Deloitte.
Insights

Keeping AI private: Homomorphic encryption and federated learning can underpin more private, secure AI

These emerging technologies for safeguarding the data used in AI applications are available and effective today. Now, the challenge is to make them more practical

Duncan Stewart, Ariane Bucaille, and Gillian Crossan

HOMOMORPHIC ENCRYPTION (HE) and federated learning (FL) are two different but related technologies that aim to solve the same problem: How can AI tasks such as machine learning be performed more privately and securely? Deloitte Global predicts that, driven by the increasing urgency of this issue, the combined market for HE and FL will grow at double-digit rates in 2022 to more than US$250 million. By 2025, we expect this market to top US$500 million.[1]

The safer data is, the more widely AI can be used

HE and FL, part of a group of technologies known as privacy-enhancing technologies (PETs),[2] are tools to make AI more private and secure. HE allows machine learning to use data while it is encrypted; all other machine learning needs to decrypt the data first, making it vulnerable. FL distributes machine learning to local or edge

devices rather than keeping all the data in the same place where one hack could expose it all, which is the case with centralized machine learning. They are not mutually exclusive: HE and FL can be used at the same time.

The major driver for growth in the HE/FL market is the burgeoning demand for more private and secure approaches to AI. Everybody knows that AI is a key technology in many industries, but multiple players are now focusing on privacy and security as never before. Companies that were using AI are looking at HE and FL as a way to reduce future risk. This is particularly true of cloud companies using AI, since data needs to be transmitted to and from the cloud and processed off-premise, both of which introduce potential privacy and security issues. Regulators are regulating AI in new ways,[3] and HE and FL may allow companies to better comply with those regulations. Very large markets, especially health care and public safety, are highly sensitive to AI's implications for privacy and security, and they are beginning to investigate HE and FL to address these concerns.

Regulators are regulating AI in new ways, and HE and FL may allow companies to better comply with those regulations.

Both HE and FL are relatively new technologies, and both are more complex than traditional AI solutions. Each, though effective, comes with drawbacks. Computing with HE is slower than computing with unencrypted data; FL requires more powerful processors on edge devices as well as fast, highly reliable connectivity between the core hardware in data centers, where the main AI software resides, and the edge, where the learning happens. ("Edge" in this case could refer to a device such as a smartphone or an appliance sitting a few hundred meters from the robots in a factory, for example).

The barriers are lower now than they were a few years ago, however. For one thing, Wi-Fi 6 and 5G wireless technologies, with their increased speed and reliability, are becoming more widely available, which makes relying on edge devices more practical. Some providers are also making HE and FL easier to use by releasing open-source tools to make the process more accessible to non-experts.[4] But the real gains in practicality are coming from improvements in processor cost/performance. While HE used to be a trillion times slower than unencrypted computing, it is now, in some cases, only 20% slower as a result of new specialized processors.[5] Similarly, the edge processors needed to power FL are becoming more powerful as well as cheaper and more widely deployed. Full HE is currently processor-intensive, and significant advances in HE-optimized processors could dramatically decrease its time and cost.[6]

We normally don't bother with predictions about technologies that are as small in dollar terms as HE and FL. Why are we making an exception? Part of it is that the two technologies are sitting at a crossroads. Regulators globally are beginning to craft AI-specific rules, and although GDPR has been around since 2016, it was not the final word in privacy regulation: New rules on the topic come out monthly, and GDPR enforcement may be ratcheting up to a new level. Because of these regulations, both vendors and users are likely to see that using AI will get more difficult in a growing number of jurisdictions and industries. And HE and FL could help companies meet those regulatory requirements, significantly expanding their opportunities to use AI.

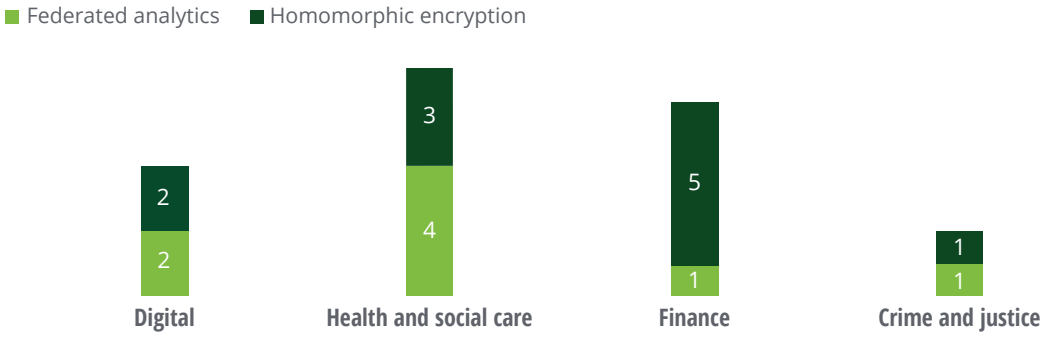
The other major reason we're talking about HE and FL now is who is using them. According to a recent repository of PETs, there are 19 publicly

announced pilots, products, and proofs of concept for homomorphic encryption and federated analytics (another term for federated learning) combined. That doesn't seem like a lot … but the companies offering them include Apple,[7] Google, Microsoft, Nvidia, IBM, and the National Health Service in the United Kingdom, and users and investors include DARPA, Intel, Oracle, Mastercard, and Scotiabank. Also, the industries involved in these early projects are among the largest. Use cases are led by health and social care and finance, with their use in digital and crime and justice also nontrivial (figure 1).[8]

FIGURE 1

HE and FL are attracting attention from some of the world's largest companies and industries

Distribution by sector of publicly announced pilots, products, and proofs of concept for homomorphic encryption and federated analytics



Source: Deloitte analysis of data from the Centre for Data Ethics and Innovation's "Repository of use cases," accessed September 30, 2021.

THE BOTTOM LINE

With some of the largest companies in the world embracing HE and FL, organizations interested in the privacy and security of sensitive data should continue to monitor these and other PETs, even though most are unlikely to find HE or FL immediately useful in 2022. Those most interested will likely be:

- Cloud providers and cloud users[9]
- Organizations in particularly sensitive industries such as health care, finance, and public sector, especially crime and justice
- Companies that want to share and compare data with competitors, but without exposing "crown jewel" intellectual property
- Chief information security officers and their teams

As with other emerging technologies such as quantum computing (discussed elsewhere in *TMT Predictions 2022*), organizations exploring HE and FL can do several things to plan for what likely lies ahead:

Understand the industry impact. What repercussions could PETs, including HE and FL, have on one's own industry as well as adjacent industries? What would more private, secure AI mean from a strategic, operational, and competitive standpoint? To understand this, leaders should keep abreast of the technology's progress, and they should monitor how peers, competitors, and ecosystem partners are investing in and experimenting with it.

Create a strategy. Organizations should convene appropriately knowledgeable people to develop a PET strategy. For now, the strategy may well be to do nothing, but leaders can prepare for the future by identifying a trigger event—such as a competitive or technological development—that signals the need to begin or increase investments and exploration. Someone should be put in charge who has the skills, knowledge, and organizational status to execute the strategy when the time comes.

Monitor technology and industry developments. The HE and FL strategy should evolve as the state of the technology and market changes. Leaders should adjust the strategy to reflect these changes and be sure not to allow their trigger event to pass by without acting on it.

Bring cyber inside earlier. Cybersecurity is often only brought into AI processes during the deployment phase. Instead, companies may want to pull cyber in earlier, at the same time as when they are using HE and FL. This more collaborative approach between AI and cyber is likely to enhance both privacy and security while minimizing transparency and accountability risks.

Privacy and security technologies, including HE and FL, are tools, not panaceas. But while no tools are perfect, HE and FL are valuable additions to the mix. By helping to protect the data that lies at the heart of AI, they can expand AI to more and more powerful uses, with the promise of benefiting individuals, businesses, and societies alike.

Endnotes

1. Reportlinker, “Federated learning solutions market research report by application, by vertical—Global forecast to 2025—Cumulative impact of COVID-19,” press release, May 14, 2021; MarketWatch, “Homomorphic encryption market size forecast 2021–2027,” August 2, 2021.
2. Holger Roth, Michael Zephyr, and Ahmed Harouni, “Federated learning with homomorphic encryption,” NVIDIA Developer blog, June 21, 2021.
3. See companion piece, “Prediction on AI regulation.”
4. Sergio De Simone, “Google open-sources fully homomorphic encryption transpiler,” InfoQ, June 29, 2021; Flavio Bergamaschi, “IBM releases fully homomorphic encryption toolkit for MacOS and iOS; Linux and Android coming soon,” IBM Research Europe, June 4, 2020; Dennis Fisher, “Microsoft open sources SEAL homomorphic encryption library,” *Decipher*, December 3, 2018.
5. Roth, Zephyr, and Harouni, “Federated learning with homomorphic encryption.”
6. Scientific Computing World, “Optical accelerator enables fully homomorphic encryption,” August 25, 2021.
7. *Keeping AI private: Homomorphic encryption and federated learning can underpin more private, secure AI* is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc.
8. Centre for Data Ethics and Innovation, “Repository of Use Cases,” accessed October 6, 2021.
9. TechTarget, “Homomorphic encryption,” accessed October 6, 2021.

About the authors

Duncan Stewart | Canada | dunstewart@deloitte.ca

Duncan Stewart is the director of research for the Technology, Media & Telecommunications (TMT) industry for Deloitte Canada. He presents regularly at conferences and to companies on marketing, technology, consumer trends, and the longer-term TMT outlook.

Ariane Bucaille | France | abucaille@deloitte.fr

Ariane Bucaille is Deloitte's global Technology, Media & Telecommunications industry (TMT) industry and also leads the TMT practice and the TMT Audit practice in France. She has more than 20 years of experience and is a chartered and certified public accountant.

Gillian Crossan | United States | gicrossan@deloitte.com

Gillian Crossan is a principal in Risk & Financial Advisory, Deloitte & Touche LLP, and leads the global technology industry sector. She has been with Deloitte for more than 25 years and has worked across sectors including energy, health care, consumer products, and technology.

Acknowledgments

The authors would like to thank **Lukas Kruger** for his contributions to this chapter.

Deloitte's Technology, Media, and Telecommunications (TMT) group brings together one of the world's largest pools of industry experts—respected for helping companies of all shapes and sizes thrive in a digital world. Deloitte's TMT specialists can help companies take advantage of the ever-changing industry through a broad array of services designed to meet companies wherever they are, across the value chain and around the globe. Contact the authors for more information or read more on www.deloitte.com.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Junko Kaji, Preetha Devan, Prodyut Ranjan Borah, Rupesh Bhat, Arpan Kumar Saha, Ribhu Ranjan, Emma Downey, Nairita Gangopadhyay, Blythe Hurley, and Aparna Prusty

Creative: Jaime Austin, Sylvia Yoon Chang, Govindh Raj, Sanaa Saifi, and Rishwa Amarnath

Audience development: Maria Martin Cirujano

Cover artwork: Jaime Austin