International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-2 Issue-15 June-2014

Mining Association Rules to Evade Network Intrusion in Network Audit Data

Kamini Nalavade[1], B.B. Meshram[2]

Abstract

With the growth of hacking and exploiting tools and invention of new ways of intrusion, intrusion detection and prevention is becoming the major challenge in the world of network security. The increasing network traffic and data on Internet is making this task more demanding. There are various approaches being utilized in intrusion detections, but unfortunately any of the systems so far is not completely flawless. The false positive rates make it extremely hard to analyse and react to attacks. Intrusion detection systems using data mining approaches make it possible to search patterns and rules in large amount of audit data. In this paper, we represent a model to integrate association rules to intrusion detection to design and implement a network intrusion detection system. Our technique is used to generate attack rules that will detect the attacks in network audit data using anomaly detection. This shows that the modified association rules algorithm is capable of detecting network intrusions. The KDD dataset which is freely available online is used for our experimentation and results are compared. Our intrusion detection system using association rule mining is able to generate attack rules that will detect the attacks in network audit data using anomaly detection, while maintaining a low false positive rate.

Keywords

Intrusion, Security, Association rule mining, Network, Data mining

1. Introduction

Communication on Internet, in spite of implementation of advanced security measures, is always under innovative and inventive attacks. Given the different type of attacks like Denial of Service, Probing, Remote to Local, User to Root and others, it is a challenge for any intrusion prevention system to detect a wide variety of attacks. The goal of intrusion detection systems is to automatically detect attack from the continuous stream of network data traffic and generate alarm for administrator. Two methods are used for intrusion detection: Signature based detection and Anomaly based detection. Signature based systems are used to detect known attacks and require prior knowledge of attack signatures. These methods perform rule matching to detect intrusions. But these kinds of systems are not sufficient to detect new or unknown attacks. Anomaly detection systems assume that an intrusion is an deviation of the system behaviour from its normal pattern. In such cases use of data mining and machine learning approaches can be used for intrusion detection. Data mining algorithms can be used to discover patterns, relationships, factors, clusters, associations, profiles, and prediction that were previously "hidden". Using normal reports, Data mining can produce decisions and create alerts when action is required.

Association rule mining is generally used to find the interesting rules from a large database depending upon the user defined support and confidence. A frequent item set is defined as one that occurs more frequently in the given data set than the user given support value. One more threshold confidence is used to restrict the association rules to a limited number. Confidence also includes the item sets having low support but from which high confidence rules may be generated. Suppose I is the set of itemsets, an association rules is an implication of the form, A=>B, where A subset of I, B subset of I & A∩B=Ø. The rules A=>B holds in transaction set T with support s if s% of the transactions in T contain both A and B. Similarly the rule A=>B holds in T with confidence c if c% of the transactions in T support A also support B. [1]

By analysing the audit logs, meaningful data can be extracted to generate better detection models. We can mine association rules from system audit data and use these generated rules to detect anomalies. Identifying association patterns in intrusion data set will help to design better Intrusion Detection and Prevention System (IDPS). The major objective of this paper is

Manuscript received May 26, 2014.
Kamini Nalavade, Computer Department, V.J.T.I., Matunga, Mumbai India.
B.B. Meshram, Computer Department, V.J.T.I, Matuna, mumbai, India.

to build an intrusion detection system using association rule mining. Association rule mining means generating interesting rules from audit data to detect unknown intrusions. The paper is organized as follows: Section 2 we provide the related work done in this research area. Section 3 explains the association rule mining and apriori algorithm for intrusion detection. In section 4 we describe our proposed system for network intrusion detection and prevention. Section 4 illustrates the experimentation and results carried out followed by conclusion.

2. Previous Work

M.Sulaiman khan, Maybin Muyeba and Frans Coenen[2] described weighted association rule mining from fuzzy data in their paper. In their paper [5], they proposed association rule mining for weighted value not necessarily binary value. The value should be continuous or discrete value to be presented in the database. Murtagh, and Farid, in their paper on Weighted Association Rule Mining Using Weighted Support and Significance Framework addressed the issues of discovering significant binary relationships in transaction datasets in a weighted setting[3]. The focused on those significant relationships involving items with significant weights rather than being flooded in the combinatornal explosion of insignificant relationships. In 2001, Li, F proposed an approach for association rule mining for weighted association rules [4].

Wang and Fan [6] proposed non-iterative improved Apriori algorithm to discover IDS alerts. They used intersection of two distinct rows of (DARPA 99 dataset to detect reoccurring patterns. If same pattern is repeated in many intersection operations, then it is considered as interesting pattern and used as Intrusion alert. Zhang yanyan and Yao Yuan [7] presented partition-based association rule detection algorithm for IDS rule generation. During first pass they partitioned training database in such a way that each partition of database can be entirely copied into a main memory of processing device. Then Large Item sets for each partition are identified independently. The union of these large item sets is then used as candidate large item sets for complete dataset. During second pass, large item sets for complete database are identified. This algorithm cannot be efficiently converted into incremental association rule detection algorithm and time complexity of it is very high.

In 2009 Flora S. Tsai [8] described network intrusion detection system using association rule mining in his paper. This method helped to generated interesting rules from the KDD data set. The intrusion detection dataset KDD99 contains variety of data starting from binary, discrete and continuous data. So, it is very difficult to generate rules for a particular attack using same approach. To find the association rules Ming-Yang Su et al [9] proposed incremental fuzzy association rules mining algorithm for Network Intrusion Detection System. They used link list of link list to store all possible candidate item sets and their support count in main memory. This information is updated periodically using network traffic data collected. Updated information is then used by incremental algorithm to identify large and interesting item sets, which are used as rules for NIDS. The major drawback of this algorithm is huge main memory requirement to sore all candidate item sets of every size.

3. Association Rule Mining for Intrusion Detection

Data mining generally refers to the process of extracting or mining knowledge from a large amount of data. This process is the core of Knowledge Discovery and Data mining (KDD). Association rule mining is the task of discovering correlations and patterns from the dataset. Association rules mining started as a technique for finding interesting rules from transactional databases [1].

Association rule problem : Given a set of items I={I1,I2,…,Im} and a database of transactions D={t1,t2, …, tn} where ti={Ii1,Ii2, …, Iik}, the Association Rule Problem is to identify all association rules A =>B which satisfy minimum support and confidence where A is subset of I and B is subset of I[13].
The support of the rule is the percentage of transactions that contains both A and B in all transactions and is calculated as

Support= $\frac{\Phi(AUB)}{\Phi(N)}$

Confidence= $P(A/B)=\frac{Support(AUB)}{Support(B)}$

The support of the rule measures the significance of the correlation between itemsets. The confidence is the percentage of transactions that contain B in the transactions that contain A. The support is a measure

of the frequency of a rule and the confidence is a measure of the strength of the relation between the sets of items.

Two Step Process of association rule mining:
i) Frequent itemset identification
Discover the large itemsets that have transaction support above a predefined minimum threshold. Given d items, there are 2^d possible candidate itemsets

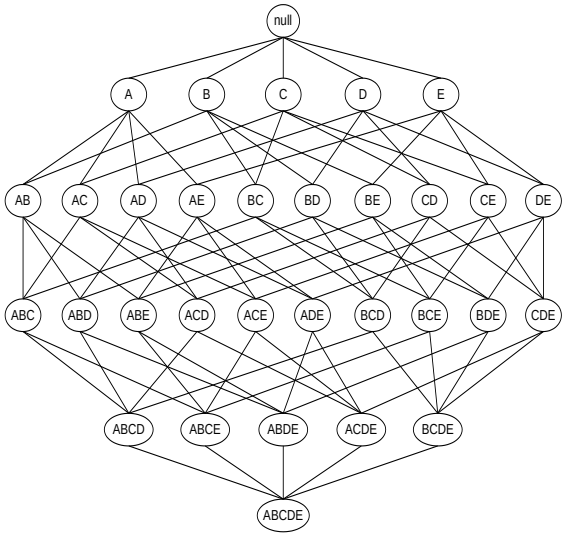


Figure 1: Frequent itemset generation

ii) Rule generation from frequent itemset
Use the obtained large itemsets to generate the association rules that have confidence above a predefined minimum threshold. Different datasets available for intrusion detection are DARPA, KDDcup99 etc. These datasets features contain values which may be binary, continuous or discrete. To discover the association rules from the dataset, various approaches should be applied for different kind of dataset as follows.

A. Association Rule Mining for Binary Value
For binary weighted value it is easy to find out the frequent item set. In association rules mining weights are considered as the highest priority. In those rules Apriori algorithm is executed in two steps. First it generates candidate sets. Second, it prunes the entire non-frequent item set after each step using the minimum support and the weight of the item. Many non-frequent itemsets are eliminated by the pruning process.

B. Association Rule Mining for Continuous Value
If a particular attribute takes a value in the range [0…1] it is taken as a continuous attribute. This could be taken as Fuzzy data and hence fuzzy weighted association rule mining as described in[2][5] could be used here. The weight of fuzzy data can be defined as Fuzzy Item Weight (FIW). Now Fuzzy Item set Transaction Weight (FITW) is the aggregate weights of all the fuzzy sets associated with the items in the item set present in a single transaction. From this FITW support and Confidence value can be calculated as per generalizing the notion of support.

C. Association Rule Mining for Discrete value
If the range of values that an attribute in the data set is very large, then normalization of the data becomes very difficult. The traditional approach to deal with this type of data is to convert each value into a set of binary values. The discrete attributes are normalized i.e. we find a set of thresholds that can be used to convert the attributes into a categorical variable. This kind of normalization affects the accuracy of the rule generation technique which may lead to higher misclassification rate [1].

Apriori Algorithm
There are different types of algorithms used to mine frequent item sets from the dataset. One of the most popular data mining approaches is to find frequent item sets from a transaction dataset and derive association rules is Apriori algorithm. Many of the patterns finding algorithms such as decision tree, classification rules and clustering techniques that are frequently used in data mining have been developed in machine learning research community. Frequent pattern and association rule mining is one of the few exceptions to this tradition. The introduction of this technique boosted data mining research and its impact is tremendous. The algorithm is quite simple and easy to implement. Since Apriori algorithm was first introduced and as experience was accumulated, there have been many attempts to devise more efficient algorithms of frequent itemset mining. Many of them share the same idea with Apriori in that they generate candidates. These include hash-based technique, partitioning, sampling and using vertical data format.

Apriori is a seminal algorithm for finding frequent item-sets using candidate generation [12]. It is characterized as a level-wise complete search algorithm using anti-monotonicity of item-sets, "if an

item-set is not frequent, any of its superset is never frequent".

Apriori Property It is an **anti-monotone** property: if a set is not frequent, all of its supersets will not frequent as well. In other words all nonempty subsets of a frequent itemset must also be frequent. An itemset I is not frequent if it does not satisfy the minimum support threshold: P(I) < min_sup If an item A is added to the itemset I, then the resulting itemset cannot occur more frequently than I.[10]

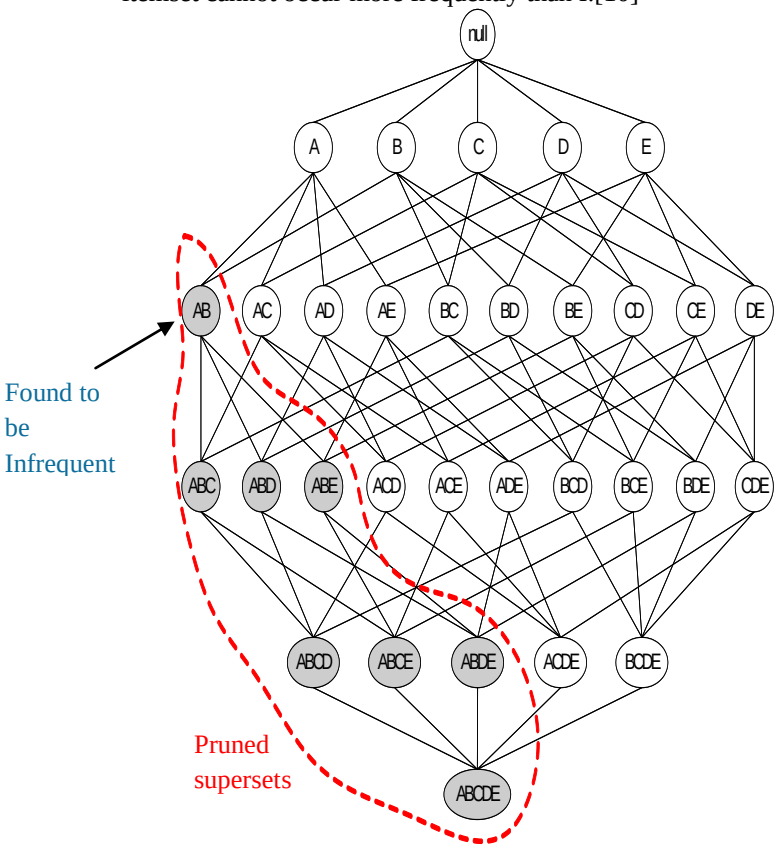


Figure 2: Apriori frequent itemset generation [10]

Pseudo code[12]
Ck: Candidate itemset of size k Lk
: frequent itemset of size k
L1 = {frequent items};
for (k = 1; Lk !=Æ; k++) **do**
- Ck+1 = candidates generated from Lk;
- **for each** transaction t in database **do**
increment the count of all candidates in Ck+1 that are contained in t;
endfor;
- Lk+1 = candidates in Ck+1 with min_support
endfor; return k Lk;

4. Proposed Intrusion Detection and Prevention System

In this paper, we propose a network intrusion detection and prevention system model that analyses the various item set generated, specifically on attribute relation. In our system, we apply association rule mining to generate attack signatures from the network traffic data. We propose an Intrusion detection and prevention system as shown below:

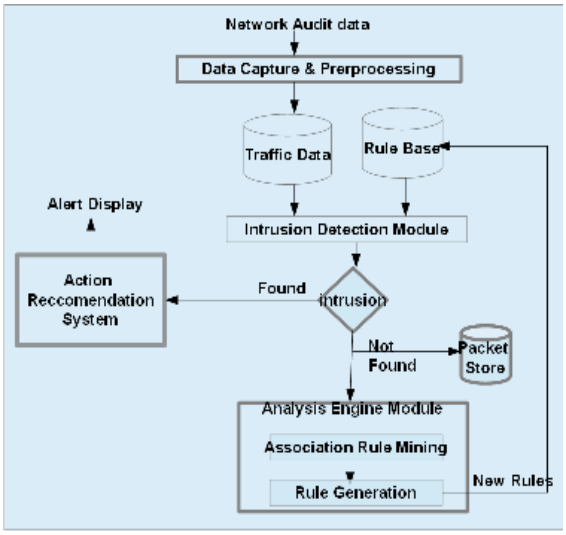


Figure 3: Proposed Intrusion Protection System

As shown in figure 3, we propose a network intrusion protection system using data mining feature which will work at all layers of TCP/IP. The modules of our system are
1. Data Pre-processing
2. Intrusion Detection Module
3. Analysis Engine
4. Recommendation system

When a packet is received Intrusion detection module performs signature matching with the Rule base. If intrusion is found Recommendation Engine is triggered. These attacks have some standard signatures which are verified with the contents of packets. As from our research we studied that the attacks are either carried out by crafting header part of protocols or inserting some malicious code in data part. Otherwise packet is stored for the future analysis. Data mining and analysis module is invoked by NIPS to perform intrusion analysis on the captured packets to decide the future security policy. Recommendation engine is capable of generating alarms along with the features of blocking IP

addresses, blocking ports, black list maintenance, discarding connection and reporting errors.
Pre-processing is the organization of collected data from sensors in a particular pattern. This data is then placed in a structured database format by means of parsing and reconstructing. The cleansing process is protocol specific as we need different attributes of packets for intrusion analysis. If packet is from blacklisted source then system should discard packet without verifying it.
The analysis begins with application of frequent itemset mining to the collection of traffic database. Our proposed system uses association rule mining algorithm to generate attack signatures. The Apriori algorithm will find out frequent itemsets from the pool of data with support and confidence values. This support and confidence values will help in decision making about the severity and sensitivity of intrusion. The generated rules are stored in the rule base for future packet inspection. Our approach for intrusion detection works as follows:

1. First algorithm finds all frequent itemsets from the data.
2. After finding the frequent item set, support and confidence values, rules have to be generated for each attack types.

Frequent itemset generation is carried out by applying Apriori Algorithm to the dataset. For Rule generation we apply the following algorithm.
Here LFset contains the largest frequent item set. Min_sup defines the user define support and Min_conf defines the user defines confidence. RULEGeneration contains the desired rules generated from data set. The algorithm is explained as follows:

Rule Generation Algorithm
Input: Large frequent itemset LFset
Minimum support Min_Ssp
Minimum confidence Min_Conf
Output: Attack Signatures

Step1 : Generate all possible subsets of LFset and store it in FSTORE.
Step2: Count SUP and CONF value for each elements of FSTORE.
Step3: If (SUP>=Min_Sup && CONF>=Min_Conf) then
Step 3.1: Choose the particular elements of FSTORE and store in RULEGeneration
Step 3.2: Continue to generate rules and save in RULE Generation for all frequent sets.
Step4: Else reject the particular element of FSTORE and go to next.
Step5: Return RULEGeneration.
Step6: End.

5. System Evaluation and Results

In this section we demonstrate how the system parameters are decided and fixed. Also the different performance parameters used to evaluate the system. Then we discuss the results achieved in intrusion detection using k-means clustering algorithm on KDD cup dataset. Next we evaluated the performance of k-means clustering algorithm with different values of initial cluster.

5.1 Dataset and Normalization of data

The dataset used is KDDcup1999 [11] intrusion dataset which contains wide variety of intrusions simulated in network environment to acquire nine weeks of raw TCP dump data for a local-area network. A connection is a sequence of TCP packets starting and ending at some well-defined times, between which data flows to and from a source IP address to a target IP address. Each connection is labeled as either normal, or as an attack, with exactly one specific attack type. It is important to note that the testing data is not from the same probability distribution as the training data. This makes the task more realistic. The attacks in each class are as shown below:

Table 1: Classes of Attacks

S.N	Class	Attack Types
1	DOS	Back, Land, Neptune,pod, smurf, Teardrop,
2	U2R	Buffer_overflow, loadmodule, perl, rootkit
3	R2L	ftp_write, guess_passwd, imap, multihop, phf, spy,warezlient, warezmaster
4	Probe	IPsweep,nmap, satan,portsweep

The 22 different types of network attacks in the KDD99 dataset fall into four main categories: DOS (Denial of Service), Probe, R2L (Remote to Local), U2R (user to remote). There are 41 features for each connection record that are divided into discrete sets and continuous sets according to the feature values. It consists of number of total records 494021. In order to know how to read the data from the audit data, we need to analyze how the audit da ta is being recorded. The audit data is processed for data mining purpose and is split into two files, the training set which

contains around five million rows and the test set with 10% of the training set.

Table 2: Distribution of records

	Original Records	Distinct Records	Reduction Rate
Attacks	3925650	262178	93.20%
Normal	972781	812814	16.44%
Total	4898431	1074992	78.05%

The table above show the distribution of KDD dataset in the 10 % training data.

5.2 Performance Parameters

There are many measures available for evaluating system performance. For evaluating intrusion detection results following measure are generally used.

1. True positive (TP) means number connections that were correctly classified as intrusion.
2. True Negative (TN) means number of connections that were incorrectly classified as intrusion.
3. False positive (FP) means number of intrusion connections that were incorrectly classified as normal.
4. False negative FN) means number of normal connections that were incorrectly classified as intrusion.

To determine how many misclassification are found we use term Recall. Precision is how many records are correctly classified by the system.

Precision=TP/TP+FP……..(1)

Recall=TP/TP+FN…… .(2)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad \text{.....(3)}$$

Confusion Matrix for Intrusion Protection System

Table 3: Confusion Matrix

	Predicted Class		
Actual Class		Normal	Attack
	Normal	TP	FN
	Attack	FP	TN

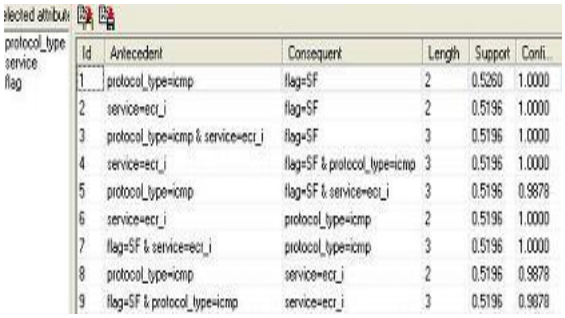
In the next section, we present two sets of experiments, each designed to demonstrate a different point. The first set is used to demonstrate the frequent item set generation from the KDDcup99 dataset using association rule mining with different support and confidence value. The second set of results shows the attack signatures generated are different cluster values for k-means algorithm affects the performance of system.

5.3 Experimental results-I: frequent item set generation, support and confidence values

The proposed method for misuse detection is carried out with KDD99 Cup database in order to compare results with other machine-learning methods. The training dataset contains 400 attack connections randomly selected from KDD99 Cup database, where four types of attacks (Dos, Probe, U2R and R2L) are included. Experiment is performed on laptop with Intel Core i5-3230M CPU@ 2.60 GHz and 4 GB Ram. Operating system installed was Windows7. Algorithm was implemented using Java language. KDD 99 dataset is used to perform experimental tests. KDD 10% training data is used for finding Association rules to detect DoS attacks. Then KDD test data with corrected labels is used to test the accuracy of generated Association rules.

Rule Mining for Symbolic features:

Initially 3 symbolic features were selected, protocol_type, service and flag. Minimum support is 50% and minimum confidence is 80%. Number of rounds performed is 10 and 9 rules were generated as shown below:



Id	Antecedent	Consequent	Length	Support	Confi...
1	protocol_type=icmp	flag=SF	2	0.5260	1.0000
2	service=ecr_i	flag=SF	2	0.5196	1.0000
3	protocol_type=icmp & service=ecr_i	flag=SF	3	0.5196	1.0000
4	service=ecr_i	flag=SF & protocol_type=icmp	3	0.5196	1.0000
5	protocol_type=icmp	flag=SF & service=ecr_i	3	0.5196	0.9878
6	service=ecr_i	protocol_type=icmp	2	0.5196	1.0000
7	flag=SF & service=ecr_i	protocol_type=icmp	3	0.5196	1.0000
8	protocol_type=icmp	service=ecr_i	2	0.5196	0.9878
9	flag=SF & protocol_type=icmp	service=ecr_i	3	0.5196	0.9878

Figure 4: Frequent Itemsets Generated with support and confidence values

Rule mining for a total of 6 attributes:

First 6 attributes that is duration, protocol type, service, flag, source bytes and destination bytes of KDD99 dataset is selected for frequent itemset generation respectively. 35 rules generated, with 11 frequent itemsets.

In third check we selected all nominal attributes of the dataset. We could generate 837 rules from the

dataset with 154 frequent itemsets. Note we have kept support and confidence value constant for the experimentation.

5.4 Experimental results-II: Rules generated

This method generates frequent rules for intrusion detection system whose occurrences exceed a predefined minimum support threshold. The threshold in proposed model is equal 70% and confidence is 80%.

The sample rules which we received from the system are shown below in table

Table 4: Rules Table

No	Rules generated	Attack Types	Description
1	(service = http, flag = S0) (service = http, flag = S0) → (service = http, flag = S0)	SYN flood attack	Means that 80% of all the http connections have duration less than one second.
2	service=ecr i, host count ≥ 5,host srv count ≥ 5.	smurf	If the service is icmp echo request, e number of connections that have the same destination host as the current one is at least 5
3	host REJ % ≥ 83%, host diff srv %≥ 87%.	satan	The % of rejected connections are at least 83%, and the % of different services is min 87%
4	hot>3 → root_shell>0	Buffer overflow	If the no of hot indicators is 3, and a root shell is obtained, then connection is a buffer overflow attack.
5	src_bytes<=100 → dst_host_same_src_port_rate	Buffer overflow	If src bytes is less than 100 and destination and host have same port no then buffe overflow
6	failed_logins>4 ->protocol=TCP, dst_port=23	Guess password	If number of failed logins is more than 4 on a telnet connection then it is an guess password attack.

The above table shows some of the rules generated from frequent itemsets. Only the sets satisfying minimum support and confidence are selected as per rue generation algorithm given above.

Although our models were intended for misuse detection, we had hoped that the features we constructed would be general enough so that the models can detect new variations of the known intrusions. We need to use anomaly detection models on network traffic or system programs to guard against the new and diversified attacks. Anomaly detection is much more challenging than misuse detection. Our future work includes developing network anomaly detection strategies, and devising a mechanical procedure to translate our automatically learned detection rules into modules for real-time IPSs. The evaluation of Apriori algorithm with the five attacks of KDD dataset is shown below in the table.

Table 5: Performance of Apriori with KDD

S.N.	Attack Type	FP Rate	Accuracy
1	Neptune	0	100
2	Smurf	3.75	0.95
3	Land	1.42	0.56
4	Pod	7.12	0.92
5	satan	0.01	0.91

6. Conclusion and Future Work

Intrusion Detection is also increasingly valued by everyone. With the rapid development of Internet, network security issues also wants to highlight, combining data mining algorithms, Intrusion Detection can prevent network intrusion, greatly improving security Currently Network-based intrusion detection detects intrusions based on signatures. The association rules mining is the base of the data mining models built. The quality of this algorithm lies in the level of efficiency and speed. The paper discusses the association rules and the Apriori algorithm which is applied to Intrusion Detection problems. Association rules algorithm is an important data mining algorithms. In this paper we present a framework to look for evasions over a given intrusion dataset. Evasion technique is used for detecting new attacks based on the information of known attacks. The aim of using our framework is not to break the detection of the NIPS. For this purpose we are using the KDD cup 1999 dataset and

applying the signature Apriori algorithm which is well known and widely used for intrusion detection. This framework used to detect the unknown attacks with high accuracy rate and high efficiency. This type of evade NIPS has very vast scope in future like one is to create our own dataset. The other is to analyse if these techniques can be applied straight to model a commercial NIPS.

Acknowledgment

I express deep sense of gratitude for my Institute Sandip Institute of Engineering & Management, Nasik for their support, appreciation and motivation.

References

[1] Asim Das, S.Siva Sathya, "ASSOCIATION Rule Mining For Kdd Intrusion Detection Data Set ", International Journal Of Computer Science And Informatics Issn (PRINT): 2231 –5292, Volume-2, Issue-3, 2012.

[2] M. Sulaiman Khan, Maybin Muyeba, Frans Coenen,"Weighted Association Rule Mining from Binary and Fuzzy Data", ICDM 2008, LNAI 5077, pp. 200–212, 2008.

[3] Tao, F., Murtagh, F., Farid, M, "Weighted Association Rule Mining Using Weighted Support and Significance Framework". In: Proceedings of 9th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, pp. 661- 666, Washington DC, 2003.

[4] Lu, S., Hu, H., Li, F, "Mining Weighted Association Rules", Intelligent data Analysis Journal, 5(3), 211 - 255, 2001.

[5] M. Sulaiman Khan, Maybin Muyeba, Frans Coenen, David Reid,"Mining Fuzzy Association Rules from Composite Items", Lecture Notes in Computer Science Volume 5433, 2009, pp 62-74.

[6] Wang Taihua, Guo Fan, "Associating IDS Alerts by an Improved Apriori Algorithm", Third International Symposium on Intelligent Information Technology a nd Security Informatics, 978-0-7695 -4020-7/10, 2010 I EEE, pp. 478 – 482.

[7] Zhang yanyan,Yao Yuan, "Study of Database Intrusion Detection Based on Improved Association Rule Agorithm",978-1-4244-5540-9/10, 2010 IEEE, pp. 673 – 676.

[8] Flora S. Tsai, "Network Intrusion Detection Using Association Rules". In International Journal of Recent Trends in Engineering, vol 2, No 2, November 2009.

[9] Ming-Yang Su, Kai-Chi Chang, Hua-Fu Wei, Chun-Yuen Lin, "A Real-time Network Intrusion Detection System Based on Incremental Mining Approach", 1-4244-2415-3/08, 2008 IEEE, pp. 179 – 184.

[10] www.seas.gwu.edu/~bell/csci243/lectures/ar.doc.

[11]kdd.ics.uci.edu/database/kddcup99/kddcup99.htm.

[12] R.Aggarwal, T. Imielinski, A. Swami, "Mining association rules between sets of items in very large database," Proceedings of ACM SIGMOD conference, 1993.

[13] Agarwal, R. Srikant, "Fast Algorithms for Mining Association Rules". In: "20th VLDB Conference, pp.487- 499, 1994.

Kamini C. Nalavade received the B.E. degree in computer science and engineering from the SGGS, College of engineering and technology, Nanded in 2001 and M.Tech degree in computer engineering from Veermata Jijabai Technological Institute (VJTI), Mumbai in 2007. She is currently PhD student in the department of computer engineering, VJTI, Mumbai. Her research interest includes intrusion detection, network security, data mining and data privacy. She has published more than 20 papers in International journals and Conferences.

Dr. B. B. Meshram is currently professor and Head of Computer Technology Department of Veermata Jijabai Technological Institute (VJTI), Matunga, Mumbai (INDIA). His areas of interest include Object oriented database management systems, Computer network security and multimedia systems. He has published more than 200 papers in National & International Conferences & refereed Journals. He has submitted more than five patents in his research interest area.