Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 11, November 2022, pg.1 – 3

Digital Transformation with AI/ML & Cybersecurity

Karthik Trichur Sundaram

Karthikts@hotmail.com

B.Tech in Electrical & Electronics Engineering, MBA Boise State University

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i11.001

Abstract— Artificial Intelligence (AI) and Machine Learning (ML) have impacted the manufacturing industry, especially in the industry 4.0 paradigm. It encourages the usage of smart devices, sensors, and machines for production. Moreover, AI techniques and ML algorithms give predictive insights into various manufacturing tasks, such as predictive maintenance, continuous inspection, process optimization, quality improvement, and more. However, there are many open concerns and challenges regarding cybersecurity in smart manufacturing.

Keywords— ML (machine language) and AI (artificial intelligence), AI/ML in manufacturing, industry 4.0 Cybersecurity, Cyber infrastructure

I. INTRODUCTION

Manufacturing is one of the most critical industries in the world's economy, as it held almost 16% of worldwide GDP in 2019, with an output generation of 13.9 trillion. It's evident that the history of the manufacturing industry has changed drastically over the last few years (Chopra et al.).

The world has plunged into the fourth industrial revolution known as 'Industry 4.0' by encompassing three latest technological trends: artificial intelligence, connectivity, and automation. The goal of industry 4.0 is to automate manufacturing processes to increase sustainability, maximize efficiency, detect system barriers, and better supply chain management.

Apart from it, Industry 4.0 links up with Informational technology (IT) and Operational Technology (OT) to establish a cyber-physical subspace of the Internet of Things (IoT), giving rise to cybersecurity concerns. Undoubtedly, additional connectivity contributes to increased productivity, but it also gives rise to potential cyber threats.

II. BENEIFTS OF AI/ML IN MANUFACTURING INDUSTRY

The benefits of using these technologies can be seen both internally, where they will help companies improve their processes so that they run more efficiently and externally, where they will allow those same companies to compete with larger companies.

From creating new products to eliminating repetitive or time-consuming tasks, AI and ML can help improve manufacturing processes by performing tasks that human workers cannot do. Manufacturers can also use AI and ML to create new products and designs that have never been seen before. The use of these technologies will help manufacturers reduce costs, allowing them to make more money from their products (Zhang, 2020).

Similarly, a training phase is required to scale AI and ML in manufacturing operations before these models can be used in production. The training phase involves creating and deploying models, which are trained on historical data. This training data should include as many relevant variables as possible to ensure that the model can accurately predict future events (Kim et al., 2021).

III. SECURITY CHALLENGES FACED BY THE INDUSTRY 4.0

AI and ML are entirely new factors in the production sector, determining business growth. While artificial intelligence and machine learning seem to be beneficial in the manufacturing industry, these technologies might come up with potential cybersecurity risks and challenges. AI/ML introduced new cybersecurity issues not only to the IT solutions that existed in the plant but also to the operational technology (Haqi Khalid, 2020).

Finding personnel with the required skills to work with these technologies is challenging as the current workforce is not capable enough to work in the technological sector. Lack of knowledge or expertise increases the risk of being compromised. Moreover, data quality is one of the major concerns in today's organization data management. The data must be cleaned and prepared before being utilized as input into business intelligence systems. Poor data compliance gives rise to serious security concerns.

There is a need to understand the gaps in implementing AI and ML in the manufacturing industry. It can be possible with a clear vision of the risks posed to an organization and its assets. To reap the full benefits of industry 4.0, there is a need to perform the following steps (Rahul Rai et al., 2021).

- Detect inherent system vulnerabilities impacting the safety
- Identify risks pertaining to cyberattacks
- Take proactive steps to address potential vulnerabilities to avoid risks.

Analyze the barriers the manufacturing industry is facing in implementing intelligent solutions.

IV. AI AND ML IN MANUFACTURING INDUSTRY

AI has been creating waves in the manufacturing industry for quite a time. However, the early adopters have noticed some enhancements in efficiency and productivity for the trend to continue. The possibilities of this tech leading us to the stars in obvious as to how it is growing in the manufacturing industry can transform traditional procedures with no agency starting garnering outstanding results from artificial intelligence instantly after embracing it. Henceforth, for better and game-changing results, meaningful usage of artificial intelligence is recommended (Haqi Khalid, 2020).

V. CONCLUSION

The manufacturing industry is facing a remarkable shift by leveraging AI/ML techniques. AI systems play a significant role in Industry 4.0 by entirely changing manufacturing methods. With these technological shifts, the need for cybersecurity in industry 4.0 will increase in the future in various infrastructures and in the consumer, area leveraging industrial IoT where physical protection and privacy are significant.

VI. ACKNOWLEDGEMENT

With bigger data pool to analyze and digest, the machine systems use them to shrink the attack surfaces in manufacturing industries via predictive analysis. Its detection might have suspicious attitude but also eases the load on cybersecurity people who must triage such events regularly. Machine learning and artificial learning are not just perfect but can also be called a silver bullet when it comes to cybersecurity defense.

REFERENCES

[1] Chopra, M., Singh, S., Sharma, S., & Mahto, D. (n.d.). *Impact and Usability of Artificial Intelligence in Manufacturing workflow to empower Industry 4.0*. Retrieved October 28, 2022, from http://ceur-ws.org/Vol-3080/4.pdf.

[2] Jianjing Zhang. (2020). *(PDF) Artificial Intelligence in Advanced Manufacturing: Current Status and Future Outlook*. ResearchGate. https://www.researchgate.net/publication/343115882_Artificial_Intelligence_in_Advanced_Manufacturing_Current_Status_and_Future_Outlook.

[3] Kim, S. W., Kong, J. H., Lee, S. W., & Lee, S. (2021). Recent Advances of Artificial Intelligence in Manufacturing Industrial Sectors: A Review. *International Journal of Precision Engineering and Manufacturing*, *23*(1), 111–129. https://doi.org/10.1007/s12541-021-00600-3.

[4] Haqi Khalid. (2020). *Cybersecurity in Industry 4.0 context: background, issues, and future directions*. ResearchGate. https://www.researchgate.net/publication/347939038_Cybersecurity_in_Industry_40_context_background_issues_and_future_directions

[5] Rahul Rai, Dmitry Ivanov, & Alexandre Dolgui. (2021). *(PDF) Machine learning in manufacturing and industry 4.0 applications*. ResearchGate. https://www.researchgate.net/publication/353913778_Machine_learning_in_manufacturing_and_industry_40_applications.

