www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 5 May 2018, Page No. 23901-23907
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i5.05

Survey on Intrusion Detection System using Machine – Learning approaches

Blessing Solomon B.C[1], Jesu Jayarin. P[2]

[1]PG Scholar, Department of Computer Science Engineering, Jeppiaar Engineering College, Chennai, India
[2]Associate Professor, Department of Computer Science Engineering, Jeppiaar Engineering College, Chennai, India

Abstract: ***Intrusion Detection Systems (IDSs) are a noteworthy line of guard for shielding system assets from illicit infiltrations. A lot of research is being done on the development of effective Network Intrusion Detection Systems. Anomaly based Network Intrusion Detection Systems are preferred over Signature based Network Intrusion Detection Systems because of their better significance in detecting novel attacks. The research on the datasets being used for training and testing purpose in the detection model is equally concerned as better dataset quality can advance offline Intrusion Detection. Recently, Machine Learning (ML) approaches have been implemented in the Network Intrusion Detection Systems (NIDS) to protect computer networks and to overcome network security issues. This survey paper aims at disclosing different strategies followed in Intrusion Detection Systems (IDSs) using machine learning over the years and because of the headway in advancements, our lucid view is just on the most recent patterns.***

Keywords: Anomaly Detection, Computer Security, Intruders, Intrusion Detection System, machine learning

1. Introduction

In the first place, there was spam. When scholastics and researchers had snared enough PCs together by means of the Internet to make a correspondences organize that offered some incentive, other individuals understood that this medium of free transmission and wide conveyance was an ideal method to publicize scrappy items, take account qualifications, and spread PC viruses.

In the interceding forty years, the field of PC and system security has come to incorporate a colossal scope of dangers and spaces: interruption discovery, web application security, malware examination, interpersonal organization security, progressed relentless dangers, and connected cryptography, just to give some examples. However, even today, spam remains a noteworthy concentration for those in the email or informing space, and for the overall population spam is presumably the part of PC security that most straightforwardly touches their own particular lives.

Spam warriors did not develop machine learning, but factually, slanted technologists who saw its potential in managing an always-advancing wellspring of mishandle immediately embraced rather it. Email suppliers and Internet specialist co-ops (ISPs) approach an abundance of email substance, metadata, and client conduct. Utilizing email information, content-based models can be constructed to make a generalizable way to deal with perceive spam. Metadata and element notorieties can be extricated from email to foresee the probability that an email is spam without taking a gander at its substance. By instantiating, a client conduct input circle, the framework can construct an aggregate insight and enhance after some time with the assistance of its clients.

PC frameworks and web administrations have turned out to be progressively unified, and numerous applications have advanced to serve millions or even billions of clients. Elements that move toward becoming referees of data are greater focuses for misuse, but on the other hand are in the ideal position to influence utilization of the information and their client to base to accomplish better security. Combined with the appearance of effective information crunching equipment, and the improvement of all the more intense information investigation and machine learning calculations, there has never been a superior time for misusing the capability of machine learning in security.

2. Machine Learning

Computerized reasoning is something that individuals have fantasized about since the beginning of the mechanical age. For a self-governing substance to settle on redress choices without being unequivocally educated how to do as such, to draw speculations and distil ideas from complex data sets - that is the epitome of insight.

Machine learning alludes to one part of manmade brainpower - particularly, to calculations and procedures that "learn" in the feeling of having the capacity to sum up past information and encounters keeping in mind the end goal to foresee future results. At the center, it is an arrangement of scientific methods, actualized on PC frameworks that empower a procedure of data mining, design revelation, and drawing derivations from information.

In addition, no broader level, directed machine learning strategies receive a Bayesian way to deal with information disclosure, utilizing probabilities of already watched occasions to gather the probabilities of new occasions. Unsupervised techniques draw deliberations from unlabeled datasets and apply these to new information. The two groups of strategies can be connected to issues of order (doling out perceptions to classes) or relapse (anticipating numerical properties of a perception).

Machine learning calculations are driven by science and insights, and the calculations that find examples, relationships, and peculiarities in the information differ broadly in unpredictability. In the coming sections, we will go further into the mechanics of the absolute most normal machine learning calculations utilized as a part of this book. This book will not give an entire comprehension of machine learning, nor will it cover a significant part of the science and hypothesis in the subject. What it will give you is basic instinct in machine learning and reasonable aptitudes for planning and executing perceptive, versatile frameworks concerning security.

3. Investigation in Detection System using Machine Learning – Review from different authors

3.1 [1] "Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning", (2018)

[1] discussed the statistical analysis and evaluation of labelled flow based CIDDS-001 dataset used for evaluating Anomaly based Network Intrusion Detection Systems. Two techniques, k-nearest neighbor classification and k-means clustering are used to measure the complexity in terms of prominent metrics. Based on evaluation results it can be concluded that both k-nearest neighbor classification and k-means clustering perform well over CIDDS-001 dataset in terms of used prominent metrics. Hence the dataset can be used for the evaluation of Anomaly based Network Intrusion Detection Systems.

Remark: [1] planned to do a comparative study of CIDDS-001 dataset with existing Network Intrusion Detection Systems benchmarking datasets in order to study the complexity of this dataset over other datasets.

3.2 [2] "Automated multi-level malware detection system based on reconstructed semantic view of executables using machine learning techniques at VMM", (2018)

[2] presented the design, implementation, and evaluation of the AMMDS as an advanced VMI-based guest assisted out-of-VM security solution that leverages both VMI and MFA techniques to estimate symptoms of malware execution and also able to accurately detect unknown malware (malicious executables) running on the CPS-based Monitored VM. The OMD of the AMMDS is able to recognize known malware whereas the OFMC is capable of detecting and classifying unknown malware by using machine-learning techniques. In [2] AMMDS extensively reduces the manual effort required to accurately identify the malware from the semantically reconstructed and forensically extracted executables as compared to other existing VMI and MFA based out-of-VM approaches. Finally, the AMMDS was evaluated against a large number of real-world Windows malware as well as benign executables to measure the malware detection rate. [2] demonstrate that AMMDS is capable of recognizing malware with an accuracy of 100%.

Remark: Further, the observed experimental results showed that the maximum performance of overhead induced by the AMMDS is 5.8% under evaluation of the Windows benchmark suite. [2] aim to evaluate the AMMDS for the Linux-based operating system to evaluate its detection rate against the propagation of the sophisticated Linux malware.

3.3 [3] "A Hybrid Approach for Alarm Verification using Stream Processing, Machine Learning and Text Analytics", (2018)

[3] presented the design and evaluation of an alarm verification system using real data from an industry application. The problem is very

challenging since it requires a combination of stream processing, batch processing and machine learning. [3] have built the system using Spark Streaming (stream processing), MongoDB (batch processing) and Spark ML (machine learning). Our experiments with various machine learning algorithms show that the system can classify alarms with an accuracy of more than 90% at a streaming rate of about 30K alarms per second, including historical data analysis.

Remark: [3] presented, preliminary results of an integration of unstructured data to increase the classification accuracy. [3] concluded with an extensive list of lessons learned that give insights for both academics and practitioners who want to build a similar system.

3.4 [4] "Advanced Machine Language Approach to Detect DDoS Attack Using DBSCAN Clustering Technology with Entropy", (2018)

Due to far-below par performance of most of the existing DDoS detection schemes and the very sophisticated nature of these attacks, [4] proposed an advanced machine learning approach to detect the distributed denial of services attacks on cloud computing environment with entropy using clustering technology. As [4] continuing this research to implement this very effective DDoS hybrid detection schemes, [4] looking forward to perform more additional regressive testing to implement this comprehensive approach at both vulnerable side of the cloud computing environment (the network and host level). Counting on the preliminary encouraging and promising experimental results, and the upcoming additional performance testing phases scheduled, [4] could be the best alternative lasting solution for cloud computing services availability.

Remark: [4] present the details of experimental findings, results, data analysis, and implementation plan on the next upcoming research paper.

3.5 [5] "A Novel algorithm for Network Anomaly Detection using Adaptive Machine Learning", (2018)

Threats in the Internet are posing high risk on Security of Information and network anomaly detection has become an important issue/area in Information Security. Data mining algorithms are used to find patters and characteristic rules in huge data and this is very much used in Network Anomaly Detection System (NADS). Network traffic has several attributes of qualitative and quantitative nature, which needs to treated/normalized differently. In general, a model is built with the existing data and the system is trained with the model and then used to detect intrusions. The major and important issue with such NADS is that the network traffic changes over time, in such cases the system should be trained automatically or retrained. [5] proposed method uses the labeled dataset for training but can adapt/learn itself and can detect new attacks. The performance measures of the algorithm can still be improved by combining this algorithm with feature weights. The algorithm has good potential to be parallelized.

Remark: [5] shall focus on parallelizing the algorithm using GPGPU processors for achieving performance as energy efficiency has become the prime concern for the Computer industry. Different sensors for different protocol types can be used for performance improvements. The authors are working on improving the algorithm and modifying it for flow based Anomaly Detection.

3.6 [6] "Anomaly detection in wide area network mesh using two machine learning anomaly detection algorithms", (2018)

[6] presents two new techniques for distinguishing system execution oddity in view of split-example characterization: AdaBoost and Simple feedforward neural system. Both methods are first tested on simulated datasets to check their sensitivity with respect to duration and amplitude of anomaly. The boosted decision tree method proved to be very fast (4seconds evaluation per one hour of data tested) and detected all the simulated anomalies. An added benefit is that it directly returns ordered list of series according to their contribution to the anomaly being flagged. With fittingly chose AUC edge, it is conceivable to tune wanted affectability/false positive level. The simple neural network model used was not hyper-parameter optimized and the one network tried proved less sensitive to short and low amplitude changes. Given that, [6] looking for the most significant anomalies this is a good feature. While the evaluation is slower at 20seconds per hour of data tested, it is still fast enough to be of practical use.

Remark: A more significant issue is that it requires a GPU for processing. Since this is a three-layer network it is difficult to get information on the importance of different time series to the resulting decision. While results on the actual data are encouraging, before using it in a production environment, different network configurations should be tested (two layers, fewer neurons per layer, etc.) and hyper-parameter tuned.

3.7 [7] "A Novel Malware Analysis Framework for Malware Detection and Classification using Machine Learning Approach", (2018)

In [7], a novel intelligent malware analysis framework has been developed for dynamic and static analysis of malware samples based on similarity in their behavior. Experimental results demonstrate acceptable performance of the proposed procedures in detecting and classifying malicious files using machine-learning models in Weka. [7] observed that J48 Decision tree shows the best performance in terms of accuracy and precision. [7] considered only 220 samples of files for analysis which may be biased, because not all the features may have incorporated using these number of samples.

Remark: [7] will add more datasets so that [7] will get extensive set of features for visualizing the performance on broad spectrum.

3.8 [8] "Wired LAN and Wireless LAN Attack Detection Using Signature Based and Machine Learning Tools", (2018)

There are various attack which is possible in the network, it may be from externally or internally. However, internal attacks are more dangerous than external. So, [8] mainly concern upon Wireless LAN and Wired LAN attacks which occurs internally. There are various Signature based tools, IDS/IPS (Intrusion detection or prevention system) available now-a-days for detecting these types of attacks but these are not sufficient due to high false alarm rate. Subsequently, [8] identify these kinds of assaults with three routes: through Wireshark, with signature based apparatuses (Snort and Kismet) and with machine learning instruments (WEKA). In wired LAN attack, my mainly concern on PING scan or PING flood, NMAP scan (portsweep) and ARP spoofing attacks. In wireless LAN attacks, [8] take care of Deauthentication attack, Disassociation attack and Access point (AP) spoofing attack. Signature based tools detect these types of the attacks based on the stored signature and timing threshold. Nevertheless, machine-learning tools take several different features to detect these types of attacks with more accuracy and low false positive rate.

Remark: Signature based parameters and machine-learning parameters can be combined for very high accuracy results along with more parameters. Concentration can be on the prevention strategy of these kinds of attacks.

3.9 [9] "IoT Security Techniques Based on Machine Learning", (2018)

Internet of things (IoT) that integrate a variety of devices into networks to provide advanced and intelligent services have to protect user privacy and address attacks such as spoofing attacks, denial of service attacks, jamming and eavesdropping. [9] investigate the attack model for IoT systems, and review the IoT security solutions based on machine learning techniques including supervised learning, unsupervised learning and reinforcement learning. [9] center around the machine learning based IoT verification; get to control, secure offloading and malware recognition plans to ensure information protection. [9] talk about the difficulties that should be routed to execute these machine learning based security conspires in useful IoT frameworks.

Remark: Several challenges have to be addressed to implement the learning based security techniques in practical IoT systems: 1) Partial state observation 2) Computation and communication overhead 3) Backup security solutions.

3.10 [10] "Survey on SDN based network intrusion detection system using machine learning approaches", (2018)

Software Defined Networking Technology (SDN) provides a prospect to effectively detect and monitor network security problems ascribing to the emergence of the programmable features. Recently, Machine Learning (ML) approaches have been implemented in the SDN-based Network Intrusion Detection Systems (NIDS) to protect computer networks and to overcome network security issues. A surge of cutting edge machine learning approaches – the profound learning innovation (DL) begins to rise in the SDN setting. [10] evaluated different late chips away at machine learning (ML) techniques that use SDN to execute NIDS. All the more particularly, [10] assessed the systems of profound learning in creating SDN-based NIDS. Meanwhile, [10] secured models that can be utilized to create NIDS models in SDN condition.

Remark: The use of deep learning has gained importance due to its efficiency in evaluating network security. Similarly, new methods of deep learning are increasing faster and efficient in data taxation. Various issues need to be considered while implementing NIDS, since the nature of the attacks are dynamic. Therefore, adaptability of detection method is required. Developing a feature selection method with classifiers, which reduces the dimensions of the dataset, is an ongoing challenge. This is another field of research to classify proper dataset using DL techniques. To design a centralized

SDN controller, that can monitor and implement real-time intrusion detection in high-speed networks is a possible future direction and will be a challenging task.

3.11 [11] "Malware classification using self organising feature maps and machine activity data", (2018)

[11] utilize machine action measurements to recognize noxious and trusted compact executable programming tests. The inspiration originates from the development of digital assaults utilizing systems that have been utilized to secretly convey Advanced Persistent Threats (APTs). APTs are ending up more complex and ready to muddle quite a bit of their identifiable highlights through encryption, custom code bases and in-memory execution. [11] can deliver a high level of exactness in recognizing pernicious from trusted examples utilizing Machine Learning with highlights got from the certain impression abandoned on a PC framework amid execution. This incorporates CPU, RAM, Swap utilize and organize movement at a check level of bytes and parcels. These highlights are nonstop and enable us to be more adaptable with the arrangement of tests than discrete highlights, for example, API calls (which can likewise be muddled) that frame the primary component of the surviving writing. [11] utilize these persistent information and build up a novel grouping technique utilizing Self Organizing Feature Maps to decrease over fitting amid preparing through the capacity to make unsupervised bunches of comparative "conduct" that are in this way utilized as highlights for characterization, as opposed to utilizing the crude information.

Remark: [11] contrast the technique with an arrangement of machine grouping strategies that have been connected in past research and exhibit an expansion of in the vicinity of 7.24% and 25.68% in characterization precision utilizing the strategy and an inconspicuous dataset over the scope of other machine order techniques that have been connected in past research.

3.12 [12] "Technical challenges and perspectives in batch and stream big data machine learning",(2018)

Big Data Machine Learning is an upcoming research field. However, traditional Machine Learning algorithms are becoming unsuitable for majority of applications as the data is acquiring new characteristics. Sensors, devices, servers, Internet, Social Networking, Smart phones and Internet of Things are contributing the major sources of data. Hence, there is a paradigm shift in the Machine learning with the advent of Big Data. Volume, Variety and Velocity data characteristics initiate the need for development of new algorithms and models for machine Learning. Several research works have been discussed in [12], which gave directions for the development of Big data machine Learning Algorithms. However, No single method or algorithm can function efficiently due to the data characteristics.

Remark: Batch Processing Machine Learning algorithms were addressed in [12] to certain extent but real time stream Mining is still an open area.

3.13 [13] "Using machine learning to detect and localize concealed objects in passive millimeter-wave images", (2018)

[13] devoted to the study of hidden object detection in PMMWIs .The main difficulty in this task arises from the low SNR and non-stationary noise that populates an image. Simple thresholding method scan be used but are most effective with high-quality images. In [13], a machine learning approach to the detection task was developed. [13] approach deals with the poor quality of passive images and outperforms state-of-the-art threat detection methods for PMMWIs. Given the lack of publicly available PMMWI datasets, [13] created one that, to the best of knowledge, is the largest, and possesses the greatest variety of object types and sizes ever used. [13] is based on a committee of classifiers defined on two highly unbalanced classes of image patches, and performed well on all experiments. [13] compared different approaches to estimate image classification functions, and found using tree sets to be the most effective, reaching an average 94% TP score with a distribution of the number of false positives in the range of one to seven. The influence of the image quality and the extracted features were also analyzed. [13] helps the detection process; Haar filter banks, very well adapted to the task, performed very well for all classifiers.

Remark: The results indicate that large objects with reduced or zero emissions are simpler to detect. The easiest threat locations to detect were those where the objects were exposed to the camera in larger areas. Threats in ankles, arms, and thighs were more difficult to detect. Comparison between this detection model and other approaches in the literature indicated that [13] is less reliant on the quality of the observed images. Furthermore, when a large image training set is available, [13] performs very well, which makes a prediction of excellent performance for a wide range of millimeter- based detection systems realistic.

3.14 [14] "Performance comparison of intrusion detection systems and application of machine learning to Snort system", (2018)

[14] investigates the performance of two open source intrusion detection systems (IDSs) namely Snort and Suricata for accurately detecting the malicious traffic on computer networks. Snort and Suricata were installed on two different but identical computers and the performance was evaluated at 10 Gbps network speed. It was noted that Suricata could process a higher speed of network traffic than Snort with lower packet drop rate but it consumed higher computational resources. Snort had higher detection accuracy and was thus selected for further experiments. It was observed that the Snort triggered a high rate of false positive alarms. To solve this problem a Snort adaptive plug-in was developed. To select the best performing algorithm for Snort adaptive plug-in, an empirical study was carried out with different learning algorithms and Support Vector Machine (SVM) was selected. A hybrid version of SVM and Fuzzy logic produced a better detection accuracy. However, the best result was achieved using an optimized SVM with firefly algorithm with FPR (false positive rate) as 8.6% and FNR (false negative rate) as 2.2%, which is a good result.

Remark: The novelty of this work is the performance comparison of two IDSs at 10 Gbps and the application of hybrid and optimized machine learning algorithms to Snort.

3.15 [15] "Quantifying the Resilience of Machine Learning Classifiers Used for Cyber Security", (2018)

[15] relies on two core concepts: total attack budget and the feature manipulation cost. Together, those two simple abstractions open the door to modeling an attacker's abilities in a given operational scenario. Based on these concepts [15] provide the defender with tools for weighting risk against attack potential and fitting the classification model to his/her needs. [15] test the approach using a case of a multisensory fusion system used for dynamic analysis. Multisensor fusion is the basis of most modern cyber defense systems in which a variety of sensors are deployed throughout the defending organization, and the sensors' readings are analyzed collectively in an attempt to identify attacks. [15] demonstrate the effectiveness of the MRB score in comparing the resilience of different classification models. [5] simulate an evasion attack, as well as an availability attack, using multiple machine learning algorithms, and in all cases the MRB provides a concise and easy-to-use comparison metric. [15] also explored the inherent resilience of different classification algorithms. The random forest classifier demonstrated superior resilience in all cases, suggesting that ensemble based classifiers are inherently more resilient to adversarial attacks. [15] results in this case coincide with the claims of past work, strengthening these assertions and providing them with additional experimental support. [15] demonstrated how the resilient feature selection algorithm yields classification models with guaranteed resilience in the face of different types of attacks.

Remark: [15] wish to test the approach on distributed multisensory organizational SIEMs. These systems employ a large collection of independent sensors which increase the potential for detection. The main challenge experienced by modern SIEMs today is how to reduce the number of false alarms, in order to improve the efficiency of the security professionals using these systems. In nearly every publicly known attack on a large organization, the forensic analysis has revealed traces of the attack that were initially overlooked due to the high volume of false alerts. Therefore, [15] goal is to test our approach in such a scenario and validate our ability to prevent an attacker from deliberately increasing the number of false alerts. [15] suggests that ensemble based classifiers are inherently more resilient than simple classifiers. [15] would like to enrich the mathematical abstraction to correctly represent different machine learning tasks, as well as cases of non-supervised learning.

4. Conclusion and Future Enhancement

This survey paper specifies that Anomaly detection is an important topic in security, and is an area that machine learning techniques has shown a lot of efficacy. Before diving into complex algorithms and statistical models, take a moment to think carefully about the problem you are trying to solve, and the data available to you. The answer to a better anomaly detection system may not be to use a more fancy and advanced algorithm, but may be to generate a more complete and descriptive set of input. As of the large scope of threats they are required to mitigate, security systems have a tendency to grow uncontrollably in complexity. In building or improving anomaly detection systems, always keep simplicity as a top priority.

References

[1] Abhishek Vermaa, Virender Rangaa, "Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using

Distance-based Machine Learning", Procedia Computer Science 125, (2018), 709–716

[2] Ajay Kumara M.A., Jaidhar C.D, "Automated multi-level malware detection system based on reconstructed semantic view of executables using machine learning techniques at VMM", Future Generation Computer Systems, Vol.79, 1(2018), 431-446.

[3] Ana Sima, Kurt Stockinger, Katrin Affolter, Martin Braschler, Peter Monte, Lukas Kaiser, "A Hybrid Approach for Alarm Verification using Stream Processing, Machine Learning and Text Analytics", ACM, (2018), https://doi.org/10.21256/zhaw-3487

[4] Anteneh Girma, Mosses Garuba, and Rajini Goel, "Advanced Machine Language Approach to Detect DDoS Attack Using DBSCAN Clustering Technology with Entropy", Information Technology - New Generations. Advances in Intelligent Systems and Computing, Vol. 558, (2018), DOI https://doi.org/10.1007/978-3-319-54978-1_17

[5] Ashok Kumar. D, S. R. Venugopalan, "A Novel algorithm for Network Anomaly Detection using Adaptive Machine Learning", Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, Vol. 564, (2018), DOI https://doi.org/10.1007/978-981-10-6875-1_7

[6] James Zhang, Ilija Vukotic, Robert Gardner, "Anomaly detection in wide area network mesh using two machine learning anomaly detection algorithms", Networking and Internet Architecture, (2018)

[7] Kamalakanta Sethi, Shankar Kumar Chaudhary, Bata Krishan Tripathy, Padmalochan Bera, "A Novel Malware Analysis Framework for Malware Detection and Classification using Machine Learning Approach", ACM, (2018), doi>10.1145/3154273.3154326

[8] Kaur. J, "Wired LAN and Wireless LAN Attack Detection Using Signature Based and Machine Learning Tools", Networking Communication and Data Knowledge Engineering, (2018), 15 - 24

[9] Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, Di Wu, "IoT Security Techniques Based on Machine Learning", (2018), https://arxiv.org/abs/1801.06275

[10] Nasrin Sultana, Naveen Chilamkurti, Wei Peng, Rabei Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches", Peer to Peer Networking and Applications, (2018), 1-9. https://doi.org/10.1007/s12083-017-0630-0

[11]Pete Burnap, Richard French, Frederick Turner, Kevin Jones, "Malware classification using self organising feature maps and machine activity data", Computers and Security, Vol.73, (2018), 399 - 410

[12]Rama Rao. KVSN, Sivakannan S, M.A.Prasad, R.Agilesh Saravanan, "Technical challenges and perspectives in batch and stream big data machine learning", International Journal of Engineering & Technology, 7 (1.3) (2018) 48-51.

[13] Santiago López-Tapia, Rafael Molina, Nicolás Pérez de la Blanca, "Using machine learning to detect and localize concealed objects in passive millimeter-wave images", Engineering Applications of Artificial Intelligence, Vol.67, (2018), 81 – 90.

[14]Syed Ali Raza Shah, Biju Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system", Future Generation Computer Systems, Vol.80, (2018), 157 – 170.

[15]Ziv Katzir , Yuval Elovici, "Quantifying the Resilience of Machine Learning Classifiers Used for Cyber Security", Expert Systems with Applications, Vol. 92, (2018), 419 – 429.