# Using Machine Learning and Statistical Models for Intrusion Detection

Kamini C. Nalavade
Computer Engineering Department
Sandip Institute of Engineering & Management

## ABSTRACT
Detecting intrusions and preventing the possible attacks is a critical aspect of computer based system security. Efforts have been made to achieve this goal such as firewalls, intrusion detection system, anti-virus, organizational security policies and many more. In this paper research work in developing general and systematic method for intrusion detection and prevention systems is discussed. This paper focuses on literature survey carried out for building efficient intrusion detection and prevention system. Previous research and applied methodologies of intrusion detection are reviewed and studied. The Denning's model and the statistical approaches for intrusion detection are described. After the comprehensive study and survey of previous work on intrusion detection systems, here we propose a model for intrusion detection and prevention using machine learning.

## General Terms
Security, Intrusion Detection, Machine learning

## Keywords
Intrusion, Network, Data mining, Anomaly, Security

## 1. INTRODUCTION
As network-based computer systems play increasingly vital roles in modern society, they have become the targets of our enemies and criminals. Therefore, it is need of today to find the best ways possible to protect our systems. The security of a computer system is compromised when an intrusion takes place. An intrusion is a formal term describing the act of compromising system resources. An intrusion can be defined as "any set of actions that attempt to compromise the integrity, confidentiality or availability of a system resource". Detecting either failed or successful attempts to compromise the system is called an Intrusion Detection. Intrusion detection systems or IDS detect possible intrusions. The goal of IDS tools is to detect computer attacks or illegal access, and to alert the concerned people about the detection or security breach [1].

Monitor, detect, and respond to any unauthorized activity are the goals of Intrusion detection systems. Network attacks such as DoS attacks can be detected by monitoring the network traffic. There are two basic types of intrusion detection: Host-based and Network-based. Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages.

Host-based intrusion detection systems (HIDS) are IDSs that operate on a single computer. HIDS monitor traffic on its host machine by utilizing the resources of its host to detect attacks. [2]

Network-based intrusion detection systems (NIDS) are IDSs that operate as stand-alone devices on a network. NIDS monitors traffic on the network to detect attacks such as denial of service attacks; port scans or even attempts to crack into computers by monitoring network traffic [2].

Intrusion prevention is rather more important than intrusion detection. Intrusion prevention techniques such as strict authorization and access policy, security rules, minimal programming and administrative errors can be implemented. The inadequacies inherent in current IDS defences have driven the development of a new class of security products known as Intrusion Prevention Systems (IPS). Intrusion prevention (IPS) is any device that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful. [1]. IPS sits online on the network and monitors it and when an event occurs it takes action based on prescribed rules. Detecting unknown attacks is the primary goal of our system design.

The rest of the paper is organized as follows: Section 2 describes intrusion detection approaches used in the intrusion detection systems. Section 3 describes the Denning's model for intrusion detection system and the statistical approaches suggested. Section 4 briefly highlights the architecture and the pseudo code of our proposed intrusion prevention system. Section 5 outlines future scope of work presented.

## 2. INTRUSION DETECTION APPROACHES
Many approaches are used in intrusion detection systems. In Anderson's study, it was postulated that one could distinguish between a masquerader and a legitimate user. Patterns of legitimate user behaviour can be established by observing past history and significant deviation from such patterns can be detected. Anderson suggests that task of detecting a misfeasor is more difficult, in that the distinction between abnormal and normal behaviour may be small. Anderson concluded that such violations would be undetectable. The basic two approaches of intrusion detection are identified which are anomaly based intrusion detection and misuse based intrusion detection. A brief review of these approaches is described below that are landmarks in the development of intrusion detection systems.

### 2.1 Anomaly based intrusion detection
First off, anomalies also known as outliers, exceptions or peculiarities are patterns in data that do not conform to a well defined notion of normal behaviour of a system [4]. The Figure 1 shows anomalies O1, O2 and O3 that differ from the normal behaviour N1 and N2.

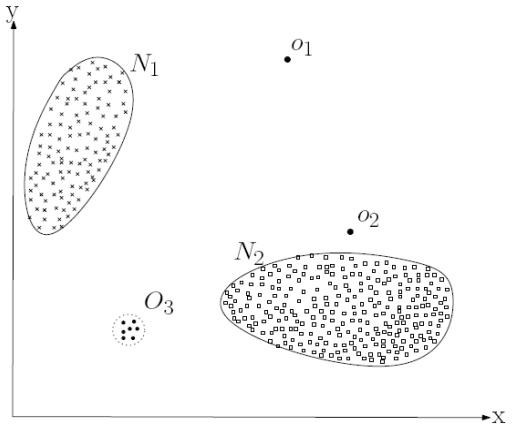


**Figure 1 Anomaly based Intrusion Detection**

Anomaly detection technique is designed to uncover the patterns of behaviour that are far from normal and anything that widely deviates from it gets flagged as a possible intrusion. Anomaly Detection Techniques represents a broad spectrum of detection techniques. One can define profiles in terms of simple thresholds or more complex statistical distributions; and profiles can be self-learned or manually set, adaptive, or static. The three categories of anomaly detection are discussed in the following paragraphs.

**1) Protocol Anomaly Detection**

As mentioned earlier protocol anomaly refers to exceptions related to protocol format and behaviour with respect to common practice on the Internet and standard specifications. This includes network and transport layer protocol anomalies and application layer protocol anomalies. Unusual conditions are checked for in the process of IP de-fragmentation, TCP reassembly. When the IDS is in-line, many exceptions leading to ambiguous interpretation by the end host can be averted. When IDS is monitoring application protocol behaviour, it must be able to perform deep application protocol parsing, which is also known as decoding.

The following anomalies are examples of protocol anomalies that could be detected when application protocol behaviour is being observed:

i. illegitimate field values and combinations

ii. Illegitimate command usage

iii. Unusually long or short field lengths, which can indicate an attacker is attempting to introduce a buffer overflow

iv. Unusual number of occurrences of particular fields/commands

v. Running a protocol or service for a non-standard purpose

or on a non-standard port

**2) Application Payload Anomaly**

Application anomaly must be supported by detailed analysis of application protocols to define accurate behaviour constraints for them. Application anomaly also requires understanding of the application semantics in order to be effective. One needs to know what type of encoding is legal for a given field, and what other applications can be embedded within it. One good example of application level anomaly is the presence of shellcode in unexpected fields. A reliable anomaly profile allows shellcode execution attacks to be detected without knowing what particular exploit code is involved, or even the existence of exploit code[3].

**3) Statistical anomaly detection**

It involves the collection of data relating to the behaviour of legitimate users over a period of time. Then statistical tests are applied to observed behaviour to determine with a high level of confidence whether that behaviour is not legitimate behaviour.

A) Threshold detection: this approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.

B) Profile based: A profile of the activity of each user is developed and used to detect changes in the behaviour of individual accounts.

## 2.2 Misuse/Signature Based Intrusion Detection

The second major category of IDS is known as misuse detection also referred to as signature-based detection because alarms are generated based on specific attack signatures. These attack signatures encompass specific traffic or activity that is based on known intrusive activity.

The following are the two techniques in misuse detection:

**1) Expression matching**

The simplest form of misuse detection is expression matching, which searches an event stream (log entries, network traffic, or the like) for occurrences of specific patterns/signatures. Signatures can be very simple to construct, however especially when combined with protocol-aware field decomposition.

**2) State transition analysis**

State transition analysis models attacks as a network of states and transitions (matching events). Every observed event is applied to finite state machine instances (each representing an attack scenario), possibly causing transitions.[3]

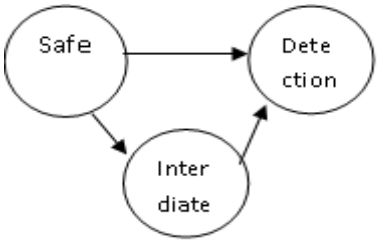


**Figure 2 State Transition Diagram**

Any machine that reaches its final (acceptance) state indicates an attack as depicted in Figure 2.

This approach allows complex intrusion scenarios to be modelled in a simple way, and is capable of detecting slow or distributed attacks, but may have difficulty expressing elaborate scenarios.

## 2.3 Data Mining Approaches for Intrusion Detection

Data mining generally refers to the process of (automatically) extracting useful information from large stores of data. The recent rapid development in data mining has made available a

wide variety of algorithms, drawn from the fields of statistics, pattern recognition, machine learning, and database. Several types of algorithms are particularly relevant to our research:

**1 Feature selection**

Feature selection, also known as subset selection or attribute selection, is a process commonly used in machine learning, wherein a subset of the features available from the data is selected for application of a learning algorithm. Feature selection is necessary either because it is computationally infeasible to use all available features, or because of problems of estimation when limited data samples are present

Feature selection from the available data is vital to the effectiveness of the methods employed. Researchers apply various analysis procedures to the accumulated data, in order to select the set of features that they think maximizes the effectiveness of their data mining techniques. Table I contains some examples of the features of TCP connection of KDDCup1999 Data set [5]. Each of these features offers a valuable piece of information to the System. Extracted features can be ranked with respect to their contribution and utilized accordingly

**Table 1: Basic Features of Individual TCP Connections**

| Feature name | Description | Type |
|---|---|---|
| duration | length (number of seconds) of the connection | continuous |
| protocol_type | type of the protocol, e.g. tcp, udp, etc. | discrete |
| service | network service on the destination, e.g., http, telnet, etc. | discrete |
| src_bytes | number of data bytes from source to destination | continuous |
| dst_bytes | number of data bytes from destination to source | continuous |
| flag | normal or error status of the connection | discrete |
| land | 1 if connection is from/to the same host/port; 0 otherwise | discrete |
| wrong_fragment | number of ``wrong'' fragments | continuous |
| urgent | number of urgent packets | continuous |

**2 Machine learning**

Machine Learning is the study of computer algorithms that improve automatically through experience. Applications range from data mining programs that discover general rules in large data sets, to information filtering systems that automatically learn users' interests. In contrast to statistical techniques, machine learning techniques are well suited to learning patterns with no a priori knowledge of what those patterns may be. Clustering and Classification are probably the two most popular machine learning problems.

## 2.1 Clustering

Clustering is an unsupervised learning technique which divides the datasets into subparts, which share common properties. For clustering data points, there should be high intra cluster similarity and low inter cluster similarity. [4] A clustering method which results in such type of clusters is considered as good clustering algorithm. Clustering methods can be classified as follows

### *2.1.1 Hierarchical clustering*

In hierarchical clustering data are not gets clustered at ones instead stepwise procedures is followed for clustering the datasets. Hierarchical clustering can be further classified as

A. Division clustering

In division clustering formation of clustering whole data point is considered as a single cluster and formation of new clusters starts from the whole data point to single datapoint. It starts form root to leave.

B. *Agglomerative Clustering*

In this type of clustering consider each data point as a cluster, and formation of the clusters starts by combining two instances based upon the certain criteria. It starts form leave to root.

### *2.1.2 Partitional clustering*

In this data points are divided into k subparts based upon certain relevance criteria.

*A.* K-Mean Clustering

In K-Mean clustering, assignment of the data points to clusters is depend upon the distance between cluster centroid and data point. There are three variation of k-mean clustering

1 k-mean: which is used for numerical data sets.

2 k-mediod : It is used for categorical datasets and

3 k-prototype: It is used for both categorical and numerical dataset.

B. Fuzzy C Mean Clustering

Another variation of K-mean clustering algorithm is Fuzzy C Mean. In this clustering algorithm along with the calculation of distance, membership of the data points with the cluster are also considered.

C. QT Clustering

QT (Quality Threshold) Clustering is an algorithm that groups datapoint into clusters. Quality is ensured by finding large cluster whose diameter does not exceed a given user-defined diameter threshold value.

## 2.2 Classification

Classification maps a data item into one of several pre-defined categories. These algorithms normally output "classifiers", for example, in the form of decision trees or rules. An ideal application in intrusion detection will be to gather sufficient "normal" and "abnormal" audit data for a user or a program, then apply a classification algorithm to learn a classifier that will determine audit data as belonging to the normal class or the abnormal class. A classification based IDS attempts to classify all traffic as either normal or malicious. The challenge in this is to minimize the number of false positives (classification of normal traffic as malicious) and false negatives (classification of malicious traffic as normal).Inductive rule generation, Genetic algorithm, Neural networks, Fuzzy logic are the techniques used for classification in intrusion detection systems.

### 3 Statistical Techniques

This approach involves statistical comparison of specific events based on a predetermined set of criteria. Statistical techniques, also known as"top-down" learning, are employed when relationship among data is finalized and can employ mathematics to aid the search. Three basic classes of statistical techniques are linear, nonlinear and decision trees [8]. The data collected from the system and the network is tested for attack analysis by statistical models. The models which have been most frequently used include the Operational Model, Average and Standard Deviation Model, the Multivaried Model, the Markovian Model and the Time Series Model. Statistical patterns can be calculated with respect to different time windows, such as day of the week, day of the month, month of the year, etc. [7], or on a per-host, or per-service basis [6].

Denning (1987) described how to use statistical measures to detect anomalies, as well as some of the problems and their solutions in such an approach. Denning's Model and statistical based techniques are described in detail in the next section.

## 3. DENNING'S MODEL AND STATISTICAL APPROACHES FOR INTRUSION DETECTIONS

Denning's model and Statistical approaches for intrusion detections

Denning proposed an intrusion detection model in 1987 which became a milestone in the research in this area. The model which she proposed forms the basic core of most intrusion detection designs in use today [3]. Denning's pioneering work in IDSs is based on the assumption that an intrusion can occur if there is a deviation from normal activity. Normal activity here is the activity performed by an authorized user using the computer—the programs that are executed, the number of logins per day, and so forth—and the activity of the computer itself—the CPU time used, the amount of I/O activity, and so forth.

According to Denning, various types of intrusions can be detected with this model:

A. Masquerading: a user that is supplanted by an intruder, in this case, it is assumed that the intruder has a different activity pattern than the normal user, trojan horses: a program that is implanted by an intruder; here the response time of the computer can be degraded.

B. Virus: a program that is embedded in another program and replicates itself, usually using CPU time or performing a lot of I/O, and then the use of resources is abnormal.

C. Break-ins: when an intruder bypasses the security of the computer and gains access to it through the use of a "guest" account, supplanting a defined user in the computer, using a trojan horse, and so forth; in this case there may be more use of CPU or different patterns of the use of the system by the supplanted user.

D. Internal intrusions: a user authorized to use the system who tries to gain access to confidential information, or as a matter of example, he or she sends information to an entity not authorized by the company for which he or she works; in this case the legitimate user can direct data to a remote printer that is not used for that purpose [12]. As mentioned previously, IDS controls the activity over the data and resources in a computer. The Denning's model has six main components:

1. Subjects: Initiators of activity on a target system-normally users.
2. Objects: Resources managed by the system-files, commands, devices, etc.
3. Audit records: Generated by the target system in response to actions performed or attempted by subjects on objects-user login, command execution, file access, etc.
4. Profiles: Structures that characterize the behavior of subjects with respect to objects in terms of statistical metrics and models of observed activity. Profiles are, then, records that store the activity in the computer, according to the policy defined. A profile is uniquely identified by name, subject, and object.
5. Anomaly records: Generated when abnormal behavior is detected.
6. Activity rules: Actions taken when some condition is satisfied, which update profiles, detect abnormal behavior, relate anomalies to suspected intrusions, and produce reports.

### 3.1 Statistical Models

In order to capture intrusions the IDS has rules that use the following statistical models (9):

**1.** The operational model where exceeding a predefined threshold is an indication of an intrusion. The threshold is normally defined by the security policy. For example, the security policy can establish that more than three failed attempts to enter a password should be reported.

**2.** The mean and standard deviation model where a deviation from mean ± threshold stdev is an indication of intrusion. The threshold in this case is different than the previous one, in the sense that this time four is normally used, because in a normal distribution almost 100% should be in that interval.

**3.** The multi-variate model where correlation between activities is used. For example, CPU time along with I/O used by a program. It could be that looking at the use of CPU time alone is not enough for detecting an intrusion.

**4.** The Markov chain model where activity is seen as events and the probability of occurrence of an event depends on the history. For example, if a programmer usually uses a set of commands in order to edit, compile, link and execute an application, then almost always the same set of commands is expected, and so the IDS can know what command is expected. If an unexpected command happens, then there is a suspicion of intrusion and the IDS will signal an alarm.

A HMM can be considered as the simplest dynamic Bayesian network. Ourston et al. [9] describe a novel approach using Hidden Markov Models (HMM) to detect complex Internet attacks. These attacks consist of several steps that may occur over an extended period of time. Within each step, specific actions may be interchangeable. A perpetrator may deliberately use a choice of actions within a step to mask the intrusion. In other cases, alternate action sequences may be random (due to noise) or because of lack of experience on the part of the perpetrator. For an intrusion detection system to be effective against complex Internet attacks, it must be capable of dealing with the ambiguities described above.

HMMs are well suited to address the multi-step attack

problem. In a direct comparison with two other classic techniques, decision trees and neural nets, the authors show that HMMs perform generally better than decision trees and substantially better than neural networks in detecting these complex intrusions. Lane [10] trained a Hidden Markov Model on the same data that he used to train an instance-based learner. He notes that the Hidden Markov Model"assumes that the state variables are hidden and correspond to phenomena that are, perhaps, fundamentally unobservable," and as such, should perform well in modeling user actions. He concluded that the HMM and the instance-based learner mentioned above, trained using the same data, performed comparably.

Warrender et al. [11] applied a Hidden Markov Model to system call data. They noted that best performance was obtained by using a number of states corresponding to the number of system calls used by an application.

Even though HMMs have been shown to improve the accuracy of IDSs they are also accompanied by high complexity. They require a lot of resources and are often considered to be too time-consuming for practical purposes.

**5.** The time series model where the time of occurrence of the activity shows its normality. For example, the time of running a banking settlement. The event occurs every business day at approximately the same time. If the activity happens at a quite different time (or has already occurred) then there is a suspicion of abnormal activity.

Besides statistical models, a metric is used. A metric is a statistical variable that corresponds to a new observation, i.e., a new audit record has been generated and so a value of the metric must be calculated according with the statistical model.

## 3.2 Profiles

In order to perform intrusion detection, Denning proposes the following data structure for a profile: name, subject, object, action pattern, exception-pattern, resource-usage-pattern, period, variable-type, threshold, and value. Name, subject and object form the key of the profile. Action-pattern is the action which can be looked for at as, for example, "read" or "delete." Exception pattern matches the return field of the audit record, usually 0 means success in the system call performed while another value indicates an exception, usually −1, for example "no such file or directory." Resource-usage-pattern corresponds to the usage of a resource such as CPU time or number of pages printed. Period corresponds to a time interval. Variable-type is the model used, i.e., operational, mean and standard deviation model, etc. Threshold is used in conjunction with the operational model and the mean and standard deviation model; and value corresponds to the actual value of the variable in observation [12]. Profiles are classified as activity profiles, template profiles and anomaly profiles. When an audit record is generated, the IDS actualizes the corresponding activity profile and, depending on the model and value, it can generate an anomaly profile and raise an alarm. If the activity profile does not exist, then it is created using a profile template. One of the difficult parts of IDSs is the creation or initialization of profiles. Denning suggests in this case the use of templates. A template is a data structure with the fields as enumerated previously. If a new user is defined in the system, when the user performs his or her first login, the IDS is not going to find activity profiles, and then the IDS is going to generate the ones needed, using the corresponding template profiles. All fields of the template are copied to the new activity profile, except subject. Profiles can be used by an individual subject or by an aggregation of them. In the same way profiles can be used by an individual object or by aggregations of them. For example, a profile for subject "diaz" with object "passwd-file" and/or a profile for subject "robotics" with object "passwd-file," where "robotics" is an aggregation of subjects.

# 4. PROPOSED SYSTEM ARCHITECTURE AND PSEUDOCODE

The Internet has changed our lives in this decade. The possibilities and opportunities on Internet are limitless; unfortunately, so too are the risks and likelihood of malicious intrusions. Intruders can be classified into two categories: outsiders and insiders. Outsiders are intruders who approach your system from outside of your network and who may attack your external presence (i.e. spam through e-mail servers, etc.) They may also attempt to go around the firewall and attack machines on the internal network. Insiders, in contrast, are legitimate users of your internal network who misuse privileges, impersonate higher privileged users, or use proprietary information to gain access from external sources. The goal of this research is to develop a Intrusion detection and prevention system which will enhance the network security. Along with detection of known attacks detecting unknown attacks is also very important. Anomaly detection methods are useful for detecting unknown attacks. Every method of intrusion detection has its own advantages over other in attack detection. The proposed system is tries to make use of both types of techniques i.e. machine learning and statistical models. As shown in Figure 3, we propose a model which combines the features of machine learning and statistical approaches for intrusion detection.

The main components of our system are

1. Data set
2. Feature Selection
3. User Profiling
4. Intrusion Detection
5. Machine learning techniques

   Classification& Clustering
6. Statistical based techniques
   1. Mean and standard deviation Model
   2. Multivariate Model(future)
7. Data Visualization
8. Intrusion Prevention

   Reports and Prevention Action

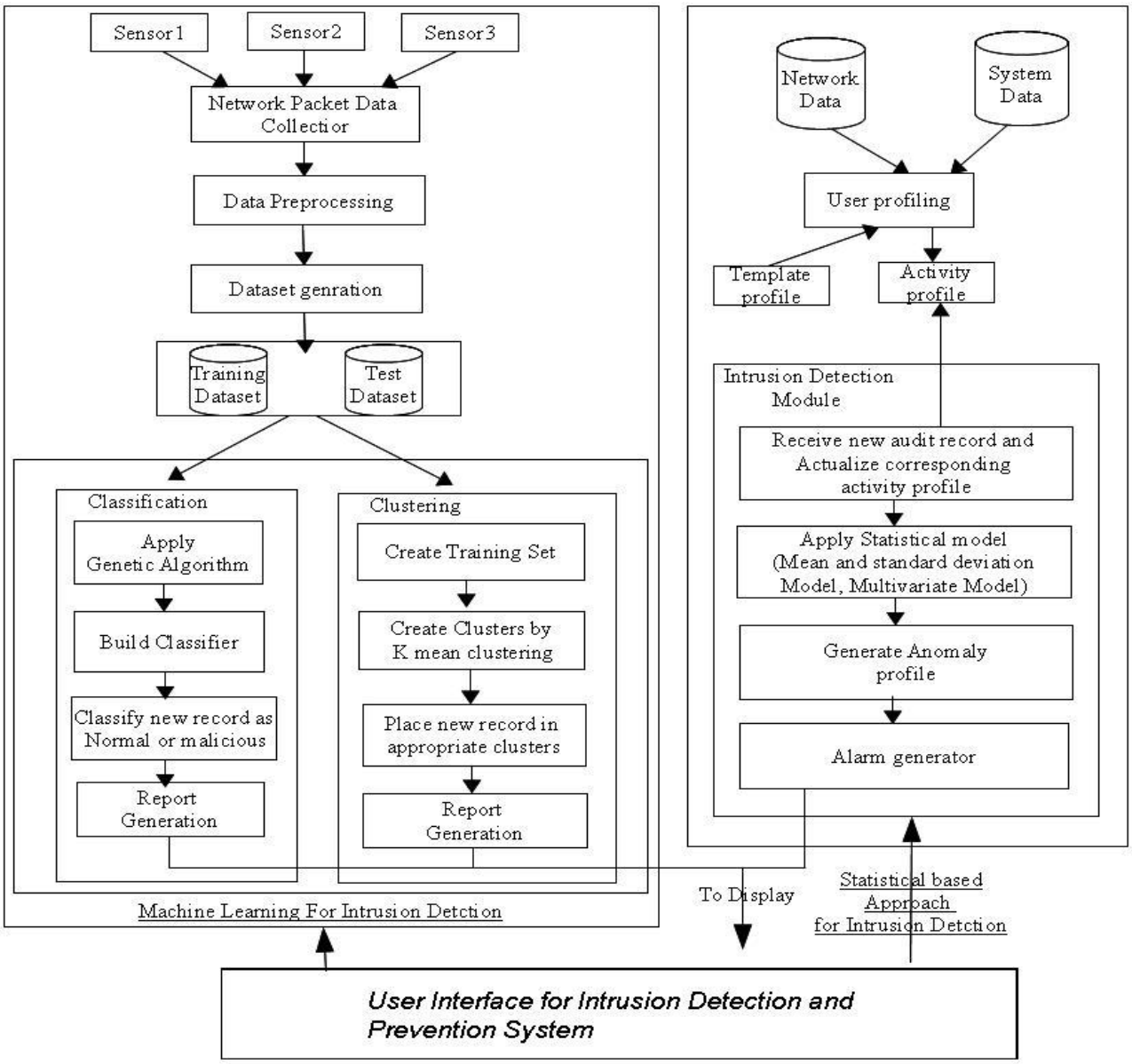


**Figure 3. Proposed System Architecture**

The proposed system considers two sets of data. One set is collected by network packets capture and another is collected by audit log of system. Supervised learning and unsupervised learning algorithms can be chosen for detecting whether activity is normal or malicious. Classification is applied to network packets data set for attack detection. The paper proposes Genetic Algorithm's use to evolve simple rules for network traffic. These rules are used to differentiate normal connections from anomalous connections. Our methodology is divided in to three phases as follows. Features were reduced based on Correlation and optimized rules were developed using Genetic Algorithm and new attack patterns were

detected by learning the patterns from the Neural Network Radial Basis Function Networks. The features are used to form rules for detecting various types of intrusions using Genetic Algorithm. This permits the introduction of higher level of generality and thus to higher detection rates. The procedure starts from an initial population of randomly generated individuals. Then the population is evolved for a number of generations while gradually improving the qualities of the individuals in the sense of increasing the fitness value as the measure of quality. The final step is to train the network using Radial Basic Function Network to detect the unknown attack. It is very important to define a good fitness function that rewards the right kinds of individuals. The paper try to consider affecting factors as complete as possible to improve the results of classification. Our fitness function is

Fitness = Error rate + Entropy measure + Rule consistency

If a rule matches a certain example, the classification it gives is its consequent part. If it doesn't match, no classification is given. An individual consists of a set of rules, the final classification predicted by this rule set is based on the voting of those rules that match the example. The classifier gives all matching rules equal weight. The error rate measure of this individual is the percent of misclassified examples among all training examples.

Clustering is a well known and researched problem. Second method employed is unsupervised learning based anomaly detection on network data. K means clustering makes several passes through the training data and in each pass cluster centre

are shifted to the mean of data points. It then reassigns the data points to nearest prototype and continues iterating until no change in cluster centre occurs.

Step1: Initialize the set of clusters, S, so the empty set.

Step2: Obtain a feature vector from the training dataset. If the cluster set is empty, then create a cluster with d as defining instance.

Step3: otherwise find a cluster C in S such that for all C' in S

distance(C, d) <= distance (C', d)

Step4: if distance (C,d)<= width of cluster then assign d to C

else create a new cluster with d as defining instance.

Step5: Repeat steps until no instance is left in the training set.

Once the clusters are created from training dataset, the system is ready to perform detection of intrusions. Given an instance d,

Step4: if distance (C,d)<= width of cluster then assign d to C else create a new cluster with d as defining instance.

Step5: Repeat steps until no instance is left in the training set.

Once the clusters are created from training dataset, the system is ready to perform detection of intrusions. Given an instance d,

Step1: convert d based on statistical information of clusters.

Step2: Find a cluster which is closed to d such that

distance (C, d) <= distance (C', d)

where C is set of clusters.

Step3: Classify d based on label of C.

The cluster which is closest to d is searched and assigns it to that cluster's classification.

The third module of our proposed system is to apply statistical models for intrusion detection.

The mean and standard deviation model is applied to data where a deviation from mean ± threshold stdev is an indication of intrusion. The multi-variate model applied to collected data where correlation between activities is discovered. For example, CPU time along with I/O used by a program may be considered. It could be that looking at the use of CPU time alone is not enough for detecting an intrusion. The implementation and analysis of the results based on attack detection rate and false alarm generation rate is the next step of our research.

## 5. CONCLUSION

Intrusion detection is an integral part of computer security. Intrusion detection improves the security of information systems by allowing the review of patterns of access in order to discover abnormal activity of users and serving as a deterrent to users' attempts to bypass system privilege or protection mechanisms. In this paper we proposed a systemic framework that employs data techniques for intrusion detection. This framework consists of classification, clustering, multivariate model and standard deviation model that can be used to detect intrusions.

The paper suggests that the classification and clustering algorithms can be used to detect intrusions in labelled and unlabelled data. The research work is in the initial stages. The many remains to be included in this paper such as the following tasks:

- Implement a prototype based intrusion detection system for real time data.
- Performance Analysis of all these techniques based on attack detection rate and false alarm generation rate.
- Investigate the methods and benefits of combining multiple simple detection models. Multiple audit data streams for experiments must be used;
- Evaluate our approach using extensive audit data sets.

Our proposed model provides powerful real-time intrusion detection capable of detecting a wide range of intrusions related to attempted break-ins, masquerading (successful break-ins), system penetrations, DOS, viruses and other abuses by legitimate users. Moreover, the model allows intrusions to be detected without knowing about the flaws in the target system that allowed the intrusion to take place. The field is deep and there are promising new ways to think about it [15].

## 6. REFERENCES

[1] Paul Innella and Oba McMillan, Tetrad Digital Integrity, LLC "An Introduction to Intrusion Detection Systems" December 6, 2001

[2] Micheal E. Whitman and Herbert J. Mattord, "Principles of Information Security" page 289-294

[3] Karthikeyan .K.R1 and A. Indra, "Intrusion Detection Tools and Techniques –A Survey", International Journal of Computer Theory and Engineering, Vol 2 , No. 6, December 2010. 1793-8201

[4] Kusum Kumari Bharti , Sanyam Shukla , Sweta Jain, "Intrusion detection using clustering", Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5 August 2010

[5] http://kdd.ics.uci.edu/databases/kddcup99/task.html

[6] W. Lee, S.J.Stolfo et al, "A data mining and CIDF based approach for detecting novel and distributed intrusions", Proc. of Third International Workshop on Recent Advancesin Intrusion Detection (RAID 2000), Toulouse, France.

[7] Yeung, D.-Y. and C. Chow, "Parzen-window network intrusion detectors", In Proc. of the Sixteenth International Conference on Pattern Recognition, Volume 4, Quebec City, Canada, pp. 385388. IEEE Computer Society, 11-15 August, 2002.

[8] Carbone, P. L., "Data mining or knowledge discovery in databases: An overview", In Data Management Handbook. New York: Auerbach Publications, 1997.

[9] Ourston et al., "Applications of Hidden Markov Models to Detecting Multi-stage Network Attacks", Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS03).

[10] Lane, T. D., "Machine Learning Techniques for the computer security domain of anomaly detection", Ph. D. thesis, Purdue Univ., West Lafayette, IN, August, 2000.

[11] Warrender, C., S. Forrest, and B. A. Pearlmutter, "Detecting intrusions using system calls: Alternative data models", In Proc. of the 1999 IEEE Symp. on Security

and Privacy, Oakland, CA, pp. 133145. IEEE Computer Society Press, 1999.

[12] Theodoros Lappas and Konstantinos Pelechrinis "Data Mining Techniques for (Network) Intrusion Detection Systems", Department of Computer Science and Engineering UC Riverside, Riverside CA 92521

[13] Lenoid portnoy, Eleazar Eskin and Sal Stolfo, "Intrusion detection with unlabeled data using clustering", Department of Computer Scinece, Columbia University

[14] S. Selvakani Kandeeban Dr. R.S. Rajesh, "A Genetic Algorithm Based elucidation for improving Intrusion Detection through condensed feature set by KDD 99 data set", Information and Knowledge Management www.iiste.org ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 1, No.1, 2011

[15] Pedro A. Diaz-Gomez and Dean F. Hougen, " Three Approaches to Intrusion Detection. Analysis and Enhancements" , National Computer and Information Security Conference ACIS 2006 – colombia

[16] Ramana Rao Kompella, Sumeet Singh, George Varghese, "On Scalable Attack Detection in the Network". IEEE /ACM Transactions on Networking, Vol. 15, No. 1, February 2007, Student Member, IEEE and Member IEEE.

[17] Moses Garuba, Chunmei Liu, and Duane Fraites. "Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems". Fifth International Conference on Information Technology: New Generations. 978-0-7695-3099-4/08 $25.00 © 2008 IEEE.Department of Systems and Computer Science, Howard University

[18] Juan D. Penpgosl, Nagarajan Prabhakaran2, Subbarao V. Wunnava. "An Efficient Scheme for Dynamic Signature Verification". 1996 IEEE. Departme3t of Electrical & Computer Engineering, School of Computer Science.

[19] Ricardo Koller, Raju Rangaswami, Joseph Marrero, Igor Hernandez, Geoffrey Smith. "Anatomy of a Real-time Intrusion Prevention System". International Conference on Automonic Computing. 978-0-7695-3175-5 2008. School of Computing and Information Sciences, Florida International University. FL 33 1996.

[20] Teenam Bansode, B.B.Meshram, "Hybrid Intrusion Prevention System for End Users", VIT Conference 2008-09

[21] Yijie Han, Sujaa Rani Mohan, E.K. Park, "An Adaptive Intrusion Detection System Using Data Mining Aproach" , University of Missouri, Kansas City

[22] Kamini Nalavade, BB Meshram, "Data Classification Using Support Vector Machine", National Conference on Emerging Trends in Engineering & Technology (VNCET) 2012.

[23] Kamini Nalavade, BB Meshram, "Evaluation of K-Means Clustering for Effective Intrusion Detection and Prevention in Massive Network Traffic Data" International Journal of Computer Applications, Vol97, Issue 62014.

.