

Kennesaw State University

DigitalCommons@Kennesaw State University

African Conference on Information Systems
and Technology

The 6th Annual ACIST Proceedings (2020)


Jul 2nd, 1:00 PM - 1:30 PM

Efficient Data Mining Algorithm Network Intrusion Detection System for Masked Feature Intrusions

Kassahun Admkie
kaseshadd@yahoo.com

Kassahun Admkie Tekle
betekas@gmail.com

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/acist>

 Part of the [Computational Engineering Commons](#), [Computer and Systems Architecture Commons](#), [Digital Communications and Networking Commons](#), [Other Computer Engineering Commons](#), and the [Robotics Commons](#)

Admkie, Kassahun and Tekle, Kassahun Admkie, "Efficient Data Mining Algorithm Network Intrusion Detection System for Masked Feature Intrusions" (2020). *African Conference on Information Systems and Technology*. 11.

<https://digitalcommons.kennesaw.edu/acist/2020/allpapers/11>

This Event is brought to you for free and open access by the Conferences, Workshops, and Lectures at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in African Conference on Information Systems and Technology by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Efficient Data Mining Algorithm Network Intrusion Detection System for Masked Feature Intrusions

Author #1. T. Kassahun Admkie (MSc), Network Security Expert, Ethiopian Institute of Agricultural Research, (DZARC/EIAR), Addis Ababa, Ethiopia.

Author #2. D. Workshet Lameneu (PhD), Addis Ababa University, College of Natural and Computational Science, School of Information Science, Addis Ababa, Ethiopia, May 2020.

ABSTRACT

Most researches have been conducted to develop models, algorithms and systems to detect intrusions. However, they are not plausible as intruders began to attack systems by masking their features. While researches continued to various techniques to overcome these challenges, little attention was given to use data mining techniques, for development of intrusion detection. Recently there has been much interest in applying data mining to computer network intrusion detection, specifically as intruders began to cheat by masking some detection features to attack systems. This work is an attempt to propose a model that works based on semi-supervised collective classification algorithm. For this study, data mining algorithms were first selected based on efficiency and accessibility criteria. An experiment was conducted using real .arff dataset to develop the model. The result shows that meta.Filtered Collective Classifier is appropriate to detect intrusions with hidden features, which scored the best classification accuracy of 96.2%.

Keywords: - Intrusion detection, Data mining, Semi-Supervised Learning (SSL), Collective classifier, Missing value dataset, Masked feature Intrusion detection.

INTRODUCTION

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Intrusion detection has been an ongoing research. In the late 70s' and early 80s', administrators typically printed audit logs on fan-folded paper, which were often stacked four- to five-feet high by the end of an average week. Searching through such a stack was obviously time consuming. In the early 90s', researchers developed real-time intrusion detection systems that reviewed audit data as it was produced. More recent intrusion detection efforts have centered on developing products that users can effectively deploy in large networks (Vigna). Since then, several researchers and practitioners in the field have contributed a lot to minimize intrusions through developing systems and identifying newly emerging intrusion behaviors. Among the Intrusion detection techniques, network intrusion detection has been considered to be one of the most promising methods for defending complex and dynamic intrusion behaviors. (H. A. a. D. C., 2008).

However, recently intruders change their behavior of attacking systems by masquerading (masking) the intrusion features with which intrusion systems are able to identify intrusions and use alarms to inform the existence of bad behavior, several communication channels. For this purpose, few researchers embarked to come up with research outputs that are able to give response to intrusions having masked features using such techniques as. Scholars reported that further works are required to deal with attacks coming with masked features in order to address the issue. Among the available techniques for this purpose is data mining, which has gained much attention in the research and practice of IDS.

Data mining is the process of discovering interesting patterns (knowledge) from large amounts of data. The data sources can include databases, data warehouses, the Web, any other information repositories or data that are

streamed into the system. Data mining is also called KDD (Knowledge Discovery in Databases). Data mining techniques can be used for misuse and anomaly intrusion detection. In misuse detection, each instance in a data set is labeled as 'normal' or 'intrusion' and a learning algorithm is trained over the labeled data. Anomaly means unusual activity in general that could indicate an intrusion. (Krishna Kant Tiwari, Susheel Tiwari and Sriram Yadav)

Though data mining techniques have been utilized much in the IDS research to detect dynamically intrusions based on various models/algorithms, there is minimal attention given to the application of data mining techniques to the detection of intrusions coming with masked features. To this end, this research aims at developing a model that employs data mining techniques to address the problem of intruders or attackers changing their behavior to damage/harm systems by masquerading the intrusion features.

However, they are not plausible as intruders began to attack systems by masking intrusion features. While researches continued to detect intrusions with masked features using various techniques, little attention was given to use data mining techniques, which is popular for development of intrusion detection models. Recently there has been much interest in applying data mining to computer network intrusion detection, specifically as intruders began to cheat by masking some intrusion detection features to attack systems. This work is an attempt to propose a model that works based on semi-supervised collective classification algorithm

We consider the general problem of learning from labeled and unlabeled data, which is often called semi-supervised learning or transductive inference (Dengyong Zhou). The data set in this study is taken from Ethiopian Institute of Agriculture Research (EIAR) data center.

Many researches had been taken concerning data mining techniques with full feature data set for Network Intrusion Detection, which can't detect masked feature intrusions. In this paper an efficient data mining algorithm of Network Intrusion Detection System (NIDS) for masked features intrusions are identified and selected.

NETWORK INTRUSION DETECTION (NID)

Network Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices (M., Karen S. and Peter, 2007), (Dokas, 1987) incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized.

With advancements in network technologies, Internet services have been also growing rapidly in network traffic, accompanied by an increasing number of anomalies such as Denial of Service (DoS) attacks, virus exploits, port scans, worms and misconfigurations. These anomalies represent a large fraction of the Internet traffic that is unwanted and prevent legitimate users from accessing network resources in an optimal manner (Richard A. Kemmerer and Giovanni Vigna Reliable Software Group). Therefore; detecting and diagnosing these threats are crucial tasks for network operators to ensure that the Internet resources remain available. Because legitimate traffic must be able to travel efficiently, quickly and accurately identifying anomalies in network traffic is important, requires development of good detection techniques. Anomalies are patterns of interest to network defenders, who want to extract them from vast amount of network traffic data.

Categories of Network Intrusion Detection

There are several ways to categorize the types of IDS, depending on the kind of activities, transactions and traffics or systems differ. Intrusion Detection system can be categorized into Network based Intrusion Detection System (NIDS) and Host based Intrusion Detection System (HIDS).

Based on the different approaches to event analysis, IDS can also be distinguished between Signature based detection and Anomaly detection. Each type of Intrusion Detection System has its own advantages and disadvantages (Jaiganesh, July, 2014) . NIDS make use of raw network packets as the data source. The IDS typically use a network adapter in licentious mode that listens and analyses all traffic in real-time as it travels across the network.

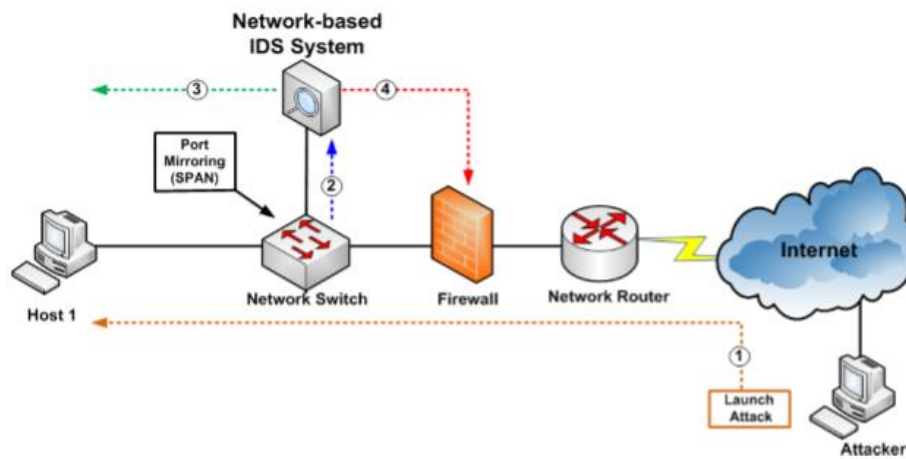


Figure 1, Network Based Intrusion Detection System (Jain, Sanket R, 2014)

Host based intrusion detection system (HIDS) monitors incoming and outgoing activity on a particular system in the network. Specifically, it monitors the dynamic behavior and the state of the computer system. As per (Boncheva M. , 2007) and (M. C. D., 2004), audit logs contain records for events and activities taking place at individual Network resources.

IDS can use signature-based detection, relying on known traffic data to analyze potentially unwanted traffic (Amir A., Ahmad H. and Hadi B., 2011). One of the advantages of Signature-based approaches result in fewer false alarms because they can be very specific about what it is and they are looking for. Because the IDS is looking for something known, a lot of information regarding what the misuse is, the potential impact, and how to respond can be provided. This knowledge is extremely important in understanding what is occurring and effectively responding (Dokas, P., Ertoz, L., Kumar, V., Lazarevic, A., Srivastava, A.J., and Tan, P.N., 1987). While the disadvantages of Signature based detection is that; Signature-based approaches can only detect misuse for which a signature exists. For a signature to exist, the form of misuse must be known about beforehand so it can be researched and programmatically identified. This means any new form of misuse will not be detected by a signature-based system until it is identified, analyzed, and then incorporated into the product. Depending on the circumstances, this could be hours, days, weeks, or even months (Amir A., Ahmad H. and Hadi B., 2011) , (Berson A., Smith S. and Thearling K., 2000) and (IATR, 2009) . If the network is small and signatures are kept up to date, the human analyst solution to intrusion detection works well. But when organizations have a large, complex network the human analysts quickly become overwhelmed by the number of alarms they need to review.

Anomaly Based Detection on the other hand is based on defining the network behavior. Behavior of the network is the predefined one, when it is accepted or else it triggers the event in the anomaly detection. The accepted behavior of the network is prepared or learned by the specifications of the network administrators (Emam, Ahmed Youssef and Ahmed, 2011).

According to (Khandelwal, 2014) the important phase in defining the network behavior is the IDS engine that is capable to cut through the various protocols at all levels. The engine is able to process the protocols and understand the goal. Though this protocol analysis is computationally expensive, the benefits it generates like increasing the rule set helps in less false positive alarms. According to (Amir A., Ahmad H. and Hadi B., 2011) the major drawback of Anomaly Detection is defining its rule set. The efficiency of the system depends on implementation and testing on all protocols that are available. Rule Defining Process is also affected by various protocols used by several vendors.

Intrusions can be detected by observing deviations from the expected behaviors of the system monitored. These “normal” behaviors can either correspond to some observations made in the past or to some forecasts made by various techniques. Everything that does not correspond to this “normal” pattern will be flagged as anomalous.

The goal of anomaly detection system is to find the intrusion in the system timely (P.Kalarani¹, Dr.S. Selva Brunda² Assistant Professor, Department of CT and IT, Kongu Arts and Science College, Erode, Tamil Nadu, India¹ Professor and Head, Department of CSE, Sasurie College of Engineering, Erode, Tamil Nadu, India², September, 2014). Therefore, the core process of anomaly detection is not to learn what is anomalous but to learn what is normal or expected (Pachghare V., Vaibhav K.,and Parag K., 2011), (Eric Bloedorn, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot), (Amir A., Ahmad H. and Hadi B., 2011). The key advantage of anomaly-based detection over the other techniques is the ability to detect new attacks, attacks for which no signature or known protocol violation exists (H. A. a. D. C., 2008).

Types of Attack

An ID is effective security tool which helps the users and administrators to prevent unauthorized access to network resources. There are various kinds of attacks that are most common in IDS. They are probe attacks, denial-of-service attacks (DoS), remote to local (R2L) and user to root (U2R) attacks (Choi, Huy Anh Nguyen and Deokjai), (Boncheva M. , 2007).

DATA MINING TECHNIQUES FOR INTRUSION DETECTION SYSTEM

Data mining techniques have been popular in extracting the behaviors of these harmful patterns from large volumes of data in recent years. Data mining is used in many areas of application, e.g., the business world, medicinal sciences, physical sciences and engineering to make new discoveries (Eric Bloedorn, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot), (Emam, Ahmed Youssef and Ahmed, 2011). Extensive studies have been performed in applying data mining techniques to network traffic anomaly detection, but the methods (F., Carl, 2003) have limitations that notably discredit them from use in real environments. In this paper, we explore the possibilities of integrating data mining techniques to identify network intrusions with significant performance improvement.

Much number of data mining techniques can be used in intrusion detection, each with its own specific advantage (M. C. D., 2004). Data mining has gained a great deal of attention in the information industry and in the society as a whole in recent years due to the wide availability of huge amounts of data and the imminent need for turning such data into useful information and knowledge.

The term knowledge discovery in databases (KDD) refers to the process of converting raw data into useful information or knowledge. Data mining is a step in the KDD process, and applies a variety of algorithm for extracting patterns from data. In addition to this, the KDD process has additional steps including data preparation, data selection, data cleaning, incorporation of appropriate prior knowledge, and proper interpretation of the results of mining to ensure useful knowledge is derived from the data (Amir A., Ahmad H. and Hadi B., 2011) and (F., Carl, 2003).

Data Mining Tasks

There are two main tasks of data mining. These are: descriptive modeling and predictive modeling. The descriptive data mining tasks characterize the general properties of the data in the database, while predictive data mining tasks perform inference of the current data in order to make prediction. Descriptive data mining focus on finding patterns describing the data that can be interpreted by humans, and produces new, nontrivial information based on the available data set. Predictive data mining involves using some variables or fields in the data set to predict unknown or future values of other variables of interest, and produces the model of the system described by the given data set.

The goal of predictive data mining is to produce a model that can be used to perform tasks such as classification, prediction or estimation, while the goal of descriptive data mining is to gain an understanding of the analyzed system by uncovering patterns and relationships in large data sets.

The descriptive task encompasses methods such as clustering, summarization, association rules and sequence analysis. (Boncheva M. , 2007)

DISCUSSION OF PROPOSED ALGORITHM

SSL is a halfway method between supervised and unsupervised learning, which, in addition to unlabeled data, receives some supervision information such as the association of the targets with some of the examples. Collective Classification for Text Classification poses as an interesting method for optimizing the classification of partially-labelled data. Collective classification is a combinatorial optimization problem, in which we are given a set of documents, or nodes, $D = \{d_1, \dots, d_n\}$ and a neighborhood function N , where $N_i \subseteq D \setminus \{D_i\}$, which describes the underlying network structure [12]. Being D a random collection of documents, it is divided into two sets X and Y where X corresponds to the documents for which we know the correct values and Y are the documents whose values need to be determined. Therefore, the task is to label the nodes $Y_i \in Y$ with one of a small number of labels, $L = \{l_1, \dots, l_q\}$ (Carlos Laorden, Borja Sanz, Igor Santos, Patxi Gal'an-Garc'ia, and Pablo G. Bringas,) and (DOBRA, AMIT DHURANDHAR and ALIN).

In semi-supervised learning, we are trying to solve a supervised learning approach using labeled data augmented by unlabeled data; the number of unlabeled or partially labeled samples is often larger than the number of labeled samples, since the former are less expensive and easier to obtain. In collective classification the class labels of multiple instances are inferred simultaneously, assuming dependencies between these instances. Thus, the class label of a particular instance depends on the class labels and sometimes even attributes of the other related instances and not just on its own set of attributes.

Meta Filtered Collective Classifier takes a filter and a collective classifier as input. The filter is only trained on the provided training set, but still applied to instances from the training and test set, as well as to any instance that

gets passed to the meta classifier (Bernhard Pfahringer, Kurt Driessens, and Peter Reutemann, February 27, 2015).

EXPERIMENTAL SET UP

Methods and Approaches

As discussed in section 2.1.2, IDS can be classified as Signature based detection and Anomaly detection. In this research a hybrid NIDS approach was used.

Hybrid intrusion detection is a system which is a combination of both signature-based and anomaly-based IDS. A signature-based IDS analyzes the network traffic looking for patterns that match a library of known signatures. These signatures are composed by several elements that allow identifying the traffic. On the other hand, anomaly-based IDSs try to find suspicious activity on the system. In the initial phase, the IDS must be trained in order to get an idea about what is considered “normal” and “intrusion”. After that, the system will inform about any suspicious activity if there is a deviation from normal.

WEKA 3.8 data mining tools with collective-classification WEKA package to execute semi-supervised techniques and expertise are utilized as means to address the research problem. For analyzing the data and classification of network attacks from a network environment, the two machine learning algorithms (I., Eibe F. and Witten, 2005) the Semi-Supervised Learning (SSL) Collective classification model called meta.Filtered Collective Classifier and J48 decision tree classifiers are used in this paper.

Meta.Filtered Collective Classifier is the proposed collective classifier having both supervised and unsupervised characteristics that help to give weight for the missing value for masked feature and predict the unlabeled class. J48 decision tree classifier is an algorithm which was preferable existed model to predict whether the newly coming instance is attack or not as compared to others ordinary classifiers.

We tried to conduct experiments on semi-supervised collective classifier called YATSI (Yet Another Two State Idea), which is successful for missing value but can't use for predicting the unlabeled class. In addition to YATSI, Meta collective wrapper was also used for conducting the experiment, but its result is less than 60% accuracy, therefore these two algorithms are failed for further investigation.

Data sets

The data analysis and classification were carried out using Weka (3.8.0 version) software environment with collective-classification-weka-package-master which is developed for evaluating Semi-Supervised Learning. Weka has collections of machine learning algorithms for data mining tasks that contain facilities for data preprocessing, classification, regression, clustering, association rules, and visualization.

The data set collected from EIAR Information Communication Data Center that was in comma separated csv format and the data was extracted to Microsoft Excel-2013 for preprocessing purpose. The dataset initially had 43 attributes and 25192 records but after the preprocessing stage, it was reduced to 28 attributes and 12596 records for building the appropriate predictive model. The dataset obtained after preprocessed were loaded in weka tool and filtered by resample and prepared 12596 instances for unlabeled/test. Therefore, the researcher used these clean, filtered and properly selected features for this research.

As described above collective-classification-weka-package-master is used, which is developed by University of Waikato for SSL semi-supervised data evaluation. The package provides three options to partition the dataset. Preparing distinct files for training and test dataset, cross validation with possibility of setting different number of

folders (the default was 10-fold) and Random split. Ordinary J48 classification with 10-fold cross validation has been also used for this research in order to increase comparative advantage and accuracy of prediction and to reduce biasness (Ragsdale D, Carver C, Humphries J, and Pooh U, 2000) .

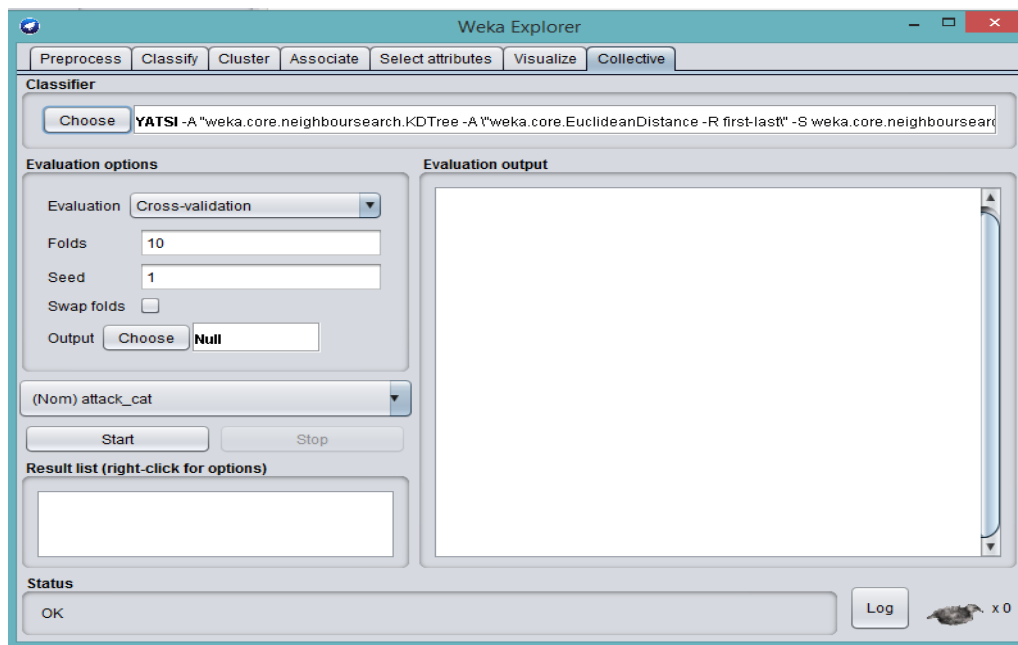


Figure 2, Collective Classifier uploaded Weka tool (3.8.0) version.

For conducting the experiments, the researcher used the data set of 55% of missing value with unlabeled class. The purpose of using missing value is to show the capability of the algorithm to detect those intrusions with masked features. For the case of this research the dataset has 12596 instances and each instance at a normal condition has 28 attributes, but 55% of the attributes for each instance are missing value including the class attribute, to detect those masked features.

RESULT AND DISCUSSION

Comparing different classification techniques and selecting the best model for predicting the network intrusions is one of the aims of this study. Accordingly the Semi-Supervised Learning collective classifier particularly meta.Filtered Collective Classifier and the J48 decision tree classification approaches were used for conducting experiments.

Summary of experimental result for the two classification algorithms is presented in Table 3 below:

Classifier/Model	Test Mode	Accuracy	
		Correctly Classified	Incorrectly Classified
Semi-supervised meta.Filtered Collective Classifier	10-fold cross validation with Other default values.	94.7	5.3
	10-fold cross validation with seed value=2	94.7	5.3
	Random split with 10% values	93.2	6.8
	Random split with 50% values	94.8	5.2
	Random split with 70% values	95.6	4.4
	Fully Training/Test set value	96.2	3.8
J48: Supervised	10-fold cross validation with Other default values(pruned) value	93.2	6.8
	10-fold cross validation with unpruned (-pruned)	94.5	5.5

Table 1, Summary of experimental result for the Semi-supervised meta.Filtered Collective Classifier and J48 decision tree classification algorithms.

Therefore, from the above experimental result, meta.Filtered Collective Classifier parameters with full Training/Test set having an accuracy of 96.2 % is selected model for real data having missing value to identifying masked features intrusions either normal or attack (DOS, R2L, Probe and U2R).

The proposed model is selected due to the characteristics of the algorithm, which is the combination of different algorithms developed for solving semi-supervised learning. In addition to this, a proposed algorithm has the capacity of filling the missed value by unsupervised filtering and gives weight around neighboring value.

CONCLUSION

The model that was created using Semi-Supervised meta.Filtered Collective Classifier parameters with full Training/Test set showed the best classification accuracy of 96.2% for dataset having unlabeled class with missing value. An algorithm has a capacity of unsupervised filtering and gives weights for the missing value and train by using labeled data to predict and classify the unlabeled new instances as Normal, DOS, U2R, R2L and probe classes. Therefore, the proposed, Semi-Supervised meta. Filtered Collective Classifier model parameters with full Training/Test set is preferable for those newly coming instances for masking their feature.

REFERENCES

- Amir A., Ahmad H. and Hadi B. (2011). A New System for Clustering and Classification of Intrusion Detection System Alerts Using SOM. *International Journal of Computer Science and Security*, Vol. 4(No. 6), PP. 589-597.
- Bernhard Pfahringer, Kurt Driessens, and Peter Reutemann. (February 27, 2015). *Collective and Semi-supervised classification*.
- Berson A., Smith S. and Thearling K., (2000). *Building Data Mining Applications for CRM*. New York, USA: McGraw Hill Professional Publishing.
- Boncheva, M. (2007). Problems of Engineering Cybernetics and - iit.bas.bg.
- Carlos Laorden, Borja Sanz, Igor Santos, Patxi Gal'an-Garc'ia, and Pablo G. Bringas,. (n.d.). *Collective Classification for Spam Filtering*. DeustoTech Computing - S3Lab, University of Deusto Avenida de las Universidades 24, 48007 Bilbao, Spain.
- Choi, Huy Anh Nguyen and Deokjai. (n.d.). *Application of Data Mining to Network Intrusion Detection: Classifier Selection Model*. Chonnam National University, Computer Science Department, 300 Yongbong-dong, Buk-ku, Gwangju 500-757, Korea.
- Dengyong Zhou, O. B. (n.d.). *Learning with Local and Global Consistency*. Dengyong Zhou, Olivier Bousquet, Thomas Navin Lal, Jason Weston, and Bernhard SchMax Planck Institute for Biological Cybernetics, 72076 Tuebingen, Germany.
- DOBRA, AMIT DHURANDHAR and ALIN. (n.d.). *Collective vs Independent Classification in Statistical Relational Learning*. University of Florida.
- Dokas, P. E. (1987). Data Mining for Network Intrusion Detection. *IEEE*.
- Dokas, P., Ertöz, L., Kumar, V., Lazarevic, A., Srivastava, A.J., and Tan, P.N. (1987). *Data Mining for Network Intrusion Detection*. IEEE.
- Emam, Ahmed Youssef and Ahmed. (2011). *NETWORK INTRUSION DETECTION USING DATA MINING AND NETWORK BEHAVIOUR ANALYSIS*. Department of Information Systems, King Saud University, Riyadh, KSA: DOI : 10.5121/ijcsit.
- Eric Bloedorn, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot. (n.d.). *Data Mining for Network Intrusion Detection: How to Get Started*. Jonathan Tivel The MITRE Corporation 1820 Dolley Madison Blvd. McLean, VA 22102 (703) 983-5274.
- F., Carl. (2003). *Intrusion Detection and Prevention*. McGraw-Hill, Osborne Media.
- H. A. a. D. C. (2008). Application of Data Mining to Network Intrusion Detection: Classifier Selection Model. *in APNOMS, Berlin*, p. 399–408.
- <https://github.com/fracpete/collective-classification-weka-package>. (n.d.). *www.weka.com*. Retrieved September 18, 2017, from <https://github.com/fracpete/collective-classification-weka-package>
- I., Eibe F. and Witten. (2005). *Data Mining—Practical Machine Learning Tools and Techniques*. 2nd Edition, Elsevier.
- IATR, I. A. (2009). *Intrusion Detection Systems*. New York: 6th ed.

- Jaiganesh. (July, 2014). *Investigation on machine learning algorithms for network intrusion detection system*. Department of Computer Science & Engineering, Manonmaniam Sundaranar University: Ph.D Dissertation.
- Jain, Sanket R. (2014). *Information Security: Intrusion Detection and Prevention System*.
- Khandelwal. (2014). *Knowledge based systems, problem solving competency and learnability*. Suresh Gyan Vihar University, Department of Computer Science.
- Krishna Kant Tiwari, Susheel Tiwari and Sriram Yadav . (n.d.). *Intrusion Detection Using Data Mining Technique*. Millennium institute of technology, RGPV University,.
- M., C. D. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art of Computer Networks. *the International Journal of Computer and Telecommunications Networking*, Vol. 44(No.5), PP. 643 - 666.
- M., C. D. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art of Computer Networks. *the International Journal of Computer and Telecommunications Networking*, vol. Vol. 44, no. No.5, pp. PP. 643 - 666.
- M., Karen S. and Peter. (2007). *Guide to Intrusion Detection and Prevention Systems*. National Institute of Standards and Technology, Department of Commerce, USA.
- P.Kalarani1, Dr.S. Selva Brunda2 Assistant Professor, Department of CT and IT, Kongu Arts and Science College, Erode, Tamil Nadu, India1 Professor and Head, Department of CSE, Sasurie College of Engineering, Erode, Tamil Nadu, India2. (September, 2014). A Survey on Efficient Data Mining Techniques for Network Intrusion Detection System(IDS). *International Journal of Advanced Research in Computer and Communication Emgineering*, Vol. 3(Issue 9).
- Pachghare V., Vaibhav K.,and Parag K. (2011). *Performance Analysis of Supervised Intrusion Detection System, JICA Special Issue on Network Security and Cryptography*. NSC.
- Ragsdale D, Carver C, Humphries J, and Pooh U. (2000). Adaptation techniques for intrusion detection and intrusion response systems . *in Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, (pp. pp. 2344-2349.).
- Richard A. Kemmerer and Giovanni Vigna Reliable Software Group, C. S. (n.d.). *Intrusion Detection: A Brief History and Overview*. Computer Science Department, University of California Santa Barbara.
- Software, W. D. (n.d.). Retrieved December 8, 2017, from <http://www.cs.waikato.ac.nz/ml/weka/>
- Vigna, C. S. (n.d.). *Reliable Software Group, Intrusion Detection: A Brief History and Overview*. Computer Science Department, University of California Santa Barbara.