Machine Learning Capability in the Detection of Malicious Agents

Anurag Sharma, Puja Archana Das, Muhammad Fazal Ijaz, and Abu ul Hassan S. Rana

Abstract The variety and volume of cyber-attacks have exponentially increased over the years. This calls for a strong security defense mechanism against the attacks. This paper discusses the advancements made in the field of cyber-security using various machine learning techniques. We review some of the common machine learning techniques used in cyber-security and also discuss the issues related to cyber-security. Overall, we focus on exploring the idea of a combination of deep learning, machine learning and human supervision.

Keywords Machine learning · Intrusion · Malicious code · Neural network · Accuracy

1 Introduction

Hacking in cyber-security is advancing daily in this world. There must be some higher security protection to stop these attacks. Several kinds of attacks are done by the attacker; some are D-dosing, man-in-the-middle, information escape, SQL injection, remote to local. They use such techniques to illegally enter restricted networks, websites or personal data from your device [1]. The attackers from within or outside are finding innovative techniques to crack the information, money or any sensitive

A. Sharma · P. A. Das
School of Computer Engineering, Kalinga Institute of Industrial Technology (KIIT) Deemed to be University, Bhubaneswar, Odisha, India
e-mail: 1829006@kiit.ac.in

P. A. Das
e-mail: 1829080@kiit.ac.in

M. F. Ijaz (✉) · A. H. S. Rana
Department of Intelligent Mechatronics Engineering, Sejong University, Seoul 05006, South Korea
e-mail: fazal@sejong.ac.kr

A. H. S. Rana
e-mail: rana@sejong.ac.kr

S. Dhar et al. (eds.), *Advances in Communication, Devices and Networking*,
Lecture Notes in Electrical Engineering 776,
https://doi.org/10.1007/978-981-16-2911-2_26

information. The innovative ideas and new methods developed promise to stop or try to reduce new methods created or developed by the hackers. Cyber-security can be stated as a method or technique to defend against various cyber-attacks done by hackers and shield sensitive data from attackers. Cyber-security within the year 2016 had multiple advances updates in machine learning techniques like auto-cars, linguistic communication process, medical field, and virtual AI [2]. These need to be used to find various databases related to the matter of various intrusion detection. Thus implement it using machine learning to update and make the security better against the intrusion. First, we need to input these into the machine learning (ML) model. This model gets practiced by the dataset model and then is known as the trained model. Once we input the dataset, next we use the machine learning formula on the dataset sample. [3]. ML formula plays a crucial part in increasing security for intrusion detection systems [3]. Machine learning algorithms are separated into two groups: unsupervised learning and supervised learning. They are distinguished based on data (i.e. input) they are settled for.

Unsupervised learning refers to the algorithms of training information that are unlabeled, with the job of deducing the classes all by itself. Supervised learning refers to the algorithms of training information that are labeled and acknowledge what differentiates the labels. The labeled information is extremely rare and the chore of the labeled data is itself exceptionally exhausting and we may not be able to sight if labels really exist.

2 Common Machine Learning Techniques Used in Cyber-Security

Regression

In regression, values of the dependent attributes are approximated on the basis of values of the independent attributes through studying the currently existing data connected to previous events. This understanding is also used to manage the new events. Regression is used to solve fraud detection in cyber-security. When a model is understood on the basis of the past database proceedings by observing the current attributes, it determines fraudulent transactions. We can learn decision tree, support vector machine, linear regression, random forest, polynomial regression and some more regression models from machine learning. Venkatesh Jaganathan used multiple regression techniques for prognosticating the effect of cyber-attacks. The all-inclusive common vulnerability scoring system (CVSS) level is taken to be a co-related feature while two non-co-related features as Y1 (vulnerabilities count) and Y2 (mean traffic). For privacy identification in a smart environment, Daria Lavrova suggested a multiple regression model, which helped to uncover the known and unknown attacks.

Classification

Classification is one of the broadly used supervisory machine learning tasks. The use of the following machine learning tools is possible due to the accessibility of a huge collection of labeled data. In cyber-security, classifications are made on the basis of ML which discriminates the provided email messages as spam or that are not used in spam detection. The spam messages are separated from non-spam messages by the spam filter models. Classifications made based on deep learning frameworks which involve recurrent neural networks (RNN), convolutional neural networks (CNN), restricted Boltzmann machines (RBM) or long short-term memory (LSTMs) cells for attribute selection through multi-layer and non-sparse neural network tend to be quite effective in handling complicated tasks with the availability of a huge collection of the past dataset. The machine learning techniques used for classification involve naïve Bayes, logistic regression, K-nearest neighbors, decision tree, support vector machine, random forest classification.

Clustering

It is indispensable to have data with the label as regression and classification in supervised learning models. But clustering is an unsupervised learning method that retrieves general patterns from raw data even though it is unlabeled. A set of indistinguishable events establishes a cluster as they share common attributes that define a specific behavioral pattern. Clustering, in cyber-security, is used for the analysis of malware, forensic analysis, anomaly detection, etc. Self-organizing maps (SOMs) based on neural networks may be useful for cluster analysis. In cyber-security, some of the ML clustering techniques used are K-means, K-Medoids, DBSCAN, Gaussian mixture model and agglomerative clustering.

3 Issues in Cyber-Security

Machine learning algorithms have an important part in four different areas, which are intrusion detection system, malware analysis, Andriod malware detection and spam detection (Fig. 1).

Intrusion Detection

If there is any exploitation of the information by malacious software or violation of company policy, intrusion detection is used. Intrusion detection can be done in many ways. It is mainly classified into two types based on signature (signature-based) and anomaly (anomaly-based) intrusion. All packages that are received are first cross-checked with the signatures present for similarities with a known malicious threat. This is signature-based intrusion detection. Monitoring of the network traffic is done by an established normality baseline in anomaly-based intrusion detection. Biswas [4] displayed machine learning-based ways that are very useful in making a better intrusion detection system. Combinations of feature selection techniques gave them

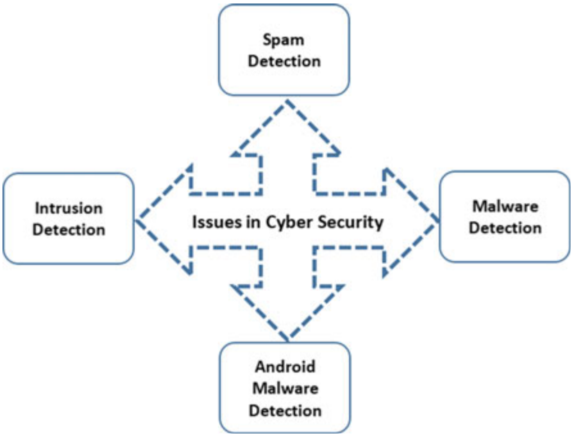


Fig. 1 Issues in cyber-security

great results. Vinaya Kumar [5] put forward a scale hybrid IDS AlertNet system which helps in analyzing networks and activities done by the host. We used deep neural networks (DNNs) to create the model. Deep belief networks for intrusion detection are proposed by Zahangir Alom [6]. We have used the features of the trained set of two-layer restricted Boltzmann machine (RBM). Shone et al. [7] gave us a DL model for intrusion detection systems operation in networks using features of machine learning and deep learning.

Malware Detection

Malware is a short form of malicious software and is one of the types of cyber-threats software in the cyber-world. It is usually used for unauthorized attacks on organizations, like filching information or getting control over the entry or deal damage to personal data of the organizer and so on. The term coined as malware is usually given for programs which are malicious in nature, like virus, bugs, bots, adware, rootkits, Trojan horses, worms, spyware, ransomware, Keylogger, backdoor. Most of the malware can be subdivided into a number of families. For example, we can classify ransomware into Jisut family, Pletor family, Simplocker family, Charger family, Koler family, RansomBO family, Svpeng family, etc. The programs which are malicious in nature can be transported concealed in a secure file and operating systems. There can be many examples, like executable and linkable files or UNIX ELF, Windows PE files (portable executables with .exe, dll, efi). Malware programs can also be document-based and kept hidden inside doc files, pdfs and rtf files. Extensions and plug-ins for famous software platforms can also have malware in the form of extensions; for example, extension for web browsers and frameworks.

Uppal et al. [8] used ngram method to put forward a classification and detection system for malware. Chowdhury et al. [9] showed a neural network-based method for malware detection. Kalash et al. [10] proposed classifying malware using CNN. They applied CNN classification to them after they converted their codes of 25 families of malware binaries to grayscale images.

Android Malware Detection

Android is exceedingly attacked by mobile malware makers as it is one of the most extensively used mobile platforms. With an alarming increase in the volume and variant of Android malware, it has become exceptionally difficult to detect and classify the types of mobile malware. Researchers have made a large number of attempts toward mobile malware detection. Arp et al. [11], Varsha et al. [12] and Sharma and Dash [13] extracted static features from Android apps and they attained satisfactory results by using machine algorithms, like decision tree, SVM, K-NN, random forest, naïve Bayes to attain satisfactory results.

Spam Detection

Spam email comes in various flavors. Many are just exasperating messages aiming to draw attention to a cause or spread wrong information. Some of them are phishing emails with the intent of attracting the receiver into clicking on a malicious link or downloading malware. Spam detection is a supervised machine learning problem. This means you must develop your machine learning model with a set of samples of spam and ham messages and let it find the pertinent patterns that separate two discrete categories [19–23].

4 Real-Life Case Scenario of Cyber-Security Risk Analysis Using Machine Learning

A real-time scenario is highlighted in this section. The main goal is to see the ability of machine learning classifiers to differentiate the different types of responses given by the classifiers for the input malicious code [14]. We used four types of machine learning algorithms to classify the malicious codes, namely naïve Bayes (NB), neural network, radial basis function and support vector machine (SVM). From four different organizations, we took a combined dataset [15, 16]. The incidents that happened in the organization were collected by a centralized hub, and then the summed up data were used for the research with a goal of analyzing the results given by the classifiers in differentiating between the various accidents that took place and learning that how different data are taken from the different organizations can help in improving the accuracy of classification [17, 18].

From the given dataset table in Table 1, we have four different organizations, and the number of events occurring whose summation is in total 1900 was used to find the behavior of malware in different classifiers. First, we calculated the precision analysis in Table 2 which shows the precision of different classifiers and how well they react to the malware. Accordingly, the rows were designed where SVM has the highest recovery precision. Table 3 shows the recall analysis which is the correct malware detection divided by the number of malware that should have returned by using different classifiers. Table 4 is the F-score analysis (the higher the F-score, the more the precision and recall) of the different classifiers and shows that for different

Table 1 Data samples distribution among four different organizations

Organization name	Number of events
Organization 1	400
Organization 2	550
Organization 3	600
Organization 4	350
Total	***1900***

Table 2 Precision analysis of classifiers in identifying the different types of responses based on malware

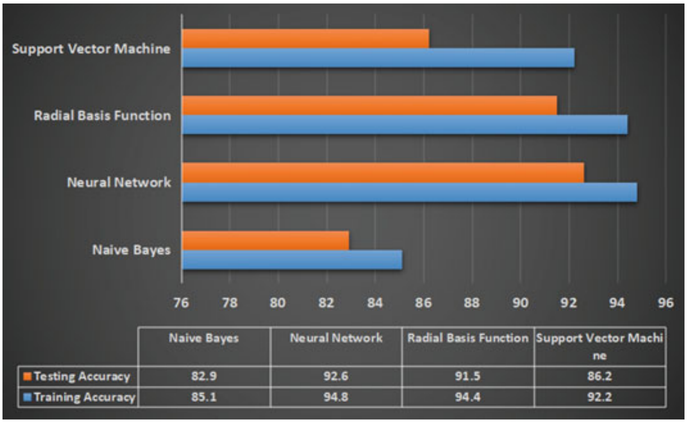
	Naïve Bayes	Neural network	Radial basis function	Support vector machine
None	0.0	0.0	0.0	0.0
Recovered	0.0	0.0	0.0	0.76
Segregated	0.96	0.94	0.88	0.9
Dropped	0.98	0.93	0.94	0.92
Undefined	0.92	0.91	0.95	0.93
Blocked	0.0	0.0	0.0	0.64

Table 3 Recall analysis of classifiers in identifying the different types of response based on malware

	Naïve Bayes	Neural network	Radial basis function	Support vector machine
None	0.0	0.0	0.0	0.0
Recovered	0.0	0.0	0.0	0.78
Segregated	0.92	0.91	0.91	0.87
Dropped	0.95	0.94	0.93	0.93
Undefined	0.93	0.92	0.94	0.95
Blocked	0.0	0.0	0.0	0.68

Table 4 F-score analysis of classifiers in identifying the different types of responses based on malware

	Naïve Bayes	Neural network	Radial basis function	Support vector machine
None	0.0	0.0	0.0	0.0
Recovered	0.0	0.0	0.0	0.77
Segregated	0.94	0.93	0.89	0.89
Dropped	0.96	0.93	0.92	0.92
Undefined	0.92	0.91	0.95	0.94
Blocked	0.0	0.0	0.0	0.67



	Naive Bayes	Neural Network	Radial Basis Function	Support Vector Machi ne
🟧 Testing Accuracy	82.9	92.6	91.5	86.2
🟦 Training Accuracy	85.1	94.8	94.4	92.2

Fig. 2 Classification accuracy rate analysis using four classifiers

functions different classifiers are better, i.e., the F-score for different functions varies for different classifiers. Figure 2 shows the training and testing accuracy of different machine learning algorithm, where the neural network has the highest training and testing accuracy; naïve Bayes has the lowest testing accuracy and SVM has a drastic decrease for the unknown dataset (resting set) whereas it works much better for the trained dataset. The radial basis function is very similar to a neural network and also shows great results in both the training and testing sets.

5 Conclusion

In order to resolve various types of cyber-security problems, machine learning techniques are extensively used. The current advancements are made in the area of deep learning and machine learning and provide encouraging solutions for cyber-security threats. But it is equivalently crucial to recognize the correct algorithm acceptable for the required application. To achieve high detection rates and to keep the solution hard against malware attacks, a multi-layered proposal is required. While solving a cyber-security problem, it is important to select the right model. In this paper, for cyber-security problems, the authors investigated state-of-the-art mechanisms. The desired results for cyber-security can be achieved by the amalgamation of machine learning techniques and human supervision.

References

1. Hatcher WG, Yu W (2018) A survey of deep learning: platforms, applications and emerging research trends. IEEE Access 6. https://doi.org/10.1109/ACCESS.2018.2830661
2. Mishra S, Tripathy HK, Mallick PK, Bhoi AK, Barsocchi P (2020) EAGA-MLP—an enhanced and adaptive hybrid classification model for diabetes diagnosis. Sensors 20(14):4036
3. Mallick PK, Mishra S, Chae GS (2020) Digital media news categorization using Bernoulli document model for web content convergence. Pers Ubiquit Comput. https://doi.org/10.1007/s00779-020-01461-9
4. Mishra S, Mallick PK, Jena L, Chae GS (2020) Optimization of skewed data using sampling-based preprocessing approach. Front Public Health 8:274. https://doi.org/10.3389/fpubh.2020.00274
5. Vinayakumar R, Alazab M (Senior Member, IEEE), Soman KP, Poornachandran P, AlNemrat A, Venkatraman AN (2019) Deep learning approach for intelligent intrusion detection system. IEEE Access 7. https://doi.org/10.1109/ACCESS.2019.2895334
6. Zahangir Alom M, Bontupalli VR, Taha TM (2015) Intrusion detection using deep belief networks. 978-1-4673-7565-8/15/$31.00 ©2015 IEEE
7. Shone N, Phai VD, Ngoc TN, Shi Q (2018) A deep learning approach to network intrusion detection. IEEE Trans Emerg Top Comput Intell 41–50, February 2018
8. Uppal D, Jain V, Sinha R, Mehra V. Malware detection and classification based on extraction of API sequences. 978-1-4799-3080-7/14/$31.00_c 2014 IEEE
9. Chowdhury M, Rahman A, Islam R (2017) Protecting data from malware threats using machine learning technique. In: 2017 12th IEEE conference on industrial electronics and applications (ICIEA)
10. Kalash M, Rochan M, Mohammed N, Bruce NDB, Wang Y, Iqbal F (2018) Malware classification with deep convolutional neural networks. 978-1-5386-3662-6/18/$31.00 ©2018 IEEE
11. Arp D, Spreitzenbarth M, Hubner M, Gascon H, Rieck K (2014) Drebin: efficient and explainable detection of android malware in your pocket. In: Proceedings of 20th annual network. distributed system security symposium (NDSS), San Diego, CA, USA, February 2014, pp 1–15
12. Varsha MV, Vinod P, Dhanya KA (2017) Identification of malicious Android app using manifest and opcode features. J Comput Virol Hacking Tech 13(2):125–138
13. Sharma A, Dash SK (2014) Mining API calls and permissions for Android malware detection. In: Cryptology and network security. Springer International, Cham, Switzerland, pp 191–205
14. Mishra M, Mishra S, Mishra BK, Choudhury P (2017) Analysis of power aware protocols and standards for critical E-health applications. In: Internet of Things and big data technologies for next generation healthcare. Springer, Cham, pp 281–305
15. Mishra S, Mahanty C, Dash S, Mishra BK (2019) Implementation of BFS-NB hybrid model in intrusion detection system. In: recent developments in machine learning and data analytics. Springer, Singapore, pp 167–175
16. Mishra S, Thakkar H, Chakrabarty A, Kimtani D (2012) Dynamic cluster based data aggregation in WSN (FDDA). Int J Electron Commun Comput Technol (IJECCT) 2(5):227–230
17. Mishra S, Mallick PK, Tripathy HK, Bhoi AK, González-Briones A (2020) Performance evaluation of a proposed machine learning model for chronic disease datasets using an integrated attribute evaluator and an improved decision tree classifier. Appl Sci 10(22):8137
18. Mishra S, Tripathy HK, Mishra BK (2018) Implementation of biologically motivated optimisation approach for tumour categorisation. Int J Comput Aided Eng Technol 10(3):244–256
19. Bhoi AK, Sherpa KS (2014) QRS complex detection and analysis of cardiovascular abnormalities: a review. Int J Bioautom 18(3):181–194
20. Bhoi AK, Sherpa KS, Khandelwal B (2018) Arrhythmia and ischemia classification and clustering using QRS-ST-T (QT) analysis of electrocardiogram. Clust Comput 21(1):1033–1044
21. Bhoi AK, Sherpa KS, Khandelwal B (2018) Ischemia and Arrhythmia classification using time-frequency domain features of QRS complex. Procedia Comput Sci 132:606–613

22. Bhoi AK, Sherpa KS (2016) Statistical analysis of QRS-complex to evaluate the QR versus RS interval alteration during ischemia. J Med Imaging Health Inform 6(1):210–214
23. Bhoi AK (2017) Classification and clustering of Parkinson’s and healthy control gait dynamics using LDA and K-means. Int J Bioautom 21(1)