Machine Learning for Cyber Defense and Attack

Manjeet Rege
Graduate Programs in Software
University of St. Thomas
St. Paul, MN, USA
Email: rege@stthomas.edu

Raymond Blanch K. Mbah
Graduate Programs in Software
University of St. Thomas
St. Paul, MN, USA
Email: kong1343@stthomas.edu

***Abstract*—The exponential advancements in processing, storage and network technologies have led to the recent explosive growth in big data, connectivity and machine learning. The world is becoming increasingly digitalized - raising security concerns and the desperate need for robust and advanced security technologies and techniques to combat the increasing complex nature of cyber-attacks. This paper discusses how machine learning is being used in cyber security in both defense and offense activities, including discussions on cyber-attacks targeted at machine learning models. Specifically, we discuss the applications of machine learning in carrying out cyber-attacks, such as in smart botnets, advanced spear fishing and evasive malwares. We also explain the application of machine learning in cyber security, such as in threat detection and prevention, malware detection and classification, and network risk scoring.**

Keywords- Cyber Security; Machine Learning; Malware; Thread Detection and Classification; Network Risk Scoring.

I. INTRODUCTION

Digital security remains a top concern as the world is becoming increasingly digitalized. With advances in network technologies, such as the Internet, access to cutting edge technology and research findings has never been this easy with research papers being made public daily and the digital world becoming increasingly open sourced. Unfortunately, cutting edge research and breakthroughs in technology are both available to the security analyst and cybercriminals who have various interests in making use of these technologies and information. Research and advances in the field of machine learning has resulted in algorithms and technologies for improving security solutions that help in identifying and decisively dealing with security threats. However, this also makes it possible for cybercriminals to use this knowledge in crafting and launching bigger and more sophisticated attacks.

Cybercriminals have a huge advantage in the cyber war since, out of many attempts, they need to be right just once. For security, on the other hand, the desired success rate needs to be 100%. Research shows that in 2017, multiple organizations, business, individuals and applications were victimized by cybercriminals [1]. Stolen information included sensitive classified intelligence data, financial records, and personally identifiable information. The use of these kinds of information can be catastrophic, especially when it is made publicly available or sold on the black market. Some research statistics with regards to the impact of cyber security to businesses, organizations, and individuals include:

- In recent years, cybercrime has been responsible for more that $400 billion in funds stolen and costs to mitigate damages caused by crimes [2].
- It has been predicted that a shortage of over 1.8 million cybersecurity workers will be experienced by 2022 [3].
- It’s been predicted that organizations globally will spend at least $100 billion annually on cybersecurity protection [4].
- Attackers currently make over $1 billion in annually revenue from Ransomware attacks, such as Wannacry and CryptoWall attacks [5].

Keeping up and countering the increasing sophistication of cyber-attacks is becoming increasingly challenging, as defense tools quickly become obsolete. In fact, on average, it can take up to 240 days to detect an intrusion [6]. The sophistication of cyber-attacks is growing both in scale and complexity making it increasingly challenging to keep up and respond to the constant emergence of new threats and vulnerabilities. One major area that is currently having a high impact on cyber security is machine learning, which will be the focus of this paper.

The rest of the paper is structured as follows. In Section II, we present an overview of machine learning, including its various categories (supervised and unsupervised learning). Section III describes the applications of machine learning in cybersecurity, such as in network risk scoring and in malware detection and prevention. In section IV, we discuss the applications of machine learning in cyber-attacks, such as in smart botnets, advanced spear fishing and evasive malwares. Section V discusses cyber-attacks targeted at machine learning models.

II. OVERVIEW OF MACHINE LEARNING

Machine learning is a sub-field of artificial intelligence that aims to empower systems with the ability to use data to learn and improve without being explicitly programmed [7]. It relies on mathematical models derived from analyzing patterns in datasets, which are then used to make predictions on new input data. Applications of machine learning span across a vast set of domains including e-commerce, where machine learning applications are used to make recommendations based on customer behavior and preferences, and health care, where machine learning is used to predict epidemics or the likelihood of a patient having

ISBN: 978-1-61208-681-1

certain diseases, such as cancer, based on their medical records.

Machine learning algorithms can be categorized as Predictive (Supervised Learning) or Pattern Discovery (Unsupervised Learning) [39]. In supervised learning, there is always a target variable, the value of which the machine learning model learns to predict using different learning algorithms e.g., based on an IP address location, frequencies of Web requests and times of request, a machine learning model can predict if a given IP address was part of a Distributed Denial of Service (DDOS) attack. A variety of Machine learning algorithms fall under the umbrella of supervised learning, including Linear and Logistic Regression, Decision Tree and Support Vector Machine (SVM) [40]. On the other hand, in unsupervised learning, there is no prediction of a target variable, rather, unsupervised algorithms learn to find interesting associations or patterns in datasets e.g., identifying computer programs, such as malwares with similar operating/behavioral patterns using clustering and association algorithms.

One particular domain where machine learning is seeing wide adoption is that of cybercrime and security which has multiple use cases for machine learning, such as in malware and log analysis. The power of machine learning is leveraged by cybercriminals as well as security experts. We will now discuss how machine learning is being used for cybercrime as well as cyber security.

III. Applications of Machine Learning in Cyber Security

With the growing threat of cybersecurity, studies are focusing on machine learning and its vast set of tools and techniques to identify, stop and respond to sophisticated cyber-attacks [21]. Machine learning can be leveraged in various domains of cyber security to provide analytical-based approaches for attack detection and response. It can also enhance security processes by automating routine tasks and making it easy for security analysts to quickly work with semi-automated tasks. Some popular applications of machine learning in cyber security are presented below.

A. Threat detection and classification

Machine learning algorithms can be implemented in applications to identify and respond to cyber-attacks before they take effect [8]. This is usually achieved using a model developed by analyzing big data sets of security events and identifying the pattern of malicious activities. As a result, when similar activities are detected, they are automatically dealt with. The models' training dataset is typically made up of previous identified and recorded Indicators of Compromise (IOC), which are then used to build models and systems that can monitor, identify and responds to threats in real time. Also, with the availability of IOC datasets, we can use machine learning classification algorithms to identify the various behaviors of malwares in datasets and classify them accordingly. Studies have been made on behavioral-based analysis frameworks that make use of machine learning clustering and classification techniques to analyze the behaviors of thousands of malwares [14]. This makes it possible to use the learned patterns to automate the process of detecting and classifying new malware. This can help security analysts or other automated systems to quickly identify and classify a new type of threat and respond to it accordingly using a data driven decisions. For example, by using a historic dataset containing detailed events of WannaCry ransomware attacks, a machine learning model can learn to identify similar attacks, thereby making it possible to automate the identification and response process of similar attacks. Machine learning techniques have also been used in IP traffic classification [15][16] which can help automate the process of intrusion detection systems that can be used to identify behavioral patterns as in the case of DDOS attacks. With the increasing number of machine learning techniques, other studies have been focused on analyzing multiple machine learning solutions for intrusion detection systems including single, hybrid and ensemble classifies [17].

B. Network risk scoring

This refers to the use of quantitative measures to assign risk scores to various sections of a network, thereby helping organizations to prioritize their cyber security resources accordingly with regards to various risk scores. Machine learning can be used to automate this process by analyzing historic cyber-attack datasets and determining which areas of networks were mostly involved in certain types of attacks. Using machine learning is advantageous in the sense that the resulting scores will not only be based on domain knowledge of the networks but most importantly, the scores will be data driven. This score can help quantify the likelihood and impact of an attack with respect to a given network area and can thus help organizations to reduce to risk of being victimized by attacks.

Studies have been carried out on the use of machine learning algorithms such K-Nearest Neighbor, Support Vector Machines, and Random Forest algorithms to analyze and cluster network assets based on their connectivity [18]. Other studies have focused on how IOT devices connected to small and Medium Sized Enterprises (SMEs) can be used to lunch attacks on SMEs [19]. Machine learning powered systems have been developed that make use of the mutual reinforcement principle to analyze massive volumes of alerts in organization networks to determine risk scores by taking into account the associations of various network entities [20].

C. Automate routine security tasks and optimize human analysis

Machine learning can be used to automate repetitive tasks carried out by security analysts during security activities. This can be done through analyzing records/reports of past actions taken by security analysts to successfully identify and respond to certain attacks and using this knowledge to build a model that can identify similar attacks and respond accordingly without human intervention. Though it is difficult to automate the full security process and replace the human security analyst, there are some aspects of the analysis that machine learning can automate including malware detection, network log analysis, and vulnerability assessments, such as network risk analysis. By incorporating machine learning in the security work flow, ‘man and machine’ can join forces and accomplish things at a degree of speed and quality that will have been otherwise impossible.

With the exponential growth of artificial intelligence, we see an increasing number of tasks being automated. It is tempting to think that artificial intelligence will increase automation, and certain tasks that are currently performed by humans will be taken over by machines. This might be true in some cases, however there are numerous cases where the combination of artificial intelligence and human intelligence produce far better results than each will produce by itself. It is for this reason that we are currently seeing the rise of artificial intelligence companies with a focus on not only creating AI product for automating tasks, but creating products that enhancing and complement the productivity of human analysts. A well-known example of such a company is Palantir [9], which creates products that make it easy for analysts to aggregate and make use of massive volumes of data.

In other to enhance security analysts activities, studies have been carried out on the use of machine learning algorithms, such as genetic algorithms and decision tries to create applications that generate rules for classifying network connections [22]. Other approaches go far as to implement a cognitive architecture to create an automated cyber defense decision-making system with expert-level ability inspired by how humans reason and learn [23]. Cybersecurity analysts typically have to spend time responding to multiple events, which sometimes include false positives, which mostly turn out to be a waste of their time. Studies have been done to show that machine learning classifiers can be trained on alert data to identify and distinguish between false positives and true positives, thereby making it possible to create an automated system that will alert the analyst only on scenarios that include true positives [24].

IV. Applications of Machine Learning in Cyber Crime

Just as machine learning is a promising tool to deal with the growing cyber threats, as shown in the previous section, it also acts as a tool that can be leveraged by malicious attackers. For instance, there have been studies that show the possibility of cybercriminals leveraging machine learning to create intelligent malware that can outsmart current intelligent defense systems [25]. Hence, as the field of machine learning progresses at a rapid rate while offering promising solutions for cyber defense, it also makes it possible for cybercriminals to use it in carrying out more sophisticated attacks at scale as well as lunch attacks targeted at machine learning models. Everyone including security analysts and cybercriminals are actively seeking new innovative AI techniques/technologies to add to their arsenal of cyber weapons. For instance, just like cyber defense specialist are actively analyzing data to better understand an attackers’ patterns, the attackers themselves can also steal data about users and analyze it to better craft their attacks. An example includes illegally accessing and analyzing a targeted users’ emails with the aim of having a better understanding of their email patterns and leveraging that to craft better phishing emails.

Some popular categories of machine learning based attack techniques include:

A. *Unauthorized Access*

Machine learning can be used to gain unauthorized access to systems, such as those involving captchas. One field that has been hugely impacted by machine learning is that of machine vision, whereby a machine is trained to identify objects. This is the same technology being used in self driving cars where cars rely on machine learning to identify and avoid obstacles. With machines being capable of identifying objects in images, they can be trained to bypass captcha-based system that relies on a user to identify the objects in an image before being authorized [10]. Also, machine learning algorithms, such as neural networks that attempt to mimic the human brain can be trained to speed up and automate social engineering techniques, such as guessing user passwords by training the model with big datasets containing data of previously hacked user information including their usernames and passwords and any kind of information that can be used to enhance the guessing process.

Multiple studies have been carried out on how machine learning can be leverage to gain unauthorized access to systems. Examples include PassGANs that can generate high quality password guesses by using Generative Adversarial Networks (GAN) and real password leaks to learn the distribution of real passwords [26]. Some studies focus on using machine learning to generate passwords for real time broot force attacks that rely on testing different variants of passwords with the aim of successfully gaining unauthorized access to a system [27]. Other studies focus on using Deep learning to bypass CAPTCHAs without human intervention [28][29], while others focus on leveraging machine learning to clone human voices. Applications exists that leverage machine learning techniques to clone voices [30], making it possible to impersonate people.

B. *Evasive Malware*

Typically, the creation of malware involves writing a malicious program which in most basic cases can be identified by security programs which have records of the malwares’ signature. However, there have been cases where machine learning has been used to generate malware code that other security programs could not detect including machine learning based systems [11]. Another example includes DeepLocker, an AI powered malware developed by IBM researchers that is capable of leveraging facial recognition, voice recognition and geolocation to identify its target before launching its attack [12]. There’s a lot of research on using machine learning to generate computer code with the goal of replacing computer programmers with AI systems in scenarios where an AI can write the code without human intervention. Examples include a recent research carried out at Microsoft to create AI systems that can generate code without human intervention [13].

C. Spear Phishing

Machine learning can be leveraged to carryout advanced spear phishing attacks for example, by illegally collecting genuine email data of targeted individuals and feeding the data to a machine learning model which can then learn from the data, derive context from the data and generate emails that look similar and genuine to those it learned from. This can then be incorporated into an automated process thereby speeding up the efficiency and speed in which cybercriminals can launch targeted phishing attacks. Some phishing attacks leverage social engineering to illegally acquire information about their targeted users.

Social engineering is a popular kind of attack technique that uses deception to manipulate individuals to get their personal information. There have been studies on using machine learning to carry out sophisticated social engineering attacks. Examples include studies that used long short-term memory (LSTM) neural network and recurrent neural network that are trained on social media post extracted from a targets time line with the aim of manipulating users into clicking on deceptive URLs [31][32]. Similar approaches can also be used to carry out email based phishing attacks.

V. SECURITY THREADS TO MACHINE LEARNING PRODUCTS

From the beginning of the computer revolution, cybercriminals have always been on the lookout for ways to exploit software vulnerabilities and carry out malicious activities. With the explosive growth of artificial intelligence technology, cybercriminals are beginning to look for ways to exploit vulnerabilities in this domain. Attacks on machine learning systems are typically discussed in the context of adversarial machine learning which is concerned with the security of applying machine learning techniques to security-related tasks, such as biometric recognition, spam filtering, network intrusion and malware detection. Attacks on machine learning algorithms can be categorized into three domains: attacks targeted at altering training datasets and introducing vulnerabilities in the final model [33]; attacks targeted at increasing the error rate of the final model [34]; attacks aimed at making it possible for a specific set of records to be classified or interpreted by the model as desired by the attacker [35].

Like we earlier said, a machine learning model is built by feeding data into a computer algorithm which then learns patterns from the data and can then use the learned patterns to predict or classify unseen data. The final product of a machine learning model can be a simple equation which is then translated as a computer code that receives input and produces output in the form of a classification or prediction. With this simple intuition of machine learning models, it can be seen that cybercriminals can interfere with a machine learning product by tempering with the training and test data or altering the final parameters of the model:

- *Poisoning the training data*: It is well known by machine learning practitioners that the success of machine learning projects relies heavily on quality of the data. This is usually called 'garbage in garbage out' meaning if you train your model on garbage data, it will produce garbage results, regardless of how advanced your model is. A possibility is that a cybercriminal gains access to the training set of a machine learning model and alters the data before the training begins without the knowledge of the machine learning engineers. Clearly, we can see that the data will already be tampered with and has lost its original quality which will result in modeling on wrong data. Hence, our final model will no longer be a reliable one since it was trained on bad data and it doesn't matter how good the modeling process goes, our predictions or model classifications will surely not be appropriate. Also, another scenario can be in a situation where a model is made to re-train itself every time it receives new records. In this case, a cybercriminal can feed the model with bad data and the model can learn from this bad data and as a result, negatively impact its performance. Multiple studies have been carried out on understanding and defending against poisoning attacks [36][37].
- *Altering a machine learning model*: In this case, a cybercriminal can illegally access a machine learning model and alter its parameters and thereby influence how it produces results. For example if after training, the final machine learning model deployed to production can be represented mathematically as $y = 1 + 2x$, where x is the input parameter and y is the output from the model, then if a cybercriminal can access the system and alter the equation to $y = 1 – 2x$, then it can clearly be seen that this can lead to wrong prediction and might result in catastrophic decisions if the results of the predictions were being used to make key business decisions.
- *Evading detection by machine learning models*: This refers to attacks that aimed at avoiding detection. This can happen in situations where an attacker alters data used during the testing phase with the aim of avoiding being classified as a threat during regular system operations. Biometric systems have been used as examples in studies to show how such attacks can be done [38].

From the points mentioned above, it can be seen that it is of vital importance that machine learning projects take security seriously. Appropriate measures should be taken to monitor machine learning models and their datasets.

VI. CONCLUSION

In this paper, we have seen how machine learning can be applied in a security context from both a defense and attack perspective as well as the potential threats targeted at machine learning models. Clearly it can be seen that machine learning is a powerful tool that can be used for automating complex defense and offense cyber activities. Hence, with cybercriminals also leveraging machine learning in their arsenal of cyber weapons, we are expected to experience more sophisticated and big attacks powered by AI. It is therefore of vital importance that security specialists as well as machine learning practitioners stay abreast with the recent advancements in machine learning including adversarial machine learning so as to constantly be on the lookout to make use of potential AI related security applications.

This paper can act as basis for future research that can focus on analyzing existing security solutions and the various challenges of leveraging machine learning to develop and deploy scalable cybersecurity systems in production environments.

REFERENCES

[1] S. Larson. 10 biggest hacks of 2017. 2017, December 20. Retrieved: November 3, 2018, from https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

[2] T. Rimo and M. Walth, “McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies”, McAfee, June 9, 2014.

[3] “2017 Global Information Security Workforce Study”, Frost and Sullivan, May 2017.

[4] Worldwide Revenue for Security Technology Forecast to Surpass $100 Billion in 2020, According to the New IDC Worldwide Semiannual Security Spending Guide. 2016, October 12. Retrieved: September 21, 2018, from https://www.businesswire.com/news/home/20161012005102/en/Worldwide-Revenue-Security-Technology-Forecast-Surpass-100.

[5] A. Cuthbertson. Ransomware attacks have risen 250 percent in 2017, hitting the U.S. hardest. 2017, May 28. Retrieved: September 21, 2018, from http://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034.

[6] B. M. Cooper. Resiliency and Recovery Offset Cybersecurity Detection Limits. 2015, January 16. Retrieved: September 21, 2018, from https://www.afcea.org/content/resiliency-and-recovery-offset-cybersecurity-detection-limits.

[7] S. Dolev and S. Lodha, “Cyber Security Cryptography and Machine Learning“, In Proceedings of the First International Conference, CSCML 2017, Beer-Sheva, Israel, June 29-30, 2017.

[8] S. Dolev and S. Lodha, “Cyber Security Cryptography and Machine Learning“, In Proceedings of the First International Conference, CSCML 2017, Beer-Sheva, Israel, June 29-30, 2017.

[9] About. (n.d.). Retrieved: November 03, 2018, from http://www.palantir.com/.

[10] G. A. Wang, M. Chau, and H. Chen. Intelligence and Security Informatics: 12th Pacific Asia Workshop, PAISI 2017, Jeju Island, South Korea, May 23, 2017, Proceedings. Cham, Switzerland: Springer.

[11] H. Weiwei., and Y. Tan. Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN. 2017, February 20, Retrieved: November 03, 2018, from https://arxiv.org/abs/1702.05983v1.

[12] M. P. Stoecklin. DeepLocker: How AI Can Power a Stealthy New Breed of Malware. 2018, August 13. Retrieved: September 20, 2018, from https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/

[13] D. Gershgorn. Microsoft's AI is learning to write code by itself, not steal it., 2017, March 1. Retrieved: November 03, 2018, from https://qz.com/920468/artificial-intelligence-created-by-microsoft-and-university-of-cambridge-is-learning-to-write-code-by-itself-not-steal-it/

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

[15] T. Nguyen, and G. Armitage. A survey of techniques for Internet traffic classification using machine learning. *IEEE Communications Surveys and Tutorials*, *10*(4), 56-76. 2008.

[16] S. Zander, T. Nguyen, and G. Armitage. Automated traffic classification and application identification using machine learning. In *Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on* (pp. 250-257). IEEE, 2005, November.

[17] C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y Lin. Intrusion detection by machine learning: A review. *Expert Systems with Applications*, *36*(10), 11994-12000, 2009.

[18] D. Arora, K. F. Li, and A. Loffler. Big data analytics for classification of network enabled devices. In *Advanced Information Networking and Applications Workshops (WAINA), 2016 30th International Conference on*(pp. 708-713). IEEE, 2016, March.

[19] J. Saleem, B. Adebisi, R. Ande, and M. Hammoudehs A state of the art survey-Impact of cyber attacks on SME's. In *Proceedings of the International Conference on Future Networks and Distributed Systems* (p. 52). ACM, 2017, July.

[20] X. Hu, T. Wang, M. P. Stoecklin, D. L. Schales, J. Jang, and R. Sailer. Asset risk scoring in enterprise network with mutually reinforced reputation propagation. In *2014 IEEE Security and Privacy Workshops (SPW)* (pp. 61-64). IEEE, 2014, May.

[21] J. B. Fraley, and J. Cannady. The promise of machine learning in cybersecurity. In *SoutheastCon, 2017* (pp. 1-6). IEEE. 2017, March.

[22] C. Sinclair, L. Pierce, and S. Matzner. An application of machine learning to network intrusion detection. In *Computer Security Applications Conference, 1999.(ACSAC'99) Proceedings. 15th Annual* (pp. 371-377). IEEE, 1999.

[23] D. P. Benjamin, P. Pal, F. Webber, P. Rubel, and M. Atigetchi. Using a cognitive architecture to automate cyberdefense reasoning. In *Bio-inspired Learning and Intelligent Systems for Security, 2008. BLISS'08. ECSIS Symposium on* (pp. 58-63). IEEE, 2008, August.

[24] L. Zomlot, S. Chandran, D. Caragea, and X. Ou. Aiding intrusion analysis using machine learning. In *Machine Learning and Applications (ICMLA), 2013 12th International Conference on* (Vol. 2, pp. 40-47). IEEE, 2013, December.

[25] R. Price. Artificial intelligence-powered malware is coming, and it's going to be terrifying. 2016, October 08. Retrieved: September 19, 2018, from https://www.businessinsider.com/darktrace-dave-palmer-artificial-intelligence-powered-malware-hacks-interview-2016-10?r=UK&IR=T.

[26] B. Hitaj, P. Gasti, G. Ateniese, and Perez-Cruz, F. Passgan: A deep learning approach for password guessing. arXiv preprint arXiv:1709.00440, 2017.

[27] K. Trieu, and Y. Yang. Artificial Intelligence-Based Password Brute Force Attacks, 2018.

[28] F. Stark, C. Hazırbas, R. Triebel, and D. Cremers. Captcha recognition with active deep learning. In GCPR Workshop on New Challenges in Neural Computation, 2015.

[29] H. Gao, W. Wang, Y. Fan, J. Qi, and X. Liu. The Robustness of“ Connecting Characters Together” CAPTCHAs. J. Inf. Sci. Eng., 30(2), 347-369, 2014.

[30] Lyrebird Ultra-Realistic Voice Cloning and Text-to-Speech. (n.d.). Retrieved: September 20, 2018, from https://lyrebird.ai/

[31] J. Seymour, and P. Tully. Generative Models for Spear Phishing Posts on Social Media. *arXiv preprint arXiv:1802.05196.* 2018.

[32] J. Seymour, and P. Tully. "Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter." *Black Hat USA* , 2016: 37.

[33] L. Huang, A. D. Joseph, B. Nelson, B. Rubinstein, and J. D. Tygar. "Adversarial machine learning". In 4th ACM Workshop on Artificial Intelligence and Security, AISec, 2011, pages 43–57, Chicago, IL, USA, October 2011.

[34] M. Barreno, B. Nelson, R. Sears, A. D. Joseph, and J. D. Tygar. Can machine learning be secure? In ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security, pages 16–25, New York, NY, USA, 2006. ACM.

[35] M. Barreno, B. Nelson, A. Joseph, and J. Tygar. "The security of machine learning". Machine Learning, 81:121–148, 2010.

[36] B. I. P. Rubinstein, B. Nelson, L. Huang, A. D. Joseph, S. h. Lau, S. Rao, N. Taft, and J. D. Tygar. "Antidote: understanding and defending against poisoning of anomaly detectors". In Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference, IMC '09, pages 1–14, New York, NY, USA, 2009. ACM.

[37] B. Biggio, B. Nelson, and P. Laskov. "Poisoning attacks against support vector machines". In J. Langford and J. Pineau, editors, 29th Int'l Conf. on Machine Learning. Omnipress, 2012.

[38] R. N. Rodrigues, L. L. Ling, and V. Govindaraju. "Robustness of multimodal biometric fusion methods against spoof attacks". J. Vis. Lang. Comput., 20(3):169–179, 2009.

[39] A. Dey. Machine Learning Algorithms: A Review. *vol*, *7*, 1174-1179, 2016.

[40] S. B. Kotsiantis, I. Zaharakis, and P. Pintelas. Supervised machine learning: A review of classification techniques. *Emerging artificial intelligence applications in computer engineering*, *160*, 3-24, 2007.