Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3426811, 8 pages
https://doi.org/10.1155/2022/3426811

Research Article

Secure Data Transmission Using Quantum Cryptography in Fog Computing

Cherry Mangla,[1] **Shalli Rani**,[1] **and Henry Kwame Atiglah**[2]

[1]*Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab 140401, India*
[2]*Department of Electrical and Electronics Engineering, Tamale Technical University, Ghana*

Correspondence should be addressed to Henry Kwame Atiglah; hkatiglah@tatu.edu.gh

Received 26 November 2021; Accepted 3 January 2022; Published 22 January 2022

Academic Editor: Muhammad Asghar Khan

Fog computing's idea is to bring virtual existence into objects used on a daily basis. The "objects" layer of fog architecture is also known as the smart object layer (SOL). SOL has provided the fog network with a strong platform to outperform. Although the fog architecture decentralizes data, uses more data centers, and collects and transmits it to adjacent servers for faster processing in fog networks, it faces several security challenges. The security problems of fog computing need to be alleviated for the exploitation of all benefits of fog computing in classical networks. This article has addressed the security challenges in fog computing, potential solutions via quantum cryptography, a use case portraying the importance of quantum cryptography in fog computing along future scope, and research directions.

1. Introduction

In the continuous evolution of the computer age, increased demand for Internet of Things (IoT) devices and the cloud has requested a middleware. To cater to the request, fog computing has emerged to provide fast and secure services. Fog computing's idea is to bring virtual existence into objects used on a daily basis. The "objects" layer of fog architecture is also known as the smart object layer (SOL). SOL has provided the fog network with a strong platform to outperform. Although the fog architecture decentralizes data, uses more data centers, and collects and transmits it to adjacent servers for faster processing, it faces several security challenges. The security problems of fog computing need to be alleviated for the exploitation of all benefits of fog computing and IoT in classical networks.

It has extended the cloud-based framework to the edge of the structure by increasing data transformation and decision making on IoT fog devices and allowing more effective communication with mediator nodes. Fog computing has extended the cloud architecture by using fog nodes (FN) on the edge of the network. It has integrated IoT and cloud concepts to provide various characteristics like low latency and location awareness, support for geographic distribution, end device mobility, the capacity of processing a high number of nodes, wireless access, real-time applications, improved quality of service, and heterogeneity [1, 2]. Fog servers act as mini data centers for various applications such as smart cities, big data analysis, and distributed data collections.

Although all these characteristics are prominent in fog computing, security is rising as one of the most gigantic challenges for it. Some current solutions in the context of cloud architecture may address some of the security problems. However, security is still one of the main concerns while collecting and processing data from various sources, and the most popular way to tackle it is data encryption. With the advent of differently distributed frameworks like cloud computing, IoT, and fog computing, securing ubiquitary computation that involves many collaborations is considered an open research area that has attracted the attention of researchers to develop novel protocols. Existing security protocols include Transport Layer Security (TLS), Secure Socket Layer (SSL), and Internet Protocol security (IPsec). Recent works primarily focus on the challenges and solutions of fog computing to safeguard data

from various threats. Consequently, quantum cryptography has begun to replace the traditional methods of encryption for enhanced data security [3, 4].

Quantum computing (QC) is a way that provides a new approach to computation over classical computing. The laws of quantum mechanics provide power to QC over classical systems. Quantum cryptography is one of the branches of QC, responsible for the secure transmission of data from one point to another. Although researchers are working on all the fields of quantum cryptography to make it work, right now only Quantum Key Distribution (QKD) is the part that is providing quantum security over classical networks in securing key exchange. The quantum channel being provided by QKD is safe from all types of attacks (classical adversary and quantum adversary). In QC, the processing is more fast and secure. QC is working on the laws of real parallel computing. Quantum cryptography is difficult to breach because it operates on both states (1 and 0) at the same time. In quantum cryptography, photons keep on spinning, which means they keep on changing the position, making the qubits dynamic in nature. Consequently, the problem of intrusion is avoided on a large scale with quantum cryptography. It can be used to secure the fog architecture where data of heterogeneous devices is gathered and processed, while increasing the transmission speed of data by having data centers in various parts of the city. In this paper, we are proposing the use of QKD for secure key exchange in fog computing architecture.

The rest of the paper is organized as follows: in the second section, we discuss fog computing architecture; next, in the third section, security attacks on the fog architecture's different communication layers (as discussed in Figure 1) are discussed. In the next section, solutions for fog computing security issues in quantum cryptography are discussed along with the importance of using quantum cryptography over classical cryptography, followed by a use case in Section V, illustrating the importance of secure and fast data transmission in the case of healthcare along with open research challenges in Section VI. Lastly, the article is concluded with the future scope.

2. A Brief Introduction to Fog Computing Architecture

Fog computing is a highly virtualized platform, and it is not a substitute for cloud computing. It provides storage, computation, and networking services between conventional cloud data centers and end devices. Fog computing architecture is a distributed computational framework that expands the cloud computing model by shifting data processing closer to end devices. It results in low system response, by reducing the time taken by the huge data transmission traveling from devices to cloud and vice versa in IoT. Fog architecture as shown in Figure 1 is a three-layer architecture. The first layer is composed of end devices of IoT (known as end-users), the second layer of fog architecture consists of FN and fog services known as the fog layer, and the third layer is comprised of cloud data centers. The core layer of fog architecture works as a gateway between FN and the cloud. It has dedicated interfaces to communicate with the fog layer. Fog layers can have multiple numbers of FNs to interact with end-users and to process the related information. The FN can be small cell base stations with proper storage, cellular base stations with processing capability, and Wi-Fi access points which can be placed on fixed locations (such as high buildings and roadside units) or mobile things (such as buses and trains).

In the given architecture, the core layer of the network has software-defined networking (SDN) nodes that accurately supervise the network and has extensive governance. Before transmitting the data of end devices of the bottom layer to the cloud, fog computing eliminates all potentially bad and ambiguous contents to reduce the load of the cloud. This is where security challenges arise and can make the transmission vulnerable. The main reason for the vulnerable security attacks is the direct interaction of the fog computing layer with heterogeneous devices. A strong and novel mechanism is required to mitigate this challenge. In subsequent sections, we have summarised all the popular attacks on various layers of fog architecture. In Section IV, solutions to all these attacks in QKD are mentioned after discussing, in brief, the importance of quantum cryptography over classical cryptography in the future.

3. Attacks on Network Communication Layers of Fog Computing

Various attacks on three layers (mentioned in Figure 1) are as follows.

3.1. Cloud Layer. It is the uppermost layer of fog architecture. It is comprised of the workings of both the physical layer and the data link layer. It consists of many sensing technologies, for instance, radio-frequency identification (RFID) tags, wireless sensor networks (WSNs), and near-field communications (NFCs), which all contribute towards building IoT infrastructure [5, 6]. The cloud layer has the following security challenges:

(a) *Node capturing*: node capturing changes or destroys the identification of physical objects which are part of IoT.

(b) *Spoofing*: hackers change the sensed data which ultimately changes the digital signals.

(c) *Denial of service (DoS)*: transmission of data to the upper layer for network transmission and processing is denied.

3.2. Edge Layer. It consists of the workings of network and transport layers. It receives the data from the cloud layer and transfers it to the fog server to process it further. A massive amount of data is generated by day-to-day objects, in which data is processed using various network technologies, such as LANs, WANs, and transmission mediums like Wi-Fi, Bluetooth, and Zigbee. The security challenges faced by the edge layer are as follows:

(a) *Selective forwarding*: in selective forwarding, data packets are selectively dropped or blocked by malicious nodes.

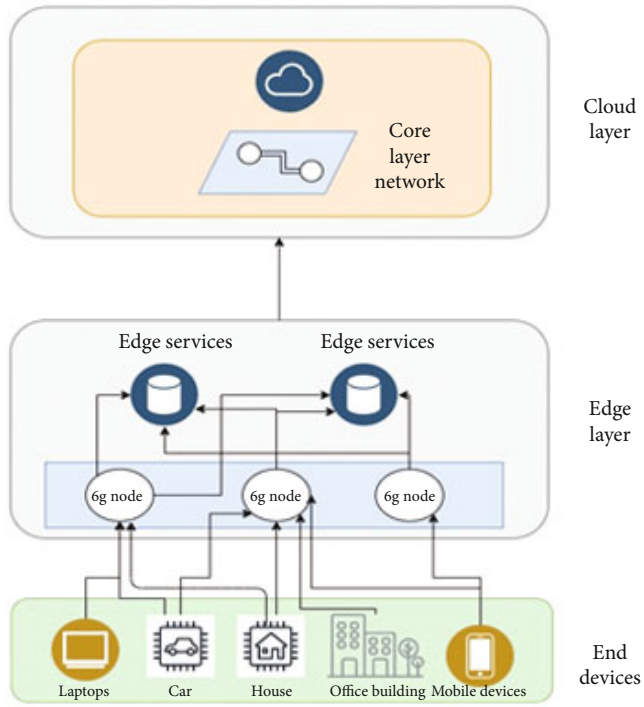

Figure 1: Fog computing architecture.

(b) *Blackhole*: false routing information is created, and all the data packets are forwarded to that address.

(c) *Wormhole*: false storage information is given to bits of data during relocation.

3.3. End Layer. The end layer consists of two parts: (a) user and (b) business layer aspects. Various applications are being differentiated using various IoT application deployment platforms [7, 8]. Security attacks faced by the end layer are as follows:

(a) *Sniffers/loggers*: personal information (like passwords and credit/debit card details) is extracted by attackers using sniffing.

(b) *Phishing attack*: credentials are accessed using the email address of the main authority, through which data can be damaged.

(c) *Node identification*: every phase of the application has a different set of users; attackers gain illegal access by harming the application.

(d) *Distributed DoS*: single system is attacked using multiple infected systems.

4. Mitigation of Fog Computing Security Issues in Quantum Cryptography

Fog computing is used as an extra layer to provide an advantage between the IoT devices and the cloud layer. It helps to reduce the load on the cloud because processed data is transmitted to the FN. There are many challenges at the fog layer in terms of security and reliability of transmitted data due to direct transmission with end devices. Here, we are proposing the use of quantum cryptography's QKD as a solution to secure it from classical as well as quantum adversaries. In subsection A, we are illustrating the importance of QKD over classical security schemes, and the B subsection is showing various QKD protocols that can be used to mitigate various above-mentioned attacks.

4.1. Importance of QKD Over Classical Cryptography. A few major differences between the classical and the quantum cryptography are illustrated in this subsection. Fog computing is an emerging technology that plays a major role in future applications. So it is necessary to secure it from classical as well as quantum adversaries. Public key cryptography schemes are easily breakable using quantum computers as shown by Shor in 1994 [9]. Also, all the classical algorithms are venerable to quantum cryptography [10]. In [11], the authors have proposed the use of blind quantum computing in fog architecture, making it feasible to merge quantum with fog computing. In this article, we have proposed the use of the QKD scheme in fog architectures to secure it against attacks in the near future. Table 1 illustrates the major differences between classical cryptography and quantum cryptography.

(a) *Fundamental dimension*: in classical cryptography, there is no such principle by which it can be defined whether the network is eavesdropped or not, whereas in quantum cryptography, two devices share correlated states; if an intruder tries to eavesdrop at any point, the state of the photon instantly changes providing more security.

Table 1: Comparison of classical cryptography and quantum cryptography.

	Classical cryptography	Quantum cryptography
Fundamental dimension	In classical cryptography, an eavesdropping attack cannot be detected as the number of keys keeps increasing every 18 months on average.	In quantum cryptography, it is easy to detect eavesdropping due to principles of quantum mechanics; minimum changes are required, i.e., it incurs less cost.
Commercial dimension	Classical cryptography can be implemented on small hardware.	Quantum cryptography is in the infant stage and requires a lot of work to shrink on small hardware.
Application dimension	Security is provided through factors of large numbers in classical cryptography.	Shor's algorithm has proven that factors of any large numbers can be easily found, leaving classical cryptography insecure.
Technological dimension	Can transmit data to any length	Quantum cryptography has only achieved a maximum of 4600 km.

(b) *Commercial dimension*: although classical cryptography is more scalable than quantum in recent times as not all the channels are made of optic wires when quantum computers will be on the market, it will be necessary to secure classical networks instead of changing the whole.

(c) *Application dimension*: most of the classical cryptography schemes are based on the factorization of the two highest prime numbers, which can be easily calculated with parallel computing of quantum principles. Shor has proven it in 1994. So all the classical cryptography schemes are vulnerable to the future of computing.

(d) *Technological dimension*: in this field, recently, quantum cryptography is lacking as classical cryptography can provide security to any length, whereas quantum cryptography has achieved the maximum of 4600 km distance [12].

In article [13], the authors have compared the performance of various block ciphers (DES (Classical and Quantum), TDES (Classical and Quantum), Blowfish (Classical and Quantum), AES (Classical and Quantum)) and the Avalanche Effect based on encryption time, decryption time, and throughput for various file sizes from 100 kb to 600 kb. Their experiments are clearly showing the better performance of quantum cryptography. They have used the BB84 protocol of QKD for comparison. Figure 2 shows the results of the throughput with various file sizes of all four schemes in both classical and quantum key exchanges.

4.2. Quantum Key Distribution: A Solution to the Fog Computing Security Threats. Machines that are based on quantum mechanical principles (superposition and entanglement) are known as quantum computers. The quantum computer can process numerous combinations of ones and zeros at the same time at a very high speed, which is termed parallel processing, making its working more complex than traditional systems and helping to easily compute the security algorithms based on mathematical computations. Therefore, it is hard to breach the key distribution performed using quantum mechanics principles. QKD is the only cryptographic scheme of quantum cryptography that can be performed on classical systems to provide a more secure key exchange. Other cryptographic schemes are mentioned by many researchers [14], but only QKD feasibly works over classical networks.

Security threats of authentication in the fog layer can be mitigated with the help of QKD. In the various critical applications of IoT such as smart health, smart grid and smart industries, etc. authentication and privacy are the major challenging issues. End Layer works as a front face in the fog hierarchy. Where the main security issue is authentication. Due to the user interface its security issues and solutions are a bit different from other layers. For data transmission, it is very crucial to secure the Edge layer, as the whole data is stored and processed on the edge layer. It is necessary to secure the data, keeping in mind the CIA model (confidentiality, availability, and integrity). Major attacks on this layer are DoS and eavesdropping.

The cloud layer of the fog hierarchy is also known as end devices. Various technologies are used to collect data from various devices like WSN, RFID tags, and NFC. Because of the heterogeneous data of IoT devices gathered in the fog layer, security becomes a crucial aspect even in fog computing.

In Figure 3, at the different layers of fog hierarchy, we have shown the potential threats and their solutions in the form of quantum cryptography protocols. The properties on which the protocols are working are also discussed adjacent to the solutions.

The following is the description of various attacks on different layers of fog architecture (Figure 1).

4.2.1. Security Solutions in Cloud Layer. The security issues in the cloud layer of fog architecture can be resolved via quantum computing's property "Superposition." Using the superposition property of quantum computing, data can be kept safe. It changes the position of qubits when intruders try to read the data. This property is used in following QKD protocols to mitigate security threats in the cloud layer of fog computing.

(a) *BB84*: a secure channel is established between sender and receiver, using polarized photons to mitigate authentication issues in fog computing [15].

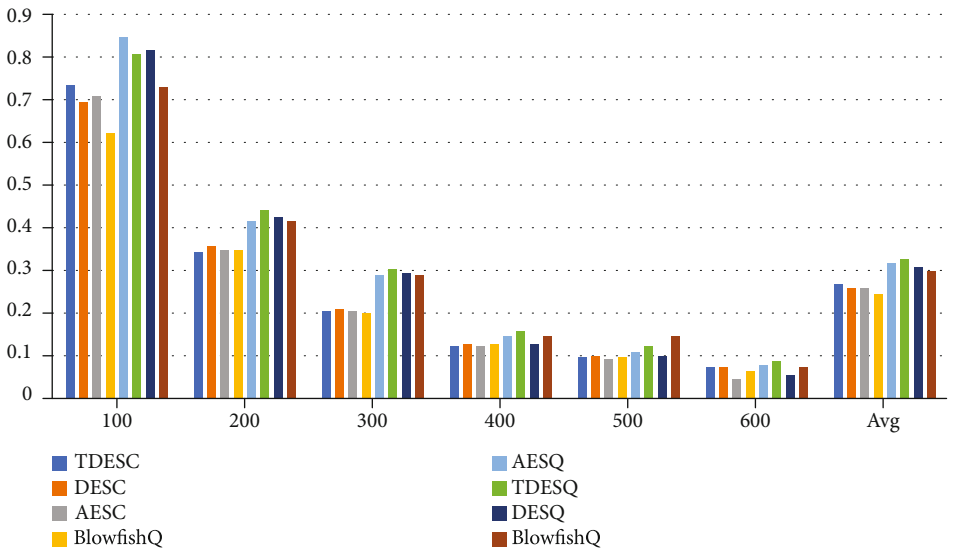

Figure 2: Throughput with different file sizes [13].

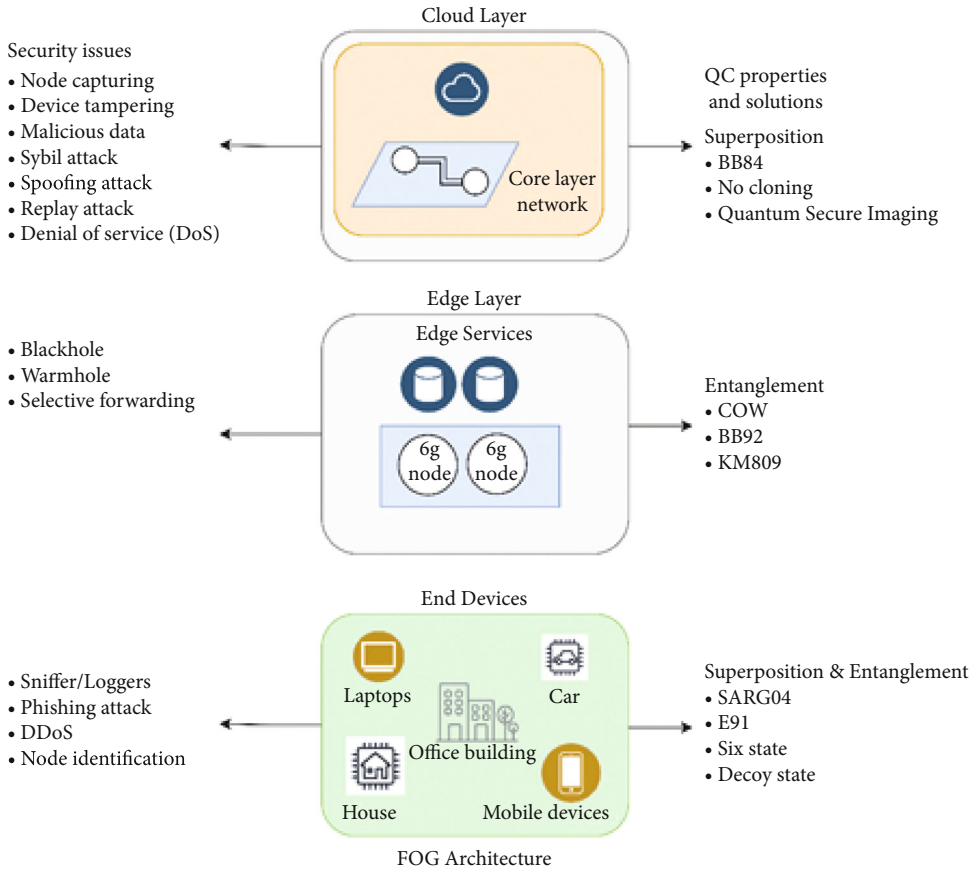

Figure 3: The security threats and solutions using quantum cryptography classification in fog computing.

(b) *No-cloning theorem*: in QC, no-cloning theorem never let copy data, copying data is one of the main issues of fog networks, i.e., adding fake nodes by copying data. As photons travel from one place to another, they keep on changing their positions.

(c) *Quantum secure imaging*: this is used to secure the layer from signal jamming.

4.2.2. Security Solutions in Edge Layer. To secure the edge layer, protocols based on quantum entanglement can be helpful. Secoqc QKD network, KMB09, photon spinning, COW protocol, and BB84 are these properties. No one can access the data when entanglement-based protocols are used on the edge layer of fog computing. Quantum annealing is a way to find the best solution for problems having multiple variables. Current quantum computers can only implement quantum annealing [16, 17], a subset of a quantum computer. Although only quantum annealing can be implemented, it embeds the properties of both quantum superposition and quantum entanglement. The following protocols are based on these properties:

(a) In Secoqc, QKD's maximum number of keys is generated and stored. These are used according to the traffic on the network. In this, it will help in the selective forwarding issue [6]

(b) COW (coherent one-way) protocol works on the principle of quantum entanglement. It transmits the data at the speed of light

(c) The KMB09 protocol works on the Heisenberg uncertainty principle. It is impossible to know simultaneously the exact position and momentum of a particle

4.2.3. Solutions in End Layer. QKD's protocols used to alleviate security issues in the end layer are using both properties of QC: superposition and entanglement. The following are the protocols against the security threats of the end layer in the fog hierarchy.

(a) The E91 protocol works on the property of entanglement, where both the sender and the receiver could have one photon each. Therefore, sniffers will not be able to log in to the system

(b) The six-state uses a six-state polarization scheme on three orthogonal bases

5. A Potential Use Case: Integrated Fog-Assisted and Quantum Secure Health Care System

We used an integrated fog-assisted and quantum secure health care system as an example use case to elaborate the importance of quantum cryptography protocol encryption in fog computing architecture and networks. An integrated fog-assisted and quantum secure health care system is illustrated to give benefits like anytime availability of patient's information for subscribing proper medication and treatment depending upon history and patient's data to save patients. In this use case, the whole scenario is divided into two subsystems.

5.1. Healthcare Subsystem for Limited Area. The healthcare subsystem for the limited area is subdivided into handling and monitoring patient data in a limited area, for instance, in region 1 of Figure 4. For sending and receiving signals for a region's fog node, a patient should be in the vicinity of it to communicate with that specific node. A patient wearing smart equipment can send numerous pieces of information about its location and everything when it comes to the coverage area of a specific fog node. The communication between the fog node and the patient's smart device makes sure the nearest specialist is based on the saved information of the patient. Patient health data is the most sensitive data, which needs strong encryption. Therefore, that data is encrypted using QKD's BB84 encryption to safeguard it from intruders. The healthcare system working in a limited area can receive the patent's file through that smart device and follow the following steps:

(a) *Step 1*: the fog node monitors and controls the health data of the patient. If the patient needs any help, then this system can provide the patient's data and it will be mapped with the medical history of the patient. Hospitals just need to authenticate the data by putting the patient's medical id on the server. On the fog node, an intelligent secure heath care control algorithm (limited area) is implemented. By using real-time patient data, it calculates the health condition of the patient. For instance, if any patient's pacemaker is not working (medical equipment), then doctors receive real-time data of the patient. This step should be implemented in real-time. Due to traveling, the response time can get impacted as the fog nodes change when the region changes and the smart device has to cope with frequently changing nodes, so the traveling time shows some impact.

(b) *Step 2*: the fog node performs some crucial steps such as it encrypts the data, preprocesses it, and changes it to statistical information useful to medical personnel before storing it to cloud servers.

5.2. Healthcare Subsystem for Large Area. The healthcare subsystem for a large area is responsible for handling the medical data from a large area perspective, for instance, combined regions 1 to 4 in Figure 4. Figure 4 depicts the distant cloud server which collects information from all the four fog nodes present in all four regions. Data mining is performed to mine the medical information. There are two algorithms used to process the data in a large area: one is an intelligent health care algorithm (for a large area) and the other one is a dynamic transmission algorithm. In the large area healthcare subsystem (on the cloud), a more difficult intelligent healthcare algorithm is used as compared to the one used in the fog nodes of the different regions. The reason for the different levels of complication is that the one present on the cloud is responsible for predicting the medical issues based on historical data as well as the real-time data fog nodes are sending. It takes more time

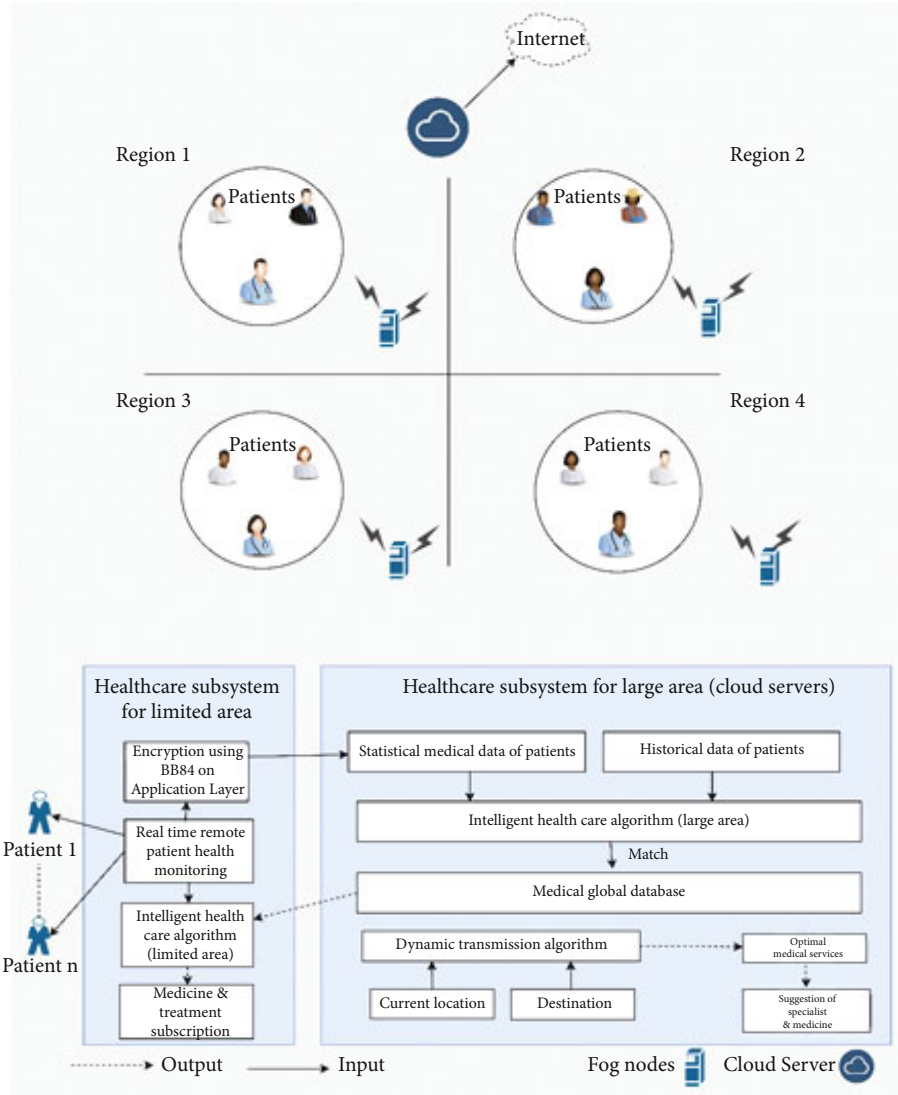

Figure 4: A fog-assisted health care system: an overview.

in processing on cloud servers than on fog nodes. Here, fog computing provides an advantage as the processing and capturing of data is done in two steps now. The mining results of this algorithm subscribe best medical treatment and medicines based on large area data comparison. After taking decisions, the results are sent to all the fog nodes in the city. The main aim is to save personal medical information by QKD protocol and process of authentication to avoid the manipulations of data of patients.

6. Open Research Challenges of Fog Computing

The network of the fog layer is dynamic in nature due to the mobility of end devices. It poses the following research challenges of quantum cryptography in fog computing:

(i) *Infrastructure*: most infrastructure problems occur when fog nodes are not communicating, then quantum cryptography requires an extra layer of security against the malicious data being uploaded on FN. This requires the development of new techniques of security.

(ii) *Virtualization*: it is the act of creating virtual network nodes when end users are being assigned different nodes continuously, as per the dynamic nature of fog nodes, it surges the problems of the virtual machine (VM) lifecycle, container, and context awareness. Quantum key distribution protocols are implemented by researchers as per the requirements of hardware for random key generation. However, if the nodes will also keep on changing, it will accelerate the problem which is again a major security threat.

(iii) *Resources and tasks*: tasks and resources are scheduled as per the time and availability correspondingly between end-users and fog nodes. The management can be better handled by QKD which will also safeguard the data. Due to the dynamic requirements of

resources as well as tasks, random key generation of quantum is an open research issue.

(iv) *Programmability*: the task of session management is difficult, and quantum cryptography algorithms for different sessions need different random key generations. Research is required to develop the common interface gateway of quantum cryptography for heterogeneous sessions of a single user.

7. Conclusion

In this article, a general description of fog computing's architecture is given along with security issues on its various layers. Quantum cryptography's QKD is provided as a solution for the security issues present on various layers of fog's architecture. A use case based on fog computing and quantum cryptography is illustrated along with a few open research challenges. Fog computing can make better decisions, and the service can be improved in the future. No system in today's world can be completely attack-free; researchers are working on providing a secured fog framework to keep the communications secure enough. The fog system's primary focus is on the need of decentralizing the safety model, and one of the best solutions currently is quantum cryptography. QKD can help in the data-sensitive applications of fog such as healthcare, critical industrial processes, and border security surveillance.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

[1] M. Pourkiani, M. Abedi, and M. A. Tahavori, "Improving the quality of service in wbsn based healthcare applications by using fog computing," in *2019 International Conference on Information and Communications Technology (ICOIACT)*, pp. 266–270, Yogyakarta, Indonesia, 2019.

[2] J. T. Chiang, J. J. Haas, J. Choi, and H. Yih-Chun, "Secure location verification using simultaneous multilateration," *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 584–591, 2012.

[3] R. A. Malaney, "Location-dependent communications using quantum entanglement," *Physical Review A*, vol. 81, no. 4, article 042319, 2010.

[4] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Generation Computer Systems*, vol. 108, p. 909, 2018.

[5] S. Wang, Y. Hou, F. Gao, and X. Ji, "A novel IoT access architecture for vehicle monitoring system," in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 639–642, Reston, VA, USA, 2016.

[6] M. Dianati and R. Alléaume, "Transport layer protocols for the secoqc quantum key distribution (QKD) network," in *32nd IEEE Conference on Local Computer Networks (LCN 2007)*, pp. 1025–1034, Dublin, Ireland, 2007.

[7] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog computing security challenges and future directions [energy and security]," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 92–96, 2019.

[8] X. Li Da, W. He, and S. Li, "Internet of things in industries: a survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[9] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Santa Fe, NM, USA, 1994.

[10] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[11] Q. Zhiguo, K. Wang, and M. Zheng, "Secure quantum fog computing model based on blind quantum computation," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–11, 2021.

[12] Y.-A. Chen, Q. Zhang, T.-Y. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[13] P. Siva Lakshmi and G. Murali, "Comparison of classical and quantum cryptography using QKD simulator," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 3543–3547, Chennai, India, 2017.

[14] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, no. 1, pp. 351–382, 2016.

[15] T. R. Raddo, S. Rommel, V. Land, C. Okonkwo, and I. T. Monroy, "Quantum data encryption as a service on demand: Eindhoven QKD network testbed," in *2019 21st International Conference on Transparent Optical Networks (ICTON),*, pp. 1–5, Angers, France, 2019.

[16] A. Nanda, D. Puthal, S. P. Mohanty, and U. Choppali, "A computing perspective of quantum cryptography [energy and security]," *Consumer Electronics Magazine*, vol. 7, no. 6, pp. 57–59, 2018.

[17] M. Jünger, E. Lobe, P. Mutzel et al., "Quantum annealing versus digital computing," *Journal of Experimental Algorithmics (JEA)*, vol. 26, pp. 1–30, 2021.