UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

DIPARTIMENTO DI INFORMATICA

PhD Program in Computer Science and Mathematics
XXXIV cycle

Research Project

PhD Student: Giuseppina Andresini

Supervisor: Prof. Annalisa Appice

Coordinator: Prof. Maria F. Costabile

PhD student signature

Supervisor signature

1. Research title:

Innovative machine learning techniques for cybersecurity (Tecniche innovative di machine learning per la sicurezza informatica)

2. Research area:

Machine Learning, Data Science, Cybersecurity, Big data analytics

3. Research motivation and objectives

Security attacks are becoming more prevalent as cyber attackers exploit system vulnerabilities for financial, political or military gain. Cyber attackers are aware of existing security controls and are continually improving their attacks. To make matters worse, cyber attackers have a wide range of tools available which allow them to bypass traditional security mechanisms. Zero day exploits, malware infection, rootkits, and browser exploit packs can be readily purchased on an underground market. Attackers can also purchase personal information and compromised domains in order to launch additional attacks [1]. A security breach is inevitable. Early detection and mitigation are the best defense to surviving an attack. Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. The Cyber Research Alliance identified the application of machine learning, in particular big data analytics, to cybersecurity as one of the top priorities for future cybersecurity research and development.

Machine learning is adopted in a wide range of domains (e.g. finance, medicine, remote sensing) due to their properties like adaptability, scalability, and potential to rapidly adjust to new and unknown challenges. In these scenarios, machine learning shows its superiority over traditional rule-based algorithms. This trend is also affecting the cybersecurity field where some detection systems are being upgraded with machine learning techniques [2].
Nowadays machine learning plays a crucial role in cybersecurity as it includes a wide spectrum of paradigms in continuous evolutions which are well suited for aggregating and correlating of a broad range of heterogeneous data from multiple sources, and has the potential to detect cyber threats within actionable time frames with minimal or no human intervention. Finding appropriate algorithms required to locate hidden patterns in huge amounts of data is just one of the several challenges that must be overcome in cybersecurity.

In this research project, we will focus on synthesizing new effective machine learning algorithms, in order to accurately detect attacks by leveraging the power of the several big dimensions (volume, velocity, variety, variability and value) of the attack data. In particular, we plan to handle recent challenges of cybersecurity applications (e.g. intrusion detection, malware analysis) by significantly advancing the machine learning research in the following paradigms:

1) **Deep Learning** in order to exploit the value in the volume of attack data [5]. Although, DL is known to outperform SL in various applications characterized by huge volumes of collected data (e.g. image analysis), this is not always the case for cybersecurity where some well configured SL algorithms may still prevail. In any case, the given growing number of DL proposals in cybersecurity emerged in the literature of the last years [7] [8] [9] clarifies the presence of a growing interest in empowering this paradigm in cybersecurity.
2) **Multiple View Learning and/or Data Fusion**, in order to deal with data collected through various sources, attributed to various behaviours and/or characterized by different modality.
3) **Data Stream Learning,** in order to actually handle the variability and velocity of attack data.

4. State of the art

In the last decade, many different approaches are investigated in cybersecurity, in order to develop systems to prevent damage caused by malware, unauthorized systems access or destruction, disclosure or theft of data.

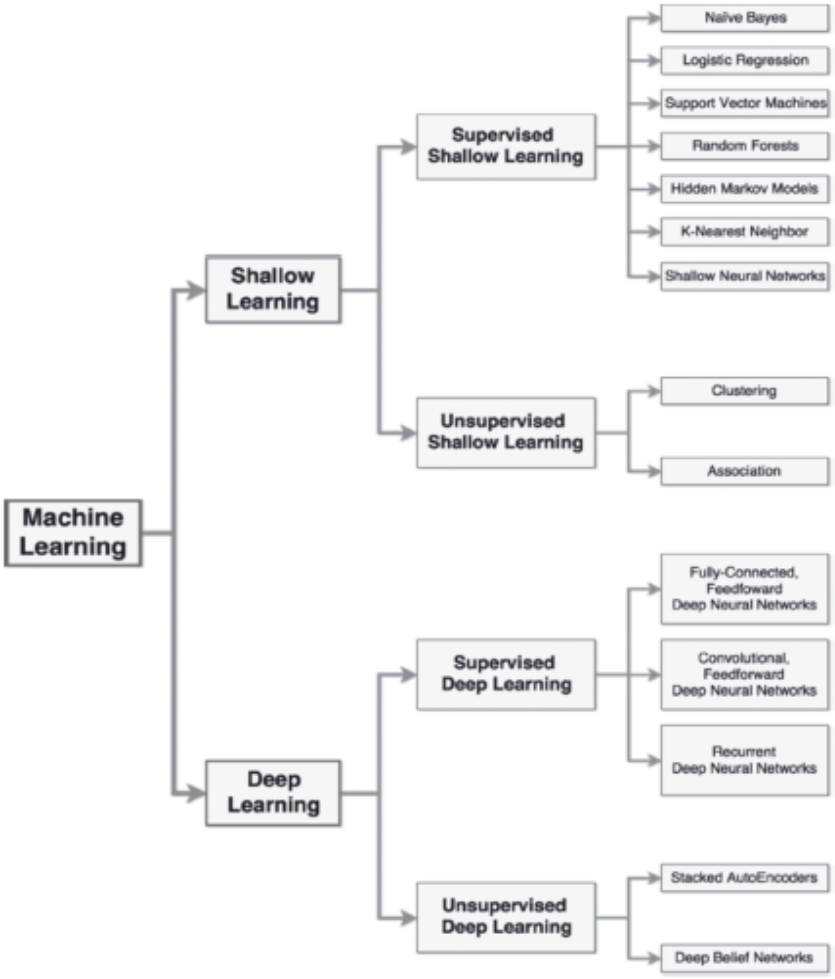

Figure 1: Cybersecurity machine learning taxonomy [2]

According to the taxonomy reported in [2] (see Figure 1), the machine learning for cybersecurity mainly includes shallow and deep learning approaches. As expected, the overall number of algorithms based on DL is considerably smaller than those based on SL. DL proposals based on huge neural networks are more recent than SL approaches. This gap opens many research opportunity.

SL requires a domain expert (i.e. a feature engineer) who can perform the critical task of identifying the relevant data characteristics before executing the SL algorithm. DL relies on a multi-layered representation of the input data and can perform feature selection autonomously through a process defined representation learning. Both SL and DL approaches can be further characterized by distinguishing between supervised and unsupervised techniques. The former techniques require a training process with a large and representative set of data that have been previously classified by a human expert or through other means. The latter techniques do not require a pre-labelled training dataset. Supervised techniques find wide application to malware analysis, less to intrusion detection; spam detection relies mainly only on unsupervised algorithms.

Specifically, unsupervised techniques include clustering and association discovery in SL; autoencoding in DL. Supervised approaches include Naive Bayes - NB, Random Forest - RF, Support Vector Machines -SVM, k-NN, Hidden Markov Models - HMM and Shallow Neural Network -

SNN(neural networks with a limited number of neurons and layers) in SL; Fully-connected Feedforward Deep Neural Networks - FNN, Convolutional Feedforward Deep Neural Networks - CNN and Recurrent Deep Neural Networks - RNN in DL. Several studies combine unsupervised and supervised learning components in the same cybersecurity framework. There are also a few machine learning approaches performing incremental learning.

In particular, the basic idea in the clustering approach is that large clusters contain normal data, while small clusters consist of attack connections. Based on this premise, a clustering approach is formulated for the intrusion detection in [12]. Clustering process is performed with algorithm k-means while the number of clusters is set equal to the number of classes to be detected. The classification is done with an k-NN classifier. A hierarchical clustering algorithm is used in [13], where fuzzy c-means based on genetic algorithm is combined with SVM classification. The described machine learning process is three-stepped (1) N fuzzy clusters are detected, (2) N SVM classifiers are learned from the N clusters and (3) classifications are merged.

Clustering is formulated for malware analysis in [14], where authors run the K-medoids algorithm on the collected sequences of system calls, in order to group malware families. Behavioral profile is created for each sample based on its interaction with the system resources. New and unknown samples are assigned to the clusters with the closest medoids. Ye et al. [15] develop an automatic malware categorization system (AMCS) for categorizing malware samples into families that share some common traits, by an ensemble of different clustering solutions generated by different clustering method. They develop a cluster ensemble framework (by combining hierarchical clustering, k-medoids and so on) and combine the individual clustering solutions based on the consensus partitions.

In fraud detection, clustering is investigated, in order to divide, all cardholders into groups based on information like the transaction amount, the number purchases and so on. Agarwal et al [16] implement a hybrid approach using clustering and outlier detection techniques to find anomalies behavior. In [17], authors extract association-based behavioral patterns from similar cardholders which fits over times (a sliding window algorithm permits to examines cardholder behavior in different timestamps).

In [18], three base classifiers, namely Bayesian Network, Naïve Bayes and J48, are considered to learn a classifier ensemble that uses the majority vote approach to discriminate normal and anomaly data. In the first phase, a hybrid feature selection (Best First, Genetic Search and Rank Search) is used to select features set. The feature selection is a crucial phase in various classifier builders. Several shallow supervised methods focus on feature selection and feature extraction. The majority of these studies use feature selection techniques like InfoGain [19] and Gain Ratio [20] or feature construction techniques like PCA [21], LSI [22] or Autoencoder [23].

Chen et al. [23] describe an ensemble to feature extraction methods (Global/Local Latent Semantic Indexing - GLSI/LLSI and Global/Local Kernel-Principal Component analysis - GKPCA/LKPCA). Global feature extraction methods are unsupervised approaches as they neglect the class information. Local feature extraction methods are supervised approaches as they divide collected data into several groups based on their class label and perform the feature extraction based on the class distribution.

Shone et al [7] investigate a nonsymmetric deep autoencoder (NDAE) for unsupervised feature extraction and they learn a Random Forest to classify the data.

Ludwing [8] implements an ensemble of deep neural techniques, in order to detect multiple classes of attacks. The attacks are detected through several classifiers: Autoencoder, Deep Belief Neural Network and Deep Neural Network. Results of multiple classifiers are combined through a majority vote approach. In [6], a DNN architecture is implemented, in order to identify anomalies in the network data. The proposed approach consists of three steps: each step trains one layer of the DNN at each time. First the approach trains the auto-encoder on the original features of the training data. Second it trains the auto-encoder on the features extracted from the first auto-encode. Finally, it trains a softmax layer, in order to classify each attack and normal data.

DL4MD [24] is a learning framework for malware detection. It uses a stacked autoencoder, followed by a supervised fine-tuning, in order to classify the malicious program behavior based on the

Windows API calls extracted from the PE (Portable Executable) files. Choi et al [25] use deep learning, in order to detect malware using malware images. Authors generate images from both benign and malicious files. They use a convolutional neural network (CNN) for the classification task. The idea is that several variants of the same malware have images which are similar to the image of the ancestor malware. This assumption is exploited and malware images are processed faster than API sequences. In [9], authors use a multimodal deep learning model for malware detection. The model is based on the analysis of various features, each group of features is considered to train a neural net. The processed feature groups are independent one to each other. The final layer of the network combine the several networks.

The adversarial learning is a machine learning approach that has received emerging attention in cybersecurity. Machine learning models are often vulnerable to adversarial examples, which are malicious perturbed input to mislead the detection at the test time. An attacker can have a perfect or partial knowledge of the targeted system in white-box (with knowledge of the model parameters), gray-box or black-box attacks (without knowledge of the feature space). Papernot et al [26] show a black-box attack strategy which is realized by observing the output labels given by model. In Madry et al [27], the robustness of neural networks is increased by injecting adversarial examples in training data. In [27] a defensive mechanism, called defensive distillation, is used to reduce the effectiveness of the adversarial samples on neural network models.
The distillation is a technique to transfer knowledge from different DNNs, with the purpose of reducing the computational complexity of a neural network model, in order to transfer knowledge from larger architectures to smaller ones. In [28], knowledge extracted from distillation (probability vectors, which include additional knowledge about classes) is used to train a classification model. In [29], an adversary-aware approach, that proactively anticipates the attacker, is used to improve the security of a malware detection based on a static analyzer.

To deal with evolving attack data, an incremental k-NN-SVM approach is proposed in [30]. This is a hybrid three-stepped incremental learning method defined as follows: (1) training data are initially inserted into a R*-tree (it will be updated as new data are collected and used to perform k-NN queries), (2) incremental training and prediction is performed with k-nn and SVM classifier and (3) the learning model and storage in R*-tree is updated continuously.
The approach described in [31] is also formulated in the incremental fashion. The machine learning method includes both an online phase and an offline phase. In the online phase, the training set is grouped in clusters through an unsupervised incremental algorithm based on self-organizing maps neural networks, namely mixed self-organizing incremental neural network - MSOINN. In the online phase, when new instance arrives at the model, clusters are updated and the instance is classified with the nearest neighbor method.

Finally, dealing with volume, velocity, variety, variability and value of attack data paves the way for boosting big data analytics for cyber security [4]. Few works have investigated the attack detection problem by resorting to a Big Data analysis approach. In [32], authors use a big dataset constructed by combining three intrusion detection datasets (KDD99 [33], DARPA98 [34] and DARPA99 [35]). To capture, manage and process this huge amount of data, authors use a NoSQL database (MongoDB). A Map-Reduce phase is used to combine common attributes. In [36], authors present an intrusion detection algorithm named Spark-Chi-SVM. This combines ChiSqSelector for feature selection and SVM for classification. The algorithm is implemented in the Spark framework programming in SCALA and using the MLlib machine learning library.

5. Problem approach

Building a machine learning algorithm for a cybersecurity application can be decomposed in two sub-tasks:

1. Feature selection and/or feature construction;
2. Pattern learning.

The feature selection and/or construction is often performed, in order to reduce the computational time and simplify the learned model and improve its interpretability. To this end, we plan to address studies on SL and DL to the activity of synthesis of new family attack-based feature selection/construction techniques able to improve the accuracy of the machine learning process by constructing separate feature spaces that will represent multiple views of the data.
We plan to identify the deep learning architectures, which are able to accurately model the attacks by limiting the false alarm rate, dealing with the unbalance nature of data in cybersecurity (i.e. the number of normal instances is usually large, while the proportion with attacks instances is often very skewed).

Appropriate fusion techniques will be also formulated, in order to determine detection patterns achieved across these multiple views. Even though several data fusion techniques [10] and multiple view learning approaches [11] have been developed in the past few years, their usage in the field of cybersecurity warrants new approaches considering many aspects including unified data representation, data sharing across threat detection system and feature separation between distinct treat based datasets, sampling and dimensionality reduction.
Pattern learning will be performed, in order to construct an intelligent system for detecting attacks (included zero-day attacks) as soon as possible, in a data stream way, and mitigating the attack damage over the network. We intend to analyze unsupervised, supervised and ensemble methods both in SL and DL. We will investigate the performance of pattern learning in dependence of the task of feature selection/construction. We will synthesize machine learning approaches, possibly spanned over multiple views or tasks, in order to improve the accuracy of the detection phase independently of the family of attack data. We will explore also data-changing machine learning approaches, such as incremental learning and concept drift learning. To deal with the streaming style and the huge heterogeneity of attack data and meet the requirements of real-time/massive data analysis, we will evaluate solutions of analysis available in Big Data technologies. The *volume*, *velocity* and *variety* of enterprise security data available pose the greatest challenge to successful cybersecurity analytics [3]. The additional challenges are the *variability* of threats and the need of an infrastructure to gather data achieving a *value*.

The iterative and interactive research approach followed in the project development will include the series of the following steps:

- Study of the state-of-the art in cybersecurity machine learning, shallow and deep learning, big data analytics, multiple view learning, data fusion and feature extraction;
- Identification of benchmark scientific and industrial data sources for the evaluation of the effectiveness of the proposed algorithms in applications of attack detection;
- Synthesis of new machine learning algorithms deployed in deep learning, multiple view learning and big data analytics, to process attack data along 5V dimension of data;
- Scientific activity dissemination.

6. Expected results

The focus will be to the synthesis of new machine learning algorithms that will be applied to specific application areas of cybersecurity, which are of interest in both scientific and industrial scenarios.
The main applications of attack detection, where the cybersecurity machine learning algorithms are commonly used, include intrusion detection and malware analysis. Intrusion detection aims at discovering illicit activities within a computer or a network (e.g. the unauthorized access to a computer system or computer network - "crackers" - or the abuse of privileges in an authorized access - "insider threat") through an Intrusion Detection System (IDS). *Nowadays any enterprise network deploys a network IDS.* Malware analysis aims at identifying modern malware that can automatically generate novel variants with the same malicious effects but appearing as completely different executable files. *Both intrusion detection and malware analysis are crucial tasks in business enterprises where security of data and services is a priority.*
Additional application areas are in phishing detection, spam detection and credit card fraud detection. In these areas, the attack vectors, the types and ramifications of these threats are manifold. On one side, malware are used for infecting computers at a large scale and conducting illegal activities, such as the distribution of spam messages or the theft of personal data. On the server side, a plethora of attacks may target the network services (e.g classic exploits, injection attacks). These attacks are regularly used for compromising web servers and retrieving sensitive data, such as passwords and credit card numbers.

To prove the effectiveness of the research products, we will consider benchmark data which have been also considered in the evaluation study of the most recent research studies in IDS and malware analysis. At present, the majority of studies evaluate the new algorithms for IDS on KDD 1999 dataset [33]. NSL-KDD is a variant of KDD-99 [37] that is built by filtering-out redundant examples. Recent papers (2017-2018) evaluate machine learning algorithm for intrusion detection on both KDD-99 and NSL-KDD. We will consider these results as a benchmark for safe comparison of the performance achieved by the algorithms that will be synthesized during this research project.
We will also consider benchmark data for malware analysis (e.g. Drebin data [29]), as well as data samples that can be requested through virustotal and virushare.
Finally, we plan to evaluate the performance of the synthesized data on attack data to will collected in real time through the HackLab Space installed at Cybersecurity Laboratory of the Department of Computer Science in Taranto

The main of goals to be achieved is the synthesis of a new machine learning framework that will be able to:

- Detect anomaly behaviors from normal with high accuracy and low false alarm;
- Identify new attacks (zero days) without manual effort;
- Analyze new data in a faster manner (incremental algorithms);
- Perform learning fast to identify and react malicious behaviors in (near) real time;
- Analyze a huge amount of data in an effective manner.

7. Phases of the project

1st year: Study of the literature, state-of-the-art and cybersecurity applicative domain

Activity 1.1 Study of the state-of-the-art regarding machine learning and big data analytics defined in the cybersecurity context with particular attention to intrusion detection and malware analysis systems;

Activity 1.2 Analysis of the methodologies and frameworks regarding cybersecurity machine learning research area and the most recent and relevant results achieved in the field;

Activity 1.3 In-depth study of the advantages and drawbacks of each approach, especially in deep learning, ensemble methods, multiple-view learning;

Activity 1.4 Attendance of courses and seminars included in the doctorate study plan, included online courses which may be relevant for this doctorate study plan;

Activity 1.5 Participation to international schools, conferences and workshop regarding topics relevant for the research theme.

2nd year: Development of methods

Activity 2.1 Definition a new proposal approach at the cybersecurity attack detection problems in relationship at works and results proposed in literature;

Activity 2.2 Development of the proposed approach;

Activity 2.3 Evaluations of the synthesized algorithms, comparison with existing approaches;

Activity 2.4 Submissions of the achieved results in journals and national and international conferences;

3rd year: Application to some domains and writing of the doctorate thesis;

Activity 3.1 Internship period in a foreign university or research centre which perform research studies which are strongly related to the research topic of this doctorate plan;

Activity 3.2 Collaboration with other research and industrial groups that pursue the same focus;

Activity 3.3 Analysis of the results obtained and improvement of the approach proposed ;

Activity 3.4 Writing of the Ph.D thesis.

8. Result evaluation

High detection rate is essential to evaluate a machine learning and data mining model in cybersecurity.

The main aspects to consider are:

- True positive (TP): number of attacks correctly detect
- True Negative(TN): number of non-attacks correctly detect
- False Positive(FP): number of non-attacks incorrectly detect
- False Negative(FN): number of attacks incorrectly detect

To evaluate the results obtained by performing, it is possible to compute different metrics as described in the related literature, such as:

- $Overall\ Accuracy = \frac{TP+TN}{TP+TN+FP+FN}$.
- $Error = 1 - accuracy$;

The overall accuracy metric measures the percentage of correct detections and number of false alarms. It is sensitive to the change in the data set and it poses interpretation problems in presence of unbalanced data [37]. To evaluate imbalanced learning, especially for unbalance classification problems, additional metrics to be considered are precision, recall, F-Score, receiver operating

characteristics (ROC), areas under receiver operating characteristics, precision-recall curves and cost curves.
The metrics are defined as:

- $Precision = \frac{TP}{TP+FP}$;
- $Recall\ (or\ True\ Positive\ Rate) = \frac{TP}{TP+FN}$;
- $False\ Positive\ Rate\ (Fallout\ or\ false\ allarms) = \frac{FP}{FP+TN}$;
- $F - measure = 2 * \frac{Precision*Recall}{Precision+Recall}$.

Precision is the fraction of relevant instances among the retrieved instance and measures the exactness of positive labeling, the coverage of the correct positive labels among all positive-labeled samples. It measures the proportion of anomaly instance classified correctly over the total number of instances
Recall is the fraction of relevant instances that have been retrieved over the total amount of relevant instances and measures the completeness of positive labeling. It measures the proportion of anomaly instance classified correctly over the total number of anomaly instances.
Precision is dependent of the data distribution, while recall is independent on data distribution. Recal, does not represent how many samples are wrongly labeled as positive, while precision does not provide any information about how many positive samples are labeled incorrectly.
F-measure combines the above two metrics and assigns the weighted importance to either the precision or recall. Consequently, the F-measure provides more insight into the accuracy of a classifier than recall and precision, while it is still dependent of the data distribution.

To address the problem of evaluating imbalanced data, many researchers have employed ROC and AUC, in order to analyze both the false-alarm rate and the true positive detection rate in one curve.
ROC curve (Receiver Operating Characteristic curve) shows the balance between the gain (True Positive Rate) and the cost (False Positive Rate) of a classification on a given data set.
The area under the ROC curve (AUC) is the probability that a classifier will rank a randomly chosen positive instance higher than a randomly chosen negative one (assuming that “positive” ranks are higher than “negative” ranks).
Another import evaluation dimension in both intrusion detection and malware analysis system is the time spent to complete the computation and/or detection. Early attack detection will allows us to take actions against possible attacks in a timely manner. There is a delay between the moment of attack and the response of the system, called total delay.

$$Total\ delay = time_{response} - time_{attack}$$

The smaller is total delay the better is an IDS. Additionally, a cybersecurity system must be to able to process attack data possibly in (near) real time. The computation time may be also evaluate as a function of the data set size.

9. Possible reference persons external to the department

Salvatore J. Stolfo, Columbia University, Intrusion Detection System Lab, https://salvatorestolfo.com/

V.S. Subrahmanian, University of Maryland, Institute for Advanced Computer Studies, https://www.cs.umd.edu/~vs/

Hans P. Reiser, Faculty of Computer Science and Mathematics, Universitat Passau, http://www.fim.uni-passau.de/en/sis/

Claudia Eckert, Technische Universitat Munchen, Fraunhofer Institute for Applied and Integrated Security, https://www.sec.in.tum.de/i20/people/claudia-eckert

10. References

[1] A. K. Sood and R. J. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," *IEEE Security & Privacy,* vol. 11.1, pp. 54-61, 2013.

[2] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. M., "On the effectiveness of machine and deep learning for cyber security," *In: 2018 10th International Conference on Cyber Conflict (CyCon),* pp. 371-390, Tallinn, 2018,.

[3] A. Kott, A. Swami and a. P. Mcdaniel, "Security Outlook: Six Cyber Game Changers for the Next 15 Years," *Computer 47.12,* pp. 104-06, 2014.

[4] A. Apurva, P. Ranakoti, S. Yadav, T. S. and R. N. R., "Redefining cyber security with big data analytics," *In: 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN),),* pp. 199-203, Gurgaon, 2017.

[5] Q. Zhang, L. T. Yang, Z. Chen and P. Li, "A survey on deep learning for big data, Information Fusion," in *Volume 42*, 2018, pp. 146-157.

[6] D. C. Potluri S., "Accelerated deep neural networks for enhanced Intrusion Detection System," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Berlin, 2016.

[7] N. Shone, T. N. Ngoc, P. D. and S. Q., "A Deep Learning Approach to Network Intrusion Detection," *IEEE Transactions on Emerging Topics in Computational Intelligence,*, vol. 2, no. 1, pp. 41-50, 2018.

[8] S. A. Ludwig, "Intrusion detection of multiple attack classes using a deep neural net ensemble," in *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, Honolulu, HI, 2017.

[9] T. Kim, B. Kang, M. Rho, S. Sezer and G. Im, "A Multimodal Deep Learning Method for Android Malware Detection Using Various Features," *IEEE Trans. Information Forensics and Security* , vol. 14, no. 3, pp. 773-788 , 2019.

[10] T. Baltrušaitis, C. Ahuja and L. Morency, "Multimodal Machine Learning: A Survey and Taxonomy," *IEEE Transactions on Pattern Analysis and Machine Intelligence.*, 2018.

[11] J. Hu, J. Lu and Y. Tan, "Sharable and Individual Multi-View Metric Learning," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 40, no. 9, pp. 2281-2288, 2017.

[12] W.-C. Lin, S.-W. Ke and C.-F. Tsa, "CANN: an intrusion detection system based on combining cluster centers and nearest neighbors.," *Knowledge-Based System,* p. 78:13–21, 2015.

[13] C. Tang, Y. Xiang, Y. Wang, J. Qian and B. Qiang, "Detection and classification of anomaly intrusion using hierarchy clustering and SVM," *Security and Communication Networks,* vol. Volume 9, no. Issue 16, pp. 3401-3411, November 2016.

[14] T. Lee and J. Mody, "Behavioral Classification," in *Proceedings of EICAR 2006*, 2006.

[15] Y. Ye, T. Li, Y. Chen and Q. Jiang, "Automatic Malware Categorization Using Cluster Ensemble," in *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ACM, New York, NY, USA, 2010, pp. 95-104.

[16] S. Agarwal and S. Upadhyay, "A Fast Fraud Detection Approach using clustering Based Method," in *Journal of Basic and Applied Engineering Research*, 2014, pp. 33-37.

[17] C. Jiang, J. Song, J. Liu, L. Zheng and W. Luan, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," *IEEE Internet of Things Journal*, vol. 5 , no. 5, pp. 3637-3647,, Oct. 2018.

[18] N. F. Haq, A. R. Onik and F. M. Shah, "An ensemble framework of anomaly detection using hybridized feature selection approach (HFSA)," in *SAI Intelligent Systems Conference (IntelliSys)*, London, 2015 .

[19] Y. Wahba, E. ElSalamouny and G. ElTaweel, "Improving the Performance of Multi-class Intrusion Detection Systems using Feature Reduction," *CoRR*, vol. abs/1507.06692, 2015.

[20] N. T. F. E. Pham, J. H. Suriadi Suriadi and L. H. F. M., "Improving performance of intrusion detection system using ensemble methods and feature selection," *Proceedings of the Australasian Computer Science Week Multiconference(ACSW)*, pp. 2:1--2:6, 2018.

[21] A. Makandar and Patrot A., "Detection and Retrieval of Malware Using Classification," *In: International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune*, pp. 1-5, 2017.

[22] H. Shahriar, I. M. and C. V., "Android malware detection using permission analysis," in *SoutheastCon 2017, pp. 1-6.*, Charlotte, NC, 2017.

[23] L.-S. Chen and S. J.S, "Feature Extraction based Approaches for Improving the Performance of Intrusion Detection Systems," in *Proceedings of the International MultiConference of Engineers and Computer Scientists* , Hong Kong, 2015.

[24] W. Hardy, C. Lingwen, H. Shifu, Y. Yanfang and L. Xin, "DL4MD : A Deep Learning Framework for Intelligent Malware Detection," 2016. [Online]. Available: https://www.semanticscholar.org/paper/DL-4-MD-%3A-A-Deep-Learning-Framework-for-Intelligent-Hardy-Chen/a6cc849f7c691e232360e9b71da0e431af2aa1e3. [Accessed 16 01 2019].

[25] S. Choi, S. Jang, K. Y. and J. Kim, ""Malware detection using malware image and deep learning," in *International Conference on Information and Communication Technology Convergence (ICTC), pp. 1193--1195*, Jeju Island, Korea (South), 2017.

[26] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik and A. Swami, "Practical Black-Box Attacks against Machine Learning," in *In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (AsiaCCS)*, Abu Dhabi, United Arab Emirates, 2017.

[27] N. Papernot, P. McDaniel, X. Wu, J. S. and S. A., "Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks," *IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA,*, pp. 582-597, 2016.

[28] S. Dua and X. Du, Data Mining and Machine Learning in Cybersecurity, Boston, MA, USA: Auerbach Publications, 2011.

[29] B. Xu, B. Chen, H. Zhang and T. Wu, "Incremental k-NN SVM method in intrusion detection," in *8th IEEE International Conference on Software Engineering and Service Science (ICSESS),*, Beijing, 2017.

[30] F. Noorbehbahani, A. Fanian, Mousavi, S. Rasoul and H. Hasannejad, "An incremental intrusion detection system using a new semi-supervised stream classification method," *Int. J. Communication Systems*, vol. 30, 2017.

[31] M. A.-. Qatf, Y. Lasheng, M. Al-Habib and K. Al-Sabah, "Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection," *IEEE Access*, vol. 6, pp. 52843-52856, 2018.

[32] M. Tavallaee, E. Bagheri, L. W. and G. A.A, "A Detailed Analysis of the KDD CUP 99 Data Set," in *IEEE Symposium on Computational Intelligence for Security and Defense Applications,*, Ottawa, ON, 2009.

[33] I. The UCI KDD Archive Information and Computer Science University of California, "KDD Cup 1999 Data," 1999. [Online].
Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. [Accessed 29 12 2018].

[34] M. Tavallaee, E. Bagheri, W. Lu and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in *Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, 2009.