The HCLTech Trends & Insights Podcast

Nick Ismail
Today we're going to be discussing the risks associated with GenAI and how organizations can overcome them. I'm joined by Govind, the practice head for engineering and R&D services at HCLTech. Govind, How are you today?

Govind Chandranani
I'm good. Hi. Thank you, Nicholas.

Nick Ismail
Excellent. Well, let's get into the discussion then. So we're seeing an explosion in AI adoption across different industries and applications. But with such rapid growth, what are the biggest risks organizations face in deploying GenAI at scale?

Govind Chandranani
Okay, before this I'll just cover, the trend I see. I am interacting with GenAI customers for the last two years and I see a shift. It was more POC experimentation and now it is more expectation of output, more projects on the ground in production. And with that, I see lots of risk, but, better I classify [GenAI demand] into some verticals because different verticals have different risks. And there are common [risks] as well. So, the industry which is more consumer based. The main risk I see, privacy, security and also these new chatbots representing actual companies. So hallucination is a risk and when they represent companies, complete accuracy is required. And we have seen the recent examples where somebody asked for a refund from an airline company. And then they [airline company] are saying we will not provide [the refund] that the chatbot committed [hallucinated, was not] based on the policy. So on consumer based industry, I think data privacy and commitment on behalf of company that is the main risk, while on some other verticals like manufacturing or healthcare or deep verticals, there the risk is cost is risk or concern, whatever you say. Second is the accuracy of models. It is not accuracy of response, but accuracy of model. Because end of the day, GenAI even standalone or with combination with the traditional AI [is] kind of black box. So companies in healthcare or manufacturing or legal firms, they want to double click or they want to see whether, these models are doing what they want based on policies. So that reliance plus cost is another risk for such companies.

Nick Ismail
Sure. And unlike traditional software, GenAI models don't produce deterministic outputs. How does this change the way we should approach testing and quality assurance? Are existing QA methods still relevant?

Govind Chandranani
Not fully. So there is a good mindset change required when you validate, GenAI versus here older traditional systems because yes, as you said, it is not deterministic. That means you have to create prompts to break the system. If I take example of simple chat bot, even simple chat bot, and so you need a mindset, different mindset, then you need more knowledge base to generate right prompt which map to Responsible AI [principles] or your functionality context of that domain and performance. So knowledge base is more required in case of this. Maybe in pyramid you need more knowledgeable people. Then GenAI testing cannot be [handled] like total manual testing. Otherwise it will mislead to these systems. That means you should be enabled by different platforms where you can make it little objective by matrices like accuracy, toxicity and hallucination index and all that. And then, GenAI is about data. If your data is biased, your system will be biased. If your data is not new you will not get the correct [output]. That means continuous validation is more important or super important in this case. So need of continuous validation, need of the platform and tools and changing of mindset. All three important elements.

Nick Ismail
Absolutely. And with this new mindset, a new topic in GenAI and AI has emerged, which is all around trustworthy and Responsible AI. But what does that really mean in practice? What are the pillars of trust when it comes to generative systems?

Govind Chandranani
I think that is so everybody talking about transparency, trust, accountability and other aspects, I will take a practical example. Suppose you are asking chatbot sample whether I will get refund for this or not. And if, your chat bot is based on recent experience or recent memory, saying, yes, you will get it. That means your chatbot is not accountable enough. That is one second is if you are in a complex system, if you are getting, results and you are not getting, how it is arriving to these results as a model owner, or as a business owner, that means it should be more accountable. It should be more transparent. It should be more trustworthy. So these are the practical element I see becoming more important on GenAI.

Nick Ismail
And there have also been a rise in regulations like the EU, AI acts and NIST AI risk management framework. How should enterprises approach AI governance given these regulations? And is there a compliance burden, or should it be more viewed as a competitive advantage?

Govind Chandranani
I think yeah, that's the important point. See, you have to see, two points. One, your internal policies. And then second, your, like legal compliances, whether it is EU or ISO. So based on your, like location or based on your domain, you can pick the right, legal compliance standard. And also you have to merge with your, your organization policies, and then you have to govern on continuous basis. And for that, two things are important. How you are doing, the continuous governance of that. Second, how you are actually closing the loop with your, model designer or app Application owners. That loop closure is important because practically there is a chance of data drift or there is a chance of model drift. And there are chances of, Because of data, You are not hundred percent reliant, aligned to, these, legal compliances.

Nick Ismail
And explainability is something that's been around for a while as a as a target for organizations adopting AI. And now GenAI as solutions. How important is it with GenAI systems, especially when decisions or outputs impact customer or carry reputational risk?

Govind Chandranani
I think that is becoming more and more important. I see this as a buzz, but after GenAI, I and everybody knows by [now] with so much of confidence GenAI component can give inaccurate response. So I'll take one example. Suppose you are creating, hardware, new hardware, and you are using generative design. That means I'm asking GenAI. Okay. I need to develop this component of this weight, under this temperature, under this cost, under this dimension. And suppose GenAI is generating, that component for me. And then, then GenAI I'm using for, simulation before it gets approved. And then, in working I am validating using GenAI generated data. Now, as there is a cost involved, there is a decision making involved. It is important, the how part as well, which is explainability and that means you have to see at a algo level, what is the decision making, what is the traceability happening in the background. What is the justification for where GenAI arrived at? And believe me, even, developer or designer, they don't know in which direction actually it will go or [how] it will get executed. That means technically and by function also, it is important the important stakeholders see the explainability.

Nick Ismail
HCLTech recently launched AI Force and joined the Responsible AI Institute to address many of these challenges and support business outcomes. Can you walk us through these and explain how they're helping us and our clients not just meet standards, but redefine them?

Govind Chandranani
I'll, again, take example. Or maybe it is sort of our journey, but when we started, validating our governing GenAI component, initially we used to create prompts manually. We used to create prompt by different practices, manually or by the AI principal manually. And then we were hardly, or we were doing manual monitoring. So that means, there is a system, required, which generates prompts, thousands of prompts very quickly, gives you very objective matrices. So every validation or assembly thinking in a similar way and make it very objective. And then you need a continuous monitoring system for your GenAI component. And then also it should be integrated with systems where you get more explainability, or you can use lots of template, to reuse, certain items. All those capabilities be bundled in a system and created that to enable validation engineers or LLM Op engineers or developer SME, so they get a very objective data. So there is an improvement in accuracy. There is improvement in objectivity. Also in future they get the external operability, attainability, view as well. So that's the system we have created and we are expanding further.

Nick Ismail
Govind, Thank you very much for your insights.

Govind Chandranani
Thank you. Thanks, Nicholas.