TechXplore

Researchers create verification techniques to increase security in AI and image processing

April 29 2024

Credit: Pixabay/CC0 Public Domain

A team of researchers from the Institute IMDEA Software, Universidad Carlos III de Madrid and NEC Laboratories Europe has introduced a novel framework that promises to improve the efficiency and practicality of verifiable computing.

The research, detailed in the paper "Modular Sumcheck Proofs with Applications to Machine Learning and Image Processing" and presented at the last ACM (Association for Computing Machinery) conference on computer and communications security, addresses the scalability and modularity challenges faced by both general proof systems and solutions tailored to specific applications in artificial intelligence and image processing.

Verifiable computation comprises a family of cryptographic techniques that provide an unforgeable guarantee that some third party, such as a company or a cloud server, has performed correct processing of a user's data. Proving that an image or a video has been edited, that a prediction made by artificial intelligence comes from an audited model, or that only customer-provided data has been used in a creditworthiness decision are some examples of what these techniques enable. In addition, verifiable computation is compatible with data privacy, so that, for example, the algorithms used by the server in the calculation are kept confidential.

Verifiable computation provides integrity, fairness and privacy, essential properties in applications that outsource data processing tasks. Within the possible solutions, there are general proof systems, such as those used in some blockchain, which have scalability problems when dealing with computations with large amounts of data. On the other hand, solutions designed specifically for these applications are more efficient, but often incompatible with each other, making it difficult to scale them up or integrate them into larger data processing chains.

The study

Researchers have introduced a new framework aimed at bridging this gap by combining the performance advantages of custom solutions with the versatility of general-purpose test systems. At its core is a modular approach to verifiable computation of sequential operations, which is based on a new cryptographic primitive known as VE (Verifiable Evaluation Scheme).

The researchers demonstrate the practical application of their framework in artificial intelligence by proposing a novel VE adapted to convolution operations, capable of handling multiple interconnected input and output channels.

"Our protocol can be easily integrated into a data processing chain to enable full verification of, for example, predictions made by convolutional neural networks (CNNs), which are the basis of most artificial intelligence models," says David Balbás, Ph.D. student at IMDEA Software and researcher of this study.

In addition, the paper also presents new VEs for image processing, which allow efficient verification of editing or retouching, including operations such as cropping, blurring, rescaling and other more complex operations.

The team has produced a prototype application of its testing systems that is a significant improvement on existing techniques. "Our benchmarking shows that our proofs are five times faster to generate and ten times faster to verify than the best existing solutions so far, in addition to introducing theoretical innovations in the algorithms," explains Damien Robissout, research programmer at Institute IMDEA Software and also co-author of the study.

These results not only improve the efficiency and scalability of cryptographic proof systems but also open up new possibilities for ensuring the integrity, fairness and privacy of data processing tasks in various applications of artificial intelligence and image processing.

"Nowadays, this approach is essential in the field of application we are considering, because a technological advance is not such if it does not merit the trust of end users," says another of the study's authors, Maribel González Vasco, Professor of Excellence in the UC3M Department of Mathematics.

The application generated in the study is open source and its modular nature paves the way for its extension and integration into various tools within a data processing chain. In this way, the researchers clear the way for versatile and robust deployment of verifiable computation in applications as diverse as financial ethics, personal data protection or artificial intelligence regulation, among others.

More information: David Balbás et al, Modular Sumcheck Proofs with Applications to Machine Learning and Image Processing, *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (2023). DOI: 10.1145/3576915.3623160

Provided by IMDEA Networks Institute

Citation: Researchers create verification techniques to increase security in AI and image processing (2024, April 29) retrieved 18 May 2024 from https://techxplore.com/news/2024-04-verification-techniques-ai-image.html