Survey on Machine learning Techniques used for Information Security

Shradha Soni

{shradha.joleya@gmail.com}

Assistant Professor
Department of Computer Science and Application
St. Aloysius' College (Autonomous), Jabalpur (M.P.)

Abstract: Today Machine learning algorithms are the driving force of many applications because of their adjustable and expandable characteristics. They are influencing almost every aspect of the research. Information security one of the evolving fields in research. Data is being generated by heterogeneous sources, which provides a great scope for the information security research and machine learning algorithms can play a vital role for this. This paper provides a literature review for information security threats and the effects of machine learning algorithms against these threats.

Keywords: Machine Learning, Information Security, Threats.

1. Introduction:

Machine learning (ML) is more accurate in prediction of outcomes without being explicitly programmed. In ML for such kind of predictions variety of algorithms are there. Recent advents in the research shows that ML is spanning in almost every field like image recognition [1], pattern recognition [2], Security [3] [4] etc.

In the recent years Information security has fascinated many researchers due to voluminous growth of the data and variety of risks. Many researchers have worked on various aspect of the security i.e. what are the different threats and how they could be resolved. Due to versatile nature of the ML algorithms some researchers have imposed these algorithms against the threats. But in current literature does not provides synchronized information about Information Security risks and their solutions using ML algorithms.

This paper tries to bridge the gap between various researches. In the coming sections of this paper various security risks for Information security and ways to captivate using ML are described which have been suggested till now. Section II gives the basic idea of ML and related algorithms. This gives a very brief introduction about the concept. Section III presents various

THEETAS 2022, April 16-17, Jabalpur, India
Copyright © 2022 EAI
DOI 10.4108/eai.16-4-2022.2318143

attacks and remedies using ML algorithms. And section IV gives the concluding remark on this review.

2. What is ML (Machine Learning)?

ML is system programming to enhance performance criterion using training data or past experiences. For this model get defined over some parameters. And these models could be descriptive and predictive or both. Descriptive models get knowledge from the data and whereas predictive make predictions for the future. In simple words we can say ML is Learning. Basically, we can categorize it as follows [5]:

Supervised learning [6]

Support Vector Machine (SVM)

Artificial Neural Network (ANN)

Naïve Bayes (NB)

K Nearest Neighbor (KNN)

Random Forest (RF)

Decision Tree (DT)

Boosted Trees (BST-DT)

Semi supervised learning

Unsupervised learning

These are the various algorithms of machine learning. Supervised learning uses training data for the predictions. Supervised learning has a variety of algorithms as mentioned above. In Semi supervised learning in the input dataset some data is labeled and some data is unlabeled. Unsupervised learning used to draw the inferences form the given dataset.

3. Machine Learning Algorithms in Information Security Environment:

Here are some ML based algorithms that are extensively used in information security:

Support Vector Machine: This method is used for malware detection. In this method after the classification of all types of files, a decision boundary has been drawn between them for optimized classification which is known as hyperplane. this hyperplane acts to separate the two classes. and the margins where extreme data points fall known as support vectors. and ultimately these support vectors perform extensive evaluation for predicting that it's a malware or correct file [7].

Artificial Neural Network: Artificial neural network usually implemented using feedforward approach where signals can travel from input to output only. This architecture has one input

layer, two hidden and one output layer where each one consists of neurons. These layers are interconnected with synapses and perform the forward and backward propagation. Based on the output the attacks get identified. if the global error value is near about 0 and 1 then considered as normal packet otherwise an attack [8].

Naïve Bayes: In order to maintain information security, the patterns of the network services over data sets labelled by the services. With the built patterns, the framework detects attacks in the datasets using the Naïve Bayes Classifier algorithm. It encodes probabilistic relationships among dependent set of variables. It uses subjective or personal beliefs (prior probabilities) directly into the analysis.

K Nearest Neighbor: While using KNN for information security first normal training dataset is made then for the test data if it is unknown then considered abnormal otherwise if get known then the training data and the test data is compared and based on the similarity conclusions are made. If similarity is lower than the threshold value then the test data is considered as abnormal [9].

Random Forest: In this algorithm at first the Mtry parameter is optimized, for that datasets are used. After that the value is selected to build patterns of the services. Random forest is used many security algorithms but when used in intrusion detection it could be done by finding unusual activities or outliers. The random forests algorithm uses proximities to find outliers whose proximities to all other cases in the entire data are generally small [10].

Decision Tree: In Decision trees inputs and outputs are explained in the training data in which data is divided according to some parameters. In the context of information security first it selects the features tree is constructed based on training data and evaluated by validation data. Then fitness computation is done and finally classification rules are made out with the tree. Based on the rule the network behavior could be made out.

Boosted Decision Trees: Boosted decision trees trains the tree for dividing data based on any feature. then decision tree is validated against training data by which misclassified data values could be identified. Then values get the weights according to their importance and by this way misclassified value's weight get increased and correctly classified value's weight get decreased and new tree get built. then comparison of old tree and new tree is made which results in finding the misclassified values. this process is performed repeatedly all classifiers. Based on votes in the classification the values of given dataset are identified whether it is an anomaly or genuine data. [11]

4. Threats to Information Security

Some of the identified threats and how they have been handled using ML, are given here.

Malwares: Malicious software postures a major threat to the security of computer systems. The application of machine learning for the detection of malevolent network traffic is interesting when the traffic is encrypted because traditional pattern-matching approaches cannot be used. Previously to automatically analyze the behavior of malware binaries two concepts based on machine learning techniques have been proposed: (a) clustering of behavior, which aims at

discovering novel classes of malware with similar behavior [12] [13] and (b) classification of behavior, which enables assigning unknown malware to known classes of behavior [14] [15]. This is found that these two mechanisms are crucial for malware analysis thus for efficient and effective malware analysis joint use of clustering and classification were proposed [16]. Later other machine learning approaches like Linear regression, Logistic regression, Decision tree, Random Forest, Support Vector Machine, Multi-Layer Perception etc. has been experimented with the network security challenges as the scale of the data, demand for very low false positive rates, evolving data streams, and noisy class labels and random forest ensemble classifier has been found most robust for such scenario [17]. For malware detection in server computing platform Distributed Support Vector Machine (SVM) algorithm approach has been found effective [7].

To classify malware family (Adware, Backdoor, Downloader, Dropper, EquationDrug, Trojan, Packed, Ransom, Spy, Worm) also the machine learning algorithms performed well. For this after analysis of input malware samples extracted features reduction and classification could be performed using ML algorithms like Random Forest, KNN, Decision Table [18].

Botnets are also the most serious threats to the Information security. Botnets represent a usually large collections of computers compromised with a sophisticated bot malware, that puts them under the control of a remote attacker. botnet traffic could be accurately detected by simple flow features and Random Tree classifier [19]. In flow-based system it has two main parts: the preprocessing entity and the classifier entity. The first entity processes traffic to find the statistical features whereas the second one is responsible for building the model of malicious / non-malicious traffic and classifying the traffic flows. Similarly, the system works in two phases which are training and testing. traffic model is trained by using a labeled training data in training phase and the model is tested by an unlabeled test data in test phase. the result system gives the classification results showing that the traffic is malicious or not.

Anomaly detection: A network anomaly is a deviation from the normal operation of the network, which is learned through observation and is signified by decreased network performance [11]. To detect network anomalies machine learning based algorithm such as AdaBoost and Simple feedforward neural network [11] , MLP, logistic regression, and extreme learning machine (ELM) [20] have been successful. While using the Simple Feedforward Neural Network two hidden layers with twice as many Rectified Linear Unit(ReLU) neurons as time series and a single sigmoid output neuron has been used. This test resulted in terms of a binary classification accuracy. Anomaly is detected if the calculated accuracy has less than 1% chance of appearing randomly.

Intrusion Detection: Intrusion detection is a process of monitoring, detecting, and analyzing the events that are considered as violation to the security policies of a networked environment [21]. For Intrusion Detection support vector machine (SVM) for classification problems and random forest for classification and regression problem, are used. Due to powerful classification power and practicality in computation SVM are suitable for high dimensional data [22], whereas Random forest algorithm is to deal effectively with uneven data [23]. Other than these algorithms Principal Component Analysis (PCA) [24], self-organizing map (SOM) [25], Semi supervised support vector machine [26], supervised clustering method MPCK-means [27] are also used for Intrusion detection.

Data injection: These types of attacks are also hazardous for information security. Here, the attacker injects incorrect data or measurements to manipulate the state measurements of the System [28]. For detection of data injection two ML techniques have been used i.e. SVM and semi supervised learning [29].

Data Acquisition: In such category of threat adversaries can influence the networks to attain illegal access and then alter communications to unfavorably affect the delivery of resources. To detect this type of threat many machine learning techniques have been experimented out of which Naïve Bays, Random Forest, OneR, J48, NNge, SVM have given the optimal results [30].

DDoS attacks: In Distributed Denial of Service (DDoS) attacks Distributed multiple agents consume some critical resources and interrupt normal Internet process and refute the services to authentic users. For identifying these type of issues Fuzzy C Means, Naïve Bayesian SVM, KNN, Decision Tree, K-Means etc. ML based techniques have been used and Fuzzy C Means ranked up for such scenario [31]. In the other experiment SVM has been found the optimal among Naïve Bayes, Random Forest and SVM itself [32].

Cyber-physical attacks: This category of threats is gaining the enough attraction of the researchers due to their high-risk factors such as uses of computers, ability to disable cameras, turn off a building's lights, make a car turn off the road, or a drone land in enemy hands. Simply we can say cyber-physical attacks can replace the physical attacks using the cyber. Many ML algorithms has contributed in detection of these types of attacks but k-Nearest Neighbor(kNN), Artificial neural networks(ANN), Support Vector Machine(SVM), Gaussian Naïve Bayes(GNB), and Decision Tree(DT) have provided the appropriate results [33].

Phishing attacks: This type of attack is also very unfavorable for information security. Here the phisher tries to attain the confidential details of the users by acting as the trustworthy entities while communicating over the network. For detection of phishing attacks Biased support vector machine (BSVM), Neural Networks, K-Means has been experimented out of which Biased support vector machine (BSVM) and Artificial Neural Networks have ranked up for higher accuracy [34]. In the other setup Logistic Regression, Decision Tree and Random Forest have provided almost similar level of precision in the results [35].

SQL Injection detection: SQL Injection (SQLi) attacks are such type of attacks that executes malevolent SQL statements and in effect of this database server behind any application could be controlled. The attackers can manipulate records in the database. To differentiate between malicious and non-malicious query ML based Naïve Bayes algorithm have been used which has provided satisfactory results [36].

5. Conclusion

ML purposes to work in real-time, with little to no human interaction. If it is implemented for information security which is very crucial nowadays, then the variety of security attacks could be stopped before they result in destructive situations. Machine Learning is being successful when applied to security problems. But still there is a lot of scope for the work because many silent problems are there which are untouched till now. Excellent results in Information Security is guaranteed by applying various latent characteristics of ML algorithms appropriately. Here

in this paper algorithms and security areas have been discussed which will be helpful to prepare a road map for the further research.

References

[1] S. I. Daisuke Komura, "Machine Learning Methods for Histopathological Image Analysis," Computational and Structural Biotechnology Journal, vol. 16, pp. 34-42, 2018.

[2] S. T. T. K. M. D. &. M. W. Dmitry S. Bulgarevich, "Pattern recognition with machine learning on optical microscopy images of typical metallurgical microstructures," Scientific Reports, vol. 8, no. 1, 2018.

[3] X. W. X. L. Y. Z. D. W. Liang Xiao, "IoT Security Techniques Based on Machine Learning," Cryptography and Security, 2018.

[4] A. R. Taleqani, K. E. Nygard, R. Bridgelall and J. Hough, "Machine Learning Approach to Cyber Security in Aviation," 2018 IEEE International Conference on Electro/Information Technology (EIT), pp. 0147-0152, 2018.

[5] S. Marsland, Machine Learning: An Algorithmic Perspective, Chapman & Hall/CRC, 2009.

[6] A. N.-M. Rich Caruana, "An empirical comparison of supervised learning algorithms," in ICML '06 Proceedings of the 23rd international conference on Machine learning, Pittsburgh, Pennsylvania, USA, 2006.

[7] A. P. A. S. S. B. C. M. G. K. Usman N Aijaz, "Malware Detection on Server using Distributed Machine Learning," pices, vol. 2, no. 7, pp. 172-175, November 2018.

[8] I. Ahmad, A. B. Abdullah and A. S. Alghamdi, "Application of artificial neural network in detection of DOS attacks," in SIN '09 Proceedings of the 2nd international conference on Security of information and networks, Famagusta, North Cyprus, October 2009.

[9] Y. Liao and V. Vemuri, "Use of K-Nearest Neighbor classifier for intrusion detection," Computers & Security, vol. 21, no. 5, pp. 439-448, October 2002.

[10] J. Zhang and M. Zulkernine, "A hybrid network intrusion detection technique using random forests," in First International Conference on Availability, Reliability and Security (ARES'06), Vienna, Austria, Austria, April 2006.

[11] I. V. R. G. James Zhang, "Anomaly detection in wide area network mesh using two machine learning anomaly detection algorithms," arXiv:1801.10094v1, 30 January 2018.

[12] J. O. A. M. M. J. N. Michael Bailey, "Automated Classification and Analysis of Internet Malware," Recent Advances in Intrusion Detection, vol. 4637, pp. 178-197, 2007.

[13] P. M. C. C. H. C. K. E. K. Ulrich Bayer, "Scalable, Behavior-Based Malware Clustering," in Proceedings of Symposium on Network and Distributed System Security (NDSS), San Diego, CA, USA, 2009.

[14] J. M. Tony Lee, "Behavioral Classification," in Proceedings of Annual Conference of the European Institute for Computer Antivirus Research (EICAR), Hamburg, Germany, April 2006.

[15] T. H. C. W. P. D. P. L. Konrad Rieck, "Learning and Classification of Malware Behavior," Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2008, vol. 5137, pp. 108-125, 2008.

[16] P. T. ,. W. T. H. Konrada Rieck, "Automatic analysis of malware behavior using machine," Journal of Computer Security, vol. 19, no. 4, pp. 639-668, 20 June 2011.

[17] D. M. Blake Anderson, "Machine Learning for Encrypted Malware Traffic Classification: Accounting for Noisy Labels and Non-Stationarity," in Proceeding KDD '17 Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, NS, Canada, August 13 - 17, 2017.

[18] M. M. S. T. N. L. H. Cho Cho San, "Malicious Software Family Classification using Machine Learning Multi-class Classifiers," Computational Science and Technology, vol. 481, pp. 423-433, 28 August.

[19] M. Stevanovic and J. M. Pedersen, "An efficient flow-based botnet detection using supervised machine learning," in International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 2014.

[20] S. G. S. V. J. A. M. S. S. J. Jabez, "Anomaly Detection by Using CFS Subset and Neural Network with WEKA Tools," Information and Communication Technology for Intelligent Systems, vol. 107, pp. 675-682, 15 December 2018.

[21] P. M. Karen Scarfone, Guide to Intrusion Detection and Prevention Systems(IDPS), Gaithersburg, MD, United States: National Institute of Standards & Technology, 2007.

[22] X. B. A. H. C. T. R. A. Elike Hodo, "Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey," arXiv:1701.02145v1, 9 January 2017.

[23] S. Thaseen and C. A. Kumar, "An analysis of supervised tree based classifiers for intrusion detection system," in International Conference on Pattern Recognition, Informatics and Mobile Engineering, Salem, India, 2013.

[24] A. D. A. E. H. A. A. Heba F. Eid, "Principle Components Analysis and Support Vector Machine based Intrusion Detection System," in International conference intelligent systems design and applications (ISDA), 2010.

[25] S. M. S. Stefano Zanero, "Unsupervised learning techniques for an intrusion detection system," in Proceedings of the 2004 ACM symposium on Applied computing, March 14 - 17, 2004.

[26] A. D. Kristin P. Bennett, "Semi-supervised support vector machines," in NIPS'98 Proceedings of the 11th International Conference on Neural Information Processing Systems, 1998.

[27] Y. G. Y. T. Chuanliang Chen, "Semi-supervised learning methods for network intrusion detection," in Int Conf Sys, Man Cybern, IEEE., 2008.

[28] J. Z. F. L. Gaoqi Liang, S. R. Weller and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," IEEE Transactions on Smart Grid, vol. 8, no. 4, pp. 1630-1638, 2017.

[29] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng and Z. Han, "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid," IEEE Systems Journal, vol. 11, no. 3, pp. 1644-1652, 2017.

[30] J. M. Beaver, R. C. Borges-Hink and M. A. Buckner, "An Evaluation of Machine Learning Methods to Detect Malicious SCADA Communications," in 12th International Conference on Machine Learning and Applications, Miami, FL, USA, 2013.

[31] R. A. Manjula Suresh, "Evaluating Machine Learning Algorithms for Detecting DDoS Attacks," in Communications in Computer and Information Science, Springer, Berlin, Heidelberg, 2011, pp. 441-452.

[32] A. R. Wani, Q. P. Rana, U. Saxena and N. Pandey, "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques," in Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab, 2019.

[33] J. Wang, W. Tu, L. C. Hui, S. Yiu and E. K. Wang, "Detecting Time Synchronization Attacks in Cyber-Physical Systems with Machine Learning Techniques," in IEEE, Atlanta, GA, USA, June 2017.

[34] S. M. A. H. S. Ram Basnet, "Detection of Phishing Attacks: A Machine Learning Approach," Soft Computing Applications in Industry, vol. 226, pp. 373-383, 2008.

[35] V. Patil, P. Thakkar, C. Shah, T. Bhat and S. P. Godse, "Detection and Prevention of Phishing Websites Using Machine Learning Approach," in IEEE, Pune, India, 2018.

[36] A. Joshi and V. Geetha, "SQL Injection detection using machine learning," in IEEE, Kanyakumari, India, 2014.