DOI: http://dx.doi.org/10.26483/ijarcs.v13i4.6893

ISSN No. 0976-5697

Volume 13, No. 4, July-August 2022

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A SURVEY ON EFFECTIVE MACHINE LEARNING TECHNIQUES IN THE FIELD OF CYBER SECURITY

Rishin Pandit
School of Computer Science and Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu, India

Lagan Gupta
School of Computer Science and Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu, India

Dr. MANIKANDAN K
Associate Professor Sr
School of Computer Science and Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu, India

Abstract: Machine learning techniques have many cybersecurity applications, and they have entered the mainstream in a variety of fields. Examples include threat analysis, anomaly-based intrusion detection of frequent attacks on important infrastructures, malware analysis, particularly for zero-day malware detection, and many others. Machine learning-based detection is being employed by researchers in many cybersecurity solutions as a result of the inefficiency of signature-based methods in identifying zero day attacks or even modest modifications of existing assaults. In this paper, we cover a number of cybersecurity applications for machine learning. We also give a few examples of adversarial assaults on machine learning algorithms that aim to corrupt classifiers' training and test data in order to render them useless.

Keywords: Machine Learning, Malware, Intrusion Detection, Cybersecurity, Support Vector Machine, CNN

INTRODUCTION

Automated learning from examples and experience without explicit programming is the foundation of machine learning. Machine learning algorithms come in a variety of forms, including supervised learning, unsupervised learning, reinforcement learning, etc. Widespread applications of machine learning include content-based retrieval from multimedia [1], object recognition, speech recognition, and computer vision [2]. Additionally, it is utilised when creating forecasting tools like stock market forecasts [3]. It can be used in systems that make recommendations for online sites, news articles, television shows, and merchandise [4]. Machine learning techniques are being used widely in many cybersecurity applications these days, as was to be expected.

For instance, machine learning is used to find versions of known assaults or zero-day attacks [5] like STUXNET [6], Sony Zero Day Attack, etc. However, in order to undermine the cyber defence, hackers and writers of malware are also working quickly. The issue originates from the fact that machine learning techniques [7] were initially created for stationary contexts in which it was expected that both the training and test data were produced using the same distribution. This working hypothesis is likely to be partially violated in the presence of intelligent and adaptive adversaries [8]. In reality, a malevolent opponent could alter the input data and use some learning algorithms' flaws to threaten the security of the whole system. In the section that follows, we go through a few machine learning applications for cybersecurity as well as some of the threats that could arise from using such techniques [9]. This paper offers a study of some machine learning applications to cybersecurity, although it is by no means exhaustive.

MACHINE LEARNING APPLICATIONS IN CYBERSECURITY

We go over a few machine learning applications for cybersecurity in this part. Machine learning approaches have recently been used in a variety of fields, including malware analysis, industrial control systems, intrusion detection in SCADA systems, intrusion detection for vehicular ad-hoc networks (VANET), power system security, etc . We do not intend for this concise evaluation to be exhaustive. We choose a few instances to give readers a taste of how machine learning [10] can be used in cybersecurity.

Security of the power system

Every nation's economy and security depend on its electric power infrastructure. Blackout [11], the most severe type of power loss that affects a sizable area and has serious societal repercussions, may be caused by a variety of factors, including a problem with a power transmission line or deliberate attacks. Blackouts spread as a result of early failures propagating through a complex and varied cascade of uncommon events. Unnecessary line trips, on the other hand, can significantly worsen the severity of an outage, aid in the geographical spread of the disturbance, and even cause a cascading blackout when the power system is under stress. Therefore, a limited cyber attack can be fatal by causing cascading failures while the power system is under stress.

The cyber attack surfaces in power systems are being increased by a number of new digital technologies, including phasor measuring units (PMUs), digital protection relays in power systems [31], adaptive protection approaches, etc. In order to identify the stressed state of the power system, the scientists applied a machine learning technique . To create a discrimination function to categorise the system state as stressed or safe, they used a decision tree-based technique. The classifier is trained using the potential predictors, which include voltage magnitudes, angle differences, mega volt-amp (reactive) (MVAr) flows, current magnitudes, etc., obtained by PMU. Decision trees (DT) [12], a supervised machine learning technique, are utilised for classification in order to forecast the proper reliability balance of the adaptive protection system based on wide area measurements. Additionally, the quantity of PMUs to be deployed and their most crucial locations have both been optimised using machine learning. The decision tree aids in the division of attributes that decide the deployment areas for PMUs. Machine learning assists power-system engineers in addressing the difficulty of planning and running future power systems with an acceptable level of security despite the complexity and uncertainty in those systems increasing.

Detection of cyber attacks on industrial control systems by zone divisions

Cyberattacks are now a significant threat, even to control systems. Therefore, we must protect them. Automatic intrusion detection systems that can secure key infrastructures and control systems can be created using machine learning techniques (CI). CI heavily relies on connected, sensitive information and communication technologies (ICT). An illustration of one of these cyber-attacks is the STUXNET [6] worm infestation. A computer virus called STUXNET infected Windows-based industrial control systems and gained control of Programmable Logic Controllers (PLCs) [37], severely harming Iran's nuclear programme. Therefore, the development of trustworthy security and safety elements for industrial control systems (ICS) is urgently required. A PLC is a tiny computer that has an operating system. In the workplace, they are utilised to manage machine operations. If they were attacked or compromised, there could be a significant financial loss. Such a detection system is created using machine learning techniques to find any undetected cyberattacks. A machine learning-based automatic detection system has been proposed by Morita et al. (2013). A straightforward plant that circulates hot water between two tanks with different heights was considered and calibrated for the experiment. For both tanks, a SCADA system [38] and operators are utilised. To find any anomalies, principal component analysis (PCA) has been employed. In essence, it recognises patterns in the data being gathered from SCADA and plant systems. As an illustration, according to the rules of physics, if the water column level is high in one tank, it must be low in the other tank, and vice versa. In the event of odd patterns, PCA will notify the two plants' abnormal behaviour. By using the data gathered from the SCADA systems to train the algorithm, this is accomplished. Finding patterns with PCA makes it possible to shrink the dataset's dimensions while preserving the majority of its information.

There is an adversarial assault [39][21] on the previously mentioned machine learning algorithm. The output of the machine learning algorithm can be altered if a hacker manages to examine and recognise the patterns in the training data. For instance, in Morita's experiment, the algorithm may not detect the abnormality and may produce false results if a system intruder manipulates the height of the column of one tank by intercepting a sensor reporting the height of the column of another tank and injecting false information to trick the controller. By confining the intrusion to a zone, this adversarial effect can be found.This reduces the likelihood that an intruder will control both zones, assisting the defensive system in spotting an intrusion pattern. Such methods paired with machine learning algorithms can be useful to create a more reliable CI defence system.

Detecting intrusions in SCADA systems

SCADA systems are crucial for maintaining and keeping an eye on CI, such as a water or sewage treatment facility or an electric power generating, transmission, and distribution facility. But because SCADA systems are now connected to IT networks, their security has grown more challenging. This has been done to enable better field operations and business network integration. As a result, the SCADA system is now more vulnerable to threats and risks from hackers. Consequently, there is a need to provide some alarm systems that would give CI operators a tool to aid them in spotting continuous intrusions. They must have stronger security from online threats like the SLAMMER worm [16] thanks to these mechanisms. The worm eventually caused a blackout in the North-Eastern US after affecting two US utilities and a nuclear power plant. Therefore, the creation of intrusion detection systems (IDS), which are used to recognise attacks and launch suitable warnings that may aid in taking appropriate response, is necessary. IDS may not be able to handle all attacks and may issue erroneous alarms. High economic dangers could result from these erroneous alerts. Support vector machine (SVM) [24] is one of the machine learning algorithms that an analyst might use to distinguish between legitimate and malicious traffic. SVM is a technique for categorising data. One class support vector machine (OCSVM) [13], a supervised machine learning system, learns a decision function for finding novel or undiscovered data.

A SCADA system can be attacked, and Maglaras and Jiang (2014) have presented two distributed IDS that can identify such attacks. They were both created and tested for the Cockpit CI project [40]. It is built on real-time perimeter IDS, which offers the essential cyber-analysis for determining and defending each CI's security perimeter. Using data from a small scale test bed, two OCSVM modules were created and tested. The first technique, K-OCSVM, aids in separating genuine alarms from false alarms. It combines the K-means clustering approach [41] and the OCSVM method. The K-OCSVM approach differs from all other comparable methods now in use that call for parameter preselection through the use of cross-validation. Cross-validation is a validation method for determining how well a statistical analysis' findings will transfer to a different data set. The output of the detection module is transmitted to the system using intrusion detection message detection exchange format (IDMEF) files, which contain information about the source, timing, and severity of the intrusion. K-OCSVM is trained offline with the aid of network traces. Although this method performed well in terms of accuracy and overhead, it does so by disregarding slight changes in the communication network that can mask attacks.

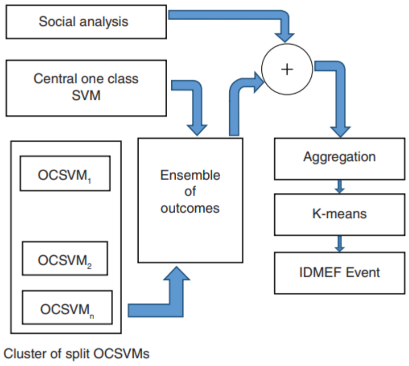

Fig1. IT-OCSVM Implementation

IT-OCSVM, a different technique with excellent accuracy and minimal overhead, was created. Figure 1 depicts the IT-OCSVM implementation. This primarily aims to do anomaly detection with high accuracy, low overhead, and efficiency. The seven stages are as follows. It begins by doing preprocessing on the testbed's raw data. In the second place, time-based features are chosen over content-based features. In the third step, the dataset is divided based on the source, and an OCSVM module is created and trained for each split dataset. Running side by side with the central OCSVM is the cluster of split OCSVMs. In essence, it generates errors that are directed towards a certain source. Fourth, the new dataset is tested using the models developed during the training phase. Fifth, the outputs of various OCSVM modules are combined using an ensemble-based technique. Spearman's rank correlation coefficient is utilised to give alerts generated from various sources more weight [25]. Finally, the outputs from the various models are compiled and communicated via IDMEF. As a result, operators have been able to develop certain containment tactics in the event of attacks like the SLAMMER worm thanks to machine learning techniques.

VANET intrusion detection systems

A developing technology in today's transportation networks that offers safety and useful information is called VANET [35]. It offers the advantages of safe driving and comfortable travel while defending the privacy of the driver from various forms of assault. They are frequently exposed to a variety of active and passive assaults, such as interference and listening in. By identifying unusual or harmful behaviours, IDS can be used to minimise dangers like control violations and unauthorised intrusions [42]. If the vehicles in VANET cooperate, this detection can be done more precisely. A way for developing a cooperative detection system over VANET is distributed machine learning. However, the main issue with collaborative learning is that nodes can risk privacy when they transmit data. A hostile node has the ability to interfere and access private data about other participating nodes. A collaborative IDS (CIDS) architecture based on machine learning has been presented by Zhang and Zhu (2018). To detect intrusions in VANET, it essentially trains a classifier. The CIDS enables the utilisation of labelled training data from other cars by the vehicles. The size of the training data for each vehicle is essentially increased. As a result of the labour being shared across all the vehicles in the network, it lessens the stress placed on each vehicle. The cars can exchange information without trading training data thanks to CIDS. The alternate direction method of multipliers (ADMM) [43], a method of distributed machine learning, has been applied. With the help of this strategy, machine learning may be distributed over a network, allowing each node to share its categorization findings. Privacy is the key issue because any nefarious outsider can view their classification findings. A privacy-preserving method [53] is employed in this. A change to any one dataset item can only slightly alter the distribution of the dataset's replies, which is a well-defined concept that can offer a strong privacy guarantee. As a result, this strategy guarantees traffic safety and protects the driver's information.

Malware Analysis

"Malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim" [19].

Attackers run malware on the victim's device in order to infect it and spread to other devices by taking advantage of flaws in web applications, operating systems, network services, etc. or by using social engineering techniques on the victims. Malware has been rapidly expanding and changing over the past few decades. These malware are now able to bypass the usual detection systems since they have become resistant to them. Malware removal is crucial for software/system security, but protecting against more sophisticated malware, such as polymorphic and metamorphic malware, which alters its structure and code after each infection, is difficult. Prior to now, malware was discovered and blocked using signature-based techniques, however these techniques struggle to detect advanced or zero-day malware [20]. Machine learning techniques are becoming more and more used in malware detection to get over these restrictions. Machine learning approaches have the advantage of providing information for the identification of new or obscured malware in addition to detecting existing malware.

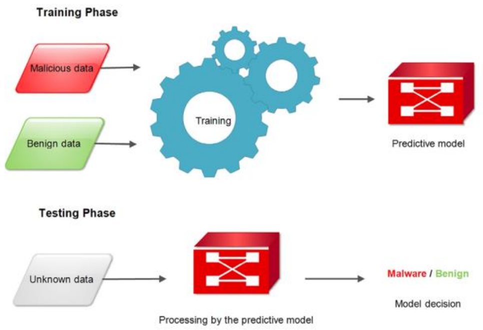

Fig 2. Operation of machine learning model while analysing malware

Figure 2 illustrates the two phases in which machine learning operates when analysing malware. In order to create a prediction model, a machine learning algorithm first goes through a training phase when it mathematically formalises the features that were taken from known dangerous and benign (non malicious) data. The extraction of these features can be done either statically, without running the executables, using data like opcode or bytecode n-grams, PE headers, etc., or dynamically, while the executable is running, using data like API or system calls, network traffic, etc.

Second, the developed predictive model processes the characteristics of unknown data during testing to determine whether it is malicious software or benign data. Naive Bayes is a common machine learning technique used by researchers to find second-generation malware [27].

ADVERSARIAL ATTACKS

Attackers are constantly looking for new assault strategies to penetrate targets in the current environment. Although machine learning is a young subject, it unfortunately draws hackers much like many other cutting-edge and inventive technology processes do.

Machine learning can be used for both profitable business endeavours and malevolent conduct. There is a chance to exploit potential weaknesses in machine learning algorithms to render such detection ineffective because many applications, such as malware detection or anomaly detection, rely on machine learning for automated decision making. During the training stage, a machine learning modelling's output can be changed by an attacker. A malware programme that has been manipulated to appear benign is an example of an adversarial attack [46] [45] [47] [43].

Two categories of high-level attacks are used to classify machine learning adversarial attacks [39]. The first is a causative or poisoning attack, in which the attacker modifies the training process by influencing the training data and degrades the performance of the classifier. The second is an exploratory or evasion attack, in which the attacker does not modify the training process . [10] but instead uses other techniques to find information to alter the predictions of a classifier that has already been trained, such as probing the learner or conducting offline analysis. Due to the potential difficulty of gaining access to the training data, the majority of attackers concentrate on exploratory attacks. Black-box and white-box evasion attacks are additional categories for these machine learning adversarial attacks.

The increase of processing capability and network communication technologies has led to the creation of cyber-physical systems (CPS) [30]. However, this development brought about a rise in dangers brought on by hostile assaults. If the hardware and software assets are not sufficiently secured, an attacker can affect the system dynamics by introducing disturbances.

Deep neural networks (DNNs) have been employed in a variety of computer vision, recognition, and artificial intelligence (AI) applications. These are now quite effective and adaptable for extracting high-level, actionable information from the raw data generated by a range of sensors in CPSs. They are also used in software for computer security, such as malware detection. Intelligent adversaries that actively strive to avoid them by disrupting the trained model present one of the difficulties in creating such models [48].

In 2018, Kolosnjaji et al. looked into the vulnerability of malware detection techniques. To learn from the unprocessed bytes of binary files, they have deployed deep neural networks. They suggested a gradient-based assault and asserted that it can circumvent a detection system (built on a deep neural network model) by altering a little portion of each malware file to make it appear innocent. Although less than 1% of malware binaries are modified, the results are encouraging and demonstrate that adversarial malware binaries have a high possibility of evading the targeted security system.

This section's numerous assaults all rely on special models that employ a particular machine learning algorithm. A defence against an adversarial assault for one machine learning model, however, might not be effective for other models. As a result, ongoing research is necessary to implement increasingly advanced protection mechanisms to shield machine learning systems against hostile attacks.

CONCLUSION

Machine learning offers a solution for a number of cyber-attack detection issues, including malware detection, intrusion detection, and—most importantly—security problems related to CI, such as power system security, industrial control system security, intrusion detection in SCADA systems, intrusion detection for VANET, etc. These issues entail the effective and efficient training and classification of vast amounts of data. A significant and developing problem is the possibility of hostile attackers who can circumvent such technologies by tricking the classifiers. This review gives an example of several cybersecurity applications for machine learning. Threats of adversary attacks that could alter the test and training data for classifiers have also been discussed.

With malevolent intent, attacks are used to alter model-based predictions. This review's objective is to raise public awareness of cybersecurity applications of machine learning. Presenting a sampling of strategies employed by adversaries to undermine current machine learning-based defences against cyberattacks

REFERENCES

[1] Lew, M. S., Sebe, N., Djeraba, C., & Jain, R. Content-based multimedia information retrieval: State of the art and challenges. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 2(1), 1–19, 2007

[2] Harandi, M., Taheri, J., & Lovell, B. C. Machine learning applications in computer vision. In Machine learning algorithms for problem solving in computational applications: Intelligent techniques (pp. 99–132). Hershey, Pennsylvania: IGI Global, 2012

[3] Choudhry, R., & Garg, K. A hybrid machine learning system for stock market forecasting, 2008\

[4] Pazzani, M. J., & Billsus, D. Content-based recommendation systems. In The adaptive web (pp. 325–341). Berlin, Heidelberg: Springer. 2007

[5] He, Z., Raghavan, A., Chai, S., & Lee, R. Detecting zero-day controller hijacking attacks on the power-grid with enhanced deep learning, 2018

[6] Farwell, J. P., & Rohozinski, R. Stuxnet and the future of cyber war., 2011

[7] Kotsiantis, S. B., Zaharakis, I., & Pintelas, P. Supervised machine learning: A review of classification

techniques. Emerging Artificial Intelligence Applications in Computer Engineering, 160, 3–24, 2007

[8] Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. Adversarial machine learning. In Proceedings of the 4th ACM workshop on security and artificial intelligence (pp. 43–58), 2011

[9] Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. Adversarial machine learning. In Proceedings of the 4th ACM workshop on security and artificial intelligence (pp. 43–58), 2011

[10] Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. The security of machine learning. Machine Learning, 81(2), 121–148, 2010

[11] Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. The 2015 Ukraine blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems, 32(4), 3317–3318. 2017

[12] Liu, W., Wang, Z., Liu, X., Zeng, N., Liu, Y., & Alsaadi, F. E. A survey of deep neural network architectures and their applications. Neurocomputing, 234, 11–26 2017

[13] Maglaras, L. A., & Jiang, J. Intrusion detection in SCADA systems using machine learning techniques. Science and information conference (SAI), 626–631. 2014

[14] Maglaras, L. A., Kim, K.-H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., … Cruz, T. J. Cyber security of critical infrastructures. ICT Express, 4, 42–45. 2018

[15] Mitchell, R., & Chen, I.-R. A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Surveys (CSUR), 46(4), 55. 2014

[16] Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., & Weaver, N. Inside the slammer worm. IEEE Security & Privacy, 99(4), 33–39. 2003

[17] Morita, T., Yogo, S., Koike, M., Hamaguchi, T., Jung, S., Koshijima, I., & Hashimoto, Y. Detection of cyber-attacks with zone dividing and PCA. Procedia Computer Science, 22, 727–736. 2013

[18] Raghavan, A. Boosted hidden markov models for malware detection. Master’s Projects, 623. https://scholarworks.sjsu.edu/etd_projects/623 2018

[19] Ranveer, S., & Hiray, S. Comparative analysis of feature extraction methods of malware detection. International Journal of Computer Applications, 120 (5), 1–7. 2015

[20] Rieck, K., Trinius, P., Willems, C., & Holz, T. Automatic analysis of malware behavior using machine learning. Journal of Computer Security, 19(4), 639–668 2011

[21] Rubinstein, B. I., Nelson, B., Huang, L., Joseph, A. D., Lau, S.-h., Rao, S., … Tygar, J. Stealthy poisoning attacks on PCA-based anomaly detectors. ACM SIGMETRICS Performance Evaluation Review, 37(2), 73–74. 2009

[22] Safavian, S. R., & Landgrebe, D. A survey of decision tree classifier methodology. IEEE Transactions on Systems, Man, and Cybernetics, 21(3), 660–674 1991

[23] Santos, I., Brezo, F., Ugarte-Pedrero, X., & Bringas, P. G. Opcode sequences as representation of executables for data-mining-based unknown malware detection. Information Sciences, 231, 64–82 2013

[24] Scholkopf, B., & Smola, A. J. Learning with kernels: Support vector machines, regularization, optimization, and beyond. Cambridge, MA: MIT Press. 2001

[25] Sedgwick, P. Spearmans rank correlation coefficient. BMJ, 349, g7327 2014

[26] Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., & Weiss, Y. Andromaly: A behavioral malware detection framework for android devices. Journal of Intelligent Information Systems, 38(1), 161–190 2012

[27] Sharma, A., & Sahay, S. K. Article: Evolution and detection of polymorphic and metamorphic malwares: A survey. International Journal of Computer Applications, 90(2), 7–11 2014

[28] Sharma, A., & Sahay, S. K. An effective approach for classification of advanced malware with high accuracy. International Journal of Security and Its Applications, 10(4), 249–266 2016

[29] Sharma, A., Sahay, S. K., & Kumar, A. Improving the detection accuracy of unknown malware by partitioning the executables in groups. In Advanced computing and communication technologies (pp. 421–431). South Korea: Science and Engineering Research Support Society. 2016

[30] Sonntag, D., Zillner, S., van der Smagt, P., & Lorincz, A. Overview of the CPS for smart factories project: deep learning, knowledge acquisition, anomaly detection and intelligent user interfaces. In Industrial internet of things (pp. 487–504). Cham, Switzerland: Springer. 2017

[31] Sortomme, E., Venkata, S., & Mitra, J. Microgrid protection using communication-assisted digital relays. IEEE Transactions on Power Delivery, 25(4), 2789–2796 2010

[32] Tobiyama, S., Yamaguchi, Y., Shimada, H., Ikuse, T., & Yagi, T. Malware detection with deep neural network using process behavior. In 2016 I.E. 40th annual computer software and applications conference (COMPSAC) (Vol. 2, pp. 577–582). New York, NY: IEEE 2016

[33] Tramer, F., Kurakin, A., Papernot, N., Goodfellow, I., Boneh, D., & McDaniel, P. Ensemble adversarial training: Attacks and defenses. arXiv, 1705, 07204 (2017).

[34] Wihersaari, K. Intelligence acquisition methods in cyber domain: Examining the circumstantial applicability of cyber intelligence acquisition methods using a hierarchical model. 2015

[35] Youse, S., Mousavi, M. S., & Fathy, M. Vehicular ad hoc networks (vanets): challenges and perspectives. In 2006 6th international conference on its telecommunications proceedings (pp. 761–766). New York, NY: IEEE. 2006

[36] Zhang, T., & Zhu, Q. Distributed privacy-preserving collaborative intrusion detection systems for vanets. IEEE Transactions on Signal and Information Processing over Networks, 4(1), 148–161. 2018

[37] Bolton, W. Programmable logic controllers. 2015

[38] Figueiredo, J., & da Costa, J. S. A SCADA system for energy management in intelligent buildings, 2012

[39] Huang, Xiao, et al. "Graphene-based materials: synthesis, characterization, properties, and applications." small 7.14, 2011

© 2020-2022, IJARCS All Rights Reserved

[40] Cruz, T., Barrigas, J., Proenca, J., Graziano, A., Panzieri, S., Lev, L., & Simões, P.. Improving network security monitoring for industrial control systems., 2015

[41] Kanungo, T., Mount, D. M., Netanyahu, N. S., Piatko, C. D., Silverman, R., & Wu, A. Y. An efficient k-means clustering algorithm: Analysis and implementation. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2002

[42] Kumar, V., Srivastava, J., & Lazarevic, A. Managing cyber threats: Issues, approaches, and challenges (Vol. 5), 2005

[43] Boyd, S. Alternating direction method of multipliers. In Talk at nips workshop on optimization and machine learning, 2011

[44] Biggio, B., Corona, I., Maiorca, D., Nelson, B., Srndic, N., Laskov, P., … Roli, F. Evasion attacks against machine learning at test time. In Joint European conference on machine learning and knowledge discovery in databases (pp. 387–402) 2013

[45] Biggio, B., Fumera, G., & Roli, F.. Security evaluation of pattern classifiers under attack. IEEE Transactions on Knowledge and Data Engineering, 26(4), 984–996, 2014

[46] Biggio, B., Nelson, B., & Laskov, P. Support vector machines under adversarial label noise. In Asian conference on machine learning (pp. 97–112), 2011

[47] Biggio, B., Nelson, B., & Laskov, P., Poisoning attacks against support vector machine, 2012

[48] Grosse, K., Papernot, N., Manoharan, P., Backes, M., & McDaniel, P. Adversarial examples for malware detection. In European symposium on research in computer security (pp. 62–79). Cham, Switzerland: Springer, 2017

[49] Baheti, R., & Gill, H.. Cyber-physical systems. The Impact of Control Technology, 12(1), 161–166, 2011

[50] Barreno, M., Nelson, B., Sears, R., Joseph, A. D., & Tygar, J. D. Can machine learning be secure? In Proceedings of the 2006 ACM symposium on information,computer and communications security (pp. 16–25), 2010

[51] Bernabeu, E. E., Thorp, J. S., & Centeno, V. Methodology for a security/dependability adaptive protection scheme based on data mining. IEEE Transactions on Power Delivery, 27(1), 104–111, 2010

[52] Dahl, G. E., Stokes, J. W., Deng, L., & Yu, D. Large-scale malware classification using random projections and neural networks, 2013

[53] Evmievski, A.Randomization in privacy preserving data mining, 2013

[54] Friedrichs, O., Huger, A., & O'donnell, A. J. Method and apparatus for detecting malicious software using machine learning techniques. Google Patents, 2014

[55] Jiang, J., & Yasakethu, L. Anomaly detection via one class SVM for protection of SCADA systems, 2013

[56] Kolosnjaji, B., Demontis, A., Biggio, B., Maiorca, D., Giacinto, G., Eckert, C., & Roli, F. Adversarial malware binaries: Evading deep learning for malware detection in executables, 2018.

[57] Lew, M. S., Sebe, N., Djeraba, C., & Jain, R. Content-based multimedia information retrieval: State of the art and challenges. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 2(1), 1–19, 2007.