Security and Trustworthiness in Scientific Computing

Xinghua Mindy Shi, Temple University, mindyshi@temple.edu.

In scientific computing and high performance computing (HPC), one of the top priorities is to provide, maintain, and sustain the security and trustworthiness of software and data in various domains of science and technology. With the advent of Artificial Intelligence (AI) and Machine Learning (ML), the security, integrity, and trustworthiness of software and data becomes even more pressing toward the realization of AI-powered science. Here, several key components of secure and trustworthy systems for AI in science are listed as below.

Security: With the ever-growing data in various scientific domains, it is critical to develop, deploy and dissemination of software in support of secure storage, transfer, and analysis of such massive datasets. Modern AI methods rely heavily on a large amount of data to train or learn, and thus the security of data should be considered at various levels such as raw data, pre-processed data, augmented data, integrated data, intermediate results, results, meta-data, tracking and log data. Moreover, AI methods including deep learning models are notoriously sensitive or susceptible to adversarial attacks. Hence, it is increasingly crucial to provide software that not only produces secure AI/ML models but also verifies or evaluates the security of these models and the underlying data.

Privacy: The privacy and confidentiality of scientific data is important in that the sharing and analysis of such data may incidentally disclose private information about data owners. Software and tools are in great need to protect and evaluate if and how data privacy is preserved. Integrative analysis of multiple datasets has increased the possibility of privacy leakage, since combining multiple sources of data and meta-data can potentially disclose private or sensitive information through techniques like linkage attacks. In the meanwhile, the adoption of AI-based analytics especially deep learning based technologies, has posed new challenges in assessing or preserving the privacy of data since privacy leakage may only be disclosed when data is analyzed (instead of before or when the data is collected). Privacy preserving technologies including differential privacy and cryptographic solutions are needed to be widely evaluated and deployed in different scenarios to evaluate their effectiveness in preserving the privacy of scientific data and AI/ML models.

Fairness: Data biases can be cryptical that may be encoded in the data or analytics, which make it hard to be identified or addressed. It is thus desirable to develop software to identify and evaluate the sources of biases in data. If biases are inevitable, methods and tools should be developed to identify and address these biases as early as possible in the life cycle of data generation and analysis. Regarding AI and ML models, it is also crucial to develop software centered around the transparent and fair AI/ML. Biases introduced in data collection and modeling can thus be well handled and informed. Relevant ethics, guidelines and policies will also be incorporated with software developed to ensure their implementation.

Provenance: In scientific computing, data and models need to be managed effectively. The ability to automatically collect and manage data provenance is thus a necessary component of HPC systems. While AI/ML models are becoming primary methods in scientific data analytics, researchers need to effectively manage these complex models in a similar way to data management. Therefore, it becomes critical to provide software systems that efficiently

manage and maintain the provenance of both scientific data and AI models at various granularities. New software and tools need to be developed and deployed to provide an easy-to-use provenance management system for AI-based HPC solutions.

Integrity: In addition to quality control of scientific data during the full life cycle, it is yet another essential problem to provide integrity guarantee of data. The integrity of data and AI/ML models should be robustly verified and successfully achieved across the full spectrum of data and models. Software systems should be developed to verify and audit the integrity of data and models at various layers.

In summary, the components listed above are necessary to support new generations of scientific discoveries powered by AI/ML technologies and big data in science. However, research in these areas is usually conducted in silos with little interaction among each other. Additionally, education and training of next-generation scientists in these areas are isolated in separate scientific domains and sub-domains. Therefore, it is of pressing need to develop integrative and cross-disciplinary plans to promote and support the education and training that bridge across diverse expertise in cybersecurity, privacy, ML/AI, databases, computer systems, HPC, scientific computing, data analytics, and ethics.