MULTI-LAYER CLASSIFIER FOR MINIMIZING FALSE INTRUSION

Shaker El-Sappagh, Ahmed saad Mohammed, Tarek Ahmed AlSheshtawy

Faculty of Computers & Informatics, Benha University, Egypt.

ABSTRACT

Intrusion detection is one of the standard stages to protect computers in network security framework from several attacks. False alarms problem is critical in intrusion detection, which motivates many researchers to discover methods to minify false alarms. This paper proposes a procedure for classifying the type of intrusion according to multi-operations and multi-layer classifier for handling false alarms in intrusion detection. The proposed system is tested using on KDDcup99 benchmark. The performance showed that results obtained from three consequent classifiers are better than a single classifier. The accuracy reached 98% based on 25 features instead of using all features of KDDCup99 dataset.

KEYWORDS

Intrusion detection, multi-layer classifier, KDD CUP 99, False Alarms

1. INTRODUCTION

Nowadays, communication technology is widely used for communication and transmission purposes in many applications working on different platform. This captures the attention towards network security. In this technology, the security becomes a challenging problem and vulnerable for intrusions. Subsequently, it is necessary to utilize a system for network security such as the intrusion detection systems (IDSs) [1, 2]. Network Intrusion Detection systems had become the most important components of recent network infrastructure due to the effects of fast security threats in today's computer network. Intrusion detection system is generating a good number of alarms; however, it deployed algorithmic procedures to reduce false positives [3]. The great number of false positive alarms is made it difficult for security analyst to recognize successful attacks and to take reconditioned actions for such threat. Alarms contain a high rate of unsuccessful alarms recognized as false alarms which demand estimation to recognize and reduce the unsuccessful ones. These are raised once an intrusive incident detected and presenting the security analyst the chance to react against any such threat [4]. Data Mining (DM) and machine leaning are commonly utilized within the scope of intrusion detection to find the hidden patterns of intrusions and their connection surrounded by each other . DM can be applied to understand from traffic data utilizing the target learning procedures to discover intrusion models of evaluation learning procedures to recognize dubious actions [5].

Classification is one of DM categorization that assigns topics to one of several classes [6].The huge issue in IDSs that the presence of huge number of false alarms; this issue motivate several experts to discover the solution for minifying false alarms.This research will be suggesting multi-classifier for handling this issue.

In this research, a new multi-classifier is suggested for improving the minifying false alarms in intrusion detection system. The basic idea is to use multi classifiers instead of using one classifier. The remaining of this paper is organized as follows: In section 2, we present previous works of

applying classification techniques for intrusion detection. Section 3, we present the description of KDDCUP99 dataset. Section 4, we discuss the attacks type of KDDCUP99. Section 5, we display the performance measure of the intrusion detection system. Section 6, we explain all steps of the proposed system, Section 7, we display the results that are obtained from the proposed system and finally in Section 8, we provide the important conclusions of the proposed system

2. PREVIOUS WORK

Many classification techniques are used for classifying intrusion detection datasets. Classifiers have been suggested and developed to reduce false alarm of intrusion detection in the scope of network security based on different ideas. Recently papers in this scope can be summarized as follows: Aggarwal and Sharma [7], selected a set of classification algorithms on the basis of their effectiveness according to speed and, the ability of handling large data-set and after that, for KDD'99 data-set simulated 10 selected existing classifiers according to Weka tool. Manju [8], analyzed the performance of the Intrusion Detection System using various classification approaches. The objective of this paper was to analyze and predict the network attacks by classifying them as normal and abnormal, and for implementing and measuring the efficiency of this system, the standard KDD99 benchmark data-set has been chosen. Gupta. et al.[9], implemented a variety of data mining procedures which consisted of linear regression and K-means for automatic generation of rules for classifying network activities. A comparative study of those algorithms for detecting intrusions has been made based on the KDD99 data-set as well. Liyu Duan and Youan Xiao [10] large volume of the data and unbalanced data ,intrusion data were inevitable obstacles. So, to solve those issues utilizing fuzzy c-means procedure to reconstruct feature vectors according to central points. This paper shows deep learning procedure for intrusion detection, which implemented in GPU-enabled TensorFlow and evaluated utilizing the KDD 99 dataset. Osamah et al [12] in his paper, introduced learning procedure for intrusion detection according to tree calculation on the KDD-99.

3. KDDCUP99 DATASET

In order to apply the proposed mechanism, the KDDCup99 dataset will be used as the standard dataset. KDDcup99 data-set has been considered the point attraction for numerous researchers in the domain of intrusion detection system. It has been most widely used for evaluating IDS. The 10% of KDDCup99 dataset is the original data-set that includes 494,020 records as showed in Figure 1 .Every record includes forty-one features with either normal or abnormal class with one fixed attack such as Dos, Probe, U2r, R2l as shown in Table 1 [13],[14].

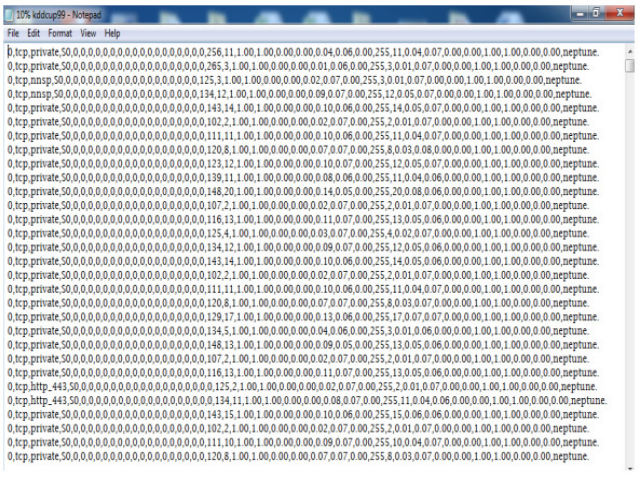

Fig1.Sample of 10% Kddcup99 in Text Format

Table 1: Num of Records and Attack category of KDD'99 Dataset

Attack Type	Original Number of Records	Number of Records after removing duplicated instances	Attack Category
back	2203	994	DoS
land	21	19	DoS
neptune	107201	51820	DoS
pod	264	206	DoS
smurf	280790	641	DoS
teardrop	979	918	DoS
satan	1589	908	Probe
ipsweep	1247	651	Probe
nmap	231	158	Probe
portsweep	1040	416	Probe
normal	97277	87831	Normal
guess_passwd	53	53	R2U
ftp_write	8	8	R2U
imap	12	12	R2U
phf	4	4	R2U
multihop	7	7	R2U
warezmaster	20	20	R2U
warezclient	1020	1020	R2U
spy	2	2	R2U
buffer_overflow	30	30	U2R
loadmodule	9	9	U2R
perl	3	3	U2R
rootkit	10	10	U2R

Features of KDD'99 Dataset can be labeled into following:

1) Standard features: standard features consists of whole attributes that can be taked from a TCP/IP link. Some of these features guiding to potential lateness in detection [15].
2) Traffic features: Traffic features consists of features that are calculated with related to a window period and is splitted into features of same service and the same host (time-based features). However, there are several slow probing attacks that scan the hosts (or ports) using a much larger time interval than 2 seconds. To fix this issue, these features are recomputed but according to the link window of 100 links rather than a period window of two seconds(based traffic features) [15].
3) Content features: To detect R2L and U2R attacks , need Content features to be fit to look for dubious attitude in the data [16].

Table 2: The No. Attributes of KDDCUP99

No.	Network attributes	No.	Network attributes	No.	Network attributes
1	duration	15	su_attempted	29	same_srv_rate
2	protocol_type	16	num_root	30	diff_srv_rate
3	service	17	num_file_creations	31	srv_diff_host_rate
4	flag	18	num_shells	32	dst_host_count
5	src_bytes	19	num_access_files	33	dst_host_srv_count
6	dst_bytes	20	num_outbound_cmds	34	dst_host_same_srv_rate
7	land	21	is_host_login	35	dst_host_diff_srv_rate
8	wrong_fragment	22	is_guest_login	36	dst_host_same_src_port_rate
9	urgent	23	count	37	dst_host_srv_diff_host_rate
10	hot	24	srv_count	38	dst_host_serror_rate
11	num_failed_logins	25	serror_rate	39	dst_host_srv_serror_rate
12	logged_in	26	srv_serror_rate	40	dst_host_rerror_rate
13	num_compromised	27	rerror_rate	41	dst_host_srv_rerror_rate
14	root_shell	28	srv_rerror_rate		

4. ATTACKS TYPE OF KDDCUP99

Attacks occur into one of the following types [17]:

a. User to Root attack : It is a type of utilizing that the intruder begins out by accessing the account of current client on the system (probably acquired by guessing password, etc).
b. Remote to local attack: This happens in the case where an intruder who are capable of sending packets to the machine is exploited some vulnerability for gaining local access as the that machine's user
c. Denial of Service attack : It is an thread where the intruder creates some of the space resources as well crowded to handle legal requests or refuse legal users access to a machine.
d. Probing attack: It is attempting to gain information concerning a network of computers for the obvious aim to circumvent its security controls.

5. PERFORMANCE MEASURE OF INTRUSION DETECTION SYSTEM

The performance of classifier can be estimated by using various procedures according to the following criteria [18]:

- True positive (TP): Number of attack is correctly identified attack event.
- True negative (TN): Number of normal is correctly identified normal event.
- False positive (FP): Number of normal is incorrectly identified attack event.
- False negative (FN): Number of attack is incorrectly identified normal. Table 3 displays the confusion matrix.

Table3: Confusion Matrix

Actual class	Predicted Class	
	Negative class(normal)	Positive class(abnormal)
normal	True negative (TN)	False positive (FP)
abnormal	False negative (FN)	True positive (TP)

- False Alarm Rate (FAR): It is the proportion of the rate samples which are incorrectly identified asn attack to the overall samples of normal behavior as shown in equation 1.

$$FAR= FP/ (TN+FP) \quad (1)$$

- Sensitivity: It is awarded an indication of the attack behavior that is correctly specified as shown in equation 2.

$$Sensitivity=TP/(TP+FN) \quad (2)$$

- Specificity (SPC): It is awards an indication of the normal behavior that is specified correctly as shown in equation 3

$$Specificity = TN/ (FP+TN) \quad (3)$$

6. THE PROPOSED SYSTEM

Multi-layer classifier can be comprised into three layers. The first layer will detect the abnormal from normal traffic using naïve Bayes, the second layer will classify the abnormal activity into 4 classes of attack and normal activity using neural network (backpropgaion), while the last one is to classify 4 classes of attack into 23 subclass and normal activity using Decision Tree. The outcomes of the Multi-layer classifier are evaluated in testing stages. The general structure of the Multi-layer classifier of classifying intrusion detection is demonstrated in details as shown in figure 2.

The proposed of multi-layer classifier is training and testing based on KDDcup99 dataset, this work have been used the whole dataset about 494,020 records which include normal behavior samples and attack types. Selected training data is about 329,510 records while the testing data is 164,510. To evaluate the proposed system cross validation will be used by splitting the training and testing data in k times. Table 4 displays the type of classes, which are used in dataset.

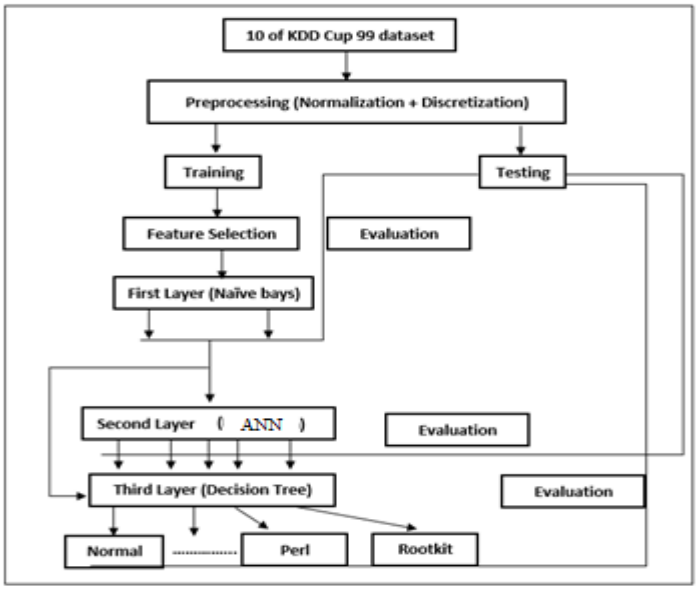

Fig 2: General Structure of the Multi-layer classifier

Table 4: Description of Category Traffic Dataset

subclass type	class category	Traffic type
Back	Dos	Abnormal
Land	Dos	Abnormal
Neptune	Dos	Abnormal
Pod	Dos	Abnormal
Smurf	Dos	Abnormal
Teardrop	Dos	Abnormal
Satan	Probe	Abnormal
Ipsweep	Probe	Abnormal
Nmap	Probe	Abnormal
Portsweep	Probe	Abnormal
Normal	Normal	Normal
guess_passwd	R2L	Abnormal
ftp_write	R2L	Abnormal
Imap	R2L	Abnormal
Phf	R2L	Abnormal
Multihop	R2L	Abnormal
Warezmaster	R2L	Abnormal
warezclient	R2L	Abnormal
Spy	R2L	Abnormal
buffer_overflow	U2R	Abnormal
loadmodule	U2R	Abnormal
Perl	U2R	Abnormal
Rootkit	U2R	Abnormal

6.1 THE PROPOSED PROCEDURES FOR CLASSIFYING INTRUSION

The proposed procedure for classifying intrusion on KDDcup99 dataset is shown in algorithm 1 according to multi-operations and multi-layer classifier. Multi-operations can be comprised into the following steps:

- Prepare dataset: take the sample of 10% kddcup99 dataset using K-fold cross- validation process to divide the dataset into three subsets of equaled size (k=3). Each time, one of the k used as testing data is about one-third of records and the remaining one for training data is about two-thirds of records.
- Normalization: Normalization is utilized on continuous features by making the values of feature in domain 0 to 1, lead to enhance effectiveness of the system .
- Discretization: it is used utilized convert the continuous attributes to discrete attributes lead to speed of the process.
- Feature selection technique: procedure for determining the relevant feature by reducing the computation time and selecting the best feature as display in algorithm 2.

Algorithm 1 : Proposed Procedure of classifying intrusion detection
Input: KDDCup99 dataset
Output: Detect the abnormal from normal traffic; classify abnormal traffic into four class type and into their subclasses type of attack.
Begin Step1: Select samples of 10% KDDCup99 dataset for building database to perform the proposed system. Apply holdout and K-fold cross validation of (k=3) to divide value of dataset number of k times into equal parts (folds). Step2: Apply normalization process Step3: Apply normalization process Transformation Step4: Select the appropriate feature based on feature selection Algorithm. Step5: Training phase will Done on training part of the dataset by building three classifiers naïve Bayes, ANN and ID3 Step6: Testing phase: will done on testing part of dataset in which Result of classifiers from training phase examine and evaluate. End

Algorithm 2 : Feature Selection
Input: features of training dataset
Output: Best five feature of training (10,15,20,30,35,All)

Begin
For all feature in training set
For all value in feature
Calculate the probability of each value in the feature.
for each value in the feature calculate the entropy
End For
End For
Select the best five features with the lowest value of entropy.
End

7. RESULTS

The Dataset includes 41 features with a label to determine the type of each record whether normal or type of attack traffic. In addition to the main class attribute of 23 subclass types in dataset, two features of class categories have been added to the data and reach up to 44 attributes according to the 23 subclass to their main class type of normal and abnormal traffic as shown in Table 2. These features are treated as class category which are used in

the experiments of the system. Kddcup99 dataset will be split randomly into two non-overlapped parts 329,510 records of training data and 164,510 records of testing data. According to the cross validation procedure, the data is splitted into 3 equal bins of folds approximately. Training and testing data are performed in k times. In first layer, fold 1 is reserved for the test data and the remaining folds (fold2, fold3) are used to train using Naïve bays classifier. The second layer, fold 2 is reserved for the test data and the remaining folds (fold1, fold3) are used to train using backpropgaion classifier , the third layer, fold 3 is reserved for the test data and the remaining folds (fold1, fold2) are used to train using ID3. Evaluation metric in terms of accuracy are used for evaluating the efficiency of the suggested system.

The experiments showed that after examining the results of the data, it was found that the accuracy of a multi-layer classifier with three classifiers as shown in Table 5, Table 6 and Table 7 was better than the accuracy by using one classifier. If one classifier as ID3 was adopted as a single part, it does not give a precision index and the second one of Naïve Bayes classifier. Especially, in the case of equal values in the results or assigned number after the interval, therefore it will use more than one level to give a better decision from a single classifier where it increases accuracy, especially applications that rely on accuracy such as intrusions.

Table 5: Total Accuracy for First Layer

No. of Features	Total Accuracy
10	80 %
15	82 %
20	96 %
25	97 %
30	99 %
35	99 %
All	99 %

Table 6: Total Accuracy for Second Layer

No. of Features	Total Accuracy
10	79 %
15	81 %
20	95 %
25	99 %
30	99 %
35	99 %
All	99 %

Table 7: Total Accuracy for Third Layer

No. of Features	Total Accuracy
10	65 %
15	71 %
20	79 %
25	98 %
30	98 %
35	98 %
All	98 %

The performance of proposed procedure showed that the total accuracy in the first layer selecting 30 features had best results, the total accuracy in second layer and third layer selecting 25 features had best results as described in Figures 3.

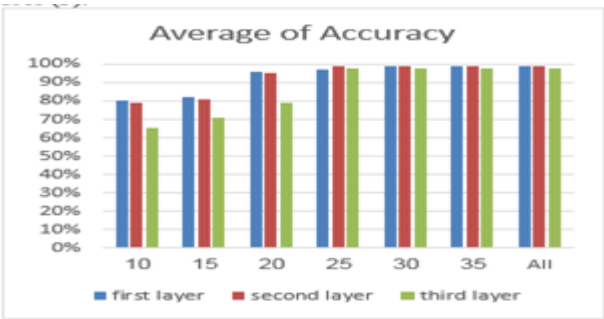

Fig 3: Average Accuracy of Three Layers

The result of the first layer, second layer and third layer were compared and evaluated with criteria FAR, specificity, sensitivity and time in minutes for 25 features as shown in Table 8. Table 9 displays the comparison of experimental result between the prior studies and proposed system.

Table 8: FAR, Specificity, Sensitivity and Time for Multi-classifier

Layer	FAR	Specificity	Sensitivity	Time
First	0.01	0.98	0.99	3
Second	0.005	0.99	0.99	5
Third	0.001	100	0.98	5

Table 9: Comparison of Related Work and Proposed System.

Reference	Method used	Accuracy Rate
Aggarwal P. and Sharma S.K.	Random forest J48 Decision table Naïve bayes	63% 64% 51% 55.8%
C Manju	Logistic regression Naïve bays	87.7% 81.8%
Gupta D. et al.	Logistic regression	80%
Proposed Procedure first layer	Naïve bays	99 %
Proposed Procedure second layer	backpropgaion	99 %
Proposed Procedure third layer	Decision tree	98 %

8. CONCLUSIONS

False alarms are a big problem in intrusion detection.This paper handled false alarms in intrusion detection by presenting a proposed multi-operations and multi-layer classifier. Depending on the results of the proposed approach to classify the type of intrusion and classifying them into their subclasses of intrusion. There are several conclusions from our study, The use of supervised machine learning classifiers such as Naive Bayes, ANN, and decision tree give the high efficiency and accuracy for the proposed approach. Using cross validation technique estimates and compares the performance of different algorithms and finds the best one from available data. Since it is very large dataset, we applied the cross validation technique to avoid falling into over fitting. The performance showed that results obtained from three consequent classifiers are better than single classifier.The accuracy reached 98% based on 25 features instead of using all features of KDDCup99 dataset.

REFERENCES

[1] Vaidya h., Mirza SH., and Mail N.,"Intrusion System", International Journal of advance research in engineering, science and technology, e-ISSN:2393-9877, p-ISSN:2394-2444,vol 3, Issue 3, Mar 2016.

[2] Nadiammai G.V and Hemalatha M.,"Effective Approach Toward Intrusion Detection System Using Data Mining Techniques", Elsevier B.V. Egyption Informatics Journal, 2014.

[3] Islam A. and Islam M., "A Novel Signature_Based Traffic Classification Engine Reduce False Alarms in Intrusion Detection systems", International Journal of Computer Networks and Communications (IJCNC) vol 7, No.1, Jan 2015.

[4] Al-Saedi K. and Manickam S., "research proposal: An Intrusion Detection System Alert Reduction and Assessment Framework Based on Data Mining", Journal of Computer Science, 9(4):421-426,2013.

[5] Dult, I. and Dr.Borah S. "Some Studies in The Intrusion Detection Using Data Mining Techniques". International Journal of Innovative Research in Science, Engineering and Technology, 4(7), 2015. .

[6] Novakovic, J., Strbac P. and Bulatovic, "Toward Optimal Feature Selection Using Ranking Methods and Classifications Algorithms". Yugoslav Journal of operations research, 2011.

[7] Goeschel K., "Reducing False positives in Intrusion Detection systems using Data-Mining Techniques utilizing Support Vector Machines, Decision Trees and Naïve Bayes for off-line analysis", IEEE, International Conference on 30 March-3 April 2016, USA, 7506774, July 2016.

[8] Mahmood D.Y., "Classification Trees with Logistic Regression Functions for Network Based Intrusion Detection System", (IOSR-JCE) Journal of computer Engineering, e-ISSN: 2278-0661, p-ISSN: 2278-8727, vol 19, Issue 3, pp 48-52, June 2017.

[9] Belavagi M.C. and Muniyal B., "Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection", (IMCIP) International Multi-conference on Information Processing-2016, Elsevier, vol 89, pages 117-123, 2016.

[10] L. Duan and Y. Xiao, "An Intrusion Detection Model Based on Fuzzy C-means Algorithm,", 8th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, pp. 120-123. (2018)

[11] Wang, Zheng. "Deep learning-based intrusion detection with adversaries." IEEE Access 6 , 38367-38384.(2018):

[12] Raheem Esraa and Saleh Alomari ,"An Adaptive Intrusion Detection System by using Decision Tree Osamah Adil", Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.2,(2018).

[13] Siddiqui M.K. and Naahid Sh., "Analysis of Kdd cup 99 Dataset Using Clustering Based Data Mining", International Journal of database theory and application, pp.23-34, vol.6, No.5(2013).

[14] Tavallaee M., Bagheri E., Lu W. and Ghorbani A.A, "A Detailed Analysis of the Kdd Cup 99 Data set", proceedings of the IEE symposium on computational intelligence in security and defense applications ,2009.

[15] Nelcileno A., R. Oliveira, A. Akira Shinoda, B. Bhargava, “Identifying Important Characteristics in the KDD99 Intrusion Detection Dataset by Feature Selection using a Hybrid Approach”, pp:2, 2010.

[16] Mahbod T., E. Bagheri, Wei Lu, and A. A. Ghorbani ,” A Detailed Analysis of the KDD CUP 99 Data Set”, p.2, 2009.

[17] Brifcani A.M.A. and Issa A.S., "Intrusion Detection and Attack Classifier based on Three Techniques: A Comparative Study", Journal of engineering and Technology, Vol.29, No.2, 2011.

[18] Wahba Y., Elsalamouny E. and El Taweel G., "Improving the performance of Multi-class Intrusion Detection Systems using features reduction", (IJCSI) International Journal of computer science Issues, Vol 12, Issue 3,2015

AUTHORS

Shaker El-Sappagh received the bachelor's degree in computer science from the Information Systems Department, Faculty of Computers and Information, Cairo University, Egypt, in 1997,the master's degree from Cairo University, in 2007,and the Ph.D. degree in computer science from the Information Systems Department, Faculty of Computers and Information, Mansura University,Mansura, Egypt, in 2015. In 2003, he joined the Department of Information Systems, Faculty of Computers and Information, Minia University, Egypt, as a Teaching Assistant. Since 2016, he has been an Assistant Professor with the Department of Information Systems, Faculty of Computers and Information, Benha University. He is currently a Postdoctoral Fellow with the UWB Wire-less Communications Research Center, Department of Information and Communication Engineering, Inha University, South Korea. He has publications in clinical decision support systems and semantic intelligence. His current research interests include machine learning, medical informatics, (fuzzy) ontology engineering, distributed and hybrid clinical decision support systems, semantic data modeling, fuzzy expert systems, and cloud computing. He is very interested in the diseases diagnosis and treatment researches. He is a Reviewer for many journals

Ahmed saad Mohammed received the bachelor's degree from the Software engineering Department, Baghdad College of Economic Sciences University, Iraq, Baghdad in 2005. His current research interests include machine learning, data mining and artificial intelligence

Dr. Tarek El-Shishtawy is a professor of Information System. His current work is vice Dean of postgraduates and researches at faculty of computers and informatics. The scientific interests in clude Information Retrieval, Data Mining, and researches related to information systems in developing countries. Dr. Tarek published and refereed many articles in NLP.