Entrepreneurship in Cybersecurity

Paper

The innovation of technology has made life simpler for entire communities around the world. Many businesses, big or small, and homes across the globe are increasingly adapting the digital way of life. The innovation of technology may have brought forth a more convenient way of living, however people fail to realize that threats are not just physical. Technology has completely changed the way of life including how crimes are being committed, therefore it is imperative that every business and organization incorporate cybersecurity awareness and prevention into their business model and plan. Globally, many companies do not stand a chance of fighting against data loss. This is a major problem because we live in a digitalized world. Cyber crime statistics reveals that over ninety percent of malware is being delivered via email and 43 percent of small businesses are data breach victims. It has also been predicted that the worldwide spending on cybersecurity alone would add up to over $130 billion, with more spending focused on the prevention and effects of the aftermath.

Artificial Intelligence has the capability to mimic cognitive functions of humans. It can simulate human thinking capabilities and behaviors. Machine learning is the subset of Artificial Intelligence which allows machines to learn from data without being explicitly programmed. It enables computer systems to make predictions using historic data and is used in various online recommender systems for email spam filters, google search algorithms, or even the Facebooks friend tagging suggestion. The issue with machine learning is that it only works for specific domains. Deep learning stems from AI and machine learning and has the capability to not only mimic how humans gain certain knowledge but also predict analysis, statistics, and improves when the data size increases.

By creating a sophisticated system that combines unsupervised Artificial Intelligence with a variety of machine learning and deep learning algorithms, industries around the world would have a much greater chance of fighting against cybercrimes and detecting malware early on. Since modern day society is transitioning into becoming little smart cities, “vulnerable actions from an individual or organization can put at entire city at risk” (Chen Ma, 2021). The innovation of AI with ML(machine learning) and DL (deep learning) aims to mitigate such problems in all aspects of the cyber realm within different businesses and organizations. Studies have shown that prior to transitioning to DL, computer systems have been using ML algorithms for malware detection. However, as the use of new technology grows, new and complex variants of malware increased, with most of them going undetected when using the traditional AI machine learning algorithms. Introduction of DL showed promising solutions to the detection of these new and complex variants of malware. Because malware variants are continuously evolving and uses various concealing techniques, the detection and classification become much more challenging therefore the need to tie three different algorithms into one big package is necessary to help mitigate such problems.

The combination of all three – AI with ML and DL algorithms – could help minimize the traffic of malware in a system. Businesses, organizations, and home users will be able to confidently store information on a device with little worries of it ever getting into the wrong hands. Moreover, it can assist various institutions at "various stages in the risk process ranging from identifying risk exposure, measuring, estimating, and assessing its effects."(Ma & Sun, 2021).Since privacy is such an important part of modern society, it is crucial that algorithms, data-mining techniques, and the designs for cybersecurity frameworks are updated and stay parallel to rise of new technologies.

It is imperative to understand that "the first step in overcoming cyber security problems in smart cities and protecting citizens' privacy is to identify cyber security challenges and threats to citizens' privacy." (Chen Ma, 2021). Smart cities need smart government and smart living to succeed. The implementation of unsupervised AI with ML/DL can help make that happen. AI has been used and integrated into different fields like those in the agriculture sector for autonomous trackers and drone monitoring, autonomous vehicles, automated warehousing and supply chain management, and the healthcare sector to improve their productivity and efficiency. AI in cybersecurity, however, is a relatively new ballpark that is still being tested through trials and errors. Although it is relatively new in cybersecurity, research have shown that it can be "used to intelligently tackle the cybersecurity issues" (Sarker et al., 2021) and can also be used "in various problem domains ranging from malware analysis to risky behavior identification that might lead to a phishing attack or malicious code" (Saker et al., 2021). Designing an AI-based modeling system flexible enough to enhance "high performance protection capabilities" (Chen Ma, 2021) prevents any serious incidents that could "lead to disastrous financial, data, credit and loss of public trust" (Chen Ma,2021).

With the number of threats rising each year "original motives for carrying out cyberattacks largely remain unchanged" and cybercriminals becoming more "increasingly sophisticated with their techniques" (Zeadally et al., 2020) the development and integration of AI techniques in the field of cybersecurity and across many application domains "show promise in enabling cybersecurity experts to counter the ever-evolving threat posed by adversaries" (Zeadally et al., 2020). The sophistication of these attacks proves that traditional solutions for cybersecurity have become "inadequate at detecting and mitigating emerging cyberattacks" (Zeadally et al., 2020) therefore updated solutions need to surpass their level of sophistication and stay one step ahead. The rising concerns from cybersecurity experts and researchers that "…conventional well-known security solutions such as antivirus, firewalls, user authentications, encryption etc. may not be effective" (Sarker, 2021) is problematic. However, the use of AI with DL "…can be used to intelligently solve different cybersecurity issues, such as intrusion detection, identification of malware or botnets, phishing, predicting cyberattacks, e.g. DoS, fraud detection, or cyber-anomalies."(Sarker, 2021). Furthermore, "Deep learning has its benefits to build the security models due to its better accuracy, especially learning from large quantities of security datasets." (Sarker,2021).

According to the Department of Homeland Security, “cyberattacks against critical infrastructure” (Lazic, 2019) was reported to have a 383% increase. With the complexity and frequency of cyberattacks, “AI is needed for defense of critical infrastructure systems to protect the public from harm” (Lazic,2019). Utilizing AI to comprehensively analyze a vast amount of data quickly saves a lot of critical time from being wasted. The only issue and limitation of current AI and machine learning is that it must be supervised. Current AI generally “cannot function without human oversight because the technology detects too many false positives and allows too many threats to slip under the radar” (Lazic,2019). Security agencies across the globe need sophisticated algorithms that could detect and protect systems from any attacks. Research and statistics have shown that “…most research focus on the supervised learning of AI to teach an AI how to protect a system against malware and other outside threats.” Furthermore, “the unsupervised learning has been applied in the latest defend system to solve that problem.” (Chan et al, 2019). By implementing unsupervised and predictive AI, threats can be stopped and eliminated before it even becomes an issue.

Cyber criminals love that organizations have turned to technology for everything. From banking to employee data, big and small corporations have become easy targets. Implementing sophisticated AI models could help guard against any sophisticated threats. Discussions of AI is not a new topic in cybersecurity, after-all data is the center of cybersecurity trends. The question is how can integrating sophisticated AI for an added layer of cybersecurity defense? This is something that can not be done overnight. Effectively integrating AI into an existing cybersecurity system requires a lot of “planning, training, and ground preparations to ensure your systems and employees can use it to its full advantage” (Lazic,2019).

The need for adequate research and testing is crucial to the implementation of AI not just in the field of cybersecurity but in other disciplines such as entrepreneurship. “AI holds great promise to transform entrepreneurship into a more relevant and impactful field” (Levesque et al., 2022). If implemented into the field of entrepreneurship, “AI can conceivably change not only the way entrepreneurial enterprises operates (The Economist,2018) but also how entrepreneurship scholars conduct research” (Levesque et al., 2022). Moreover, AI in the businesses of entrepreneurs have been attracting substantial “academic attention” (Levesque et al., 2022) but the use of AI to conduct research by entrepreneurship scholars’ has not.

Implementing sophisticated AI into all systems in various fields will help strengthen security both locally and nationally. The “innovative approach to planning, conducting, and applying entrepreneurship research could help stimulate entrepreneurship theory development and help close the gap between theory and practice” (Levesque et al., 2022). AI in various fields like that of a healthcare sector, has proven that it works. If we take those algorithms and combined them with various machine and deep learning techniques, the result will be far more beneficial for all types of fields. The sophistication of this innovation will not only protect citizens’ privacy but will withstand attacks from all corners of the cyber realm.

According to much research done in the past, AI has and does work in other fields. Corporations have been using sophisticated systems to guard and protect against sophisticated attacks. I am confident that with all the research done, this new implementation of various working algorithms

will work. Just like any innovation, this will need a lot of planning, research, training and testing to make sure it is fully functional. Cybersecurity experts from different countries as well as IT experts from different fields will need to work together to improve national security and the security within the cyber realm. With technology continuously evolving, strengthening the protection against cybercriminals needs to correlate with the rising technology.

References:

L. Chan *et al.*, "Survey of AI in Cybersecurity for Information Technology Management," *2019 IEEE Technology & Engineering Management Conference (TEMSCON)*, 2019, pp. 1-8, doi: 10.1109/TEMSCON.2019.8813605.

Chen Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations", Energy Reports, Volume 7, 2021, Pages 7999-8012, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.124.

LAZIĆ, L. (2019, October). Benefit from Ai in cybersecurity. In *The 11th International Conference on Business Information Security (BISEC-2019), 18th October 2019, Belgrade, Serbia*.

Lévesque, M., Obschonka, M., & Nambisan, S. (2022). Pursuing impactful entrepreneurship research using artificial intelligence. *Entrepreneurship Theory and Practice*, *46*(4), 803-832.

Ma, L., & Sun, B. (2020). Machine learning and AI in marketing–Connecting computing power to human insights. *International Journal of Research in Marketing*, *37*(3), 481-504.

Sarker, I.H., Furhad, M.H. & Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN COMPUT. SCI.* **2,** 173 (2021). https://doi.org/10.1007/s42979-021-00557-0

S. Zeadally, E. Adi, Z. Baig and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," in *IEEE Access*, vol. 8, pp. 23817-23837, 2020, doi: 10.1109/ACCESS.2020.2968045