TOPIC: A REVIEW TO UNDERSTAND THE ROLE OF MACHINE LEARNING IN THE CYBERSECURITY THREAT DETECTION AND PREVENTION

INTRODUCTION

The cyberspace has been a growing platform for user interaction, a central secondary source of information, and has even become the largest marketplace in recent times. What used to be a luxury for a select few in a marginal percentage of the population has become a necessity for a vast number of day-to-day operations all over the world.
This has been made possible by huge investments into technological research and innovation in computer hardware and software, giving rise to a new class of devices that merely existed in the mind and fictitious novels and movies a few decades ago. The result, more affordable devices, capable of storing large amount of data and better penetration of affordable data services in both rural and urban regions, thereby, increasing the number of internet users.
However, with the rise in internet usage is also a rise in targeted attacks by cybercriminals, looking to exploit the unsuspecting users.

Background of the study

Inspite of the progress made in threat detection following the in flux of interest in the cybersecurity research space, traditional approaches which rely on signature and heuristics based detection – as used in firewalls and antivirus programs - have struggled to keep pace with the sophistication of cyber threats. Machine learning offers a better alternative. It uses large datasets to identify patterns in confirmed malicious activities, and transfers this learning to newly observed data to predict new threats.

Problem statements

Even with the potentials and excitement that comes with introducing machine learning to cybersecurity, there still exists some challenges. As security analysts are researching new ways to detect and prevent threats, cyber criminals also have access to sophisticated and smart systems, manned by seasoned professionals as well. This results in even more complex threats and never before seen exploitations. Also, the uprising of adversarial and generative AI possess a challenge in that machine learning algorithms can be manipulated by attackers.
The development and subsequent deployment of machine learning based solutions also requires careful considerations so as to ensure it is scalable, compatible, and ethically viable (Yaseen, n.d.).

Research Aim

The aim of this study is to understand the role of machine learning in cybersecurity threat detection and prevention. We hope to investigate the state-of-the-art in machine learning based security models and justify the need for more research interests in the field.

Research Objectives

This study intends to achieve the following objectives:
To review the existing literature on machine learning techniques with application in cybersecurity.
To identify the gaps and key challenges associated with the use of these models
To make recommendations to the advancement of machine learning application in cybersecurity.

Research Questions

In the course of this study, we aim to answer the following research questions:
What are the current trends in machine learning application to cybersecurity?
What are the main challenges limiting the performance of existing machine learning based solutions?

What new machine learning models or techniques have an intuitive approach that can be applied to cybersecurity?

Significance of the Study

By investigating the role of machine learning in cybersecurity, this Study seeks to inform cybersecurity practitioners, researchers, and other stakeholders, of the current state-of-the-art in machine learning based cybersecurity solutions, and recommend more robust security strategies so as to combat criminal activities in the cyber space.

Conclusion

In conclusion, utilizing the strength and robustness of machine learning models in cybersecurity represents a promising venture, with great potentials in the defense against cyber threats. This study intends to contribute to this advancement by recommending more robust and effective solutions to this defensive attack.

BASIC CONCEPTS AND TERMINOLOGIES

CYBERSECURITY

Cybersecurity is the technology of protecting the internet from attacks and unauthorised access. The wide-spread use of gadgets and internet enabled devices has given rise to potential targets for cybercriminals, and as such, it is expedient that there is continuous effort in safeguarding unsuspecting users from cyberattacks.

In May 2017, one ransomeware virus caused a loss of USD 8 Billion to industries in finance, healthcare, energy, and universities (Sarker et al., 2020).

Also, in a 2018 report, it was reported that 236 billion emails are exchanged daily, out of which 53.5% are spam emails and the FBI reported a loss of USD 12.5 Billion to businesses due to spamming attack (Karim et al., 2019).

MACHINE LEARNING

Another field of computing that has greatly benefited from the recent technological improvements in hardware and software capabilities is Artificial Intelligence and Machine Learning. Machine Learning is mathematical model that brings meaning to a collection of data.

Machine Learning as a technology has found base in virtually all areas of human life, with major applications in health and medicine, economy and finance, education, entertainment and gaming. Currently, the immediate applications of machine learning range from sorting defective from healthy fruits, identifying ripe and juicy ones, to detecting cancer, to image recognition, recommender systems, fraud detection and even generative models. Simply put, machine learning sifts through a lot of data, identifies patterns that may be obscure to humans, and answers questions by extrapolating from the knowledge it has acquired from the data.

Machine learning is broadly classified into three (3) main types: supervised learning, unsupervised learning, and reinforcement learning. Althought, there are researchers who believe there are more categories, including semi-supervised learning, ensemble learning, multi-task learning, and so on (Mahesh, 2018).

SUPERVISED LEARNING TECHNIQUES

Supervised learning is a class of machine learning in which data is labelled based on its class and a methematical model is trained using this feature-label dataset. The model is then tested with new data, and tasked with the challenge of predicting the label.

Applications include image recognition, language translation, sentimental analysis, speech recognition, text-to-speech systems, and so on.

Supervised learning models can be classified into two (2) based on their general application area:

1) Regression
    - Linear Regression
    - Logistic Regression
    - Polynomial Regression

2) Classification
    - Naive Bayes
    - Decision Trees
    - Random Forest Model
    - Support Vector Machines (SVM)
    - Artificial Neural Networks (ANN)
    - Deep learning: Examples include Convolutional Neural Networks (CNN), Recursive Neural Network (RNN), Deep Belief Network (DBN)

UNSUPERVISED LEARNING TECHNIQUES

While supervised learning models are trained with a lot of human intervention – in the shape of mapping data to their classes or giving some meaning to each data in the set – unsupervised learning is a technique in which its models are not trained in a feature-label pair as seen in supervised learning. It is similar to the activity that goes on in the brain when trying to learn something new without a trainer or instructor (Mahesh, 2018). These machine learning models go through the data they are provided with, and begin to connect the dots, in terms of hidden structure and patterns, hence, clusters begin to develop as data with similar features are identified.

These kind of algorithms are used in recommender systems, to monitor the activity of entities over a period of time and associate other activities with them based on patterns identified. Other applications of unsupervised learning algorithms include generative applications, imaginative reasoning, language modelling, creative writing algorithms, speech synthesizers, etc.

There are three classes of unsupervised learning models:

- Clustering (K-Means clustering, C-Means clustering)
- Association Rules (Decision Trees, Apriori algorithms)
- Dimensionality reduction (Principle Component Analysis, Singular Value Decomposition)

REINFORCEMENT LEARNING TECHNIQUES

Reinforcement learning is a machine learning technique that gives positive rewards to positive traits and actions and gives negative rewards to undesirable actions. This is a technique in which learning is done using an exploration-exploitation approach or in a layman’s term, using trial and error approach (Bi et al., 2019). Over time, the system learns to take more positive actions so as to maximize reward and thus, learning takes place.

MACHINE LEARNING AND CYBERSECURITY

MALWARE DETECTION

Malware (malicious software) is a general term used for a class of software threat that is designed to disrupt the routine and smooth running of computerized systems. This is done by gaining unauthorized access to computer systems or networks in order to gather confidential information for illicit gains, to frustrate network users, or to damage system resources (Naseer et al., 2021).

This software can either be a virus, worm, or a trojan. A virus is a computer program that duplicates itself in the host machine by spreading across multiple files. Worms on the other hand are designed to multiple computer systems by spreading through the nodes of a computer network. A Trojan is an application that feigns its function as a useful program but is intended to capture keystrokes with the intent of identifying key combinations that resemble card details and login credentials, and sometimes, record the screen of the system user so as to forward them to the author of the malware.

Threats from malware has plagued the cyber space for a long time, and as one of the longest standing cyber threats, there has been a lot of research into the detection of malware. Early researches, focused on the use of anomaly-based detection, signature-based detection and heuristic techniques (Aboaoja et al., 2022) were often faced with scalability and operating system compatibility issues as certain operating systems and file systems have been shown to be more susceptible to malware attacks than others (Naseer et al., 2021). Botacin et al equally noted that some challenges and pitfalls exist in the research of malware detection and prevention, some of which are not well defined threat models, lack of proper understanding of what malware research should be all about, too broad or too narrow modelling, and this is typical of traditional detection methods as a proper understanding of the problem is expected before solution can be proferred (Botacin et al., 2021).

With machine learning introduced into malware detection, an intrinsic understanding of how malwares are designed and function may not be needed as the concept of machine learning defeats that challenge. Models are trained with examples of software programs, correctly labelled as malware or not, it is the responsibility of the model to identify salient features with which it distinguishes between the software for future predictions. There have been significant improvements in the success rate in detecting malware using ML – specially, CNN and RNN – over traditional techniques (Al-Mansoori and Salem, n.d.; Varun Shah, 2022).

SPAM DETECTION

Spam is generally referred to as unsolicited attention aimed at irritating, confusing, or luring unsuspecting victims into unwanted and sometimes, ungenuine purchases and subscriptions. They are often sent as emails but other methods exist such as blogs and search engines (Martínez Torres et al., 2019).

Traditional methods of spam detection employed authentication schemes, sender policy frameworks, architectural modifications, and heuristic filtering models, which all had varying performances in spam detection (Shaukat et al., 2020).

Upon applying ML models – such as Artificial Neural Networks, SVM, KNN – to these existing methods, there was nearly 50% improvement in accuracy of spam detection (Karim et al., 2019).

INTRUSION DETECTION

Intrusion detection is a major concern in cybersecurity as one of the ways cybercriminals perpetrate their act is by first gaining unauthorized access.

Traditional techniques based on pattern, rules, heuristics, statistics, have shown that there is still a lot to be desired in terms of performance (Khraisat et al., 2019; Singh and Khare, 2022).

Compared to the other cyberthreats detection, the use of machine learning in intrusion detection is less studied (Xin et al., 2018) but deep learning based intrusion detection systems have shown great potentials, with as much as 94% - 97% detection accuracy (Varun Shah, 2022).

CHALLENGES OF USING ML WITH CYBERSECURITY

1. Cybersecurity-based metrics: While ML has shown improvement in detection accuracy over existing traditional methods, there is a need for new performance metrics by which the performances will be measured.
2. Availability of relevant datasets: Quality and standardized training data which are better suited for cyber threats are needed (Gibert et al., 2020)
3. Technological growth: What has been a blessing over time is also turning out to be a curse; cybercriminals also have access to systems with high computational power, hence, they are also developing newer attacks which defy existing security measures and sometimes elude detection (Bharadiya, 2023).
4. Adversarial attacks: The widespread development of adversarial networks and algorithms makes it possible for cybercriminals to attempt to counter their own attacks under a test environment so as to build more robust attacks.

RECOMMENDATION

In conclusion, having investigated the role of machine learning in cybersecurity threat detection and prevention, it is has been established that there are great potentials and improvements in the implementation.

Considering that cybersecurity is not a purely technical challenge, as there are human factors involved, further research is encouraged, in which more intuitive hybrid models such as the Deep Reinforcement Learning are explored in mitigating some of the persisting threats.

Also, it is important that relevant datasets are developed along with cybersecurity-centric performance metrics to measure their performances.

REFERENCES

Aboaoja, F.A., Zainal, A., Ghaleb, F.A., Al-rimy, B.A.S., Eisa, T.A.E., Elnour, A.A.H., 2022. Malware Detection Issues, Challenges, and Future Directions: A Survey. Appl. Sci. 12, 8482. https://doi.org/10.3390/app12178482

Al-Mansoori, S., Salem, M.B., n.d. The Role of Artificial Intelligence and Machine Learning in Shaping the Future of Cybersecurity: Trends, Applications, and Ethical Considerations 8.

Bharadiya, J., 2023. Machine Learning in Cybersecurity: Techniques and Challenges. Eur. J. Technol. 7, 1–14. https://doi.org/10.47672/ejt.1486

Bi, Q., Goodman, K.E., Kaminsky, J., Lessler, J., 2019. What is Machine Learning? A Primer for the Epidemiologist. Am. J. Epidemiol. kwz189. https://doi.org/10.1093/aje/kwz189

Botacin, M., Ceschin, F., Sun, R., Oliveira, D., Grégio, A., 2021. Challenges and pitfalls in malware research. Comput. Secur. 106, 102287. https://doi.org/10.1016/j.cose.2021.102287

Gibert, D., Mateu, C., Planes, J., 2020. The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. J. Netw. Comput. Appl. 153, 102526. https://doi.org/10.1016/j.jnca.2019.102526

Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K., Alazab, M., 2019. A Comprehensive Survey for Intelligent Spam Email Detection. IEEE Access 7, 168261–168295. https://doi.org/10.1109/ACCESS.2019.2954791

Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., 2019. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity 2, 20. https://doi.org/10.1186/s42400-019-0038-7

Mahesh, B., 2018. Machine Learning Algorithms - A Review 9.

Martínez Torres, J., Iglesias Comesaña, C., García-Nieto, P.J., 2019. Review: machine learning techniques applied to cybersecurity. Int. J. Mach. Learn. Cybern. 10, 2823–2836. https://doi.org/10.1007/s13042-018-00906-1

Naseer, M., Rusdi, J.F., Shanono, N.M., Salam, S., Muslim, Z.B., Abu, N.A., Abadi, I., 2021. Malware Detection: Issues and Challenges. J. Phys. Conf. Ser. 1807, 012011. https://doi.org/10.1088/1742-6596/1807/1/012011

Sarker, I.H., Abushark, Y.B., Alsolami, F., Khan, A.I., 2020. IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. Symmetry 12, 754. https://doi.org/10.3390/sym12050754

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., Xu, M., 2020. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. IEEE Access 8, 222310–222354. https://doi.org/10.1109/ACCESS.2020.3041951

Singh, G., Khare, N., 2022. A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. Int. J. Comput. Appl. 44, 659–669. https://doi.org/10.1080/1206212X.2021.1885150

Varun Shah, 2022. Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. https://doi.org/10.5281/ZENODO.10779509

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., Wang, C., 2018. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access 6, 35365–35381. https://doi.org/10.1109/ACCESS.2018.2836950

Yaseen, A., n.d. The Role of Machine Learning in Network Anomaly Detection for Cybersecurity.