NATIONAL SECURITY AND AEROSPACE NEWSMAGAZINE
FORCE

Books | Technological Vulnerabilities

Quantum computing may render currently used cryptographic techniques obsolete. An extract

Ajay Singh

There are many who believe that blockchain technology could be the ultimate solution for cybersecurity. Blockchains are also set to become the cornerstone of Web 3.0. The role of blockchain technology in maintaining distributed ledgers and creating trust in an ecosystem that it is lacking in or needs high levels of trust is crucial. The relative success of blockchain technology in the context of building a secure ecosystem for cryptocurrencies is often cited to illustrate how the technology ensures data integrity, auditability and availability.

The financial services industry was among the early adopters of blockchain technology, but adoption by other industries has been slower than expected. The primary reasons for this are related to the technology's inherent features such as low scalability, complexities in technology design, interoperability, the lack of standardization and talent availability. Nevertheless, other features like immutability, transparency and distributed ledgers all lend themselves to help solve cybersecurity issues. Security experts are optimistic that blockchain technology will redefine the way many business processes, workflows and organisational supply chains function along with addressing regulatory and compliance requirements.

Beyond the hype, it is reasonable to expect that blockchain technology can go mainstream across industries given the overwhelming operating advantages like business continuity, strong cybersecurity and resilience.

Quantum Computing and Cybersecurity

Quantum computing represents a revolutionary change by unleashing computing power of a magnitude that will radically alter the dynamics of information technology as it exists today. The basic unit of quantum computing is the qubit, which can be considered similar to a bit that processes information in traditional computing. A bit can exist in only one (binary) state at a time, either zero or one, a qubit can be in both zero and one at the same time.

The characteristic property of a qubit to be in a superposition (the principal which states that a quantum particle can exist in two distinct locations at the same time) gives it the ability to exponentially speed up computing operations, as well as to hold and process enormous amounts of information. It is expected that quantum computing will help solve large and complex problems through a combination of mathematical modelling and phenomenal computing power such as weather forecasting, drug discovery and traffic management and optimization across several fields. The concept of quantum entanglement, which refers to the ability of quantum particles to correlate their measurement results with each other, enhances the time to process between qubits, enabling tasks such as quantum cryptography, superdense coding (a form of secure quantum communication) and teleportation (the transfer of quantum information from a sender at one location to a receiver some distance away).

The battle for achieving quantum supremacy is underway between the world's leading companies such as IBM, Google, Honeywell and Amazon and even some countries which are making their own efforts in this space. Quantum supremacy is said to be the threshold or point where a quantum computer can solve a computational task which a traditional computer cannot complete within a reasonable time. Google's Sycamore, a 54-qubit superconducting processor, achieved this in 2019, by calculating in 200 seconds what could take present-day supercomputers over 10,000 years to complete. The University of Science and Technology of China has also claimed that their quantum processor could complete in 200 seconds a task that would have taken as many as 600 million years to complete with traditional computers.

While these breakthroughs represent an exponential leap in processing power, capabilities to handle and much larger data sets and execute machine AI and ML algorithms at much faster speeds, we are not likely to see quantum computing make a significant impact before the year 2030.

How does all this add up in the context of cybersecurity? Does the entry of quantum computing have an impact on how cybersecurity is implemented today? Cybersecurity experts are concerned that one of the key areas where cybersecurity will be affected by quantum computing is that it could render currently used cryptographic techniques obsolete. This poses a significant threat to cybersecurity, requiring us to effect changes in the way we encrypt date. We may find ourselves in a position where we cannot wait for quantum computers to start breaking our encryption but must move quickly to explore new ways of encrypting data that could withstand the impact of quantum computing. Experts are of the opinion that encryption algorithms such as the Diffie-Hellman key exchange, RSA encryption and elliptic curve cryptography are quantum-breakable and other encryption techniques such as lattice-based cryptography, code-based cryptography and multivariate cryptography can be considered quantum-secure.

There is a high degree of excitement and anticipation about the introduction of quantum computing and the benefits it can provide, and companies around the world are building different cybersecurity solution that leverage quantum technologies for key distribution, quantum random number generation, quantum-resistant

cryptography, and more. It is important for organizations to evaluate the potential impact of quantum computing with regard to cybersecurity and incorporate the use of technologies that can boost their cybersecurity in the near term and make them resistant to quantum-technology-leveraged cyberattacks in future.

INTRODUCTION TO CYBERSECURITY: CONCEPTS, PRINCIPLES, TECHNOLOGIES AND PRACTICES

Ajay Singh

Universities Press (distributed by Orient Blackswan Pvt Ltd), Pg 304, Rs 595