Chapter 75
Post-Quantum Security Measures for the Internet of Things

Ilgın Şafak
https://orcid.org/0000-0002-2788-7276
Fibabanka R&D Center, Istanbul, Turkey

Fatih Alagöz
Boğaziçi University, Computer Engineering Department, Istanbul, Turkey

Emin Anarim
https://orcid.org/0000-0002-3305-7674
Boğaziçi University, Electrical & Electronics Engineering Department, Istanbul, Turkey

ABSTRACT

The internet of things (IoT) has been used in a wide range of applications since its emergence, including smart cities, intelligent systems, smart homes, smart agriculture, and healthcare. IoT systems rely on information processing and sharing, where data leakages may jeopardize their security and privacy. On the other hand, quantum computers are poised to solve complex problems that traditional computers cannot. However, due to the fact that the majority of cyber algorithms are based on significant computational complexity, quantum computing poses a substantial threat to the cyber security of global digital infrastructure, including IoT networks, smart cities, banking, and intelligent infrastructure. This chapter discusses potential security and privacy measures for a post-quantum world against threats posed by quantum computing, including post-quantum cryptography, quantum software testing, post-quantum blockchain technology, and architectural considerations for creating post-quantum secure IoT systems.

INTRODUCTION

Since its emergence, the Internet of Things (IoT) has been utilized in a wide variety of applications, including smart cities, intelligent systems, smart homes, smart agriculture, healthcare, banking, etc. The collection, processing, and sharing of information are vital for the successful operation of IoT systems. The leakage of these data can adversely affect privacy in the IoT networks. Cyberattacks on IoT net-

DOI: 10.4018/978-1-6684-7366-5.ch075

This chapter published as an Open Access Chapter distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

works include data theft, sniffing, botnet attacks like Mirai, distributed denial of service (DDoS) attacks, malicious code injection, reprogram attacks, and access control attacks. A rigorous testing process is needed in order to quantify the level of risk associated with the deployment of IoT devices in various applications. However, it is difficult to develop a unified strategy for IoT security because a wide range of technologies and platforms are used. Since the security of IoT devices can significantly increase their energy consumption, it is simply not possible to implement security measures on some devices due to a lack of computing power and/or memory. Therefore, it is critical to identify possible threats and then implement appropriate countermeasures tailored to the specific requirements of the IoT system (Lin, et al., 2017) (Fouladi, Ermis, & Anarim, 2022).

In parallel with this development, quantum computing gained considerable attention. According to the industry trade publication, The Quantum Insider, approximately 600 companies, more than 30 national laboratories and government agencies around the world are developing quantum computing technology. Among these companies are US based tech giants such as Amazon, Google, Hewlett Packard Enterprise, Hitachi, International Business Machines (IBM), Intel, and Microsoft, as well as the Massachusetts Institute of Technology, Oxford University, and Los Alamos National Laboratory. A number of other countries have made significant investments in quantum computing technologies, including the United Kingdom (UK), Australia, Canada, China, Germany, Israel, Japan, India and Russia. It is projected that the global quantum computing market size will reach USD 4,375 Billion in 2028 from USD 866 Million in 2023, at a compound annual growth rate of 38.3% (Markets and Markets, 2022). Some companies already released their first quantum computers for commercial use (D-Wave, n.d.) (IBM, n.d.) (Microsoft, n.d.) (Quantinuum, n.d.). Quantum computing can be potentially used in industries such as pharmaceuticals, healthcare, manufacturing, cybersecurity, banking and finance, as well as for tasks such as integer factorization and simulations (Markets and Markets, 2023).

Traditional computers utilize electrical impulses to encode data in bits 1s and 0s. A quantum computer, on the other hand, uses subatomic particles, such as electrons or photons, to calculate. These particles can exist in more than one state (i.e., 1 and 0) at the same time (superposition) with quantum bits (qubits) (see Figure 1). This enables quantum computers to perform a variety of computations simultaneously. Moreover, quantum entanglement links the states of qubits, allowing instantaneous influence over large distances. This allows quantum computers to perform extraordinarily complex tasks. As a result of quantum superposition and entanglement, computational capabilities have been vastly enhanced, offering solutions to previously insurmountable problems.

Quantum computers have no memory or processor, since they are structured merely of superconducting qubits, and process information differently compared to classical computers. Qubits are used in quantum computers to run multidimensional quantum algorithms. Unlike a bit, which can exist in one of two states, a qubit can exist in multiple states. Therefore, as more qubits are added, the processing power of quantum computers increases exponentially, whereas the processing power of classical computers increases linearly as more bits are added. Therefore, quantum computers represent a significant advancement in computing capability over traditional computers, and have the potential to provide large performance gains in specific applications. For example, a quantum computer can solve a problem in minutes that would take a classical computer thousands of years to solve (Kim, et al., 2023). Another example would be the combinatorial problems that can be easily solved using quantum computers, e.g., to break encryption codes.

Quantum computing has ground-breaking applications including quantum cryptography, drug discovery, climate modeling, machine learning (ML), material design, speech and image recognition, fault

42 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/post-quantum-security-measures-for-the-internet-of-things/340024

Related Content

Information Privacy, Cultural Values, and Regulatory Preferences
John H. Benamati, Zafer D. Ozdemirand H. Jeff Smith (2021). *Journal of Global Information Management (pp. 131-164).*
www.irma-international.org/article/information-privacy-cultural-values-and-regulatory-preferences/277186

Open Educational Resources for Improving the Visualization and Reasoning Cognitive Process: A Way to Learn Math
Claudia Orozco (2021). *Information Technology Trends for a Global and Interdisciplinary Research Community (pp. 134-156).*
www.irma-international.org/chapter/open-educational-resources-for-improving-the-visualization-and-reasoning-cognitive-process/270003

After the Command Economy: Russia's Information Culture and Its Impact on Information Resource Management
Elia V. Chepaitis (1994). *Journal of Global Information Management (pp. 5-11).*
www.irma-international.org/article/after-command-economy/51243

Investigating the Usage of IoT-Based Smart Parking Services in the Borough of Westminster
Guochao Peng, Paul David Clough, Andrew Madden, Fei Xingand Bingqian Zhang (2021). *Journal of Global Information Management (pp. 1-19).*
www.irma-international.org/article/investigating-the-usage-of-iot-based-smart-parking-services-in-the-borough-of-westminster/274065

Can E-Government Serve as a Tool for Public Authorities to Manage Public Resources More Efficiently?
María Del Rocío Moreno-Enguix, Laura Vanesa Lorente-Bayonaand Ester Gras-Gil (2019). *Journal of Global Information Management (pp. 122-135).*
www.irma-international.org/article/can-e-government-serve-as-a-tool-for-public-authorities-to-manage-public-resources-more-efficiently/226218