Journal of
Telecommunications & System management

Abstract

Making AI Safer through identificaiton and remediation of AI Risks Across Security, Ethics, Transparency, Compliance and Other Pillars

Murai Rao & Kashyap Murali
Founders – SigmaRed Technologies Inc.

Abstract:

100 Billion Dollars. That's how much AI spending is projected to rise to in a mere 3 years. With such rapid investment in a next-generational technology, its safety becomes of heightening concern to everyone that comes in touch with it from customers to vendors alike. Questions about the AI models safety across any potential security risks, particular bias towards a minority group, a lack of transparency in the decision-making process, or compliance violations from the AI environment are raised, and don't have a proper answer. These questions don't just apply to a specific vertical but it's domain-agnostic and ensuring that a businesses AI is safe is what will set them apart from their customers. This talk will explore what AI safety is, why we need it, and how to ensure that one's AI model is safe both technically and procedurally.

Biography:

Kashyap is a published AI and Deep Learning Researcher and patent author who has performed AI internships from ed-tech startups to multi-billion dollar firms to NASA. He's also presented a demo on Deeply Inclusive AI at the United Nations AI for Good Global Conference at Geneva, Switzerland, as part of IVOW, and at a TEDx Conference in Cape May where he presented on cultural AI. He was the Dean of the Princeton School of AI where he taught over 780 students in the local community and had 18,000 students across 152 countries as part of his online AI course.

Murali has 22 years of experience in cybersecurity practice and consulting, technology compliance, management controlling, IT, and ERP implementation. He has designed and developed AI-enabled cybersecurity solutions. He has also trained more than a thousand professionals in AI. He brings in a critical mix of strong cybersecurity consulting, AI-enabled cybersecurity, and business expertise, all of these critical for our mission of making global AI Safer.

Publication of speakers:

1. Ritz, A. 2020. Real-time Tools for Teaching English [Computer Software]. http://www.realtimetools.co.uk/
2. X. Schmitt, S. Kubler, J. Robert, M. Papadakis and Y. LeTraon, "A Replicable Comparison Study of NER Software: StanfordNLP, NLTK, OpenNLP, SpaCy, Gate," 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS), Granada, Spain, 2019, pp. 338-343.
3. The Bullock Committee report, Her Majesty's Stationery Office, London, 1975.
4. George A. Miller (1995). WordNet: A Lexical Database for English. Communications of the ACM Vol. 38, No. 11: 39-41.

Citation: Murai Rao & Kashyap Murali, Making AI Safer through identificaiton and remediation of AI Risks Across Security, Ethics, Transparency, Compliance and Other Pillars; Robotalks 2020; October 05, 2020; 4:30PM IST