ISSN:0975-9646

Use of Genetic Algorithm with Fuzzy Class Association Rule Mining for Intrusion Detection

Dipali Kharche [1], Prof. Rahul Patil[1]

[1.] *M.E. Student, Dept. of Computer Engineering, PCCOE College Pune*

[2.] *Assistant Professor, Dept. of Computer Engineering, PCCOE College Pune*

***Abstract*— In today's life Intrusion Detection System gain the attention, because of ability to detect the intrusion access efficiently and effectively as security is the major issue in networks. This system identifies attacks and reacts by generating alerts or blocking the unwanted data/traffic. Intrusion Detection System mainly classified as Anomaly based intrusion detection systems that have benefit of detecting novel attacks having false positive rate, and Misuse based intrusion detection systems fails to detect the novel attacks. The proposed system includes Genetic algorithm and the data mining method of fuzzy logic which is a class association rule mining. Genetic algorithm is used to extract the rules which are required for anomaly detection system. The use of the fuzzy logic in proposed model deals with mixed types of attribute and avoid sharp boundary problem. As association rule mining is used to extract the sufficient rules for the user purpose rather than to extract all the rules which are useful for the misuse detection. KDD dataset from the MIT Lincoln Laboratory is used which provides high detection rates.**

***Keywords*— Data Mining, Rule Mining, Intrusion Detection System (IDS), Genetic Algorithm (GA), Network Security, Fuzzy Logic.**

I. INTRODUCTION

In recent years, computer network security becomes the important priority for all types of users. This is due to the tremendous growth internet and the use of computers. Network security is generally defined as the security of computing systems against attacks or threats to confidentiality, integrity and Availability. Threats have many sources like accidents (fire), natural forces (flood), failure of service (power) and the people or unknown users known as intruders. There are two types of intruders are the internal intruders that refers to those with the access permissions who perform the unauthorized actions, and external intruders who are unauthorized users of the machines who attack by using

various techniques. There are many methods to support the network security such as encryption, firewall, VPN etc., but all these are too fixed to give an effective Protection. Therefore, Intrusion Detection which gives the dynamic protection to network security.

When an intruder attempts to perform an action that is not legally allowed, these actions referred as intrusion. Intrusion techniques may contains password checking, exploiting software bugs, and sniffing unsecured traffic. An IDS is a system for detecting intrusion and reporting to the proper specialist. Intrusion detection technology identifies and deals with malicious use of computer and network resources[1].

Intrusion Detection System categorized into misuse detection and anomaly detection, misuse detection focuses for specific known patterns or the sequence of programs and specific user behaviors that matches the well-known malicious activities. Anomaly detection which develops normal network behavior and new intrusions are detected by estimating deviation from the normal user behavior. The strength of anomaly detection is it may detect unseen intrusions that have not been observed.

Intrusion Detection System also is classified into two groups depending on where they look for intrusive behavior: Network-based IDS (NIDS) and Host-based IDS (HIDS). Network based IDS refers to system which identify the intrusions by monitoring traffic through network devices (e.g. Network Interface Cards NIC)and data that collected through network generic stream passing through network segments such as internet packets.

II. RELATED WORK

There are various methods for Intrusion Detection Systems are classified as:

1. Supervised Learning Based Approach
2. Unsupervised Learning Based Approach
3. Data Mining Based Approach

A. Data Mining

In general Data Mining is process of extracting important rules from the large data. Data Mining Techniques have the different benefits towards the solution of various problems in different issues. Data mining system can easily perform data summarization and visualization that helps the security analysis in several areas. Data mining techniques applied to Intrusion Detection System are machine learning, statistical techniques, and feature selections. Intrusion Detection can be useful for classification problem as it can classify each audit records into different sets of categories like either normal or particular kind of intrusion.

In Classification techniques it classifies the instances of dataset into a particular class i.e. either normal or malicious. The challenges in this method are to minimize the number of false positive rate and false negative rate. As one of the most popular data mining method used for different applications, association-rule mining is used to determine association rules or correlations among a set of attributes in a dataset.

1) Association Rule Mining

Association rule mining which finds the association or correlation relationships among a huge data set of data items and expressed by A ⇨ B. where A and B contains a set of attributes. This means that if a tuple satisfies A, it is should also satisfy B. The most popular technique for association rules from databases is the apriori algorithm. This algorithm measures association rule with two factors: support and confidence. However, this algorithm may suffer from large computational complexity for rule extraction from the dense database. A typical example of association rule mining is market basket analysis.

Let M = $\{i_1,i_2,i_3.....,i_m\}$ be the set of items, Let P be the set of database transactions where each transactions T is set of item such that T ⊆ M. Let A be the set of items. A transaction T is contain A if and only if A ⊆ T. an association rule is in the form as A⇨B, where A ⊂ J, B ⊂ J, and A ∩ B = ∅. The rule A⇨B holds in transaction set P with support 's' and confidence 'c' in the transaction set P i.e.

Support (A ⇨ B) = P (A ∪ B)

Confidence (A ⇨ B) = P (B|A)

Rules that satisfy minimum support threshold (min_sup) and minimum confidence threshold (min_cof) are solid.

2) Genetic Algorithm

Genetic algorithms are search algorithms based on natural selections and genetics and inspired by the biological evolution of living beings. Genetic Algorithms evolves population of initial individuals to populations of high quality individuals, where each individual represents solutions of the problem to be resolved. The quality of each rule is measured by a fitness function as the quantitative representation of each rule adaption. The procedure starts from an initial population of randomly generated individuals.[2] Individuals are represented by a string of symbols. Each individual called as chromosome and it composed of predefined number of genes. During each generation it includes the operations like crossover, mutation, and selection operations.

a. Selection: Selection is an operator that makes more copies of better strings in a new population. Selection is usually the first operator applied on a population.

b. Crossover: A crossover operator is used to recombine two strings/parents to get better new two strings/kids. It is important to note that no new strings are formed in the reproduction phase.

c. Mutation: Mutation adds new information in a random way to the genetic search process. It is an operator that introduces diversity in the population whenever the population tends to become homogeneous due to repeated use of reproduction and crossover operators.

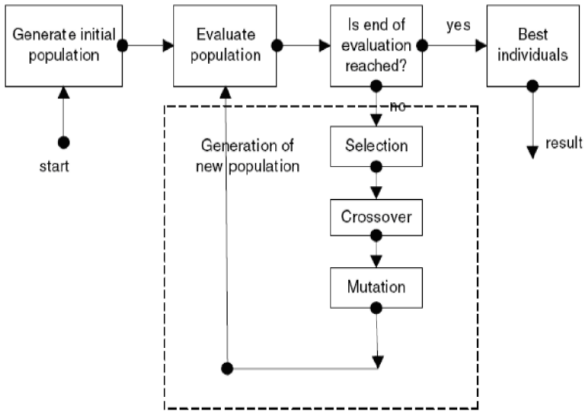


Fig.1. Flowchart of GA system

3) *Fuzzy Theory*

Crisp sets are discriminating between members and non-members of a set by assigning 0 or 1 to each object of the common set. Fuzzy sets simplify this function by passing on values that fall in a specified range, typically 0 to 1, to the elements. Fuzzy set theory overcomes the sharp boundary problem by allowing different degrees of memberships. Let X is the universal set. The function μA is the membership function which defines set A, where $\mu A: X \rightarrow [0, 1]$. Fig. 2 shows difference between non-fuzzy sets and fuzzy sets.

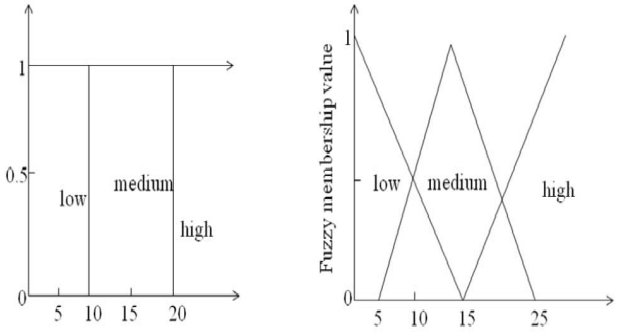


Fig. 2(a) Non-fuzzy sets

Fig. 2(b) Fuzzy sets

4) Data set

KDD99Cup dataset and the Defense Advanced Research Projects Agency (DARPA) datasets provided by MIT Lincoln Laboratory [6] are widely used as training and testing datasets for the evaluation of IDSs.

This database contains a standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment. There are approximately 4,940,000 kinds of data in the training dataset, 10% of which is provided, there are 3,110,291 kinds of data in test dataset, and there are totally 41 types of network connection characteristics (characterized by continuous data and discrete data) in each kind of network connection record. Its property can be divided into three major types: characteristic of network connection content, network transmission characteristic, and Basic characteristic of network connection. Data pattern include numeric, nominal, and binary.[4] The data set contains a total of 24 attack types (connections) that fall into 4 major categories: Denial of service (Dos), Probe, User to Root (U2R),

Remote to User (R2L). Each record is labeled either as an attack, or as normal attack, with exactly one specific attack type.

Probe: Attackers relate probe to get information, to determine the targets and the type of operating system.

Dos (Denial of service): Such attack may cause the server cannot provide services and the stop of server operation. The attack usually occupies the Band-width and disables system resource and makes operation stop. Common attacks are Ping Flooding, SYN Flooding and so on.

U2R (User gain root): In the attack, users take advantage of system leak to get access to legal purview or administrator's purview, such as: Buffer Overflow is among them.

R2L (Remote file access): The attack is to apply the advantage of server providing services, to get related safety setting or user's encrypted files, such as: Unicode leak, SQL Injection, and so on.

III. Proposed Work

A. Fuzzy Class-Association Rule mining with use of Genetic Algorithm

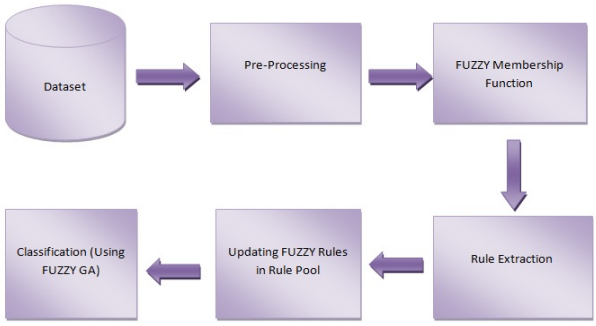
The association-rule mining algorithms, predictable association-rule mining based on GA is able to extract rules with attributes of binary values. However, in real-world applications, databanks are suitable to be composed of both binary and continuous values. For extracting the rules with attributes of continuous value, fuzzy set model is collective with association rule mining algorithm. Fuzzy Class-association-rule mining created on GA method for intrusion detection system overcomes many problems like sharp boundary problem, deals with a mixed database, and increases rule pool size. Therefore, extraction of many rules as compared to other method is possible. Support and fitness factors are calculated for each rule. Fitness function contributes to mining more rules with higher accuracy.

Main Purpose of this system are as follows:

- Avoiding the sharp boundary problem by using fuzzy set theory.
- Use of mixed database, increases the detection rate and increases accuracy.
- Increases the size of rule pool by using the genetic operators.
- Flexibly applied to both misuse and anomaly intrusion detection.

B. System Architecture and Algorithms for Proposed System

The proposed intrusion detection using fuzzy data mining approach with GA contains two major modules each works in a different phase. In the training phase, using fuzzy-association rule mining algorithm and Genetic Algorithm, a set of classification rules are produced from KDD dataset. In the intrusion detection phase, the produced rules are used to classify received data from a test file. Once the rules are produced, the intrusion detection is simple and efficient. Fig 3 shows the proposed system architecture.



C. Data Pre-processing

Intrusion detection methods are misuse intrusion detection and anomaly intrusion detection. For detecting intrusion, rules are mandatory (i.e. rules for attack and normal data). For these, categorization of attack records and normal records from KDD training dataset is essential. Inputs of some main features of this organized dataset are given to the pre-processor. The same pre-processing phases are required for both datasets (i.e. normal and attack dataset). Steps for pre-processing of attributes/features are shown in the following algorithm:

Algorithm: Feature extraction, Classify KDD dataset,
Input: KDD dataset
Output: Dataset into two classes i.e. rule pool (attack and normal)

1. Select the KDD dataset
2. Classify full dataset into "attack" and "normal" class
3. Convert attributes to numeric value
4. Discovered maximum value for each attribute
5. Select main attribute
6. Store rules in rule pool

In above algorithm, data mining classification method is used for classifying the entire dataset into two classes i.e. "attack" and "normal". Feature selection is necessary because the use all available features are computationally infeasible.

D. Genetic Algorithm

Data pre-processing procedure produces rules which are kept in the rule pool like attack rule pool holds records for intrusion and normal rule pool contains normal records the following algorithm is collective for both i.e. attack and normal rule pool and explains about the genetic algorithm and its operators.[3]

Algorithm: Rule pool generation using genetic algorithm.
Input: Pre-processed dataset, number of generations (G), and population size.
Output: Large no. of rules in the Rule pool.

1. Initialize the population
2. N is population size, T (minimum fitness value) = 0
3. User input for number of generations (G)
4. Initialize individuals (I) = 1
5. Initialize fitness counter (K) = 1
6. Select two chromosomes (or rules) from population
7. Increment I by 2, K by 1

8. Apply crossover operator to the chromosome
9. Apply mutation operator to the chromosome
10. If rule is present in rule pool then go to step14 for next rule
11. Else
Estimate the number of connections *Ntc properly* detected by rule *r*
Compute the number of connections in the training data *Nt*
Compute the number of normal connections *Nni* wrongly detected by rule *r*
Estimate the number of normal connections in the training data *Nn*
Compute Fitness value of new chromosome

$$\text{fitness} = \frac{Ntc}{Nt} - \frac{Nni}{Nn}$$

12. If fitness is greater or equal to T then, Improve newly generated chromosome to rule pool
13. Else go to step 14 for next rule
14. Repeat step 10 until K equals to 3
15. Repeat step 5 until I equals to N/2.
16. Increase G by 1.
17. If number of generations is not extended, go to step 4.
18. Show number of rules generated for the input generations.
19. Go to next algorithm that is fuzzy rule extraction.

In the above algorithm, each rule is mentioned to as a chromosome. In each generation, apply crossover and mutation to growth the amount of rules. For Crossover a duo of individuals is determined by first choosing two individuals from the rule pool. A single opinion crossover is used to replicate more individuals. In a single point crossover, interchange of attributes value among two individuals with respect to some point is passed out.
Range of fitness value is [-1, 1], so threshold fitness is 0 in this method. Once the individuals are selected for creation of a pair, avoid repetitive selection of individuals to make other couples. The above procedure is then repeated until no individuals for making pairs are remaining. At the end of this algorithm, a huge number of rules will be obtainable for additional processing. For Anomaly detection, the amount of rules matters more than quality, while for misuse detection quality rules are required. So for together detection systems this algorithm is finest suited.
Once the rule is extracted by GA, then the overlap of the attributes among the rules and already stored rules is checked to decide the rule is newly extracted or not. The fitness of GA individuals for the network intrusion detection is defined by

$$F = \sum_{r \in R} \{w1 * fitness\, r + w2 * \alpha\, new\, (r)\}$$

Where
R = set of suffixes of association rules extracted by individuals

$$\alpha \quad new \quad = \begin{cases} \alpha new & if\ rule\ r\ is\ new \\ 0 & otherwise; \end{cases}$$

w1,w2 = control parameter

E. Fuzzy Logic
Subsequently applying a genetic algorithm on intrusion and normal rule pool, all possible combinations of rules will be simulated. On a huge dataset, apply fuzzy logic to avoid the sharp boundary problem. In this module, kinds of attributes i.e. continuous and discrete are used. For continuous attributes like source bytes, duration, destination bytes, find the maximum values for each attributes and then divide these values into LOW, MEDIUM and HIGH series, and find the fuzzy membership value for each attribute. For discrete attributes, numbers of columns are stable on the basis of types of values for that attribute that is protocol attribute is divided into ICMP, TCP and UDP. The following algorithm displays fuzzy logic implementation for the rule pool.

Algorithm: Fuzzy Rule Extraction.
Input: Attack or Normal rule pool.
Output: Fuzzy Rules in rule pool
1.β= average value of attribute Ai; γ = the largest value of attribute Ai in the dataset;
2. Select features from rule pool
3. Check for missing record for all records
4. Select record from the rule pool
5. Process all selected attribute
6. Divide each continuous attribute into HIGH, MEDIUM and LOW
7. Set fuzzy membership value for each continuous attribute
$\boldsymbol{\alpha + \gamma = 2\beta}$
8. Estimate fuzzy membership value for each continuous attribute
9. Divide each discrete attribute into a number of types
10. Set binary value for each discrete attribute
11. Store all fuzzy rules in fuzzy rule pool
12. Repeat step 5 until all selected columns are covered
13. Repeat step 2 until all records in the rule pool is considered.

Each value of continuous attributes in the database is converted to three linguistic terms (low, middle, and high). A predefined membership function is allocated to each continuous attribute and the linguistic terms can be conveyed by the membership function. The parameters *α*, *β,* and *γ* in a fuzzy membership function for attribute Ai is set as follows:
β is average value of attribute Ai in the database
γ is the largest value of attribute Ai in the database

F. Class-Association-Rule mining (CARM)
After fuzzy operation, the fuzzy rule pool will be created and this rule pool is given as an input to association rule mining. Association Rule Mining is a two-step process:
1. Discovered all frequent item sets by Apriori algorithm.
2. Produce strong association rules from the frequent item sets
For rule generation, antecedent part is produced by using apriori algorithm and for consequent; classification method is used in which the whole KDD dataset is distributed into two classes that is attack and normal class on the base of

labels supplied in the dataset. The following algorithm is used for evaluating the frequent item sets from the dataset that is Apriori algorithm:

Algorithm: Apriori algorithm for finding frequent item sets.
Input: Normalize dataset, minimum support (min_sup) = 0.2
Output: Frequent item sets.
1. Initialize I (no. of records) = 1
2. Scan each record of the fuzzy rule pool.
3. Find number of items (N), number of transactions (M)
4. Increment I by 1 and repeat step 2 until last record in the rule pool
5. Initialize k (number of item set) =1
6. Find frequent item set Lk from Ck of all candidate itemsets
Scan D and count each itemset in Ck,
If count is greater than minimum support (min_sup), then it is frequent
7. Form Ck+1 from Lk; k = k + 1
Join Lk-1 itemset with itself to get the new candidate itemsets,
If found a non-frequent subset then remove that subset.
8. Store frequent itemset in the rule pool
9. Repeat step 6 and step 9 until Ck is empty

At the end of above algorithm, the rule pool contains rules which are used for testing of the system. For misuse detection, train the system by giving attack data as an input and form the rules for attack data. For anomaly detection, train the system by giving normal data as an input and form the rules for normal data.

I. Intrusion Detector Parameter
Detection of intrusions can be evaluated by following metrics:

- False positive (FP): Corresponds to the number of detected attacks but it is in fact normal.
- False negative (FN): Corresponds to the number of detected normal instances but it is actually as attack, in other words these attacks are the target of intrusion detection systems.
- True positive (TP): Corresponds to the number of detected attacks and it is in fact as attack.
- True negative (TN): Corresponds to the number of detected normal instances and it is actually normal.

The accuracy of an intrusion detection system is measured with respect to detection rate and false alarm rate.

A. Detection rate (DR)
Detection rate mentions to the percentage of detected attack between all input test data, and is defined as follows:

$$Detection\ Rate = \frac{TP}{TP + TN} * 100$$

B. False Positive Rate (FPR)
False positive rate mentions to the percentage of normal data which is incorrectly recognized as an attack, and is evaluated as follows:

$$False\ Positive\ Rate = \frac{FP}{FP + TN} * 100$$

C. False Negative Rate (FNR)
False negative rate mentions to the percentage of attack data which is incorrectly recognized as normal, and is defined as follows:

$$False\ Negative\ Rate = \frac{FN}{FN + TP} * 100$$

IV. Experimental Result

In this segment, the efficiency and effectiveness of the proposed technique are calculated using KDD 1999 Cup dataset.

A. Misuse Detection
The proposed method for misuse detection is carried out with KDD 99 Cup database in order to compare results with other machine-learning methods. The training dataset contains 400 attack connections randomly selected from KDD 99 Cup database, where four types of attacks (Dos, Probe, U2R and R2L) are included. A total of 6 attributes are involved in every connection; first 6 attributes is duration, protocol type, flags, service, source bytes and destination bytes respectively. Every rule is extracted if it happens recurrently with a statistically major level in the database. So, each rule is extracted from the entire database by taking into version all the connection data.
The testing database holds 500 labeled connections wherever 400 are labeled intrusion connections and 100 are normal connections. The detection output obtained by the proposed misuse detection classifier are shown in Table 1, where T signifies the label of the testing results shown by the classifier and C represents the correct label. DR, FPR and FNR are the criteria for evaluation of testing results.

Table 1 Testing Outcome of Misuse Detection

	Normal	Attack	Total
Normal	98	2	100
Attack	12	388	400
Total	110	390	500

*Detection Rate (DR) = ((98 + 388)/500)*100 = 97.2 %*
*False Positive Rate (FPR) = (2/100)*100 =2%*
*False Negative Rate (FNR) = (12/400)*100 = 3%*

Table 2 shows an evaluation between fuzzy data mining and crisp data mining for a misuse detection method. For crisp data mining used 3342 connections casually from the KDD dataset.[7] For fuzzy data mining simply 400 connections are used. The comparison table shows that detection rate for crisp data mining methodology is 98.3% by using 3342 original population. But proposed approach (fuzzy data mining) gives 97.2% outcome by seeing 400 connections as an initial population and 250 numbers of generations. This displays fuzzy data mining technique provides extra accurate outcomes than other method. For misuse detection, if attack rule pool includes accurate signatures for intrusion, then system will provide extra accurate result.

Table 2 Comparison of the Detection Rate between Crisp Data Mining and Fuzzy Data Mining in the Misuse Detection

	Proposed Approach (%)	Crisp Data Mining (%)
Detection Rate (DR)	97.2	98.3
False Positive Rate (FPR)	2	0.67
False Negative Rate (FNR)	3	5

B. Anomaly Detection

The proposed technique for anomaly detection is calculated by KDD database. The training database is intrusion-free for the determination of anomaly detection. It contains 350 normal connection records. After some generations, 1758 rules connected to the normal connections are extracted. The testing database holds 500 connection records containing 100 labeled normal records and 400 labeled intrusion records. Since the training database for anomaly detection is intrusion-free (normal rule pool), all types of intrusions (such as back, land, ipsweep, pod, neptune, port sweep, satan, teardrop and smurf) are measured as intrusion.

Table 3 Testing Result of Anomaly Detection

	Normal	Attack	Total
Normal	97	3	100
Attack	18	382	400
Total	115	385	500

*Detection Rate (DR) = ((97 + 382)/500)*100 = 95.8 %*
*False Positive Rate (FPR) = (3/100)*100 =3%*
*False Negative Rate (FNR) = (18/400)*100 = 4.5%*

Table 4 shows a evaluation among fuzzy data mining and crisp data mining for a misuse detection method. For crisp data mining used 9137 connections casually from the KDD dataset. For fuzzy data mining simply 350 connections are used. So the result is greater than this for 9137 connections. This shows that the fuzzy data mining method gives more accurate results than other method. For anomaly detection, the system involves more normal rules than accurate; if numbers of rules are various then system will give great detection rate.

Table 4 Comparison of the Detection Rate between Crisp Data Mining and Fuzzy Data Mining in Anomaly Detection

	Proposed Approach (%)	Crisp Data Mining (%)
Detection Rate (DR)	90.3	98.3
False Positive Rate (FPR)	10.3	0.67
False Negative Rate (FNR)	9.5	5

V. CONCLUSION

Data mining techniques are proficient of extracting patterns habitually and adaptively from a huge amount of data. Various methods related to intrusion detection system are compared and studied. Crisp data mining methods are used for intrusion detection but suffer from sharp boundary problem which gives less accurate results. In proposed technique, use of fuzzy logic overcomes the sharp boundary problem. Class-Association rules have been used to mine training data to established normal patterns for anomaly detection. An actual intrusion with a small eccentricity may match the normal patterns and thus not be detected. Therefore, integration of fuzzy logic with class-association rules and GA generates extra flexible patterns for anomaly detection.

In this paper, we have proposed a GA-based fuzzy Class Association Rule Mining with Sub-Attribute Consumption and its application to classification, which can deal with continuous and discrete attributes at the equal time. In addition, this technique was applied to both misuse detection and anomaly detection. Experiments were achieved with practical data provided by KDD99 Cup. The experimentation results show that for misuse detection, the proposed technique can delivers high detection rate and low false positive rate, which are two important criteria for security systems. For anomaly detection, the process provides high detection rate and reasonable false positive rate even without prior information of attack signatures, which is a significant improvement over other techniques.

REFERENCES

[1] Mabu S., Chen C., Shimada K., "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming," IEEE Transactions Systems, Man, Cybernetics C, Application and Reviews, volume 41, number 1, pp. 130–139, January 2011.

[2] Hoque M., Mukit M. and Bikas M., "An Implementation of Intrusion Detection System using Genetic Algorithm," International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012 .

[3] Lu W. and Traore I., "Detecting new forms of network intrusion using genetic programming," Computer Intelligence, volume 20, no. 3, pp. 474–494, 2004.

[4] Sathya s., Ramani R., Sivaselvi K., "Discriminant Analysis based Feature Selection in KDD Intrusion Dataset," International Journal of Computer Applications (0975 – 8887), Volume 31– No.11, October 2011

[5] Denning D., "An intrusion detection model," IEEE Trans. Software Eng., vol. 13, no. 2, pp. 222–232, Feb. 1987.

[6] Ektefa M., Memar S., ―Intrusion Detection Using Data Mining Techniques,‖ IEEE Trans., 2010.

[7] Kddcup 1999data [Online]. Available: kdd.ics.uci.edu/ databases/kddcup99/kddcup99 .html.

[8] Harshna, NavneetKaur, ―Survey paper on Data Mining Techniques of Intrusion Detection‖, IJSETR, vol-II, issue-4, April 2013.

[9] Z. Bankovic, D. Stepanovic, S. Bojanic, ―Improving Network Security using Genetic Algorithm Approach,‖ Computer and Electrica l Engineering, pp. 438-451, 2007

[10] Semaray J., Edmonds J., and Papa M., "Applying data mining of fuzzy association rules to network intrusion detection," presented at the IEEE Workshop Information, United States Military Academy, West Point, NY, 2006.

[11] Abdullah B., Abd-alghafar I., "Performance Evaluation of a Genetic Algorithm Based Approach to Network Intrusion Detection System," 13th International Conference on Aerospace Sciences & Aviation Technology, ASAT- 13, 2009

[12] Shanmugam B. and Idris N., "Hybrid Intrusion Detection Systems (HIDS) using Fuzzy Logic", Advanced Informatics School (AIS), University Technology Malaysia International Campus, Kuala Lumpur, Malaysia.