Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-021-03402-7

ORIGINAL RESEARCH

Secure quantum fog computing model based on blind quantum computation

Zhiguo Qu[1,2,3,4] · Kunyi Wang[4] · Min Zheng[5]

Received: 3 April 2020 / Accepted: 14 July 2021

Abstract

As a computing service platform closer to users, fog computing has many advantages such as extremely low latency, good mobility, accurate location perception and wide distribution. It has developed rapidly in recent years. However, due to the wide distribution of fog nodes, complex network environments, and limited resources, the security of fog nodes is vulnerable to a variety of attacks, such as denial of service and abuse of resources. In order to effectively deal with these attacks, this paper proposes a quantum fog computing model based on blind quantum computation and verifiable quantum secret sharing. The model mainly relies on blind quantum computation to realize the security joint operation characteristics of multiple fog nodes, and the identity verifiable and channel detection protection features provided by the quantum secret sharing protocol, which can not only efficiently perform the functions of the classic fog computing, but also guarantee the security of information transmission and data calculation. Through the complete security analysis, the new quantum fog computing model proposed in this paper can effectively resist on a variety of fog computing attacks, thus achieving information security protection in both the content and process of fog computing.

Keywords Fog computing · Blind quantum computation · Quantum secret sharing · Quantum identity authentication

1 Introduction

Since its concept was first proposed in 2006, cloud computing, as a configurable shared computing resource pool model (Peter Mell 2011), has developed rapidly over the past decade. Users can access and send requests at any time through the network, which greatly reduces the cost of information interaction with the server. Later, with the rise and development of the Internet of Things, Internet technology began to expand to the edge. The practical application of the Internet of Things generally requires virtual reality information interaction through cloud computing, big data and artificial intelligence. With the gradual application of cloud computing, it is found that there are complex resource allocation, low service delay, inability to solve local services in real time, and poor mobility. The fog computing is thus generated. As a new computing model, fog computing is an "edge" extension of cloud computing. The fog computing is between the cloud computing data center and the users, providing computing, storage and services to the end user.

In 2012, Cisco first proposed the concept of "fog computing". This company's Bonomi et al. proposed fog computing for the shortcomings of existing cloud computing models.

✉ Zhiguo Qu
qzghhh@126.com

✉ Min Zheng
zmyjl761218@163.com

[1] Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology, Nanjing 210044, China

[2] Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Nanjing University of Information Science and Technology, Nanjing 210044, China

[3] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

[4] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

[5] Hubei University of Science and Technology, Xianning, China

Published online: 10 August 2021

In 2013, Hong et al. of the Georgia Institute of Technology in the United States proposed the concept of moving fog. In 2014, Lui et al. (2014) of the United States made a comprehensive definition of fog computing, and compared the difference between cloud computing and fog computing, and proposed the threat of fog computing. In 2016, a white paper on fog computing for the overview of fog computing architecture was released. The White Paper introduces the Open Fog computing architecture and qualitatively discusses the security, scalability, autonomy, programmability, reliability, and applicability of the architecture. In the same year, Yi et al. ((2015) of the United States William Mary College first discussed the definition of fog computing and similar concepts. They analyzed the development goals and challenges of fog computing, and then gave several application examples to expand the application scenarios from fog computing. In 2017, Chang et al. (2016) of Princeton University in the United States reviewed the opportunities and challenges of fog computing. They focused on the combination of fog computing with the Internet of Things, 5G, and embedded artificial intelligence, and opened up ideas for the application of fog computing to new scenarios and technologies. In 2018, Zhang et al. (2017) elaborated on the Fog Radio Access Network (FRAN), which focused on mobility management and resource optimization in FRAN. On July 2018, Open Fog was adopted by the IEEE as the official standard reference architecture. Fog computing extends services to the edge of the network as a complement to cloud computing. The intermediate nodes that are physically closer to the object are used as the fog nodes to perform calculation, storage, and network service between the terminal device and the cloud computing data center. The introduction of fog computing solves the problems of complex resource allocation, low service delay, inability to solve local services and poor mobility in the Internet of Things in cloud computing applications, and improves real-time and work efficiency. Then, due to the characteristics of fog computing in information calculation and transmission, it is difficult to combat multiple fog computing attacks in untrusted environments, such as denial of service, abuse of resources, privacy leakage, privilege escalation attacks, virtual machine operations and service operation, etc.

Blind Quantum Computation (BQC) is a quantum computation technique in which the client does not have enough ability to solve the problem of quantum computation by entrusting the remote quantum server to complete its own computing tasks. In this process, it can effectively ensure the input, output and algorithm security of the client in an untrusted environment (Childs 2005; Sun et al. 2019; Broadbent et al. 2009; Liu et al. 2018; Dou et al. 2019; Qu et al. 2019; Morimae and Fujii 2013; Qu et al. 2018; Tan et al. 2018). The two main features of BQC are blindness and verifiability. In fact, blind quantum computation can be seen as a combination of quantum cryptography and quantum computation. In 2005, Childs proposed the first blind quantum computation protocol based on the quantum circuit model (Childs 2005). The protocol requires the client Alice to have quantum memory and the ability to execute SWAP gates. Arrighi and Salvail then proposed a BQC protocol that can only compute some specific functions. This protocol is not universal, and it also requires the client to have the ability to prepare and measure entangled states. Subsequently, in 2009, Broadbent et al. proposed the Brickwork state, and based on this, proposed the first universal blind quantum computation protocol (Broadbent et al. 2009). In the protocol, Alice only needed a classic computer and was able to prepare a primary quantum device with rotating single qubits. In addition, Alice is not required to have any quantum storage capabilities, and the protocol is unconditionally secure. For Bob, no matter what he does, he can't know Alice's input, output, and algorithm. Then blind quantum computation expands from single server to dual server mode (Morimae and Fujii 2013), three server mode (Li et al. 2014), and even to multi-party quantum servers. In 2010, Stefanie et al. demonstrated the correctness of the protocol in optical systems through physical experiments (Barz et al. 2012). The introduction of the universal blind quantum computation protocol and the success of its physics experiments have contributed to the development of blind quantum computation. As a follow, a large number of scholars studied blind quantum computation, enriching the content of blind quantum computation. In 2012, Morimae et al. implemented fault-tolerant blind quantum computation (Morimae and Fujii 2012), which is a blind topology quantum computation protocol based on quantum measurement. It has been proved that the error threshold of this blind topology model is equivalent to the error threshold of the non-blind topological Quantum computation (Raussendorf et al. 2007). In the same year, Tomoyuki proposed blind quantum calculation based on continuous variables (Morimae 2012). In 2013, Morimae et al. implemented the blind quantum calculation (Morimae and Fujii 2013) using the Affleck-Kennedy-Lieb-Tasaki (AKLT) (Affleck et al. 1988) state. The blind quantum protocol utilizes the advantages of the AKLT state to protect quantum computation and efficiently and accurately prepares resource states in linear optics with two-photons. At the same year, Sueki et al. proposed the auxiliary quantum bit-driven quantum computation (Sueki et al. 2013). In 2016, Kong et al. proposed a flexible multi-server blind quantum computation protocol based on the network environment (Kong et al. 2016). In this protocol, users can flexibly adjust the number of participating servers according to the conditional transformation of the network. The protocol stipulates that users can send service requests to up to three quantum servers.

Due to the classic fog computing is difficult to resist a variety of attacks of fog computing in the untrusted environment, so there is a clear threat for the security of computing content and information transmission. In order to effectively solve this security threat, this paper proposes a new quantum fog computing model based on blind quantum computation from the perspective of quantum information security. This paper combines the security advantages of blind quantum computation in computing and the security advantages of verifiable quantum secret sharing (Tan et al. 2013) in information transmission. The new model can not only effectively deal with multiple security threats that classical fog computing needs to face, but also make the fog computing model better applicable to reality.

The paper is organized as follows. Section 1 mainly introduces the related concepts of fog computing and blind quantum computation, as well as the security threat of fog computing and the security advantages of blind quantum computation. Section 2 presents a model of classical fog computing and studies the possible security threats of fog computing. And the basic knowledge of the quantum aspect blind quantum computation and verifiable secret sharing protocol required in this paper is given in Sect. 3. Section 3 proposes the new quantum fog computing model based on blind quantum computation and verifiable quantum secret sharing protocol for the security threat of fog computing, and describe its specific steps in details. In Sect. 4, the complete safety analysis to the proposed quantum fog computing model is carried out, and the feasibility of the quantum fog computing model is further illustrated as well. Finally, the conclusions and prospects are given in Sect. 5.

2 Preliminary

2.1 Classic fog computing model

A typical fog computing framework is divided into three layers: user layer, fog computing layer, and cloud computing server layer. The structure diagram is shown as Fig. 1.

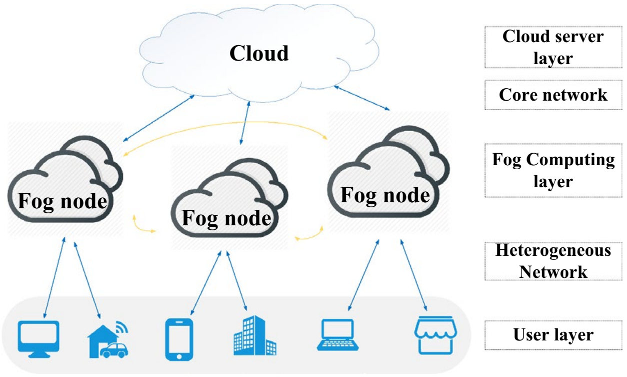

Fig. 1 Classic fog computing model

The user layer includes various user terminals and devices, and generally has heterogeneous terminals of mobile phones, computers, sensors, vehicles, etc. It responds to send service requests to complete the requirements. At the user level, there may be different terminal devices in different practical application scenarios. The fog service layer is composed of various fog nodes, and each fog node can communicate with each other. The fog node is close to the edge of the network and has certain storage and computing capabilities. It can independently or cooperatively complete the service request sent from the user layer. The cloud service layer includes a cloud server, and the information is exchanged with the fog node through the core network, while the fog node is managed and deployed. It is farthest away from the user layer at physical distance.

2.2 General blind quantum computation protocol

The main function of blind quantum computation is to help users achieve secure joint computing in an untrusted environment through multiple nodes with limited computing performance or a powerful server. For the convenience of explanation, this paper gives a blind quantum computation protocol between a user and a single server. For the specific execution steps of the blind quantum computation protocol based on Brickwork structure and quantum bit measurement between multiple servers, please refer to the literature (Wenqian 2017).

2.2.1 The related knowledge of quantum computation

1. Quantum computation based on quantum bit measurement There are two types of quantum computation: one is to design the corresponding quantum circuit and quantum logic gate as the basis of calculation through the corresponding unitary transformation, thus realizing blind quantum calculation (Deutsch 1989; Barenco et al. 1995); the other is the quantum calculation based on quantum bit measurement (Raussendorf and Briegel 2001), which through the entangled state of the Cluster state, continuously measures the corresponding qubits and simultaneously corrects the measurement angle, thereby realizing the function of blind quantum computation. Since the entangled state is used in quantum computation based on quantum bit measurement, according to the quantum no-cloning theorem, when quantum bit measurement is performed, the quantum state will collapse and cannot be reused. Therefore, such a computational model is also referred to a "one-way" quantum computer (1WQC). The 1WQC computation model simulates each quantum logic gate by measuring the

order of the Cluster state, and each quantum measurement angle depends on the previous measurement result, thereby achieving the calculation purpose. It is versatile because it can simulate individual quantum logic gates. The specific measurement of the Cluster state is given as follows(Briegel and Raussendorf 2001). The measurement base is $M_z = \{|0\rangle, |1\rangle\}$, $M(\theta) = \left\{ 1 \Big/ \sqrt{2}\left(|0\rangle + e^{i\theta}|1\rangle\right) \right\}$. Each single qubit logic gate U can be represented as:

$$U = R_x(\zeta)R_z(\eta)R_x(\xi) \tag{1}$$

where ζ, η, ξ are the measurement angles.

$$R_X(\theta) = e^{-i\theta X \big/ 2} = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{2}$$

$$R_Z(\theta) = e^{-i\theta Z \big/ 2} = \begin{bmatrix} e^{-i\theta \big/ 2} & 0 \\ 0 & e^{i\theta \big/ 2} \end{bmatrix} \tag{3}$$

The process of simulation calculation is as follows: firstly, four are prepared, and four controlled initial gates are used to connect four initial states to form a one-dimensional Cluster state. The process of simulating $U|\varphi\rangle$ is described as follows. At first, four qubits $|+\rangle$ are prepared, and four $|+\rangle$ and initial state $|\varphi\rangle$ are connected by a C-Z gate to form a one-dimensional Cluster state. And then, it measures the first particle with the measurement base X , and records the result s_1 ; while measuring the second particle with the measurement base $M(-(\text{ - }1)^{s_1}\xi)$, and recording the result s_2 . Meanwhile, it also will measure the third particle with the measurement base $M(-(\text{ - }1)^{s_2}\eta)$, and record the result s_3 , as long as using the measurement base $M(-(\text{ - }1)^{s_1+s_3}\zeta)$ to measure the fourth particle and record the measurement result s_4 . As a result, the fifth particle will become L in the unmeasured state $X^{s_2+s_4}Z^{s_1+s_3}U|\varphi\rangle$, where X and Z are Pauli operations, respectively. The correction is performed by applying a relative Pauli operation to the fifth particle. To eliminate the side effects $(X^{s_2+s_4}Z^{s_1+s_3})$ generated during the measurement process , $U|\varphi\rangle$ an be obtained, thereby completing the operation of the quantum logic gate U. Then, it completes the quantum computation. The measurement process of the cluster state is shown as Fig. 2.

2. Brickwork state preparation If the 1WQC computation is performed using the Cluster state, the measurement will use not only $M(\theta) = \left\{ 1 \Big/ \sqrt{2}\left(|0\rangle \pm e^{i\theta}|1\rangle\right) \right\}$, but also the base $M_z = \{|0\rangle, |1\rangle\}$ that is used as the cropping of the Cluster state in order to eliminate useless particles. In the computation process, the quantum server can simplify the Cluster state by viewing the measurement position of the measurement base, thereby obtaining the user's quantum initial state and obtaining partial information, which is not conducive to user privacy protection. Therefore, Broadbent, Fitzsimons and Kashefi proposed a universal blind quantum computation protocol based on 1WQC (BFK-UBQC protocol). The protocol first proposed the concept of the Brickwork state, which was used to form the initial state of quantum computation. The Brickwork state is an entangled state composed of $n \times m$ qubits, denoted as $G_{n \times m}$, where m satisfies the congruence $m \equiv 5(\text{mod}\,8)$. The Brickwork state preparation process is give as follows. First, it prepares $n \times m$ qubits, while their states are all $|+\rangle$. Each qubit is corresponding to a set of markers (i,j) , while the row label $i \in [1, n]$ and the column label $j \in [1, m]$. Then, a controlled $C - Z$ gate operation is applied to the associated pairs of particles as follows.
3. Brickwork state representing a generic U door

(1) Apply $C - Z$ gate operations to particles (i,j) and $(i,j+1)$ in each row, that is, there is an associated edge between adjacent particles in each row $(j \in [1, m\text{ - }1])$.
(2) When the column $j \equiv 3(\text{mod}\,8)$ and the row i are odd rows. The $C - Z$ gate operations are applied to parti-

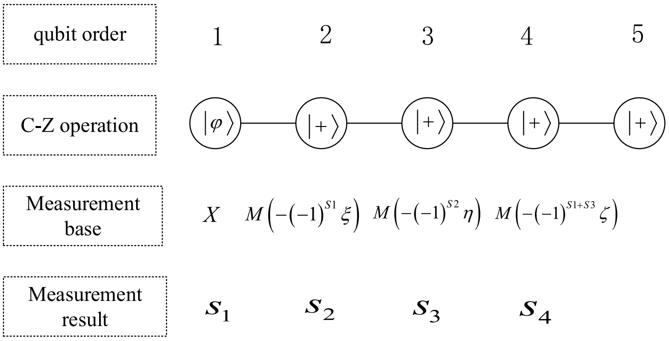

Fig. 2 Cluster state measurement process

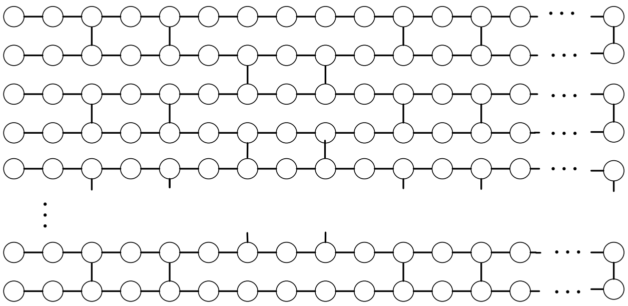

Fig. 3 Brickwork structure

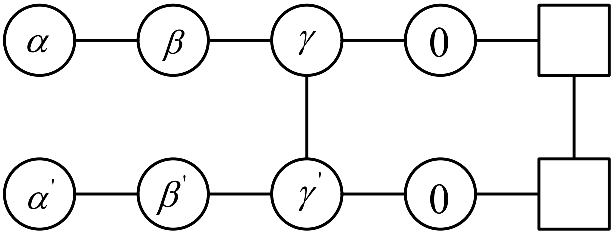

Fig. 4 Rotational measurement model

cle pairs of (i,j) and $(i+1,j)$, and the particle pairs of $(i,j+2)$ and $(i+1,j+2)$.

(3) When the column $j \equiv 7(\mathrm{mod}8)$ and the row i are even rows. The $C-Z$ gate operations are applied to particle pairs of (i,j) and $(i+1,j)$, and the particle pairs of $(i,j+2)$ and $(i+1,j+2)$

.

The constructed Brickwork is shown as Fig. 3.

By measuring the combination of the model and the rotation angle, we can get a rotation measurement model, as shown in Fig. 4.

The general quantum U gate set can be implemented as $\left\{H, \frac{\pi}{8}, CNOT\right\}$ by using the Brickwork state, which are shown as Fig. 5. The models of these gates can be combined to construct a universal quantum gate U of any lines, as shown in Fig. 6.

2.2.2 General blind quantum computation protocol

The agreement is divided into two phases, called the preparation phase and the calculation phase. The preparation phase requires preparation of a multi-qubit Brickwork state for measurement for the calculation phase, where client Alice prepares a single qubit and server Bob constructs a Brickwork state. The specific preparation process is given as follows.

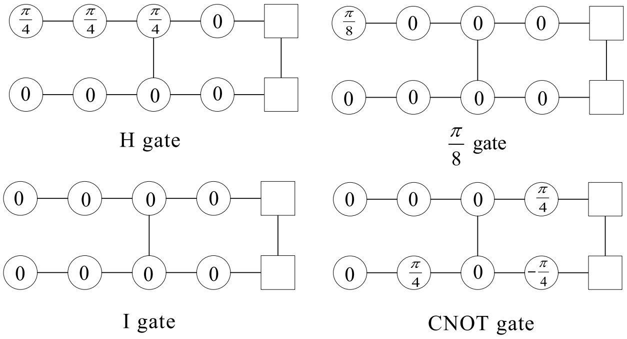

Fig. 5 Universal U gates

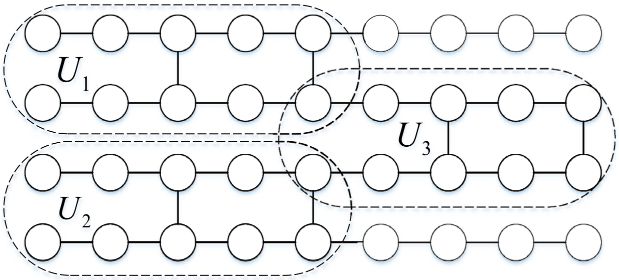

Fig. 6 Quantum universal gate

(1) Alice prepares m qubits. Each qubit state is $\left|\varphi_i\right\rangle = |0\rangle + e^{i\theta_i}|1\rangle$, $\theta_i \in \left\{\frac{k}{4}\pi | k = 1, 2, ..., 7\right\}$. Alice sends the qubit to Bob.

(2) After receiving the qubits from Alice, Bob constructs the Brickwork state. In the calculation phase, Alice and Bob cooperate to complete each qubit measurement in the Brickwork state structure in turn. The specific measurement process can be described as follows.

(3) Alice randomly selects $r_i \in \{0, 1\}$ and calculates $\delta_i = (\theta_i + \phi_i{}' + r_i \times \pi) mod 2\pi$. Among them, ϕ_i is determined by the last measurement result $\phi_i{}'$ and the correction U transformation $\{X, Z\}$, $\phi_i{}' = (-1)^{s_i}\phi_i + s_i\pi$. Subsequently, Alice needs Bob to measure the i quantum state and then sends δ_i to Bob.

(4) Bob uses the measurement base $\left|\pm\delta_i\right\rangle$ to make measurements and sends the results $s_i \in \{0, 1\}$ back to Alice.

(5) If $r_i = 1$, Alice reverses s_i and $r_i = 0$ without the flip. After the Bob measurement is completed, it will turn to the step (3) and cycle through the measurement process of the next qubit until the end of all qubit measurements.

2.3 Quantum secret sharing protocol

In this paper, due to a multi-party and multi-party secret sharing scheme (Briegel and Raussendorf 2001) is used, then this one-to-one verifiable quantum secret sharing protocol based on entanglement switching is present here.

The steps of this protocol are given as follows.

(1) Alice prepares three pairs of EPR pairs $|\psi(0,0)\rangle_{1,2}$, $|\psi(0,0)\rangle_{3,4}$ and $|\psi(0,0)\rangle_{5,6}$. Send 2, 3 particles to Bob.

(2) Alice and Bob randomly select two operational sequences: channel security authentication mode and information sharing mode.

  A. Channel safety certification: First, Bob randomly selects the X-base or Z-base to measure the particle 2, and exposes the selected measurement base and measurement results to Alice. Alice uses the measurement basis selected by Bob to measure the particle 1, and then Alice compares her result with that of Bob. If they are the same, the channel is proved to be safe. And if the a operation is performed firstly, the b operation will be performed. On the contrary, if their result is different, the channel will be proved to be unsecure. The protocol will be terminated from the need to discard the information passed.

  B. Information sharing mode: Alice performs Bell-based measurements on 1, 4 particles, and Bob performs Bell-based measurements on 2, 3 particles. The particles 1, 4 are in an entangled state and the particles 2, 3 are in an entangled state. Thus, Bob obtains the shared partial secret information by measuring the result.

(3) For secret sharing with Charlie, Alice sends 4, 5 particles to Charlie, and completes channel detection and information shari ng between Alice and Charlie in the same way as the steps (1) and (2). Alice announces the measurement $|\psi\rangle_{1,6}$ for the particles 1, 6.

(4) Bob and Charlie can combine Alice's secrets based on the sub-passwords they get.

3 Quantum fog computing

3.1 Fog computing model under quantum angle

The proposed model of quantum fog computing can be shown as Fig. 7. In this quantum fog computing model, the user processes and calculates information through the fog nodes. It means that the user will send a request to a fog node through the quantum network, and the fog node performs data processing and returns the result to the user. In the information interaction phase, the information transmission between the fog node and the cloud server is completed by using a verifiable quantum secret sharing protocol.

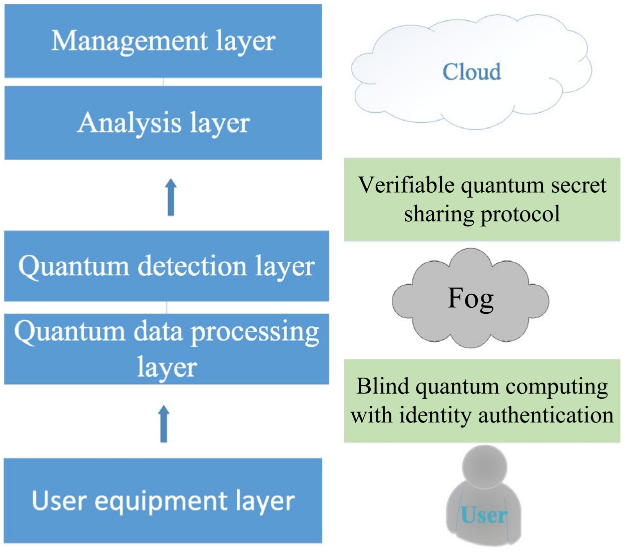
Management layer
Analysis layer
Quantum detection layer
Quantum data processing layer
User equipment layer
Cloud
Verifiable quantum secret sharing protocol
Fog
Blind quantum computing with identity authentication
User

Fig. 7 New framework diagram of quantum fog computing

3.2 The proposed model

3.2.1 Computation model between user and fog nodes

In the quantum fog computing model, during the calculation process between the user and the fog node, let refer to the blind quantum computation protocol with identity authentication proposed in the literature (Li et al. 2018). We propose a method of calculating and processing the fog node based on blind quantum computation. In this computational model, the user Alice and the fog node Bob will complete the identity authentication and calculation request through the blind quantum computation with authentication. The TTP is a trusted third party.

The specific steps shown as Fig. 8 are presented as follows.

Step1 Alice prepares $m+l$ qubits through a quantum network to form a set P . The state of the l qubits is one of four states of random BB84, and constitutes a set V . The quantum bit state in the set P - V is $|\varphi_i\rangle = |0\rangle + e^{i\theta_i}|1\rangle$, $\theta_i \in \left\{ \frac{k}{4}\pi | k = 1, 2, ..., 7 \right\}$ .Alice sends the qubit to Bob.

Step2 During the process that Alice sends qubits to Bob, each qubit first performs a U transform $U_i \in \{X, Z, I\}$ through the trusted third-party, without measurement. Bob receives all $m+l$ qubits.

Step3 Then, Alice sends the set V selected by Bob. After receiving the qubits, Bob will use X or Z basis measurements to measure received qubits of the set V.

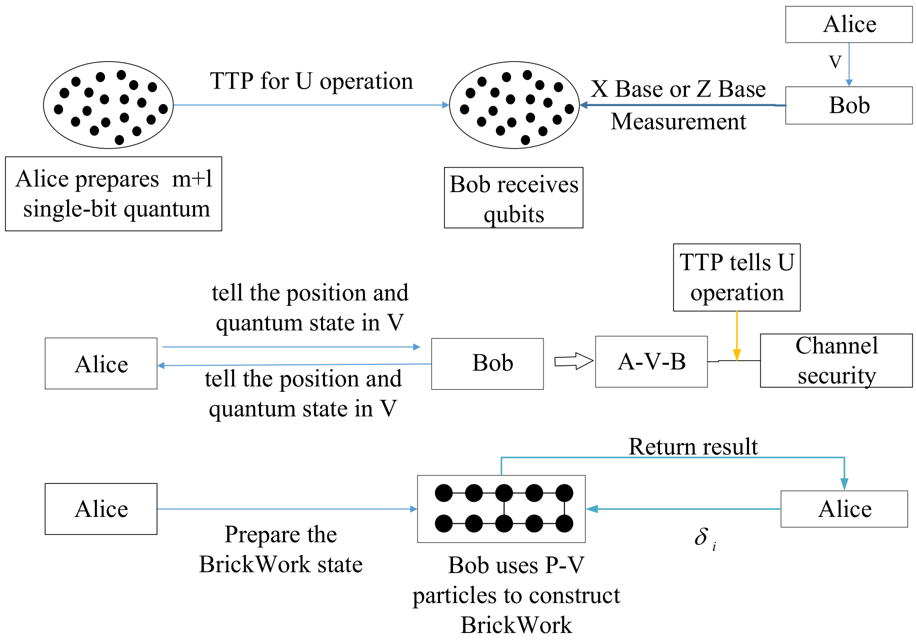
Alice
V
Bob
TTP for U operation
X Base or Z Base
Measurement
Alice prepares m+l single-bit quantum
Bob receives qubits
TTP tells U operation
tell the position and quantum state in V
Alice
Bob
A-V-B
Channel security
tell the position and quantum state in V
Return result
Alice
Alice
Prepare the BrickWork state
δ_i
Bob uses P-V particles to construct BrickWork

Fig. 8 Conceptual diagram of a new quantum fog computing model

Step4 As a follow, Alice randomly selects the set $A \in V$ and tells Bob the state and order of the qubits in the selected set A . At the same time, Bob also randomly selects set $B \in V$ and tells Alice the state and order of the qubits in the selected set B. Alice and Bob find the quantum corresponding to the same position in the sets A and B to form the set $A - V - B$.

Step5 The trusted third-party publishes the selected U transform. Alice and Bob will check if the process of U-transformation and measurement is normal or not. If it is normal, the identity authentication is successful. Otherwise, the protocol will be terminated.

Step6 After succeeding the identity authentication, Alice sends a request to construct a BrickWork state to Bob.

Step7 Then, Bob selects the qubit in the set P - V from the qubits sent by Alice to generate the BrickWork state.

Step8 When $i \in P - V$, Alice randomly selects $r_i \in \{0, 1\}$ and calculates $\delta_i = (\alpha_i + \phi_i{}' + r_i \times \pi) mod 2\pi$. Here, the trusted third-party selects $U_i = X$, $\alpha_i = 2\pi - \theta_i$ and $U_i = Z$, $\alpha_i = \theta_i + \pi$. The $\phi_i{}' = (-1)^{s_i}\phi_i + s_i\pi$ is determined by the last measurement result ϕ_i and the corrected U transformation $\{X, Z\}$. Subsequently, Alice needs Bob to measure the i quantum state and will send it to Bob.

Step9 Corresponding to $i \in P - V$, Bob uses the measurement base $\left|\pm\delta_i\right\rangle$ to measure and sends the result $s_i \in \{0, 1\}$ to Alice.

Step10 If $r_i = 1$, Alice reverses s_i and $r_i = 0$ without the flip. After Bob's measurement is completed, it will go to the step 8 and cycle through the measurement process of the next qubit until the end of all qubit measurements.

3.2.2 Verifiable quantum secret sharing

The new model uses verifiable quantum secret sharing technology for information interaction between users, fog nodes and cloud servers. We take the information sharing between the fog node and the cloud server as an example to describe the algorithm. Among them, Alice is regarded as a cloud server and also is a secret sender. The Bob and Charlie as fog nodes are secret recipients. The identity of Alice, Bob and Charlie can change from each other. The specific steps are given as Fig. 9.

Step1 At first, Alice, Bob and Charlie share the identity authentication sequences S_b and S_c through the authentication key (Liu et al. 2012), and use a one-way function h to generate secret authentication information, where $h_{AB} = h(S_b)$, $h_{AC} = h(S_c)$.

Step2 Then, Alice prepares three pairs of EPR pairs $|\psi(0,0)\rangle_{1,2}$, $|\psi(0,0)\rangle_{3,4}$ and $|\psi(0,0)\rangle_{5,6}$. She sends the particles 2,3 to Bob. At the same time, in order to verify the channel security and prevent eavesdropping, Alice prepared some detection particles. And the mixed particles are sent to Bob.

Step3 After Bob receives the particles, Alice tells Bob where the detection particles is in the transmission particle sequence and their states. Bob selects the measurement base and measures the detection particles. After the measurement is completed, Bob announces the selected measurement basis and the measurement results to Alice, and compares the particle change process between Alice and Bob. If the change process is correct, the channel is safe. Otherwise, the eavesdropping existence can be confirmed in the channel.

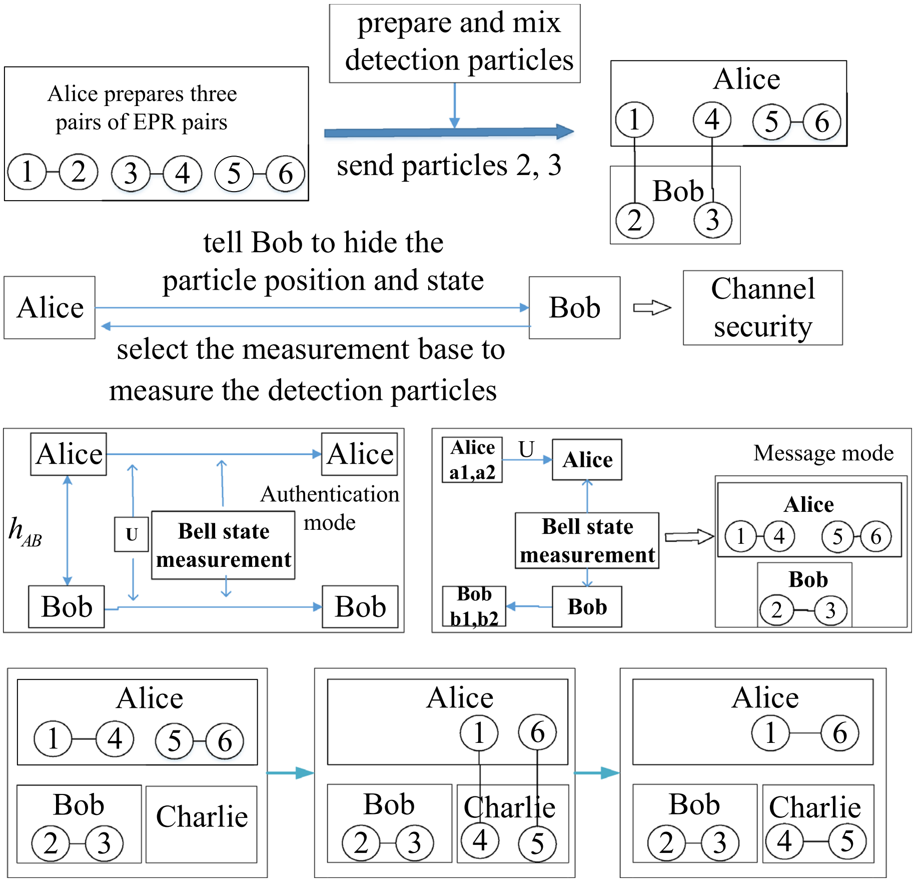

Fig. 9 Specific execution flow chart of the new quantum fog computing model

Step4 Alice and Bob randomly choose two operations: authentication mode and information sharing mode.

Authentication mode:

Firstly, Alice and Bob correspond to h_{AB} for 1 and 2 particles where $h_{AB} = 0$. Then, Alice transforms $h_{AB} = 1$, and perform H gate operation on them. After Alice and Bob correspond to the Bell state measurement of the particles, one party publishes its own measurement results, and the other party obtains the certification result based on the known counterpart measurement results and its own measurement results. If the error rate is above the threshold, the protocol will be terminated.

Information sharing mode:

Alice will perform a positive operation on the particle 1 based on the secret message $(a_1, a_2), a_i \in \{0, 1\}$ that is to be transmitted. After Alice performs Bell-based measurements on the 1, 4 particles, Bob also performs Bell-based measurements on the 2, 3 particles. Thus, Bob obtains the shared secret (b_1, b_2) by measuring the result.

Step5 For secret sharing with Charlie, Alice sends 4,5 particles to Bob and performs channel detection and authentication between Alice and Charlie in the same way by following the steps (3) and (4). In the secret sharing phase, Alice performs Bell-based measurements on the 1,6 particles, and Charlie performs Bell-based measurements on the 4, 5 particles. Then, Charlie can get the shared secret (c_1, c_2).

Step6 Alice announces the measurement for the particles 1, 6.

Step7 Bob and Charlie can combine Alice's secrets based on the sub-passwords they share.

4 Security analysis

For convenience of analysis, the possible security threats and possible intrusions for the classical fog computing model are present firstly. After that, the security of the novel quantum fog computing model proposed are analyzed in details.

4.1 Fog computing may encounter threats

Due to the wide distribution of fog nodes and the complex network environment and limited resources, fog nodes are easily attacked by intruders. Therefore, for the calculation of fog, it is extremely urgent to solve its safety problems. In general, fog computing security threats mainly include :

(1) Denial of service (DoS). Malicious virtual machines exhaust running host resources (including compute,

network, and storage resources), and makes fog nodes unable to serve normal users. Under the fog computing architecture, denial of service attacks are mainly performed on distributed fog nodes.

(2) Abuse of resources. A malicious virtual machine can execute various malicious programs targeting the edge data center to achieve the purpose of occupying resources and abusing resources.

(3) Privacy disclosure. Due to the architectural nature of fog computing, most of the virtualized infrastructure at the edge data center is not completely transparent: the fog node can implement various APIs locally that provide information about the physical and logical environments. If these APIs are not protected, the malicious virtual machine can get sensitive information about the execution environment and the environment around the edge data center.

(4) A privilege escalation attack. A malicious virtual machine attempts to exploit the vulnerability in the host to hack it. This type of attack can lead to a variety of outcomes, such as isolation failures, privilege attacks, and so on.

(5) Virtual Machine (VM) operation. A host system controlled by an intruder can initiate several attacks on VMs running inside it. These attacks mainly include extracting server information and manipulating virtual nodes that are performing computational tasks in the VM.

(6) Service manipulation. In a fog computing environment, devices may participate in the provisioning of services, and intruders control users to manipulate services.

4.2 Intrusion process under fog computing

The fog computing is in the process of being invaded (Fig. 10) and may have the following steps:

(1) Under the heterogeneous network environment between the fog node and the user, there may be loopholes such as operating systems and communication protocol. An intruder can invade a fog node by sending a service request to the fog node to detect a fog node vulnerability. When the intruder requests are too large, it may cause a denial of service attack (DOS) on the fog node.

(2) When the intruder successfully invaded the fog node, it caused serious harm to users, fog nodes and cloud servers. For the user, the fog node is invaded and the user's privacy is leaked. For the fog node, the intrusion of a certain fog node has a bad influence on information interaction and service cooperation between other nearby fog nodes. In addition, intruders can also perform remote user attacks and privilege attacks on fog nodes. After the intruder successfully attacks the attack, the cloud server receives the intruder's denial of service attack and port attack.

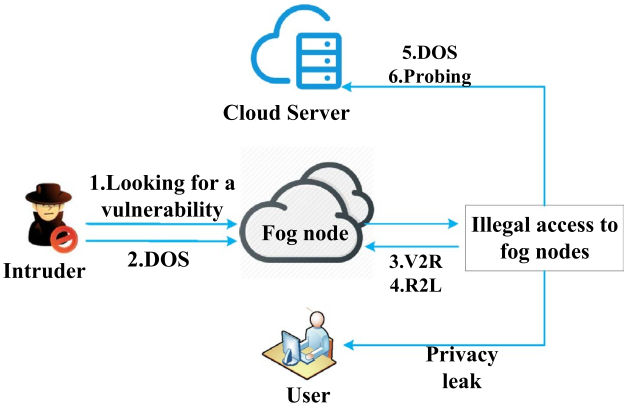

Fig. 10 Intrusion process under fog computing

(3) If the intruder succeeds further through denial of service attacks and port attacks, the cloud server is compromised and information is leaked. This is also the ultimate goal of the intruder.

From the intrusion process of fog computing, there are mainly the following types of security threats that can better understand fog computing:

A. The intruder sends a service to the fog node by attacking the user or simulating the virtual machine, and has service control, privilege escalation attack, denial of service attack, abuse of resources, and channel eavesdropping attack threat.

B. The intruder attacks the fog node, has a privacy leak, and the threat of the virtual machine.

C. When the information is transmitted between the fog node and the cloud server, channel eavesdropping is performed.

4.3 The security analysis to the new model

In Sect. 3, the new model of quantum fog computing has been given. The quantum fog computing model is based on blind quantum computation with identity verification and verifiable quantum secret sharing. According to references Briegel and Raussendorf (2001) and Li et al. (2018), it's known that these two protocols are safe and feasible. Based on the security threats summarized in Subsect. 4.1, let analyze the security threat from the perspective of the intruder attack object in the fog computing model, and prove that it is eliminated by the advantages of the quantum fog computing model.

(1) The intruder sends services to the fog node by attacking the user or simulating the virtual machine, with

service control, permission escalation, denial of service attack, abuse of resources, and channel eavesdropping attack threat. Firstly, for the threat of channel eavesdropping attacks, the security of the certifiable quantum secret sharing protocol proposed in this paper has been proved, and the channel eavesdropping security analysis of the quantum fog computing platform can be proved by the security of the protocol. Assuming that there is an eavesdropper Eve on the channel, the user Alice sends the particle to the quantum fog node Bob, and through Bob's publication of the measurement base and the measurement result, according to quantum no-cloning theorem, Alice can calculate and compare the Bob measurement result. Equivalent, so that there is an eavesdropper Eve conclusion in the channel. Second, for the problem of denial of service attacks, abuse of resources and service control, intruders control the user to send requests and malicious request attacks to the server. In the two protocols proposed in this paper, there is an identity authentication function. Before Bob performs the service, Alice and Bob mutually authenticate each other through a trusted third party, so that such problems can be solved. Thus, even if the intruder invades the user successfully, Bob does not generate services for the invaded user through the quantum fog computing proposed in this paper. Finally, for the privilege escalation attack, the intruder further invades the fog node to obtain higher privilege by invading the user, thereby threatening other fog nodes and cloud server layers of the fog computing layer, but in the quantum fog computing, the user The service between the layer and the fog node is based on the blind quantum computing with identity authentication, thus solving the threat of privilege escalation attacks. It is thus possible to prove the safety of the quantum fog computing between the user and the fog node.

(2) The intruder attacks the fog node, which poses a threat to the virtual machine operation to the nearby fog node, causing serious consequences for the user to leak privacy, and generating a port attack (Probing Attack) and a denial of service attack on the cloud server. First, for virtual machine operation, in the quantum fog computing model, participants must first verify the information before sharing the information between the fog nodes. The fog nodes that are attacked are discarded and do not participate in information sharing. Only the secure fog nodes can share information. For example, when the fog node A is invaded, when the quantum secret sharing protocol is implemented between the fog nodes, when the node A and the other node B are in the secret shared protocol, the calculation of the Bell state is performed in the authentication link to compare the calculations of A and B. As a result, it is found that the error rate is higher than the threshold value, thereby detecting that there is an invaded node in A and B, and the next operation is not performed, so the threat of redundant virtual machine operation can be eliminated. Secondly, for the user's privacy leakage problem, firstly, the fog node Bob is serving the user Alice based on the blind quantum computation protocol. According to the blind quantum computation protocol, the particles are all calculated by Alice and Bob constructing the Brickwork state. In the calculation phase, the measurement angle δ_i is given by Alice, $\delta_i = (\alpha_i + \phi_i{}' + r_i \times \pi) mod 2\pi$. For Bob, Bob can only know the angle α_i received by Alice. For the measurement angle δ_i , due to Alice's random selection of r_i , Bob's measured particles are randomly $|\varphi\rangle = |0\rangle + e^{i(\phi' + \alpha_i)}|1\rangle$ and $|\varphi\rangle = |0\rangle - e^{i(\phi' + \alpha_i)}|1\rangle$. ϕ' is based on the basis of the last measurement, and is random, so Bob can't judge Alice's measurement angle, and thus can't get the calculation result that Alice wants. Therefore, Bob could not get Alice's information and avoided the threat of privacy breach. Finally, for the port attack and the denial of service attack received by the cloud server, it is similar to the attack defense of the virtual machine operation. It is impossible to pass the authentication fog node to request the information exchange to the cloud server. Therefore, when the invaded fog node sends information to the cloud server, the agreement will be aborted.

(3) For the channel eavesdropping threat problem between the fog node and the cloud server, the channel detection method in the certifiable quantum secret sharing protocol is applicable to the quantum fog computing. Its safety has also been proven, here is a brief description. In this protocol, each fog node and other fog nodes are individually transmitted particles, and will be measured or detected immediately after transmission. If there is an external eavesdropper, the real sending order cannot be obtained, and the key cannot be obtained from the obtained sending particles. And if there is an internal cheating party, suppose that a fog node Charlie is the cheating party. He has successfully obtained the information of particle 5 and wants to obtain the information of particle 6 based on the entanglement measurement, thereby obtaining a new particle 5* and 6 *, and then infer the measurement result of another fog node Bob, but unfortunately, at this time, the 5 particles and 6 particles are no longer entangled. Particle 5 and particle 4 are in an entangled state, and particle 6 and particle 1 are in an entangled state, so Bob's information cannot be obtained. In addition, the fog node Alice and the other two fog nodes transmit information separately and also have a verification link, so the existence of internal cheating parties can be prevented.

5 Conclusion

In order to effectively deal with various security attacks that are difficult to solve in classical fog computing, this paper proposes a novel quantum fog computing model based on blind quantum computation and verifiable quantum secret sharing. The new model makes full use of blind quantum computation to perform secure joint calculation by using multiple quantum fog nodes with limited computing power in an untrusted computing environment to ensure the security of computational content. At the same time, it also makes full use of the identity verification of the quantum secret sharing protocol, and realizes the security protection of the information transmission process. The quantum fog computing proposed in this paper absorbs the advantages of both, fully considers the physical properties of quantum, and combines it with the classical fog computing model. The quantum fog computing can not only efficiently complete the functions of the classic fog computing, but also ensure the security of information transmission and calculation. Through the complete security analysis, the new fog computing model proposed in this paper can effectively resist various forms of fog computing attacks such as denial of service, abuse of resources, privacy leakage, privilege escalation attack, virtual machine operation and service manipulation. Therefore, the information security protection of the content and process of the fog computing can be realized.

Acknowledgements This work was supported by the National Natural Science Foun- dation of China (No. 61373131, 61601358, 61501247, 61672290, 61303039, 61232016), Natural Science Foundation of Jiangsu Province (Grant No. BK20171458), Sichuan Youth Science and Technique Foundation (No.2017JQ0048), Open Foundation of State key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) (SKLNST-2020-1-17), PAPD and CICAEET funds.

References

Affleck I, Kennedy T, Lieb EH, Tasaki H (1988) Valence bond ground states in isotropic quantum antiferromagnets. Commun Math Phys 115(3):477–528

Barenco A, Bennett CH, Cleve R, DiVincenzo DP, Margolus N, Shor P, Sleator T, Smolin JA, Weinfurter H (1995) Elementary gates for quantum computation. Phys Rev A 52(5):3457–3457

Barz S, Kashefi E, Broadbent A, Fitzsimons JF, Zeilinger A, Walther P (2012) Demonstration of blind quantum computing. Science 335(6066):303–308

Briegel HJ, Raussendorf R (2001) Persistent entanglement in arrays of interacting particles. Phys Rev Lett 86(5):910–913

Broadbent, A, Fitzsimons J, Kashefi E (2009) Universal blind quantum computation. In: 2009 50th annual IEEE symposium on foundations of computer science, IEEE, pp 517–526

Chiang M, Zhang T (2016) Fog and iot: an overview of research opportunities. IEEE Internet Things 3(6):854–864

Childs AM (2005) Secure assisted quantum computation. Quantum Inf Comput 5(6):456–466

Deutsch DE (1989) Quantum computational networks. Proc R Soc Lond Ser Contain Papers Math Phys Character 425(1868):73–90

Dou Z, Xu G, Chen X, Yuan K (2019) Rational non-hierarchical quantum state sharing protocol. CMC-Comput Mater Con 58(2):335–347

Kong X, Qin L, Wu C, Fang Y, He J, Sun Z (2016) Multiple-server flexible blind quantum computation in networks. Int Nt J Theor Phys 55(6):3001–3007

Li Q, Chan WH, Wu C, Wen Z (2014) Triple-server blind quantum computation using entanglement swapping. Phys Rev A 89(4):040302

Li Q, Li Z, Chan WH, Zhang S, Liu C (2018) Blind quantum computation with identity authentication. Phys Rev A 382(14):938–941

Liu XF, Yan XH, Yao ZQ (2012) Multiparty quantum secret sharing protocol with authentication. J Chin Comput Sys 33(11):2518–2521

Liu W, Chen Z, Liu J, Su Z, Chi L (2018) Full-blind delegating private quantum computation. CMC-Comput Mater Contin 56(2):211–223

Morimae T (2012) Continuous-variable blind quantum computation. Phys Rev Lett 109(23):230502

Morimae T, Fujii K (2012) Blind topological measurement-based quantum computation. Nat Commun 3:1036–1037

Morimae T, Fujii K (2013) Secure entanglement distillation for double-server blind quantum computation. Phys Rev Lett 111(2):020502

Mell P, Grance T (2011) The NIST definition of cloud computing. Commun ACM 53(6):50–53

Qu Z, Zhu T, Wang J, Wang X (2018) A novel quantum steganagraphy based on brown states. CMC-Comput Mater Contin 56(1):47–59

Qu Z, Wu S, Liu W, Wang X (2019) Analysis and improvement of steganography protocol based on bell states in noise environment. CMC-Comput Mater Con 59(2):607–624

Raussendorf R, Briegel HJ (2001) A one-way quantum computer. Phys Rev Lett 86(22):5188–5189

Raussendorf R, Harrington J, Goyal K (2007) Topological fault-tolerance in cluster state quantum computation. New J Phys 9(6):199–199

Sueki T, Koshiba T, Morimae T (2013) Ancilla‐driven universal blind quantum computation. Phys Rev A 87(6):060301

Sun Y, Chen Y, Ahmad H, Wei Z (2019) An asymmetric controlled bidirectional quantum state transmission protocol. CMC-Comput Mater Contin 59(1):215–227

Tan X, Feng Z, Jiang L, Fang A (2013) Verifiable quantum secret sharing protocol. In: 2013 Fourth international conference on emerging intelligent data and web technologies, IEEE, pp 227–230

Tan X, Li X, Yang P (2018) Perfect quantum teleportation via bell states. CMC-Comput Mater Con 57(3):495–503

Vaquero LM, Rodero-Merino L (2014) Finding your way in the fog: towards a comprehensive definition of fog computing. Acm Sigcomm Comp Com 44(5):27–32

Wenqian L (2017) The study on key problems of secure multi-party quantum computation. Southeast University, Jiangsu

Yi S, Hao Z, Qin Z, Li Q (2015) Fog computing: platform and applications. In: 2015 Third IEEE workshop on hot topics in web systems and technologies (HotWeb), IEEE, pp 73–78

Zhang H, Qiu Y, Chu X, Long K, Leung VC (2017) Fog radio access networks: mobility management, interference mitigation, and resource optimization. IEEE Wirel Commun Le 24(6):120–127