Security and Ethical Issues to be aware of while using AI for Project Managers [1]

Gopinath Venu

Introduction

Artificial Intelligence (AI) and Machine Language (ML) has been a trending topic in every industry, practices and discipline. It's been used in every field from chatbots to fraud detection, automate the processes, etc. Basically, the prediction techniques these AI tools provide are helpful when there is large volumes of data involved.

In Recent months, Project Managers have been seriously thinking on how to leverage AI for their project management. AI can be a powerful tool for project managers, no doubt about it because we can use AI to automate tasks, make better decisions, and improve communication, and be more efficient, effective, and strategic in our work.

While every organization adapts AI to accelerate the delivery of projects by leveraging these techniques and powerful capabilities, it has a significant risk on what kind of services that we choose to use. It can also bring in Ethics, Security and Privacy Issues if we don't choose the right AI tools.

Simple Analogy

Consider a free email service like google. Will you be comfortable using Gmail if it's not a well secured service. If you are willing to experiment with another email service, we would look for the following features:

- Secure.
- Spam Blocking Capabilities.
- Offer MFA.
- Data stored safely in the cloud.
- Confidential Mode.
- Password protected emails.

[1] How to cite this article: Venu, G. (2023). Security and Ethical Issues to be aware of while using AI for Project Managers, *PM World Journal*, Vol. XII, Issue XI, November.

These are the minimum set of criteria to look for in an email service. Of course, it's a free service but it deals with your own personal data isn't.

Now the question arises, what should Project Managers do to leverage AI in their projects without compromising on the project data? There is no one stop solution for this. AI is still an evolving technology, and it takes some time to do our due diligence to see which AI tool is safe to use for sensitive data.

Background on AI at a very high level in perspective of LLMs

AI tools run on Large Language Models known as LLMs. These LLMs are mostly open source and have immense amounts of data. Every day new AI tools emerge based on customization of their specific use cases and package them into an AI tool that addresses a problem. These LLMs are not going to shrink but keep growing massively. There is no centralized Gatekeeper for these LLMs and no one has any control over it to monitor what goes in and out of LLMs as well as no control over what the LLMs learn from prompts given by end users.

Now the following questions arise,

- How secure are these LLMs?
- What is the probability that my data is being stored in their knowledge base?
- What if my prompt to AI is misused?
- What if Malicious code is injected by bad actors?
- What if LLM has False information injected? (Junk in, Junk out).

The questions and self-doubt go on and on. Therefore, it's important to understand the AI ecosystem and do a Risk Assessment before using an AI tool.

Project Risk Analysis

As Project Managers, we are responsible for the risk analysis process. Using the wrong AI tool in the decision-making process can be detrimental for the overall scheme of things.

Following are some of the trends that's happening in the project world and the implications of using it. Please note that I do not recommend using these AI tools.

Project Requirement Analysis

Business requirement documents are very sensitive for any organization. It does take time to read through all the pages of the document and have brainstorming sessions to get things clarified.

AI tool: ChatPDF, Humata

The AI tools such as ChatPDF or Humata have an ability to skim through all your document pages and summarize it for you. It can even come up with a list of clarification questions that can be asked.

Implications

We do not want to upload a sensitive project document to Chat PDFs/Humata LLM. We don't know how secure they are even though they claim it. There is no secure LLM as of today to provide such a service. Just think about this. What is the Benefit that these Open Source LLMs have in providing such a service.

Resource Allocation & Workflow Planning

Project planning, workflow management and resource allocation are some of the critical areas which need a human touch. Though it could be tempting to use AI tools and could save time, we need to be aware that the AI tool cannot judge things like an experienced Project Manager unless there are some future AI tools which have a Reinforced Learning Capability.

AI tool: Wrike

Implications: In order to use this tool, you have to share sensitive data such as Work streams of your project, task priorities, to-do lists, Gantt charts etc. I have listed Wrike as an example, but there are many tools which automate your workflow. As I said earlier, we don't know how secure these tools are. You do not want your entire Project plan of your organization to go to the wrong hands. Please be mindful of that.

Project Budgeting

Managing Project Budget can be an overwhelming task and it needs meticulous planning, investing more time and energy into it. There are several moving parts to it and nothing can beat human intelligence, at least as of today.

AI Tool: AI Planner

Implications: It's in its early stage and data manipulation could influence conclusions and forecasts.

Now let's see some of the reasons why we should be cautious in using AI tools and we need to do our due diligence in evaluating tools available freely in the market.

Risk of Adversarial attacks

AI Models like ChatGPT are still a black box. These are improving on a daily basis as they are constantly being updated. Someone can tactfully use subtle variations, analyze the response and lead it to unexpected outputs/outcomes.

Risk of Watermark attacks

This kind of attack is to constantly query about a particular subject or entity, asking about things surrounding that subject. Attackers analyze the response and build a model that would trigger the revelation of the code logic.

Risk of Data poisoning

The user will not even recognize if the data model that they are seeing is a real time page or a sequence of snapshots of fake models hosted in a different server.

Conclusion

When the Internet was invented and available to the public several decades ago, the maturity and technology level was primitive in the initial years. Browsers like Netscape Navigator, search engines like direct hit, and Altavista did not sustain, and they no longer exist. AI is still evolving, some models will thrive and evolve, and some models will not. Therefore, new players will emerge to build robust and secure AI models in the near future

by addressing all the security, privacy concerns. Project Managers have to be extremely cautious and evaluate existing AI tools available now after going thru the Pros and Cons of it before they test it out. AI will make the job easier for Project Managers and will help them to get the job done much faster with accuracy just like a Match Referee who benefits from all the new video assistant technology support system/sensors available to analyze and track the game.

About the Author

Gopinath Venu

Texas, USA

Gopinath Venu has about 19 Years of experience in the IT Industry. He is certified in PMP, PMI-ACP from Project Management Institute (PMI), SAFe Advanced Scrum Master Certification from Scaled Agile Institute. He also holds a certification in AWS as a Certified Practitioner and Azure Certified from Microsoft. He has done multiple roles such as Project Manager, QA Manager, Scrum Master in his career. He is an active member of International Toastmasters. He has presented papers in PM conferences organized by local chapters of PMI. He presented a paper on Agile in the 15th Annual PMI Symposium organized by PMI Dallas and The University of Texas at Dallas. He also contributes to articles and discussions on www.projectmanagement.com.