International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 5 Issue 1, January - 2021, Pages: 88-93

A Review on the Use of Machine Learning Techniques in Information Security

[1]Waseem Ahmad and [2]Abubakarsidiq Makame Rajab

[1, 2]Department of Information and Communication Engineering; Huazhong University of Science and Technology Wuhan, Hubei, China.

Email: [1]waseem.cath47@gmail.com and [2]abubakarsidiqrajab@gmail.com

Abstract — *Machine learning techniques are adopted in many scientific fields due to their unique characteristics, such as scalability and the ability to adapt quickly to new and unknown challenges. Information security is a rapidly growing area and has much interest due to the great advancement in social networks, web, online banking services, cloud technologies, mobile environment, etc. Many machine learning methods have been used to deal with information security problems. This review highlights machine learning applications in the information security field and problems related to the safety of machine learning technologies themselves, and how to use it in information security in hackers' attacks and defense, including the attacks on machine learning models. This review also explains the application of machine learning in information security, such as the detection and classification of spam, fake news, spyware, malware, and viruses and prevention of threats.*

Keywords— Machine learning, information security, malware, attacks, social media, spam.

I. Introduction

The major developments in information and communications technology have given rise to new threats to information security. Cybercriminals rely on new and advanced technologies to increase the efficiency, efficiency, speed, and scope of their attacks. To achieve this, it must rely on robust and adaptive electronic defense systems that can detect various threats in real time and deal with them.. In recent years, there has been an increasing reliance on machine learning technologies that have a critical role in detecting and preventing information security threats. Many areas use and benefit from machine learning, such as games, health care, cloud technologies, the web, internet banking, mobile environment, smart grid, manufacturing, natural language processing, education, and commerce. This trend also affects information security, as machine learning is used in attack and defense in information security. Also, threats can use machine learning to enhance the complexity of attacks.

Machine learning is also being used to improve defense, as defense systems become more efficient and robust, ensuring that they adapt to changes in the environment to reduce impacts. Through machine learning, intelligent machines can be created to learn from the experience, allowing them to operate and interact as humans do. They process large amounts of data and identify patterns in them. Machine learning - sometimes more generally referred to as AI as it is a powerful tool used by information security companies. As "AI" supported by machine learning is an important method that enables us to extend the scope of detection and classification of malware.

This review paper explores the impact of machine learning on information security and attacks by reviewing the most important new literature on applications of machine learning in information security. The work is organized as follows: in the second section an overview of machine learning. The third section highlights on the machine learning in information security. The fourth section explains the impact of machine learning on information security. The fifth section explains security threats in the areas of machine learning. The sixth section provides the most important modern applications of machine learning in information security. In the last section, the conclusion.

II. Machine Learning

Machine learning is a branch of artificial intelligence that its current applications are mostly limited to. Artificial Intelligence and machine learning are used more widely in industries and applications than ever before due to the increase in the power of computers, storage capacities, and the method of data collection, which is inconsistent with traditional programming where machine learning teaches the machine how to make a decision on its own, which leads to giving the machine explicit instructions to answer specific questions. ML algorithms try to make decisions and find ways to solve problems by training models based on sample inputs.

There are many types of ML, and each works in a completely different way. ML can be defined into three categories: supervised, unsupervised and reinforcement learning.

A. Supervised Learning

It includes a system or machine training wherein training sets are provided with the system's target pattern to perform a task. Supervised learning usually means monitoring and directing the execution of tasks and activity, so it is often divided into:

a) Regression analysis.

b) Classification analysis.

It uses labeled datasets to train a model for classifying or predicting upcoming data outcomes.

B. Unsupervised Learning

Unsupervised learning can be a set of algorithms used to extract conclusions from sets of information that consist of the input data while the outcome is not used. A common unsupervised learning methodology aims to analyze information to search for hidden patterns or clusters in it.

C. Reinforcement Learning

Reinforcement learning solves the tough problem of correlating immediate actions with the delayed outcomes that result from them. Its algorithms generally need to contend with delayed gratification to see the outcomes of their actions or choices created within the past.

III. Machine Learning in Information Security

Information security is considered one of the most important fields of information technology. It is defined as representing the various procedures that are performed to protect networks, computers, and information against illegal access and vulnerabilities provided by hackers. Security is about protecting network-based digital information, and devices from unauthorized access and change.

The most challenging element of security is the rapid development and complexity of security risks. Previously, attacks on devices and the network that connected them were minimal, as viruses, Trojans, and worms were the main threats to system damage. Artificial intelligence methods are powerful and flexible, so their use has expanded to protect and secure information and improve defense methods against increasing threats [3] [11]. Machine learning is an effective tool that can be used in many areas of information security. Through its strong algorithms, it provides a source of anti-phishing and intrusion detection. It may help develop authentication systems, assess protocol implementation, assess the integrity of proofs of human interaction, determine smart meter data, etc. [10]. It also contributed to and strengthened the information security industry, as its methods can greatly improve threat detection accuracy [11].

IV. The impact of machine learning on information security

The great progress in artificial intelligence in general and machine learning in particular in many fields such as robotics, expert systems, image recognition, natural language processing, and other fields have had a major role in people's lives.

Unfortunately, it also caused many new information security problems as it posed a real challenge to it, so manual analysis became ineffective for the performance of a data explosion and the increases risk at a high rate, so new threats are very adaptive, common, and difficult to detect and predict. Moreover, developing an algorithm base to prevent and implement threats takes a lot of time, money, and energy. Also, working to recruit specialists in this field is difficult and costly. Therefore, machine learning-based methods are expected to address these information security problems [5].

A. Positive uses of machine learning in information security

Machine learning is used to enhance defense capabilities. Its powerful automation capabilities can analyze large amounts of data with great efficiency, speed, and accuracy. Its techniques can use information about past threats to identify similar attacks in the future, although the variations in the attacks, as it has many advantages in information security, allow it to discover new and advanced changes.

In contrast, traditional technology relies heavily on attackers and known attacks, leaving room for blind spots when detecting events. Currently, the old technical limitations are being addressed with smart technology. For example, the activity on a computer network is monitored, so any significant progress in access operations will indicate a potential internal threat. If an increase in activity is detected, the device will increase the procedures and become more sensitive to detecting these patterns in the future. With the additional data, the machine will learn and adjust to detect abnormal processes. This is especially useful when attacks become more accurate and hackers develop new methods.

Machine learning can enhance network security by developing independent security systems to detect attacks and respond to violations. Especially, when a large amount of security data is created and transmitted over the network every day, network security experts will find it difficult to track and identify attack factors quickly and with effective reliability, and thus machine learning here can facilitate this by discovering suspicious activities and expanding the scope of monitoring.

B. The disadvantages and limitations of using machine learning

Machine learning has great capabilities that can help in information security, but its application has some limitations. Creating a machine learning system requires many input samples, and the ability to obtain and process samples takes a long time and many resources. Besides, building and maintaining the platform requires massive resources, including computing power, data, and memory. Also, repeated false alarms are a problem for end-users, which leads to the disruption of work by delaying any necessary response and thus affects efficiency. So, the exact tuning process is a trade-off between maintaining a safe level and reducing false alarms.

Attackers can use various attack techniques that target machine learning systems, such as data poisoning, hostile inputs, and model theft. This bad use of artificial intelligence is an important aspect that needs to be studied and considered. On the other hand, this technology also uses as a means to improve threats. For example, malicious actors can take advantage of ML technology to create a virus variable that is difficult to detect quickly [3].

V. SECURITY THREADS TO MACHINE LEARNING PRODUCTS

With the great development in machine learning, hackers have begun to search for new tools and methods to exploit weaknesses in this field. The attacks on machine learning algorithms are classified into three areas:

a) Attacks that aim to enable a specific set of records to be classified by the model as desired by the attacker

b) The attacks aim to increase the error rate in the final model.

c) The attacks aim to change training data sets in the final model and introduce vulnerabilities in them.

A machine learning model is built by entering data into an algorithm that then learns patterns through them and can predict or classify invisible data. The machine learning model can be a simple equation that receives inputs and produces outputs in classification or prediction. The cybercriminal can interfere with the machine learning product by weakening training data or changing model final parameters, such as training data poisoning of a model that is well known before.

The success of machine learning projects depends on the quality of the data entered. So, the cybercriminals aim to access the training set for the machine learning model and change the data before training the model without the knowledge of the machine learning engineers. Therefore, the final model will not be reliable, as it was trained on bad data, and certainly, the model expectations or classifications will not be reliable. Also, in cases where a model is created to retrain itself every time it receives new records, the cybercriminal can feed the model with bad data. Thus, the model will learn from these bad data, which negatively affect its performance. Evasion of detection through machine learning models also indicates attacks aimed at avoiding detection. This occurs when the attacker changes the data used during the testing phase to avoid classification as a threat during normal system operations [4].

VI. APPLICATION OF MACHINE LEARNING ON INFORMATION SECURITY

Behavior models can be built using machine learning algorithms and used to predict new input data, analyze security threats and incidents, and automatically respond to attacks. They have been applied to information security challenges as :

a) Spam detection.

b) Phishing detection.

c) DoS attack detection

d) Malware detection.

e) Network anomaly detection.

f) Biometric recognition.

g) Social media analysis.

Below, the most important information security problems and solutions of using ML technologies are listed:

A. Spam detection

Junk email, known as spam, is a major reason why implementing email categorization measures is important and necessary, as out of 80 billion email messages received daily, 48 billion are spam [12]. This has led to the need to distinguish between Desirable and spam messages so that spam can be categorized directly in the spam folder and not in the inbox. With the increased use and improvement of spam technology, it has become more complicated, as it needs to use advanced algorithms that can filter spam quickly and with great efficiency.

The goal of sending spam is to make money, spread malicious codes, fraud, etc. On the other hand, Spam can damage the computer system and disable its networks. It can also be used to launch Denial of Service (DoS) attacks that will be highlighted later. Spam can be handled in several ways as a filtering procedure based on the textual content of emails.

This case is similar to text classification, so machine learning techniques and algorithms like TF-IDF, Naive Bayes, SVM, n-gram are used to filter spam based on the text content. However, some limitations and challenges arise when using these technologies to obtain a lot of training data and processing power.

B. phishing detection

Phishing is a type of social engineering threats as it exploits the system's vulnerabilities in the user. The system might be technically protected, but an unconscious user may leak their password when an attacker sends a password update request through a fraudulent website. Thus, a phishing attack is when an attacker sends a URL or email pretending to be a person or thing to extract sensitive information from the victim by exploiting his curiosity or sense of urgency. Phishing is a huge problem, and there is no single solution to reduce it effectively, and therefore multiple techniques are implemented for that [13]. Through phishing, cookies can be stolen from the system, or all user keystrokes can be stored and sent to the attacker.

ML-based detection algorithms can be used for combining different types of features that phishing relies on as the domain, page, content, and URL. It is a supervised classification problem, and therefore disaggregated data containing samples of phishing pages is needed in the training phase. These data are an important component of building a successful detection mechanism. For this purpose, ML technologies such as Decision Tree, SVM, Naive Bayes, etc., were used to detect phishing pages.

C. DoS attack detection

Threats of denial-of-service （DOS） are the most significant threats to network functionality among all website attacks that deplete the network resources of a system or service. Consequently, users lose access to these resources as A DOS attack floods the target system with traffic that sends harmful information that could cause the system to crash [14]. This attack can be implemented in different OSI model layers such as network, application, and transport layers [15]. Recently, Machine learning methods have been implemented to detect advanced DoS attacks and improve the robustness and efficiency of a system of detecting this type of intrusion [16] as machine learning has shown satisfactory results for identifying malicious attacks and anomalous network traffic and has been widely used in classification tasks [17].

D. Malware Detection

Malware is designed specifically for unauthorized access to computer systems to breach, disrupt, or damage. It is categorized into different types, such as spyware, viruses, trojans, adware, depending on how the hacker takes advantage of system vulnerabilities. Many new variants of malicious code were speedily created due to the common use of automated generation tools.

According to reports published by software security groups in 2019, there is a 25% increase in the use of damaging malware compared to 2018, enterprise infections increased 12%, and financial Trojans increased 4% [7].

Many machine learning solutions rely on dynamic analysis such as support vector machine (SVM), decision trees, logistic regression, naive Bayes classifier, neural network [8] [9]. These technologies are used to detect, compile, and expect malware, which is grouped into several groups based on specific features identified by ML algorithms [6].

E. Network anomaly detection

This is done by judging in real-time whether the recent network behavior is not normal by creating a network behavior pattern and comparing it with the past patterns. It is decided if this behavior is normal or not when the value exceeds the threshold of the standard value. A distributed denial of service attack (DDOS) is an attack that results in abnormal network traffic behavior as it uses a large number of controlled hosts, which are widely distributed. It aims to send many invalid connections or a large number of data packets Short and massive for the target computer at the same time. Thus, creating a large number of network connections in a relatively short time, which causes millions of data messages to flow to the target computer and the target network at the same time.

In this way, it increases the use of system resources (CPU and memory) for the target computer or target network and caused slow or unresponsiveness to normal user requests. The network's inability to communicate normally leads to system paralysis and the target network at the end of the attack [18]. ML algorithms help systems to monitor behavior through their actual data, as supervised learning is important in training and analyzing abnormal behavior in the network [19]. This is done by analyzing abnormal situations in a particular network and training algorithms on multiple data to track network exploitation and detect attacks and predict them.

F. Biometric recognition

Biometrics is an automatic way to know people Through behavioral and physiological characteristics. Fingerprints, retina, iris, handwriting, and voice are among these unique characteristics of the body, as they are easy to identify [20]. Simultaneously, some of these features can be simply captured, such as the face is accessible to everyone, and the fingerprint stays on the surface unintentionally. Consequently, biometric information can be taken and false information produced; thus, it is difficult to identify a person reliably. Therefore, it is advisable to use multiple biometric techniques to increase efficiency, accuracy, and safety. In this way, the person identification performance is higher, and the information about him is more powerful and accurate.

In recent years, interest in this field has increased, especially in behavioral biometrics features such as walking and whole-body analysis, improving, identifying, and increasing safety factors [23]. Biometrics occupies an important place in machine learning techniques [21]. Its algorithms such as SVM, ANN, LDA, LBP, GMM, NB, PCA, and fuzzy logic techniques were used in all biometric applications. However, SVM, ANN, and NB technologies remain the most powerful and popular compared to other technologies [22].

G. Social media analysis

Social media have a fundamental role in the lives of users to keep in touch with others, activities, news and much more. The media often suggest stunning articles for their readers without any credible guarantee. Although some handy websites verify whether the news is real, they do not match the amount of information and the speed of its spread across the Internet, especially social media. For the sake of social good, social network data must be analyzed to extract fragments from it.

One of the most important challenges faced today is fake news, how to prevent the spread of false and harmful information on social media, and how to ensure the accuracy and integrity of social media data [27]. On the other hand, currently, it is well known that social media companies provide their data to researchers to conduct experiments. These data are misused in some cases by cybercriminals. Thus, these major challenges pose the most significant risks for companies of social media. To solve this issue, several automated fact-checking technologies have been improved to meet the need for scalability and automation [26]. Machine learning techniques define metrics to characterize opinion accuracy and identify the main factors that affect it, namely feelings, social impact, and other factors [25].

VII. CONCLUSIONS

Machine learning approaches are increasingly used for multiple applications and are also adopted for information security. Hence it is important to assess when and which Machine learning algorithms can achieve appropriate results. This review presented how to implement machine learning in information security from the point of defense and attack and potential threats that may be exposed to the models of machine learning. It can be seen that machine learning is a powerful tool that can be used to automate complex defense and cybercrime activities. Consequently, with cybercriminals benefiting from machine learning in their cyberattacks, we are expected to see more large attacks supported by machine learning. Therefore, it is important for security professionals and machine learning engineers to be kept informed of recent machine learning developments, including hostile machine learning. They are always on the lookout to take advantage of potential security applications related to artificial intelligence.

REFERENCES

[1] Alpaydin, Ethem. Introduction to machine learning. MIT press, 2020.

[2] Zhang XD. (2020) Machine Learning. In: A Matrix Algebra Approach to Artificial Intelligence. Springer, Singapore

[3] Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.

[4] Rege, Manjeet, and Raymond Blanch K. Mbah. "Machine learning for cyber defense and attack." DATA ANALYTICS 2018 (2018): 83.

[5] Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. Information, 10(4), 122.

[6] J. Sun, K. Yan, X. Liu, C. Yang and Y. Fu, "Malware detection on android smartphones using keywords vector and SVM," 2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS), Wuhan, 2017, pp. 833-838, doi: 10.1109/ICIS.2017.7960108.

[7] K. Sethi, R. Kumar, L. Sethi, P. Bera and P. K. Patra, "A Novel Machine Learning Based Malware Detection and Classification Framework," 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, United Kingdom, 2019, pp. 1-4, doi: 10.1109/CyberSecPODS.2019.8885196.

[8] A. Utku, İ. A. Doğru and M. A. Akcayol, "Decision tree based android malware detection system," 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, 2018, pp. 1-4, doi: 10.1109/SIU.2018.8404151.

[9] M. Kumaran and W. Li, "Lightweight malware detection based on machine learning algorithms and the android manifest file," 2016 IEEE MIT Undergraduate Research Technology Conference (URTC), Cambridge, MA, 2016, pp. 1-3, doi: 10.1109/URTC.2016.8284090.

[10] Jordan, Michael I., and Tom M. Mitchell. "Machine learning: Trends, perspectives, and prospects." Science 349, no. 6245 (2015): 255-260.

[11] Proko, Eljona, Alketa Hyso, and Dezdemona Gjylapi. "Machine Learning Algorithms in Cyber Security." In RTA-CSIT, pp. 203-207. 2018.

[12] S. Shrivastava and R. Anju, "Spam mail detection through data mining techniques," 2017 International Conference on Intelligent Communication and Computational Techniques (ICCT), Jaipur, 2017, pp. 61-64, doi: 10.1109/INTELCCT.2017.8324021.

[13] V. Patil, P. Thakkar, C. Shah, T. Bhat and S. P. Godse, "Detection and Prevention of Phishing Websites Using Machine Learning Approach," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-5, doi: 10.1109/ICCUBEA.2018.8697412.

[14] Y. Zhou and J. Li, "Research of Network Traffic Anomaly Detection Model Based on Multilevel Autoregression," 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 2019, pp. 380-384, doi: 10.1109/ICCSNT47585.2019.8962517.

[15] P. J. Shinde and M. Chatterjee, "A Novel Approach for Classification and Detection of DOS Attacks," 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, 2018, pp. 1-6, doi: 10.1109/ICSCET.2018.8537341.

[16] S. Wankhede and D. Kshirsagar, "DoS Attack Detection Using Machine Learning and Neural Network," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-5, doi: 10.1109/ICCUBEA.2018.8697702.

[17] N. Zhang, F. Jaafar and Y. Malik, "Low-Rate DoS Attack Detection Using PSD Based Entropy and Machine Learning," 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 2019, pp. 59-62, doi: 10.1109/CSCloud/EdgeCom.2019.00020.

[18] K. Wehbi, L. Hong, T. Al-salah and A. A. Bhutta, "A Survey on Machine Learning Based Detection on DDoS Attacks for IoT Systems," 2019 SoutheastCon, Huntsville, AL, USA, 2019, pp. 1-6, doi: 10.1109/SoutheastCon42311.2019.9020468.

[19] S. B. Wankhede, "Anomaly Detection using Machine Learning Techniques," 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 2019, pp. 1-3, doi: 10.1109/I2CT45611.2019.9033532.

[20] R. E. O. Paderes, "A Comparative Review of Biometric Security Systems," 2015 8th International Conference on Bio-Science and Bio-Technology (BSBT), Jeju, 2015, pp. 8-11, doi: 10.1109/BSBT.2015.12.

[21] B. Arslan, E. Yorulmaz, B. Akca and S. Sagiroglu, "Security Perspective of Biometric Recognition and Machine Learning Techniques," 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, 2016, pp. 492-497, doi: 10.1109/ICMLA.2016.0087.

[22] O. C. Kurban, T. Yildirim and A. Bilgiç, "A multi-biometric recognition system based on deep features of face and gesture energy image," 2017 IEEE International Conference on INnovations in Intelligent SysTems and Applications (INISTA), Gdynia, 2017, pp. 361-364, doi: 10.1109/INISTA.2017.8001186.

[23] S. Cresci, M. Petrocchi, A. Spognardi, M. Tesconi and R. D. Pietro, "A Criticism to Society (As Seen by Twitter Analytics)," 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW), Madrid, 2014, pp. 194-200, doi: 10.1109/ICDCSW.2014.31.

[24] Y. Zhang, W. Mao, D. Zeng, N. Zhao and X. Bao, "Exploring Opinion Dynamics in Security-Related Microblog Data," 2014 IEEE Joint Intelligence and Security Informatics Conference, The Hague, 2014, pp. 284-287, doi: 10.1109/JISIC.2014.56.

[25] N. X. Nyow and H. N. Chua, "Detecting Fake News with Tweets' Properties," 2019 IEEE Conference on Application, Information and Network Security (AINS), Pulau Pinang, Malaysia, 2019, pp. 24-29, doi: 10.1109/AINS47559.2019.8968706.

[26] B. Thuraisingham, M. Kantarcioglu and L. Khan, "Integrating Cyber Security and Data Science for Social Media: A Position Paper," 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), Vancouver, BC, 2018, pp. 1163-1165, doi: 10.1109/IPDPSW.2018.00178.