How Companies Can Utilize AI and Quantum Technologies to Improve Cybersecurity

The next revolution in data privacy is coming. Be ready.

March 19, 2021 4 min read

Opinions expressed by *Entrepreneur* contributors are their own.

In this digital-oriented world, hackers are evolving in parallel to technological advancements. Fortunately, engineers, mathematician and physicists are simultaneously working on innovative concepts that harness the progression of classical encryption methods. New devices are utilizing principles of quantum physics and deploying sophisticated and powerful algorithms for safe communication.

Related: Platform With International Community Adopts Quantum Computing For Humanity

What is cryptography?

Cryptography is a means of securing data and information to dodge malicious hackers. Thanks to cryptographic methods, everything from web conferences to individual browsing history remain privileged and safe. Data are protected using algorithms that require a unique key for decryption and encryption. Utilization of the same private key, i.e. a specific string of bits for decryption and encryption, is called symmetric cryptography. Utilization of public keys for encryption and private keys for decryption – each of which are

created by algorithm-fueled random number generators – is called asymmetrical cryptography.

Genuine randomness is considered unachievable by purely classical means, but can be accomplished with the added application of quantum physics.

Quantum key distribution

There are two methods by which large-scale quantum and classical computers can obscure private information.

Quantum key distribution (QKD) is a quantum cryptographic primitive designed to generate unbreakable keys. QKD ensures key agreement, including well-known BB84 and E91 algorithms. In 2017, a Chinese team successfully demonstrated that satellites can perform safe and secure communications with the help of symmetrical cryptography and QKD.

Still, it’s clear that QKD alone can’t satisfy all protection requirements, but there are other mechanisms for security enhancement by utilizing “quantum-safe” encryption algorithms based on solving mathematical problems instead of laws of quantum physics.

An optimistic view of quantum-computing obstacles

The most immediate challenge is accomplishing the most sufficient number of fault-tolerant qubits to boost quantum computing’s computational promises. Tech giants such as Google, Amazon, IBM and Honeywell are taking this problem under consideration and investing in it to come up with a solid solution.

Currently, quantum computers are programmed for individual quantum logic gates. This might be acceptable for small-scale

quantum computers, but less so once we come across a large number of qubits. Organizations such as IBM and Classiq are developing more and more abstract layers in the programming stack, allowing developers to nurture incredible and powerful quantum applications to provide solutions to real-world problems.

For the implementation of complex problems including error-correction schemes, organizations need to prove that they can control numerous qubits. This control must have low latency and it must come from adaptive-feedback control circuits based on CMOS. Ultimately, the issue of “fan-out” must be addressed. The question that needs to be answered is how to pace up a number of qubits within a quantum chip. Multiple lasers or control wires are currently required, but it’s hard to see how we can develop multiple qubit chips with millions of wires connected to the circuit board or coming out of the cryogenic measurement chamber.

Applying quantum computing to cybersecurity

In recent years, researchers and analysts have been striving for the development of quantum-safe encryption. According to American Scientist, the United States National Institute of Standards and Technology is presently evaluating 69 new methods known as “post-quantum cryptography,” or PQC. Quantum computing offers an eminent, potential solution to cybersecurity and encryption threats. Any security-forward organization ought to develop an understanding of crypto agility.

Related: AI For Cybersecurity: Maximizing Strengths And Limiting Vulnerabilities

Quantum revolution is uncertain. While the intense impact of extensive fault-tolerant quantum computers may be far off,

near-time quantum computers still present enormous advantages in enhancing levels of communication privacy and security. All organizations must consider developing innovative strategies around the long-term benefits and risks of quantum technology and computing, and be ready for the forthcoming quantum revolution.

https://www.entrepreneur.com/article/367167