HOW CAN EMERGING QUANTUM COMPUTING BECOME A THREAT TO EVERY DIGITAL SYSTEM?

Ruxshona Farxodova
Student at Specialized Secondary School №1 in Almalyk City
ruxshonafarxodova568@gmail.com

Abstract: The paper provides an overall outlook on the potential of quantum computing in the near future and its threats to information security. The defensive measures have been addressed, and the next steps have been analysed.

Key words: supercomputers, quantum environment, supercomputational.

Introduction.

The 21st century has become an era of technological innovation that has shaped the world in ways unlike those of the last 200 years of revolution. It started with digital transformation in the 20th century and has reached the highest level of digitalisation in history. However, even the digital era, at its peak, is being surpassed by the next transformation in the tech world: quantum computing and engineering. Many scientists, and even most startups, are apparently focused on quantum transformation, though estimates suggest it will be achieved within the next 10-15 years. This kind of supercomputational quantum environment will enable many complex tasks to be solved immediately, whereas they would take years or even centuries with bit-run digital computers. So, as the features change, what about information security when supercomputers aim higher than what we have now? Will it help to strengthen or destroy the security?

The potential power of quantum computing.

Quantum computing is a new and revolutionary technology that can improve many sectors due to its capabilities, as Gill and Buyya (2024) suggest. The next decade can be a big win for sectors such as defence, drug manufacturing, finance, and chemical engineering (Gills and Buyya 2024). Its power mainly enables researchers to discover complex theories and ideas by using algorithms run on qubits, thousands of times faster than many other traditional supercomputers. The statements above already show the supremacy of quantum computing. Additionally, it can be developed and used in urban areas to monitor cameras and traffic lights, and even make them more precise. It will also enable high-performance AI by boosting it and contributing to robotics and automation.

Today's classical cryptography vs quantum.

As many can embrace quantum power, there is a high risk of its misuse. Since the beginning of the digitalisation era, cryptography has developed to address traditional computer threats, and cryptography systems such as RSA and ECC have been developed. These encryption tools supported many public key exchanges and have therefore been used worldwide to date. Nevertheless, there is a more powerful and faster threat, such as Shor's or Grover's algorithm, against classical and hash cryptography systems, which enables easy hacking of both protection tools, as Eboseremen et al. (2023) mention. These algorithms are a problem for all sectors, as they affect all financial services, government databases, and, especially, AI used by billions globally.

Actions against upcoming threats.

On the other hand, measures are being implemented to ensure the security of all information technology systems. Cybersecurity is one of the cornerstones of everyone's security. One of the solutions to quantum threats is to use lattice-based cryptography, in other words, post-quantum cryptography (Eboseremen et al. 2023). Another post-quantum cryptography system is code-based cryptography, which is being designed for use in communication. There are even more such systems, but they all need to be developed and deployed properly before quantum computing takes hold.

Conclusion.

The technology is getting advanced and revolutionised day by day. Quantum lovers are already writing the next expected transformation. Therefore, another aspect of the development should focus on its safety as well. Although cryptographic systems might cause operational problems due to their complexity, this at least ensures safety. Because operational loss will definitely be less than the real potential threat posed by quantum supercomputing, the developed countries in this case will be rushing to adopt safety measures soon.

REFERENCES

1. Eboseremen, B.O., Okare, B.P., Aduloju, T.D., Kamau, E.N. and Stephen, A.E. (2023). The future of quantum computing: A review of potential impacts on the IT industry. *International Journal of Multidisciplinary Research and Growth Evaluation.* https://doi.org/10.54660/.IJMRGE.2023.4.3.1164-1174
2. Gill, S. S., & Buyya, R. (2024). Transforming research with quantum computing. *Journal of Economy and Technology.* https://doi.org/10.1016/j.ject.2024.07.001