Chapter 4
Security and Privacy Aspects Using Quantum Internet

Nilay R. Mistry
https://orcid.org/0000-0001-5683-3499
Gujarat Forensic Sciences University, India

Ankit Y. Dholakiya
Gujarat Forensic Sciences University, India

Jay P. Prajapati
Gujarat Forensic Sciences University, India

ABSTRACT

Quantum internet is an innovative approach to secure communication. Quantum internet is the next revolution in technology that enables the devices to perform operations that are beyond the classical internet. Quantum internet with quantum cryptography is one of the best solutions for secure data communication. Quantum internet uses the fundamental laws of quantum physics, which make it secure against sophisticated network attacks. In this research, the authors described quantum cryptography, which enhances the secure transmission over quantum internet using cryptographic protocols. These protocols use random bits transformations, which prevent attackers to make out the patterns of random bits transformations. Also, they introduced the conceptual OSI model for quantum internet, which makes it easy to understand the working of the quantum internet at different layers. Quantum internet can be implemented in intelligence network, satellite communication, critical infrastructure, etc. This can mark a significant change in secure communication.

I. INTRODUCTION

The Internet is the collection of networks that uses Internet Protocol suite for communication as well as a nice medium to connect with the entire world. However, this Classical Internet is vulnerable to Eavesdropping, Masquerading, and Sniffing of data. Due to such vulnerabilities like this, the Classical

DOI: 10.4018/978-1-7998-6677-0.ch004

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Internet is not safe from sophisticated Cyber Attacks. So, to overcome these vulnerabilities it is a necessity to develop a network that is more secure as compared to the Classical Network. Quantum Internet is a novel approach for communication as well as securely access the Internet. The development of Quantum Internet is inspired by the concept of Quantum Computing and the vulnerabilities exist in the Classical Internet. Quantum is the smallest amount of entity that can be excitation of quantized wave or field, as a photon and also it could be used as a physical entity in an interaction. This interaction is possible with the help of Quantum bits which are also known as Qubits. So, a Qubit is a unit that is used to measure Quantum Information. To transfer Quantum Information over Quantum Channel an approach is used called Quantum Teleportation. This can be achieved through entanglement of photons / information which is known as swapping of information / photons, in simple terms. The phenomenon of entanglement forms the basis of a quantum internet. There are some fundamental differences between a future quantum internet and therefore the internet that we see today. Stephanie Wehner said that two quantum bits are often 'entangled' Such entanglement is sort of a connection this is often very different to things for classical link layer protocols where we typically just send signals. therein case, there's no sense of connection inbuilt at a fundamental level. (Quantaneo, 2019)

Quantum Internet may be able provide reasonable level of security by utilizing the mentioned terms and principles. In this chapter we will cover each of the above-mentioned topics as well as introduced OSI reference model for Quantum Internet which will be helpful to understand the Quantum communication flow. The basics of the quantum communication based on Quantum physics principles which are "Heisenberg Uncertainty Principle" and "No cloning theorem" are well explained in this chapter. The goal of Quantum internet security can be achieved through Quantum cryptography, which have been described here as an essential element of securing Quantum communication which will overwhelm weakness into the classical internet. Although a fully comprehend quantum network is still a far-off vision, recent breakthroughs in transmitting, storing and manipulating quantum information have convinced some physicists that a simple proof of principle is imminent. (Anathaswamy A., 2020)

A. Quantum Bit

Quantum bit (or Qubit) is a unit that represents Quantum information on Quantum Internet. The term "qubit" was introduced by Ben Schumacher in a "intriguing and valuable conversations" with Bill Wootters paper published in 1995. (Whurley, 2017) There is the number of elemental particles like electron or photon that can be used in Quantum Computer and their charge represents 0 and/or 1 which are known as Qubit. In the Classical Internet, the Classical bit has two possible states, either 0 or 1 at a time. On the contrary, the Quantum Internet possesses two states of Qubit, 0 and 1 simultaneously. So, two Qubits can contain information about four states. In general, the state of a Qubit is described by:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Where α and β are probability amplitudes and can in general both be complex numbers and ψ is Qubit.

This type of phenomenon of Qubit known as a state of superposition. Quantum Information can be in a variety of forms such as (i)The Polarization State of Photon, (ii) The Spin of an Electron and (iii) Excited State of an Atom.

18 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/security-and-privacy-aspects-using-quantum-internet/272365

Related Content

An Area-Efficient Composite Field Inverter for Elliptic Curve Cryptosystems
M. M. Wongand M. L. D. Wong (2014). *Multidisciplinary Perspectives in Cryptology and Information Security (pp. 218-237).*
www.irma-international.org/chapter/an-area-efficient-composite-field-inverter-for-elliptic-curve-cryptosystems/108032

Secure and Privacy Preserving Keyword Search over the Large Scale Cloud Data
Wei Zhang, Jie Wuand Yaping Lin (2016). *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security (pp. 200-215).*
www.irma-international.org/chapter/secure-and-privacy-preserving-keyword-search-over-the-large-scale-cloud-data/153077

Efficient Implementation of Digital Signature Algorithms
Sumathi Doraikannan (2018). *Algorithmic Strategies for Solving Complex Problems in Cryptography (pp. 78-86).*
www.irma-international.org/chapter/efficient-implementation-of-digital-signature-algorithms/188514

Future Blockchain Technology for Autonomous Applications/Autonomous Vehicle
Arnab Kumar Show, Abhishek Kumar, Achintya Singhal, Gayathri N.and K. Vengatesan (2021). *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles (pp. 165-177).*
www.irma-international.org/chapter/future-blockchain-technology-for-autonomous-applicationsautonomous-vehicle/262701

Blockchain Technology: A Review of the Contemporary Disruptive Business Applications
Tarek Taha Kandil, Shereen Nassarand Mohamed Taysir (2019). *Architectures and Frameworks for Developing and Applying Blockchain Technology (pp. 86-109).*
www.irma-international.org/chapter/blockchain-technology/230192