techniques. Here we will discuss all the mentioned quantifiable classification elements in detail one by one. Our classification schema is firstly categorized into some broad category which are further refined and made a deep classification. As shown in Figure1, classification schema have first category as “Anomaly Based detection” The anomaly based detection schema has been further divided into many categories shown in Figure 2 and discussed below:

A. Anomaly Based Detection

Anomaly detection is based on the normal behavior of a subject (e.g., a user or a system); any action that significantly deviates from the normal behavior is considered as intrusive. Anomaly based technique uses profile matching mechanism, i.e, normal and abnormal behaviour. In this technique, a base line of NORMAL data is being set after training the data for normal behaviour. If the incoming string or data deviates from its base-line of NORMAL, the traffic will be considered as anomaly otherwise not [19] [20] [21] [67].

Anomaly detection can be further divided into two categories as under:

1. Self-Learning.
2. Programmed.

1. **Self-Learning:** As per the English dictionary self-learning is the Learning done by oneself, without a teacher or instructor. Thus we can say that self-learning intrusion detection system mechanism are the systems which will learn it-self for the detection mechanisms. Self-learning systems learn by example, which constitutes base line for normal. Typically by observing traffic for an extended period of time and building some model of the underlying process. Here in our proposed classification the self learning has been further divided into four categories as under:

   i. Biology Inspired
   ii. Data Mining
   iii. Cognitive Based
   iv. Machine Learning

These sub sets have been further categorized as under:

i. Biological Inspired:

Biological organisms cope with the demands of their environments using solutions quite unlike the traditional human-engineered approaches to problem solving. Biological systems tend to be adaptive, reactive, and distributed. Bio-inspired computing is a field devoted to tackling complex problems using computational methods modeled after design principles encountered in nature. This course is strongly grounded on the foundations of complex systems and theoretical biology. It aims at a deep understanding of the distributed architectures of natural complex systems, and how those can be used to produce informatics tools with enhanced robustness, scalability, flexibility and which can interface more effectively with humans. It is a multi-disciplinary field strongly based on biology, complexity, computer science, informatics, cognitive science, robotics, and cybernetics. This field has been further divided into two categories as under:

1. Evolutionary

Evolutionary methods (Biologically driven) are mechanisms inspired by biological evolution, such as reproduction, mutation and recombination.

2. Artificial Immune System.

Immune based IDS are developed based on human immune system concepts and can perform tasks similar to innate and adaptive immunity. In general, audit data representing the appropriate behavior of services are collected and then a profile of normal behavior is generated [22] [16]. One challenge faced is to differentiate between self and non-self data which when trying to control causes scaling problems and the existence of holes in detector sets. The field of computer science uses artificial immune system (AIS) as a category of computational intelligent systems inspired by the biological process of immune system of vertebrates.

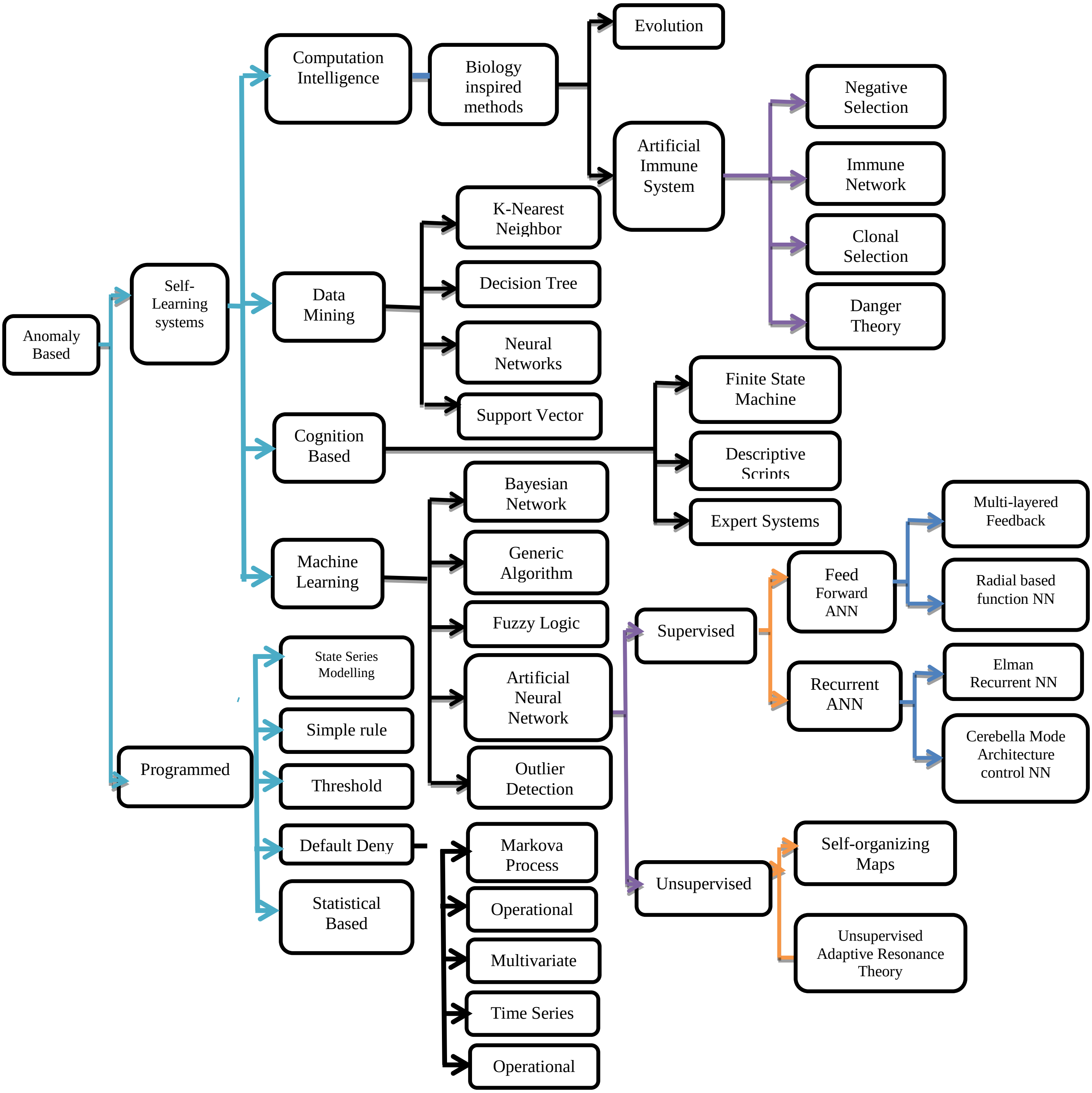

Fig. 2: Anomaly Based IDS

The field of computer science uses the characteristics and principles of human immune system for the purpose of learning and memorizing the events or things. This field has emerged as a computational tool or technique towards solving computational problems from mathematics, IT and engineering etc. Now-a-days the AIS are being used to design and development of intrusion detection systems. There have been several attempts to implement immunity-based systems. Some have experimented with innate immunity which is the first line of defense in the immune system and is able to detect known attacks. For example, Twycorss and Aickelin [23] implemented libtissue that uses a client/server architecture acting as an interface for a problem using immune based techniques. [24].

Furthermore Artificial Immune system has been categorized into four categories as shown under:

a. Negative Selection

Negative selection algorithm is basically inspired by positive and negative selection processes, which occurs during the maturation of T-Cells in the thymus called T-Cell tolerance. Negative selection refers to the identification and deletion of self-reacting cells that is T cells that may select for and attack self tissues. This class of algorithms is typically used for classification and pattern recognition problem domains where the problem space is modeled in the complement of available knowledge. For example in the case of an anomaly detection domain the algorithm prepares a set of exemplar pattern detectors trained on normal (non-anomalous) patterns that model and detect unseen or anomalous patterns.

b. Immune Network

This Algorithm is basically driven from the idiotypic network theory proposed by Niels Kaj Jerne that describes the regulation of the immune system by anti-idiotypic antibodies (antibodies that select for other antibodies). The algorithms focus on the network graph structures involved where antibodies (or antibody producing cells) represent the nodes and the training algorithm involves growing or pruning edges between the nodes based on affinity (similarity in the problems representation space). Immune network algorithms have been used in clustering, data visualization, control, and optimization domains, and share properties with artificial neural networks [25].

c. Clonal Selection

The Clonal selection algorithm is used by the natural immune system to define the basic features of an immune response to an antigenic stimulus. It establishes the idea that only those cells that recognize the antigens are selected to proliferate. The selected cells are subject to an affinity maturation process, which improves their affinity to the selective antigens [26].

d. Danger Theory

This Algorithm gives a new direction to information security; the algorithm suggests that the immune system reacts to counter the danger signals. It also provides a method of ‘grounding’ the immune response, i.e. linking it directly to the attacker. Little is currently understood of the precise nature and correlation of these signals and the theory is a topic of hot debate [27].

ii. Data Mining:

According to R.L. Grossman [28] in "Data Mining: Challenges and Opportunities for Data Mining during the Next Decade", he defines data mining as being "concerned with uncovering patterns, associations, changes, anomalies, and statistically significant structures and events in data." Simply put it is the ability to take data and pull from it patterns or deviations which may not be seen easily to the naked eye. Another term sometimes used is knowledge discovery [16], [28].

iii. Cognitive Approach:

Cognition refers to mental activity including thinking, remembering, learning and using language. When we apply a cognitive approach to learning and teaching, we focus on the understanding of information and concepts. If we are able to understand the connections between concepts break down information and rebuild with logical connections, then our rention of material and understanding will increase. When we are aware of these mental actions, monitor them and control our learning processes it is called metacognition [16]

iv. Machine Learning:

Machine learning is a system capable of acquiring and integrating the knowledge automatically. The capability of the systems to learn from experience, training, analytical observation, and other means, results in a system that can continuously self-improve and thereby exhibit efficiency and effectiveness. A machine learning system usually starts with some knowledge and a corresponding knowledge organization so that it can interpret, analyze, and test the knowledge acquired. [29] Machine learning techniques are based on establishing an explicit or implicit model that enables the patterns analyzed to be categorized. A singular characteristic of these schemes is the need for labeled data to train the behavioral model, a procedure that places severe demands on resources. In many cases, the applicability of machine learning principles coincides with that for the statistical techniques, although the former is focused on building a model that improves its performance on the basis of previous results. Hence, a machine learning IDS has the ability to change its execution strategy as it acquires new information. Although this feature could make it desirable to use such schemes for all situations, the major drawback is their resource expensive nature [30]. The machine learning have been further divided into five different categories which are as under:

a. Bayesian Network.

Bayesian networks also known as Belief

Networks or Bayes Nets for short is basically from the family of probability graphical model (GM's) [30], [31]. The system is used to describe the conditional probability of a set of possible causes for a given observed events. These types of networks are mainly suitable for complex pattern matching. They are suitable for extracting complex patterns from sizable amounts of input information that can also contain significant levels of noise. Several systems have been developed using Bayesian network concepts. In the following system, Scott's [32] IDS is based on stochastic models of user and intruder behavior combined using Bayes theorem which mitigates the complexity of network transactions that have complicated distributions. Intrusion probabilities can be calculated and dynamic graphics are used to allow investigators to use the evidence to navigate around the system. [16]

b. Generic Algorithm.

Genetic algorithms are a family of problem-solving techniques based on evolution and natural selection. Potential solutions to the problem to be solved are encoded as sequences of bits, characters or numbers. The unit of encoding is called a gene, and the encoded sequence is called a chromosome. The genetic algorithm begins with chromosomes population and an evaluation function that measures the fitness of each chromosome. Finally, the algorithm uses reproduction and mutation to create new solutions [16] [66].

c. Fuzzy Logic.

Fuzzy logic is an approach which is based on Boolean logic. It provides the opportunity for modelling conditions that are inherently imprecisely defined. Fuzzy technique is of the form of approximating the decision with the powerful reasoning capabilities. Dr Zadeh [33] introduces the term fuzzy logic. Fuzzy logic is a multi-valued logic, which allows intermediate values to be defined between conventional evaluations [34].

d. Artificial Neural Network.

Artificial Neural Network is a system based on the basic principles of biological neural networks. This field contains a large number of interconnected processing elements (neurons) working with each other to solve a particular problem [35].

e. Outlier Detection.

An outlier is based on the concept of deviation of observations, which deviates from the already observation in order to give alert of the suspicious that it was generated by a different mechanism [36].

Furthermore the Artificial Neural Network has been categorized into two categories.

a. Supervised Learning

Supervised learning is a form of machine learning technique which sets the parameters of an artificial neural network from training data [37]. The process of learning of artificial neural is a set of steps. Firstly we have to set the value of its valid input parameters after having seen output value. The training data consist of pairs of input and desired output values that are traditionally represented in data vectors. Supervised learning can also be referred as classification, where we have a wide range of classifiers, each with its strengths and weaknesses. Choosing a suitable classifier for a given problem is however still more an art than a science. The different types of supervised type learning are as:

i. Feed Forward ANN

In such an ANN solution, the data moves from the input to the output units in a strictly feed-forward manner. Data processing may spawn multiple layers, but no feedback connections are implemented. Examples of feed-forward ANN's would be a Perceptron (Rosenblatt) or an Adaline (Adaptive Linear Neuron) based net [38].

i. Recurrent ANN

These types of ANN's incorporate feedback connections. Compared to feed- forward ANN's, the dynamic properties of the network are paramount. In some circumstances, the activation values of the units undergo a relaxation process so that the network evolves into a stable state where these activation values remain unchanged. Examples of recurrent ANN's would be a Kohonen (self-organizing map) or a Hopfield based solution [38] [39].

b. Un-Supervised

Un-supervised learning is also a machine learning technique in which the output unit is trained in response to the pattern in the input framework. I.e. in which the networks learn to form their own classifications of the training data without external help. [40] In this kind of situation, the system is given a task to show / discover all the possible patterns based on the input population. Compared to the supervised learning method, there is no a priori set of categories into which the patterns are to be classified; rather the system has to develop its own representation of the input stimuli. For supervised and unsupervised learning methods, basically all the learning rules reflect a variant of the Hebbian learning rule [37]. The different types of un-supervised learning are as under:

i. Self-Organizing Maps.

Neural networks that contain two layers and in implementation, a winner take all strategy in the output layer. Rather than taking the output of individual neurons, the neuron with the highest output is considered the winner. SOM's are typically used for classification related problems, where the output neurons represent groups that the input neurons are to be classified into. SOM's are usually trained with a competitive learning strategy.

ii. Unsupervised adaptive Resonance theory.

Adaptive resonance theory is a neural theory which helps us to learn the concepts about how the brain develops and learns to recognize the objects and then recall them in his whole life. The process shows how to learn, categorize the events; in order to deal with coming events based on the categories already learned [40].

Also from supervised section, the Feed Forward ANN and Recurrent ANN have been divided into two sub-categories as:

Feed Forward ANN

a. Multilayer Feedback
b. Radial Based function

Recurrent ANN

a. Elman Recurrent.
b. Cerebella Mode Architecture control NN.

2. Programmed

The programmed learning needs some agent either it be a user or some other, who teaches the system, program it to detect the different anomalies or malicious events. Thus the user or the programmer of the system forms an opinion or idea on what is considered abnormal enough for the system to signal a security violation [41][42]. The techniques used for intrusion detection system which comes under this category are as:

i. State Series modelling detection.

The technique state series modelling involves the operations of encoded as a set of states. The transitions in between all the states are maintained internally in the model, not explicit as when we code a state machine in an expert system shell. In any state, the match will be carries out, once the match is there for the state, the intrusion detection system engine waits for the next transition to occur. If the monitored action generated by the state is described as allowed the system continues, else if the transition would take the system to another state, any unknown (implied) state that is not described in the action list, then the system will sound an alarm [43] [44]. The monitored actions that can trigger transitions are usually security relevant actions such as file accesses (reads and writes), the opening of 'secure' communications ports, etc. The rule matching engine is simpler than and not as powerful as a full expert system. There is no unification, for example. It does allow fuzzy matching, however— fuzzy in the sense that an attribute such as 'Write access to any file in the /tmp directory' could trigger a transition. Otherwise the actual specification of the security operation of the program could probably not be performed realistically [41].

ii. Simple Rule based detection.

Rule-based techniques [7] detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is suspicious. The system involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder [41].

iii. Threshold based detection.

The technique threshold based detection is considered to be the simplest technique among the programmed descriptive statistics detectors. Threshold detection actually maintains mechanisms of counting the number of frequency of a specific event type over an interval time. If the count surpasses what is considered a reasonable number that one might expect to occur, then the intrusion is assumed [45]. The system works on the pre-defined statistics. i.e the system collects the necessary statistics and user can program predefined threshold in the form of range which will finally suggest that alarm may be generated or not for that statistical data or we can say that when the system has collected the necessary statistics, the user can program predefined thresholds (perhaps in the form of simple ranges) that define whether to raise the alarm or not. An example is '(Alarm if) number of unsuccessful login attempts >3 [46] [41].

iv. Default Deny.

The method uses defaults deny security policy under which we define or state the observations as the deviation from the normal. In This method, the deviation flags are used for the operations. The model uses flags for checking the intrusive activities in the system. The formulation comes from the general legal system, which labels each and every thing as legal and illegal [41].

v. Statistical Based.

Statistical based systems use profiling technique [47].The system determines the normal activity "Normal" and all the traffic which comes to system if falls under these conditions will be treated as normal and if the traffic falls outside the scope of normal is treated as abnormal or anomalous. The system will build profile of normal statistical behavior by the system of collecting descriptive statistics on a number of parameters [41]. The categories which come under the category of statistical based system are as:

a. Markova Process

A Markova process is the method/ technique applied to form programmed intrusion detection systems. Markov process is a stochastic process which will have finite states or finites states of possible outcome. Also the outcome of any of the stage that we are supposed to get directly depends on the outcome of the previous states. Also the most possible outcome of the states must be constant over time [42]. This model identifies intrusion by examining the system at fixed intervals and keeping track of its state. A probability for each state at a give time interval is computed when an event occurs it changes the state of the system and if the probability for that state to occur at that time interval is low that event is considered anomalous. This model might be useful for looking at transitions between certain commands where command sequences were important [43].

b. Operational Model

This model is based on the range of events generated i.e maximum and minimum. Therefore based on the cardinality of events that happens over a period of time an alarm is raised if fewer then m or more than n events occur [43]. For Example: An E-Banking account, a user after unsuccessful 5 login attempts locks the account for any more transactions. Similarly The size of executable files allowed to be downloaded in some organizations is restricted to some value e.g. Gmail the size of file uploaded is 25 MB..The challenge in this sub-model is determining m and n.

c. Multivariate Model

The Multivariate model is popular statistical tool that uses multiple variables to forecast possible investment outcomes. Multivariate models predict outcomes of situations that are affected by more than one variable, and are widely used in the financial world. The model works on the mechanism of the mean and standard deviation, therefore the model is based on correlations among two or more metrics. This model would be useful if experimental data show that better discriminating power can be obtained from combinations of related measures rather than individually-e.g., CPU time and 1/0 units used by a program, login frequency, and session elapsed time (which may be inversely related). [43].

d. Time Series Model

The model uses two parameters interval time and event count. The model takes these parameters into account of the order and inter-arrival times of the observations as well as their values. The new observation which we got can be treated as if the probability of occurring of that event is very low. It uses probabilistic its probability of occurring at that time is too low, but the disadvantage of being more costly than mean and standard deviation [43].

B. Misuse Based IDS

Mis-Use based intrusion detection system is based on rules. The rules used for the detection purpose in this technique may either be preconfigured by the system or these may be setup manually by the administrator. These rules will look for signatures on the network and then system operations try to catch known attack that should be considered as Misuse [18] [44] [68]. You can think of Misuse detection as a specific deny rule firewall. Example: We can model certain user's daily activity very minutely and very effectively. Suppose the user for which we are making profile logs in around 10 am, login in mails, and performs some transactions and takes break at 1: 00 pm, has very little number of access errors, no debugging tool used and so on. If the system that the system is being logged in at 3:00 am, start using compilers and debugging tools and has large number of file access errors, the system will flag this activity as suspicious and will raise alarm.

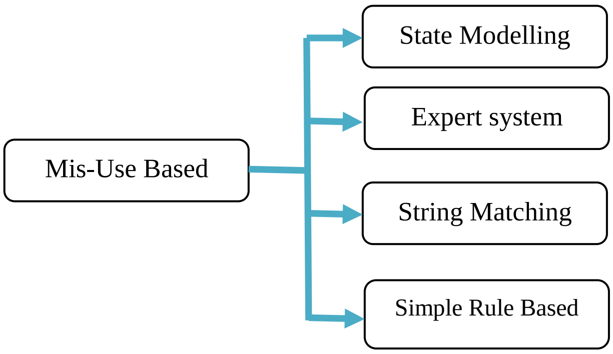

Fig. 3: Mis-Use Based IDS

The Mis-use can be further classified in the following sub groups which are as under:

i. State Modeling

A state model is a representation of the process model for one type of change request. A state represents the status of an individual change request. State-modelling encodes the intrusion as a number of different states, each of which has to be present in the observation space for the intrusion to be considered to have taken place [45]. They are by their nature time series models. Two subclasses exist: in the first, state transition, the states that make up the intrusion form a simple chain that has to be traversed from beginning to end; in the second, Petri-net, the states form a Petri-net. In this case they can have a more general tree structure, in which several preparatory states can be fulfilled in any order, irrespective.

ii. Expert System

An Expert system is based on the statistical profiles of users, events etc. and then use the same for the intrusion detection process [46]. Thus expert system is employed to reason about the security state of the system, given rules that describe intrusive behaviour. The system works on the principle of previously defined set of rules which when assembles in sequence represent an attack. In expert system, all the events that have been incorporated in an audit trail are translated in the form of if-then-else rules. However it is very hectic to get a perfect rule for input data stream.

iii. String Matching

String match is very simple and based on the character matching pattern but are case sensitive in nature. In this type of techniques, Sub-strings characters are being matched in the text that has been ment for transmission. These systems are not flexible, but it has the virtue of being simple to understand [41].

iv. Simple Rule Based

These systems are similar to the more powerful expert system, but not as advanced. This often leads to speedier execution [41]. The system observes events on system & applies rules to decide if activity is suspicious or not. The rule-based anomaly detection analyzes historical audit records to identify usage patterns & auto-generate rules for them. They also observe current behavior & match against rules to see if conforms. It does not required prior of flaws as like statistical anomaly detection [7], [47].

C. Composite

The composite or hybrid system is the system which implements multiple IDS approaches to coexist in a single system. In these types of techniques, the researchers have used both anomaly as well as Mis-use based intrusion detection in combination and can be classified in following categories as shown in fig 4 below:

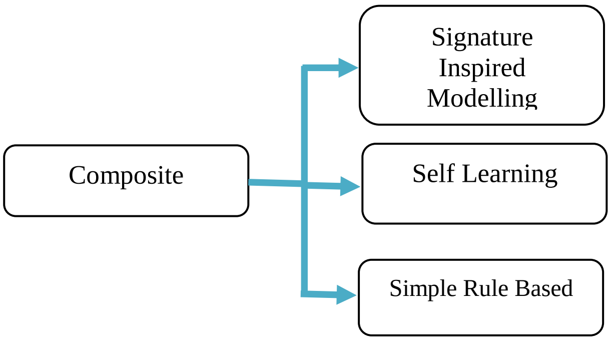

Fig. 4: Composite IDS

v. Signature Inspired

Signature inspired detectors form a compound decision in view of a model of both the normal behaviour of the system and the intrusive behaviour of the intruder. The detector operates by detecting the intrusion against the background of the normal traffic in the system [48]. At present, we call these detectors 'signature inspired' because the intrusive model is much stronger and more explicit than the normal model. These detectors have at least in theory - a much better chance of correctly detecting truly interesting events in the supervised system, since they both know the patterns of intrusive behaviour and can relate them to the normal behaviour of the system [49]. These detectors would at the very least be able to qualify their decisions better, i.e. give us an improved indication of the quality of the alarm. Thus these systems are in some senses the most 'advanced' detectors surveyed.

vi. Self-learning

These systems automatically learn what constitutes intrusive and normal behaviour for a system by being presented with examples of normal behaviour interspersed with intrusive behaviour [41]. The examples of intrusive behaviour must thus be flagged as such by some outside authority for the system to be able to distinguish the two. Automatic feature selection there is only one example of such a system in this classification, and it operates by automatically determining what observable features are interesting when forming the intrusion detection decision, isolating them, and using them to form the intrusion detection decision later [50].

D. Design Based

The intrusion detection systems can be classified on the basis of Design. The sub-class which comes under the strategy is as:

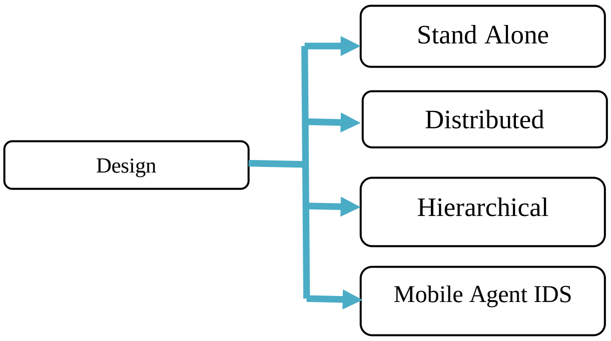

Fig. 5: Design Based

i. Stand Alone

Standalone intrusion detection system is executed independently for each and every client/ node over the network and the decision taken for that node is solely on the data collected from that particular node / client [51] . In this type of detection, node has no idea of the position of other data on the network and also no network alert crosses over the network. This type of systems is most suitable for flat network system .Due to less information about the rest of the nodes in detection mechanisms this type of system is not opted in many intrusion detection systems [52] , [53].

ii. Distributed

In this type of system, we have collaborative work between the clients / nodes. Here the system each node co-operates with the other node to make the detection successful. Each IDs node/agent/ client is responsible for detection, data collection and response generation [54]. In the system, nodes co-operate with each other when there is not convincing evidence in global intrusion detection. This architecture is bit sophisticated as each node has to maintain local as well as global intrusion detection process, which may lead to overloading of memory [9].

iii. Hierarchal

The Hierarchical intrusion detection system is a well developed distributed intrusion detection system. The system has been particularly developed for multi-layered infrastructure which uses clusters for the purpose of detection. Each cluster has a cluster-head associated with it, which has more responsibility compared to other members [55]. In this system, each IDS-agent is performed on every node and is locally responsible for its node, thus we can say that for monitoring and deciding on the locally detected intrusion. Each cluster-head is locally in charge of its node and globally in charge of its cluster. [56].

iv. Mobile Agent IDS

As we know that the mobile agents do not involve directly in improving techniques for detection, but the mobile agents can be applied for reshaping the way of they will be applied in order to enhance the efficiency and effectiveness of that particular technique [57]. One area in which mobile agent is used is reducing the log data in inner nodes of distributed system within hierarchical intrusion detection system. In this scenario, the agents visit data repositories and mine results in an efficient manner [58] [57]. In addition to the reducing of network load, the mobile agents are being used in minimizing the ability of an attacker to deceive IDS through discrepancies between protocol stack of the target and protocol model. Based on the concept, the agent replicates itself and will reside on multiple platforms. Based on multiple platforms, multiple agents runs concurrently to reduce the potential of dropping packets while maximizing the potential for triggering a quick response to a detected intrusion. When the network is using network level encryption, availability of resident components at the host also provides the means of viewing the packets in clear text format. Mobile agents can help in the implementation of robust, attack-resistant IDS architectures [59]. When agents sense some danger or some suspicious activities in the network, the Agents can relocate and thus operate autonomously and asynchronously from where created, collaborate and share knowledge, and be self organizing (e.g., dynamically reconfiguring relationships to compensate for failure of key components) [60].

E. Time Aspect Based IDS

This category can be divided into two sub-categories as under:

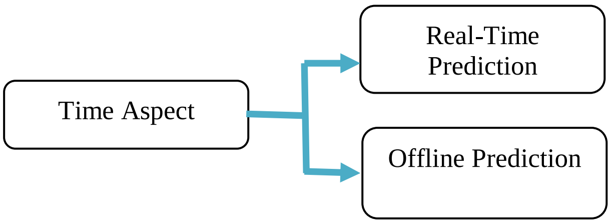

Fig. 6: Time Aspect Based IDS

i. Real time based

In this type of system, the data is being analyzed for some intrusion while session is in progress and raises alarm immediately when the system detects some suspicious data as an attack. Thus the data over the network is check for any intrusion in the real time aspect scenario.

ii. Offline based

In this type of system, the data which we are going to analyze for some intrusion has been collected previously. i.e. the data to be analyzed are already there stored somewhere in term of log and are later processed for intrusion detection process. These types of systems are mainly used for understanding the attack behaviour.

F. Monitoring

The intrusion system can be also classified on the scope of monitoring. The sub-classes are:

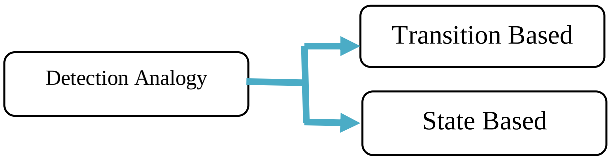

Fig. 7: Monitoring Based IDS

i. Transition based

In this approach [61] [62] attacks are represented as a sequence of state transitions of the monitored system. States in the attack pattern correspond to system states and have Boolean assertions associated with them that must be satisfied to transit to that state. Successive states are connected by arcs that represent the events/conditions required for changing state. These conditions, or signature actions, are not limited to a single audit trail event, but may be a complex specification of conditions.

ii. State Based

In this approach, attacks can be detected on the single state i.e current state of the node/ client, thus identifies the intrusion on the state itself instead of changing of states ie. Transition as we have in transition based intrusion detection system [62].

G. Architecture Based

The intrusion detection system can also be classifies in accordance to their architecture. The different possible architectures are as:

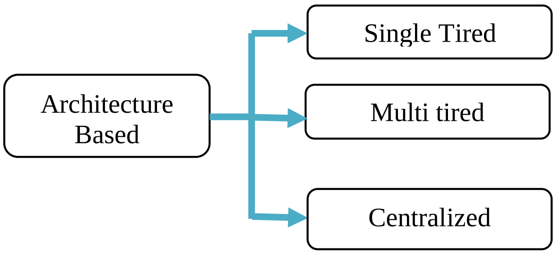

Fig. 8: Architecture Based

i. Single tired Architecture

A single tired architecture, the most basic of the architecture, in which components in IDS collect data and process data themselves, rather than passing the output they collect to another set of components [1] Example HIDS tool that takes the output system logs and compares it to known patterns of attack.

ii. Multi tired Architecture:

A multi-tiered architecture involves multiple components that pass information to each other **[1]** IDS mainly consists of three parts and they are as under:

- Sensors
- Analyzers or agents
- Manager

iii. Centralized

A centralized architecture relays on one server that is attached to all other clients, which regulates the traffic for these node [1], which mean all the incoming traffic and outgoing traffic make through that server and checks for the intrusion.

H. Position of Deployment

The intrusion detection can be classified by the nature of deployment of intrusion detection system. The classification based on the position of deployment is as under:

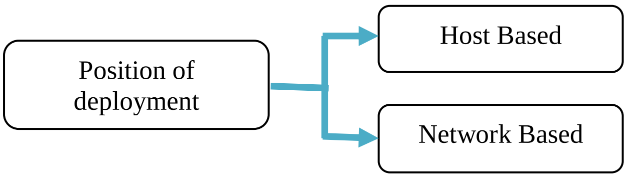

Fig. 9: Position of deployment

i. Host based

The host-based intrusion detection system (HIDS) is a system which monitors and analyzes the network or system data for some intrusion for a particular node. The system will analyze several areas to determine whether the data over that host is malicious or not. The host based system will consult several types of log files and then compare those log files against the internal database for known attacks [63]. The host-based IDS filters logs (which, in the case of some network and kernel event logs, can be quite verbose), analyzes them, re-tags the anomalous messages with its own system of severity rating, and collects them in its own specialized log for administrator analysis. The host based system can also check the integrity of important data file. It uses the checksum method by creating the checksum for each file and stores the same in a simple text file. Then the system periodically checks for the checksum already stored, if the checksum doesn't match for any file, the IDS will make an alert to the administrator by email or message [64], [65].

ii. Network based

Network based intrusion detection system is the system which inspects the individual packets flowing across the network. The NIDS can detect malicious packets that are designed to be overlooked by a firewalls simplistic filtering rule [65]. A network-based intrusion detection system comprising at least one monitoring network interface card (NIC) for collecting packets of traffic to be analyzed from a network, and at least one response NIC for sending a packet for execution of a suspicious network activity operation and session kill operation to the network Where a plurality of monitoring NICs analyze traffic, they possess response NICs in an individual or shared manner, respectively. A response gateway is further provided to route a packet from a response NIC to the network under the condition that the response NIC cannot send the packet directly. Therefore, the network-based intrusion detection system can actively interrupt and hinder intrusion attempts irrespective of a network configuration type upon detecting network intrusions such as hacking, service attacks, scanning, etc., thereby minimizing improper measures to hacking and accurately monitoring a plurality of networks at the same time [66].

VI. Conclusions

The intrusion detection systems are used to detect the attacks coming towards the critical data of the user. As there are many types of intrusion detection system which detects these known as well as unknown attacks coming towards the user's data but up to this, there was no better classification in the literature of intrusion detection, this paper presents a better and elaborated classification based on the various parameters mentioned in the paper. The paper also describes each and every category discussed in the classification diagram. The paper gives a better idea about the category of intrusion detection available in classification.

References

[1] Beigh, Bilal Maqbool, and M. A. Peer. "Intrusion Detection and Prevention System: Classification and Quick." (2011).

[2] Easttom, William Chuck. Computer security fundamentals. Pearson Education India, 2012.

[3] Bhat, Wasim Ahmad, and S. M. K. Quadri. "Design Considerations for Developing a Disk File System." PhD diss., 2012.

[4] Wang, Defeng, Daniel S. Yeung, and E. C. Tsang. "Weighted mahalanobis distance kernels for support vector machines." Neural Networks, IEEE Transactions on 18.5 (2007): 1453-1462.

[5] Jaiganesh, V., Mangayarkarasi, S., & Sumathi, P.(2013). Intrusion Detection Systems: A Survey and Analysis of Classification Techniques. International Journal of Advanced Research in Computer and communication Engineering ,Vol. 2, Issue 4, April 2013

[6] Asmaa Shaker ashoor and Sharad Gore, "Intrusion Detection System (IDS): Case Study," in IACSIT Press, Singapore, 2011, pp. 6-9.

[7] Anderson, J. P. Computer Security Threat Monitoring and Surveillance, James P. Anderson Co., Box 42, Fort Washington. PA 19034 Technical Report Contract 79F296400, 1980.

[8] Denning, Dorothy E. "An intrusion-detection model." Software Engineering, IEEE Transactions on 2 (1987): 222-232

[9] Desai, M. D. Distributed intrusion detection (Doctoral dissertation, Indian Institute of Technology, Bombay). 2002.

[10] Lippmann, Richard, Joshua W. Haines, David J. Fried, Jonathan Korba, and Kumar Das. "The 1999 DARPA off-line intrusion detection evaluation." Computer networks 34, no. 4 (2000): 579-595.

[11] Bace, Rebecca. "Technology Series Intrusion Detection", Macmillan Technical Publishing, 2000

[12] Kozushko, Harley. "Intrusion detection: host-based and network-based intrusion detection systems." on September 11 (2003).

[13] Kemmerer, Richard A., and Giovanni Vigna. "Intrusion detection: a brief history and overview." Computer 35, no. 4 (2002): 27-30.

[14] Zhang, Yongguang, Wenke Lee, and Yi-An Huang. "Intrusion detection techniques for mobile wireless networks." Wireless Networks 9.5 (2003): 545-556.

[15] Caswell, Brian, Jay Beale, and Andrew Baker. Snort Intrusion Detection and Prevention Toolkit. Syngress, 2007.

[16] Amer, Suhair H., and Jr John A. Hamilton. "Input Data Processing Techniques in Intrusion Detection Systems? Short Review." Global Journal of Computer Science and Technology 9, no. 5 (2010).

[17] Castro, Jaime Daniel Mej á, Jorge Maestre Vidal, Ana Lucila Sandoval Orozco, and Luis Javier Garc á Villalba. "TAXONOMY OF NETWORK INTRUSION DETECTION SYSTEM BASED ON ANOMALIES." (2013).

[18] Ning, Peng, and Sushil Jajodia. "Intrusion ‑ Detection Systems." Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, Volume 3: 403-420.

[19] Roesch, Martin. "Snort: Lightweight Intrusion Detection for Networks." In LISA, vol. 99, pp. 229-238. 1999.

[20] Bloedorn, Eric, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot, and Jonathan Tivel. Data mining for network intrusion detection: How to get started. MITRE Technical Report, 2001.

[21] Rajasegarar, Sutharshan, Christopher Leckie, and Marimuthu Palaniswami. "Anomaly detection in wireless sensor networks." Wireless Communications, IEEE 15, no. 4 (2008): 34-40.

[22] Powers, Simon T., and Jun He. "A hybrid artificial immune system and Self Organising Map for network intrusion detection." Information Sciences 178, no. 15 (2008): 3024-3042.

[23] Twycross, Jamie, and Uwe Aickelin. "Towards a conceptual framework for innate immunity." Artificial Immune Systems. Springer Berlin Heidelberg, 2005. 112-125.

[24] Pagnoni, Anastasia, and Andrea Visconti. "An innate immune system for the protection of computer networks." In Proceedings of the 4th international symposium on Information and communication technologies, pp. 63-68. Trinity College Dublin, 2005.

[25] Timmis, Jon, Mark Neal, and John Hunt. "An artificial immune system for data analysis." Biosystems 55, no. 1 (2000): 143-150.

[26] DeCastro, L., Timmis, J.: Artificial Immune Systems: A New Computational Intelligence Approach. Springer, Heidelberg (2002).

[27] Aickelin, Uwe, Peter Bentley, Steve Cayzer, Jungwon Kim, and Julie McLeod. "Danger theory: The link between AIS and IDS?." In Artificial Immune Systems, pp. 147-155. Springer Berlin Heidelberg, 2003

[28] Grossman, R. L. "Data mining: challenges and opportunities for data mining during the next decade." Dispon ível: Magnify site. URL: http://www. magnify. com, Consultado em dez (1997).

[29] Gaikwad, D., Sonali Jagtap, Kunal Thakare, and Vaishali Budhawant. "Anomaly Based Intrusion Detection System Using Artificial Neural Network and Fuzzy Clustering." International Journal of Engineering 1, no. 9 (2012).

[30] Ben Gal, I., "Bayesian Networks" in Encyclopedia of Statistics in Quality and Reliability, Ruggeri, F., Kenett, R. S. and Faltin, F. (editors in chief), Wiley, 2007.

[31] Pearl J. Pearl, “Reverend bayes on inference engines: a distributed hierarchical approach,” in Proc. of the National Conference on Artificial Intelligence, 1982, pp. 133–136..

[32] Scott, Steven L. "A Bayesian paradigm for designing intrusion detection systems." Computational statistics & data analysis 45, no. 1 (2004): 69-83.

[33] Zadeh, Lotfi A. "Is there a need for fuzzy logic?." Information Sciences 178, no. 13 (2008): 2751-2779.

[34] Dhanalakshmi, Y., and I. Ramesh Babu. "Intrusion detection using data mining along fuzzy logic and genetic algorithms." International Journal of Computer Science and Network Security 8, no. 2 (2008): 27-32Moradi and Zulkerniene, 1980 outlier detection

[35] Hawkins, Douglas M. Identification of outliers. Vol. 11. London: Chapman and Hall, 1980..

[36] Suzuki, Kenji, ed. Artificial neural networks-methodological advances and biomedical applications. InTech, 2011.

[37] Zhang, Yuwen, X. Ding, Y. Liu, and P. J. Griffin. "An artificial neural network approach to transformer fault diagnosis." Power Delivery, IEEE Transactions on 11, no. 4 (1996): 1836-1841.

[38] Kohonen, Teuvo. "The self-organizing map." Proceedings of the IEEE 78, no. 9 (1990): 1464-1480.

[39] Carpenter, Gail A., and Stephen Grossberg. Adaptive resonance theory. Springer US, 2010.

[40] Axelsson, Stefan. Intrusion detection systems: A survey and taxonomy. Vol. 99. Technical report, 2000.

[41] Gross, George. "Stochastic processes." (1996).

[42] Qayyum, A., M. H. Islam, and M. Jamil. "Taxonomy of statistical based anomaly detection techniques for intrusion detection." In Emerging Technologies, 2005. Proceedings of the IEEE Symposium on, pp. 270-276. IEEE, 2005.

[43] KHEM, DHAWAL, HARIN VADODARIA, MANISH AGGARWAL, MITESH M. KHAPRA, and NIRAV UCHAT. "Intrusion Detection Systems." (2007).

[44] Kuperman, Benjamin A. "CERIAS Tech Report 2004-26 A CATEGORIZATION OF COMPUTER SECURITY MONITORING SYSTEMS AND THE IMPACT ON THE DESIGN OF AUDIT SOURCES." (2004).

[45] H. Debar, M. Becker and D. Siboni,”A neural network component for an intrusion detection system,” Proceedings of 1992 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 240-250, Oakland, CA, May 1992.

[46] Luger, George, Arthur Maccabe, and Mark Servilla. The architecture of a network-level intrusion detection system. Department of Computer Science, College of Engineering, University of New Mexico, 1990.

[47] Greensmith, Julie, Uwe Aickelin, and Steve Cayzer. "Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection." In Artificial Immune Systems, pp. 153-167. Springer Berlin Heidelberg, 2005.

[48] Patcha, Animesh, and Jung-Min Park. "An overview of anomaly detection techniques: Existing solutions and latest technological trends." Computer Networks 51, no. 12 (2007): 3448-3470.

[49] Portnoy, Leonid, Eleazar Eskin, and Sal Stolfo. "Intrusion detection with unlabeled data using clustering." In In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001. 2001

[50] Farhan, A. F., D. Zulkhairi, and M. T. Hatim. "Mobile agent intrusion detection system for mobile ad hoc networks: A non-overlapping zone approach." In Internet, 2008. ICI 2008. 4th IEEE/IFIP International Conference on, pp. 1-5. IEEE, 2008

[51] Rafsanjani, Marjan Kuchaki, and Ali Movaghar. "Developing a Hybrid Method for Identifying Monitoring Nodes in Intrusion Detection Systems of MANET." Contemporary Engineering Sciences Journal 2, no. 3 (2009): 105-116.

[52] T. Anantvalee and J. Wu, “A survey on intrusion detection in mobile adhoc networks”, Springer J. Wireless Network Security, pages 159-180, 2007.

[53] Samad, Kashan, Ejaz Ahmed, and Waqar Mahmood. "Simplified clustering scheme for intrusion detection in mobile ad hoc networks." In 13th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia. 2005.

[54] Fu, Yingfang, Jingsha He, and Guorui Li. "A distributed intrusion detection scheme for mobile ad hoc networks." In Computer Software and Applications Conference, 2007. COMPSAC 2007.

[55] Huang, Yi-an, and Wenke Lee. "A cooperative intrusion detection system for ad hoc networks." In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 135-147. ACM, 2003.

[56] Jansen, Wayne A. "Intrusion detection with mobile agents." Computer Communications 25, no. 15 (2002): 1392-1401.

[57] Toth, Thomas. "Applying mobile agent technology to intrusion detection." (2001)..

[58] Mell, Peter, Donald Marks, and Mark McLarnon. "A denial-of-service resistant intrusion detection architecture." Computer Networks 34, no. 4 (2000): 641-658.

[59] Helmer, Guy, Johnny SK Wong, Vasant Honavar, Les Miller, and Yanxin Wang. "Lightweight agents for intrusion detection." Journal of Systems and Software 67, no. 2 (2003): 109-122.

[60] Porras, Phillip A., and Richard A. Kemmerer. "Penetration state transition analysis: A rule-based intrusion detection approach." In Computer Security Applications Conference, 1992. Proceedings., Eighth Annual, pp. 220-229. IEEE, 1992.

[61] Ilgun, Koral. "USTAT: A real-time intrusion detection system for UNIX." In Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer Society Symposium on, pp. 16-28. IEEE, 1993.

[62] De Boer, Pieter, and Martin Pels. "Host-based intrusion detection systems." Amsterdam University (2005).

[63] Vokorokos, L., and A. Balaz. "Host-based intrusion detection system." In Intelligent Engineering Systems (INES), 2010 14th International Conference on, pp. 43-47. IEEE, 2010.

[64] Bilal Maqbool Beigh, Uzair Bashir and Manzoor Chahcoo."Intrusion Detection and Prevention System: Issues and Challenges" International Journal of Computer Applications Published by Foundation of Computer Science, New York, USA 76(17) 2013:26-30.

[65] HAN, Dong-Hun. "NETWORK BASED INTRUSION DETECTION SYSTEM." WIPO Patent 2002096028, issued November 29, 2002.

[66] Xiao-Pei, Jing, and Wang Hou-Xiang. "A new Immunity Intrusion Detection Model Based on Genetic Algorithm and Vaccine Mechanism." International Journal of Computer Network and Information Security (IJCNIS) 2.2 (2010): 33.

[67] Singh, Preet Inder. "Robust Security System for Critical Computers." International Journal of Information Technology and Computer Science (IJITCS) 4.6 (2012): 24.

[68] Govindarajan, M. "Hybrid Intrusion Detection Using Ensemble of Classification Methods." International Journal of Computer Network & Information Security 6.2 (2014).

Bilal Maqbool Beigh was born in 1985. Bilal is Ph. D. candidate in Department of computer science, University of Kashmir, Srinagar, India. He completed his bachelor's in computer science and application from Shri Pratap College, M.A.Road Srinagar J&k, He completed his Master degree from University of Pune in 2009. He did his M.Phil in computer sciences and application from University of Kashmir in 2012. The area of interest is information security and intrusion detection systems. The author has published more than 15 papers in different national and international Journals and conferences.

How to cite this paper: Bilal Maqbool Beigh,"A New Classification Scheme for Intrusion Detection Systems", IJCNIS, vol.6, no.8, pp.56-70, 2014. DOI: 10.5815/ijcnis.2014.08.08