Exploiting Geo-Distributed Clouds for a E-Health Monitoring System With Minimum Service Delay and Privacy Preservation

Qinghua Shen, *Student Member, IEEE*, Xiaohui Liang, *Student Member, IEEE*, Xuemin (Sherman) Shen, *Fellow, IEEE*, Xiaodong Lin, *Senior Member, IEEE*, and Henry Y. Luo

***Abstract*—In this paper, we propose an e-health monitoring system with minimum service delay and privacy preservation by exploiting geo-distributed clouds. In the system, the resource allocation scheme enables the distributed cloud servers to cooperatively assign the servers to the requested users under the load balance condition. Thus, the service delay for users is minimized. In addition, a traffic-shaping algorithm is proposed. The traffic-shaping algorithm converts the user health data traffic to the nonhealth data traffic such that the capability of traffic analysis attacks is largely reduced. Through the numerical analysis, we show the efficiency of the proposed traffic-shaping algorithm in terms of service delay and privacy preservation. Furthermore, through the simulations, we demonstrate that the proposed resource allocation scheme significantly reduces the service delay compared to two other alternatives using jointly the short queue and distributed control law.**

***Index Terms*—E-health monitoring system, geo-distributed clouds, privacy preservation, resource allocation.**

I. Introduction

E-HEALTH monitoring systems integrate the wireless technologies and information platforms to improve the quality of healthcare delivery. It receives health data, such as electromyography [1] and electrocardiography [2] from patients in real time, which help their doctors remotely deal with chronic conditions and identify malignant disease before the disease causes incurable damage. As the aging population grows, the overloaded burden of current hospital facilities continuously degrades the healthcare service quality, such as unexpected service delay and reduced service time. As such, there is a strong motivation to promote e-health monitoring systems in the short future, completely revolutionizing the way of healthcare delivery. In the e-health monitoring systems, huge amounts of health data are quickly and simultaneously uploaded to the servers via heterogeneous networks, such as wireless body area networks, ad hoc networks, and cellular networks. Each patient would require the servers to safely and reliably maintain their privacy-sensitive and accumulative health data and timely report the data to their family doctors or specialists. In this case, the amount of required data storage by users dramatically increases in every minute, while the access of these data must be real time and efficient [3]. For example, the real-time critical medical data traffics require delay smaller than 250 ms and cannot tolerate data loss rate [4], [5]. These stringent requirements of e-health monitoring systems raise many research challenges among of which server resource allocation and data privacy preservation are most important.

Cloud computing emerges as a computing infrastructure with the ability to coordinate many networked computers to perform data storage and computation simultaneously. Geo-distributed cloud service is a trend in cloud computing which, by spanning multiple data centers at different geographical locations, can provide a much more economical solution to offer efficient services to groups of users in their proximity in terms of reduced bandwidth costs and increased availability [6], [7]. When applying geo-distributed clouds for e-health monitoring systems, how to minimize the service delay is a challenging research problem due to the user mobility and the distributed management of cloud servers. Some research works [7]–[10] suggest to utilize the location information of cloud servers in resource allocation to reduce the service delay, while not consider e-health monitoring systems with special service delay requirements. A special-tailored distributed resource allocation scheme for an e-health monitoring system is of great research value and practical significance.

Privacy preservation is another important concern of users when applying the cloud computing for e-health monitoring systems. Since users may transmit their health data to the remote servers, the long-distance and insecure transmission channel could suffer from various security attacks. For example, *traffic analysis* (TA) attacks [11] aim to analyze the traffic statistics, such as the length of underlying data or the number of packets during a unit time, to determine the type of data. In the e-health monitoring systems, without security protection, the TA attacks could analyze the potential diseases of the target user or derive the real identity from the data patterns [12]. In

Manuscript received June 30, 2013; revised October 11, 2013; accepted November 17, 2013. Date of publication November 27, 2013; date of current version March 3, 2014. This work was partially supported by Natural Sciences and Engineering Research Council of Canada and Care in Motion and the International Cooperative Program of Shenzhen City (ZYA201106090040A).

Q. Shen, X. Liang, and X. (S.) Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, ON N2L 3G1, Canada (e-mail: q2shen@uwaterloo.ca; x27liang@uwaterloo.ca; sshen@uwaterloo.ca).

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON L1H 7K4, Canada (e-mail: xiaodong.lin@uoit.ca).

H. Y. Luo is with Care in Motion Technology Inc., Waterloo, ON N2V 1G4, Canada (e-mail: henryhongluo@hotmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JBHI.2013.2292829

this case, user's privacy would be undermined and the use of e-health monitoring systems would put user's life in danger. The traffic-shaping algorithm, which shapes the distribution of traffic, has been proposed in [13] as a countermeasure to TA attacks. In [13], Wright *et al.* conclude that it is necessary to minimize the difference in distribution between the shaped traffic and target traffic to preserve privacy from TA attacks. However, the algorithm in [13] does not preserve the time dependency of a target process. The time dependency can be measured by the autocorrelation of a random process. Autocorrelation gives the correlation between values of a process at different times. It has been proven to be an effective method to identify traffic flows [14]. Thus, an efficient shaping algorithm, which is capable of shaping health data to nonhealth data while considering the autocorrelation, is desirable.

In this paper, we propose an e-health monitoring system supported by geo-distributed clouds. The geo-distributed clouds consist of many cloud servers which are geographically deployed over a large region [15]. The proposed e-health monitoring system consists of two parts, a resource allocation scheme for servers and a traffic-shaping algorithm for users. The servers are initialized with the same resource allocation scheme. When users require to connect to the system, the local server (geographically-close to the users) handles the request and checks the workloads of other servers. It then runs the resource allocation scheme and responds to the users with the assigned servers. After receiving the responses, users apply a traffic-shaping algorithm on their health data before transmitting the data to the assigned servers. The traffic-shaping algorithm hides the original health data and preserves user privacy. Specifically, our contributions are twofold.

First, we propose a resource allocation scheme to achieve the minimized service delay and the reduced communication costs. We first derive a sufficient condition in resource allocation to ensure the stability of cloud servers. Considering this condition, we design the resource allocation scheme: each server only redirects the requests to others who have shorter queue lengths; and the number of redirected requests must be proportioned to the difference of their queue lengths and reciprocal to the service delay between them. We also prove that the proposed resource allocation scheme satisfies the derived sufficient condition in the balanced state. In addition, we compare the scheme with two other alternatives using jointly the short queue (JSQ) and distributed control law (DCL), both of which are proven to be stable. Through extensive simulations, we show that our scheme achieves a much smaller average service delay than the JSQ-based and DCL-based schemes.

Second, we propose a traffic-shaping algorithm to prevent the health data of users from being detected by the TA attackers. We focus on the health data traffics generated by e-health monitoring systems, such as heart rate and blood pressure, which are typically modelled as deterministic processes [16]. We analyze the statistical differences between the health data traffic and nonhealth data traffic. Our proposed shaping algorithm is designed such that: the distribution of the shaped health data traffic is the same as the distribution of the nonhealth data traffic; and the autocorrelation of the shaped health data traffic is close to the autocorrelation of the nonhealth data traffic. We propose to preserve the autocorrelations of the target process. Note that the proposed algorithm introduces a delay, referred as shaping delay, on the user side which is related to the privacy requirement. We provide the numeric results on this relation. Then, we model the shaping delay by the D/M/1 queue, and consider the shaping delay into the resource allocation scheme. The simulation results show that our resource allocation scheme is still efficient with the shaping delay.

The remainder of this paper is organized as follows. Section II presents related works, and Section III describes the system model. In Section IV, the resource allocation scheme and traffic-shaping algorithm are proposed, with the numerical analysis and the performance evaluation in Sections V and VI, respectively. Finally, the conclusions and future works are given in Section VII.

II. Related Works

In this section, we review the related works in resource allocation and privacy preservation for e-health monitoring systems.

A. Resource Allocation for E-Health

E-health monitoring systems have attracted great attention recently, and their applications have been developed widely [17], [18]. Due to the surging computing and storage demands from these applications, geo-distributed clouds have been regarded as promising solutions [6], [19]. In geo-distributed clouds for e-health monitoring systems, resource allocation acts as a critical component to provide timely and reliable services [20]. Previous works on resource allocation for geo-distributed clouds have two objectives: one is to reduce the service delay for users and the other is to reduce the cost for the service provider. From a user's perspective, Alicherry and Lakshman [21] proposed a centralized resource allocation scheme for geo-distributed clouds to minimize the service delay among selected servers, and a heuristic algorithm to partition a requested resource among the chosen servers. By exploiting the characteristics of social influences, Wu *et al.* [9] proposed an online resource allocation scheme to efficiently migrate contents, and redirect user requests to appropriate servers for timely responses. To reduce the operating cost for service providers, a scheme that distributes requests among geo-distributed clouds to utilize the spatial differences in electricity price is proposed in [8]. For service providers, load balance is also an important requirement for its crucial role played to maintain the stability of all servers. As pointed out by paper [22], without proper resource allocation, requests may be redirected to a single server, leading to congestions. Manfredi *et al.* [23] designed a distributed scheme for geo-distributed clouds, which stabilizes all the servers. In this paper, we study the resource allocation in geo-distributed clouds for e-health monitoring systems, where both average service delay and stability of clouds are considered as design objectives.

B. Privacy Preservation for E-Health

The flourish of e-health monitoring systems faces the challenges in privacy preservation [24], [25]. TA attacks have been recognized as effective methods to reveal the type of users' health data [12]. Two countermeasures have been proposed, one

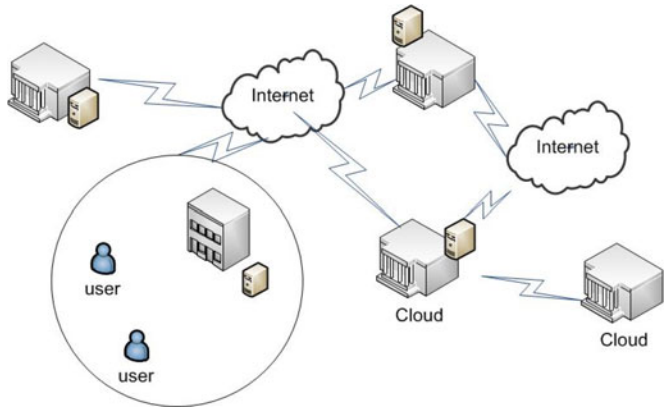

Fig. 1. Geo-distributed clouds environment.

algorithm is padding and the other algorithm is traffic shaping [13]. Padding algorithms obfuscate the packet length and rate by padding random amount of plaintext. The drawback of padding algorithms is that a large amount of bandwidth is required. In e-health monitoring systems, sensors on human body have limited energy and communication capabilities [3]. Thus, padding algorithms are not suitable for e-health monitoring systems. The traffic-shaping algorithm shapes the distribution of a traffic [13]. The key of this algorithm is to randomly sample a predefined matrix for the distribution transformation. As indicated by [11], this algorithm is not effective in preserving a user's privacy for it does not consider the time dependency of a random process. In this paper, we plan to design an efficient traffic-shaping algorithm for e-health monitoring systems by addressing the aforementioned problems.

III. System Model

A. System Model

We consider geo-distributed clouds in e-health monitoring systems. As shown in Fig. 1, N cloud servers locate in different geographic regions. Each region $\{1, \ldots, N\}$ has one server. The server in the ith region is denoted by S_i. The service capacity is evaluated by the number of virtual machines, a server has. Thus, the service capacity is limited. We consider time is slotted. At a different time slot, servers have different available service capability due to the dynamic allocation. Let $\mu_i(t)$, $i \in \{1, \ldots, N\}$ denote the available service capacity of server S_i during time slot t.

The service requests for a server come from the users in the region that the server locates. Let $Q_i(t)$ denote the number of waiting requests (queue length) of server S_i at the beginning time slot t. Let $A_i(t)$ denote the number of arrival requests for the server S_i during time slot t. $A_i(t)$ is considered as a Poisson process with arrival rate λ_i. For each arrival request, it contains certain amount of traffic. We consider the traffic from one request is a deterministic process with constant traffic arrival rate λ_m [16].

The service delay for any request includes two parts. One is the shaping delay due to the traffic-shaping algorithm. The other one is the communication delay. Let D^p denote the shaping delay by the traffic-shaping algorithm, and $D^c_{i,j}$ denote the communication delay between region i and region j. As indicated by [21], the communication delay in geo-distributed clouds cannot be negligible. We consider the communication delay over the Internet by measuring the geographic distance, i.e., communication delay increases linearly with the geographic distance [8]. Let $L_{i,j}$ denote the distance between region i and region j. From [8], we consider the slop of the linear function as

$$\frac{\delta(\text{time})}{\delta(\text{distance})} \approx 0.02 \text{ ms/km}. \tag{1}$$

The communication delay $D^c_{i,j}$ can be calculated as

$$D^c_{i,j}(\text{ms}) = 0.02(\text{ms/km}) \times L_{i,j}(\text{km}) + 5(\text{ms}). \tag{2}$$

We consider the TA attacks in the geo-distributed clouds environment. Such attacks aim to analyze the traffic statistics to determine the specific type of the health data. We measure the capability of TA attacks by using the Kullback–Leibler (K-L) divergence [26]. The K-L divergence is also referred as relative entropy to measure the difference between two probability distributions. Let P denote the distribution of the health data traffic and Q denote the distribution of the nonhealth data traffic. Let $D_{\mathrm{KL}}(P\|Q)$ denote the K-L divergence. We have

$$D_{\mathrm{KL}}(P\|Q) = \int \ln\left\{\frac{f_p(x)}{f_q(x)}\right\} f_p(x)dx \tag{3}$$

where $f_p(x)$ and $f_q(x)$ are the probability density functions of distributions P and Q, respectively. The K-L divergence reaches its minimum when $f_p(x) = f_q(x)$. When two distributions P and Q are the same, the capability of TA attacks is reduced to the minimum.

IV. Proposed E-Health Monitoring System

In this section, we propose an e-health monitoring system with minimum service delay and privacy preservation. The system consists of two parts, the traffic-shaping algorithm and the resource allocation scheme. The traffic-shaping algorithm converts the health data traffic to the nonhealth data traffic such that the capability of the TA attacks is largely reduced. The resource allocation scheme considering load balance as a necessary condition aims to minimize the service delay.

A. Traffic Shaping

In this section, we propose an effective traffic-shaping algorithm to preserve users' privacy against TA attacks. We choose voice traffic as target traffic for two reasons: different from other common internet traffics, voice traffic is not heavy tailed and thus consumes less bandwidth; and voice traffic is given higher priority than data traffics in communication protocols [27], which helps health data to reduce the medium access time when competing with other traffics.

We demonstrate why the existing traffic-shaping algorithm is not suitable for time-dependent random process. Consider a voice source. Due to its characteristics that voice source could be divided into talk spurt and silent period, voice traffic is modeled using the ON–OFF model. Let α and β denote the average ON and OFF period of voice, respectively. During the talk spurt, the voice source generates packets with length L_{voice} with packet

interarrival time t_a, whereas during silent period, no packet is generated. In existing traffic-shaping algorithm in use, the distribution of voice traffic is preserved in the following way. Whenever a packet is available for transmission, with probability $\frac{\alpha}{\alpha+\beta}$ the packet is transmitted. Thus, the probability of the output traffic in ON state is $\frac{\alpha}{\alpha+\beta}$, which is the same as the voice traffic. However, the average length of the ON period might not be α. Namely, the time-dependence feature of voice traffic is not shown in the shaped traffic. As a result, a TA attacker could use autocorrelation to distinguish the shaped traffic from real-voice traffics.

1) Traffic-Shaping Algorithm: Since the arrival rate of health data λ_m could be larger than that of a single voice source, the target traffic could be a traffic containing multiple voice sources. Given a constant health data arrival rate λ_m, a user first decides the number of voice traffics in the target traffic, denoted by N_v. The choice of N_v shall satisfy the condition that the average traffic rate of the target traffic should be no less than the average arriving rate of health data. Otherwise, the shaping delay caused by this algorithm could not be limited, since the departure rate is less than the arrival rate. Given the utilization factor ρ_v of a voice traffic equals to $\frac{\alpha}{\alpha+\beta}$ and the traffic rate λ_v of a voice traffic during talk spurt, the number of voice traffics should satisfy

$$N_v \geqslant \left\lceil \frac{\lambda_m}{\rho_v \lambda_v} \right\rceil \tag{4}$$

where $\lceil x \rceil$ is the minimum integer greater than x.

After choosing the number of voice sources N_v, the user accumulates traffics in its buffer and then transmits them according to the traffic generation rate of N_v voice sources. The traffic rate of N_v voice sources is a binomial process with each voice source in ON state with probability $\frac{\alpha}{\alpha+\beta}$. Thus, the probability of the traffic generating rate equals $i\lambda_v$ is

$$\Pr\{r = i\lambda_v\} = C_{N_v}^{i} \left(\frac{\alpha}{\alpha+\beta}\right)^{i} \left(\frac{\beta}{\alpha+\beta}\right)^{(N_v - i)} \tag{5}$$

where $C_{N_v}^{i}$ is equal to $\frac{N_v!}{i!(N_v-i)!}$. For each time slot, a user chooses a traffic generating rate based on the probability described by (5), and uses the rate to transmit.

The output traffic of the shaping algorithm is not identical to N_v voice sources. The reason is that the probability that health data available are insufficient for a chosen traffic rate is positive. In the previous study, this problem is solved through adding redundant plaintext. However, this algorithm introduces extra delay and energy cost of a mobile device. Since mobile devices are power limited, we choose not to pad redundant plaintext in these cases for energy saving purposes.

B. Resource Allocation

In this section, we design a resource allocation scheme for the e-health monitoring systems with stabilized server queues and reduced service delay.

A server receives requests from the users in the local region and performs the resource allocations. Specifically, the server first collects the queue length $Q_j(t)$ from other servers $j \in \{1, \ldots, N\}$. Considering the service delay and the queue length, the server then determines the allocation strategy where some requests will be redirected to other servers. Let $A_i^U(t)$ denote the number of request arriving at server S_i during time slot t after the redirections are made. The queue length of server $i \in \{1, \ldots, N\}$ at time slot $t+1$ can be represented as

$$Q_i(t+1) = \max[Q_i(t) + A_i^U(t) - \mu_i(t), 0]. \tag{6}$$

Then, the local cloud feedbacks its decision to end users. Each user directs its traffic directly to the assigned server.

1) Resource Allocation Constraints: We present the stabilization concept and explain the importance of stabilizing all servers. Based on the stability condition, to ensure the stability of server S_i, we need resource allocation scheme such that

$$E_t\left[A_i^U(t)\right] \leqslant E_t[\mu_i(t)] \tag{7}$$

where $E_t[x]$ is the expectation of random process x over t.

In the e-health monitoring systems, failure or overload of any server could cause fatal results. Thus, the resource allocation scheme for health data must achieve the stability condition for all servers, i.e., (7) needs to be satisfied for any $i \in \{1, \ldots, N\}$. To design the resource allocation scheme satisfying the aforementioned conditions is difficult. For each server could redirect parts of its requests to other servers, which requires a scheme to consider the interactions among different servers.

To solve this problem, we first investigate a sufficient condition to achieve stability. Considering this condition, we then propose a delay aware algorithm.

2) Sufficient Condition: We derive a sufficient condition, which ensures the stability for all servers in the geo-distributed clouds environment. We start from the definition of stability.

Definition 1: Suppose a process $q(t)$ has an equilibrium q_e, if for every $\epsilon > 0$, there exists a $\delta = \delta(\epsilon) > 0$ such that, if $\|q(0) - q_e\| < \delta$, then $\|q(t) - q_e\| < \epsilon$, for every $t \geqslant 0$.

From definition 1, we can see that, if a process $q(t)$ reaches q_e at time slot n, namely $q(n) = q_e$, any scheduling policy that guarantees $q(n+1) - q(n) = 0$ can stabilize $q(t)$. Thus, $\Delta q = q(n+1) - q(n) = 0$ is a sufficient condition for a process to achieve stability.

Let a vector $[Q_1(t), \ldots, Q_N(t)]'$ be the queue length of the interactive servers, denoted by $\overrightarrow{Q(t)}_{1\times N}$. The sufficient condition could be represented as

$$\Delta\overrightarrow{Q(t)} = \overrightarrow{Q(t+1)} - \overrightarrow{Q(t)} = \vec{0}, \text{given } \overrightarrow{Q(t)} = \overrightarrow{Q_e}. \tag{8}$$

Since our purpose is to design a resource allocation scheme that makes decisions based on current queue length, the change in queue length of all servers can be presented by

$$\Delta\overrightarrow{Q(t)} = \mathbf{U}\overrightarrow{Q(t)} \tag{9}$$

where $\mathbf{U}$ is an $N \times N$ matrix, and $U_{i,j}$ represents the number of requests that server S_i redirected to server S_j. Based on this interpretation, the sufficient condition for multiple interactive queues (8) can be written as

$$\mathbf{U}\overrightarrow{Q_e} = \overrightarrow{0}. \tag{10}$$

Equation (10) could also be written as a system of equations

$$\begin{cases} U_{11}Q_{e1} + U_{12}Q_{e2} + \cdots + U_{1N}Q_{eN} = 0 \\ \vdots \\ U_{11}Q_{e1} + U_{12}Q_{e2} + \cdots + U_{1N}Q_{eN} = 0. \end{cases} \tag{11}$$

To design a resource allocation scheme, which ensures the stability of all servers, is to determine the value of each U_{ij} such that the system of equations (11) is satisfied. The system of equations (11) has N equations and $N \times N$ unknown. Thus, there is more than one solution to (11). In other words, there are multiple schemes, which can satisfy the constraints.

3) Resource Allocation Scheme: In this subsection, we design a resource allocation scheme that satisfies (11). The idea is based on the fact that zero is an eigenvalue of any Laplacian matrix corresponding to vector $[1, 1, \ldots, 1]_{1\times N}$ [23], [28]. In addition, the resource allocation scheme is designed to minimize service delay.

In a resource allocation scheme, we need to design a matrix $\mathbf{U}$ to satisfy condition (10). We present how eigenvalue could facilitate the scheme design. An eigenvector of a square matrix $\mathbf{U}$ is a vector $\overrightarrow{e_u}$ that satisfies

$$\mathbf{U}\overrightarrow{e_u} = \mathbf{m_u}\overrightarrow{e_u} \tag{12}$$

where m_u is the corresponding eigenvalue. For the Laplacian matrix, zero is always an eigenvalue corresponding to $\overrightarrow{1}$. Consider an equilibrium state of all servers is balanced, namely $\overrightarrow{Q_e} = q_e\overrightarrow{1}$, then any $\mathbf{U}$, which is a Laplacian matrix, can stabilize all servers in the geo-distributed clouds. Thus, designing a resource allocation scheme such that $\mathbf{U}$ is a Laplacian matrix can achieve load balance. Based on this observation, we design a resource allocation scheme in the following.

Algorithm 1: Resource Allocation Scheme

1) For each server S_i: the server measures the communication delay $D^c_{i,j}$ between itself and server S_j for all servers $j \in [1, N], j \neq i$;
2) Based on link information, each server S_i sets the the privacy requirements $D^{i,j}_{KL}$, in terms of K-L divergence, for different link $L_{i,j}$, then calculates the shaping delay $D^p_{i,j}$ incurred for privacy preservation requirements. Specifically, in our proposed privacy preservation scheme, a server S_i chooses the number of voice traffic N_v such that

$$D_{KL}(N_v) \leqslant D^{i,j}_{KL}; \tag{13}$$

a server S_i uses the result from equation (13) to calculate the shaping delay $D^p_{i,j}$ for each link.
3) A server S_i calculates the service delay for accessing each server S_j, $D_{i,j} = D^c_{i,j} + D^p_{i,j}$.
4) A server S_i updates the buffer length information of other servers $Q_j(t)$, and redirects request according to

$$Q_i(t+1) = Q_i(t) + \sum_j M_{i,j}(t), \tag{14}$$

where

$$M_{i,j}(t) = \begin{cases} \frac{(Q_i(t)-Q_j(t))A_i}{D_{i,j}M_i^{max}} & \text{Otherwise} \\ -M_{j,i} \text{ for } j \in (Q_i(t) < Q_j(t)), \end{cases} \tag{15}$$

where $M_i^{max} = \sum_{j\in(Q_i(t)>Q_j(t))} \frac{(Q_i(t)-Q_j(t))}{D_{i,j}}$.

The scheme design utilizes two facts: to stabilize all servers, the server with shorter queue length shall serve more requests; to reduce delay, a request prefers servers with less service delay. Thus, a good design should have two characteristics: requests should only be directed to servers with shorter queues; and the amount of redirected requests shall be an increasing function of queue length difference, and be a decreasing function of service delay.

V. Numerical Analysis

This section evaluates the performances of our proposed traffic-shaping algorithm and resource allocation scheme.

A. Performance of the Traffic-Shaping Algorithm

In this section, we present the analysis of the shaping delay and the privacy preservation of the proposed traffic-shaping algorithm.

1) Shaping Delay Performance: The arrival rate of health data is a constant, whereas the departure rate of the shaping algorithm is a random process that obeys binomial distribution. Since the binomial distribution converges to a Poisson distribution as the number of tests goes to infinity, we approximate the service process as a Poisson process in this paper. Based on this approximation, the delay introduced by the traffic-shaping algorithm could be analyzed through a D/M/1 queue. Based on the analysis in [29], the queue stationary distribution utilization factor $\rho = \frac{\lambda_m}{N_v\lambda_v\rho_v} < 1$ is given by

$$\pi_i = \begin{cases} 0, & \text{when } i = 0 \\ (1-\delta)\delta^{(i-1)}, & \text{when } i > 0 \end{cases} \tag{16}$$

where δ is the smallest absolute value of all solutions to equation

$$\rho = -\frac{1-\delta}{\ln\delta}. \tag{17}$$

Further, the average shaping delay introduced by the shaping algorithm could be calculated based on (16). Let $D_m(N_v)$ denote the average shaping delay with N_v voice sources; it can be calculated as [29]

$$D_m(N_v) = \frac{1}{N_v\rho_v\lambda_v}\frac{\delta}{1-\delta}. \tag{18}$$

2) Privacy Preservation: In the following, we present the analysis of the privacy preservation capability, which is measured by the K-L divergence, of our proposed traffic-shaping algorithm.

To analyze the privacy preservation performance of our proposed traffic shaping algorithm based on the K-L divergence, we need to know the distribution of the target traffic and the distribution of our algorithm output. The target traffic obeys Poisson as discussed previously, whereas the distribution of the output is unknown. We present the analysis on the distribution of the output as follows.

The output of our proposed algorithm has the same distribution as that of the output of D/M/1 queue. Given utilization factor $\rho < 0.2$, the output of D/M/1 queue is not Poisson, namely the distribution of the time between two consecutive departure does

not obey exponential distribution [30]. Low utilization factor ρ represents a high service rate compared to the arrival rate, thus smaller average waiting time. However, in this case, the leakage risk is high, since the output deviates from the target traffic significantly. As utilization factor ρ goes from 0.2 to 1, the difference between the output and Poisson process diminishes, and is 0 when ρ is 1 [30]. We do not consider the situation where utilization factor $\rho > 1$, for the queue is stable under this condition. Motivated by the previous facts, we adopt Poisson process to approximate the output of our proposed traffic-shaping algorithm for utilization factor $\rho \in (0.2, 1)$.

Based on the previous analysis, the privacy preservation performance of our proposed traffic shaping-algorithm can be described by the K-L divergence of two Poisson processes. Since the interarrival time is the identity of a Poisson process, we consider the K-L divergence of two exponential distributions, which represents the interarrival time of the algorithm output and the target traffic, respectively. The average interarrival time of the algorithm output is equal to that of the input, namely the average interarrival time of the health data $\frac{1}{\lambda_m}$. The average interarrival time of the target process is $\frac{1}{N_v \rho_v \lambda_v}$. The K-L divergence between them is

$$\begin{aligned} D_{\mathrm{KL}}(P\|Q) &= \int_0^\infty \lambda_p e^{-\lambda_p x} \ln\left(\frac{\lambda_p e^{-\lambda_p x}}{\lambda_q e^{-\lambda_q x}}\right) dx \\ &= \int_0^\infty \lambda_p e^{-\lambda_p x} \left(\ln\left(\frac{\lambda_p}{\lambda_q}\right) + (-\lambda_p + \lambda_q)x\right) dx \\ &= \ln\left(\frac{\lambda_p}{\lambda_q}\right) \int_0^\infty \lambda_p e^{-\lambda_p x} dx + E_p[(-\lambda_p + \lambda_q)x] \\ &= \ln\left(\frac{\lambda_p}{\lambda_q}\right) + \frac{-\lambda_p + \lambda_q}{\lambda_p} \end{aligned} \tag{19}$$

where $\lambda_p = \lambda_m$ and $\lambda_q = N_v \rho_v \lambda_v$.

B. Performance of Resource Allocation Scheme

In the following, we show that the resource scheme proposed could stabilize all servers.

Theorem 1: If the network operates under our proposed algorithm 1, the network will stay in the balanced state.

Proof: We prove theorem 1 through showing that (14) satisfies the sufficient condition (9).

Equation (14) could be written as

$$Q_i(t+1) - Q_i(t) = \sum_j M'_{i,j}(t)(Q_i(t) - Q_j(t)) \tag{20}$$

where $M'_{i,j}(t) = \frac{M_{i,j}(t)}{(Q_i(t) - Q_j(t))}$.

Equation (20) could also be written in the form of (9). Thus, the relationship between $M'_{j,i}$ and $U_{i,j}$ could be described by

$$\sum_j U_{i,j}(t) Q_j = \sum_j M'_{i,j}(Q_i(t) - Q_j(t)). \tag{21}$$

Solving (21), we obtain

$$U_{i,j}(t) = \begin{cases} -M'_{i,j}, & \text{for } j \neq i \\ \sum_{j \neq i} M'_{i,j}(t) & \text{for } j = i. \end{cases} \tag{22}$$

Fig. 2. Map of Canada's major cities.

Based on (15) and (22), it is easy to verify that the matrix $\mathbf{U}$ generated under our propose scheme is a Laplacian matrix. As a result, condition (10) is satisfied when the distributed clouds are in the balanced state. □

VI. Performance Evaluation

In this section, we evaluate our proposed traffic-shaping algorithm and resource allocation scheme through simulations. We first choose to compare our proposed traffic-shaping algorithm with an existing traffic-shaping algorithm. We are interested in autocorrelation feature preservation, and the tradeoff between delay performance and privacy preservation ability. Then, we compare the proposed resource allocation scheme with the JSQ-based approach [31] and DCL-based approach [23]. We are interested in the delay performance and the queue length performance.

A. Simulation Setup

We consider a geo-distributed clouds environment where cloud servers are deployed in Canada. As shown in Fig. 2, the servers are placed on $N = 17$ cities (regions) in Canada. The distance between any two regions $L_{i,j}$ for $i, j \in \{1, \ldots N\}$ are measured using Google Maps. The request arrival rate of ith server λ_i is chosen to be proportional to the population of the region, whereas the service rate is chosen to be proportional to the number of hospitals of that region. In order to evaluate our resource allocation, we initialize servers with different queue lengths. Note that a saturated network is defined [23] when

$$\sum \lambda_i = \sum \mu_i. \tag{23}$$

We slightly increase the arrival rates such that the previous (23) could be satisfied. The detailed settings can be found in Table I.

TABLE I
NETWORK PARAMETERS

City Name	arrival rate	service rate	initial buffer
S.t. Johns	2	2	200
Charlottetown	1	1	100
Halifax	4	9	50
Fredericton	1	1	250
Quebec	6	7	200
Montreal	17	33	100
Ottawa	9	9	200
Toronto	55	24	100
Winnipeg	7	9	50
Regina	2	2	250
Saskatoon	3	3	100
Edmonton	11	12	100
Calgary	11	11	250
Vancouver	23	23	200
Victoria	3.5	8	100
Whitehorse	0.3	1	50
Yellowknife	0.2	1	150

TABLE II
TRAFFIC PARAMETERS

Parameter	Value	Parameter	Value
α	352 ms	β	650 ms
A_v	4kbps	A_m	30kbps

For each service request, we set the arrival rate as 30 kbps [16]. For the traffic shaping target, we choose a coded version voice traffic according to GSM 6.10 codec. The average duration of ON state, OFF state, and the average arrival rate are listed in Table II.

In the existing traffic-shaping algorithm, a matrix, which is designed based on the distributions of the source and target traffic, is sampled randomly to shape the traffic distribution. To shape a medical traffic with a constant arrival rate into the ON–OFF traffic, a vector $[1, 1]$ is sampled based on probability $[\frac{\alpha}{\alpha+\beta}, \frac{\beta}{\alpha+\beta}]$.

In the JSQ scheme [31], the server with the shortest queue is chosen to serve the users. Specially, server i chooses the j^*th server to redirect its requests, based on

$$j^* = \text{argmin}_{j\in\{1,\ldots,N\}} Q_j(t). \tag{24}$$

In the DCL algorithm, the amount of traffic from server j to server i is calculated as

$$U_{i,j}(t) = \frac{(Q_i(t) - Q_j(t))A_i}{\sum_{j\in N_{i-}}(Q_i(t) - Q_j(t))}. \tag{25}$$

B. Traffic-Shaping Algorithm Evaluation

In this section, we provide simulation results to show: 1) our proposed traffic-shaping algorithm can preserve the autocorrelation features of the target process; and 2) there is a tradeoff between shaping delay and privacy leakage risk. We use TM and TS to denote the traffic-shaping algorithm in [13] and in this paper, respectively.

Fig. 3 shows simulation results of the normalized autocorrelation of voice traffic, a medical traffic shaped by TM, and shaped by TS with lags no larger than 20. The results show that TS

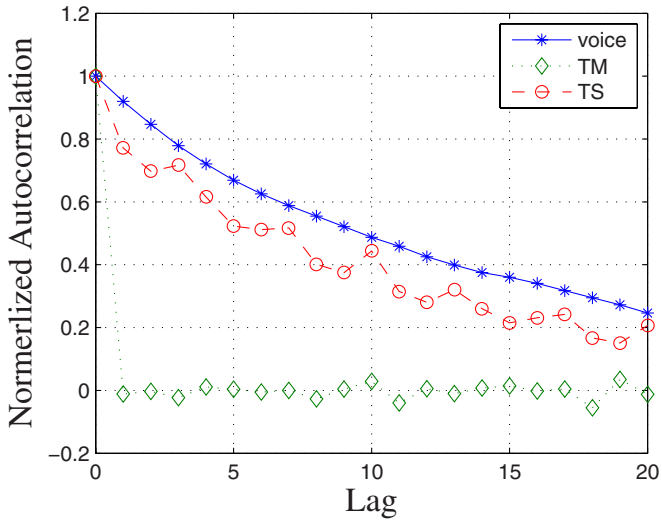

Fig. 3. Autocorrelations of voice, TM and TS.

outperforms TM significantly in preserving the autocorrelation features of voice traffic. As it can be observed that, the autocorrelation of the output of algorithm TM is almost 0 when lag is larger than 0. That is to say, the time dependency feature of a target process, in terms of autocorrelation, is not preserved in TM, as explained in Section IV-A. In comparison, the autocorrelation of TS is similar to that of a target traffic. The reason is that, TM shapes the traffic based on the time dependent features of a target traffic. Specifically, TM shapes the medical traffic to mimic the ON–OFF behavior of voice traffic.

Consider a TA attacker runs a classifier, which chooses the changing rate of the autocorrelation as the classification characteristic [32]. As we can observe from Fig. 3., the decreasing rate of the autocorrelation of voice increases slowly and smoothly. The decreasing rate of autocorrelation of TS is similar as that of voice only with small turbulences. In comparison, the autocorrelation of TM decreases sharply and remains almost constant. In this case, the TM could be identified by the TA attacker, whereas TS is hard to detect. When a classifier is adopted by a TA attacker, the autocorrelation between the shaped and the voice traffic needs to have significant similarity to avoid being identified [33]. Thus, we can conclude the improvement of TS over TM in terms of autocorrelation is important for privacy preservation.

Fig. 4 shows the tradeoff between shaping delay and privacy leakage risk using our proposed traffic shaping scheme. The results are obtained through numerical simulation based on the analysis on the average shaping delay and privacy preservation capability in Section V. It can be observed that as the number of the chosen voice source increases, the shaping delay of our proposed algorithm decreases, whereas the K-L divergence increases. The reason is that, when the number of voice source adopted increases, the number of voice traffics that are in ON state increases, leading to shorter time for the health data waiting to be packeted and transmitted. However, in this case, the probability of insufficient health data packets increases at the same

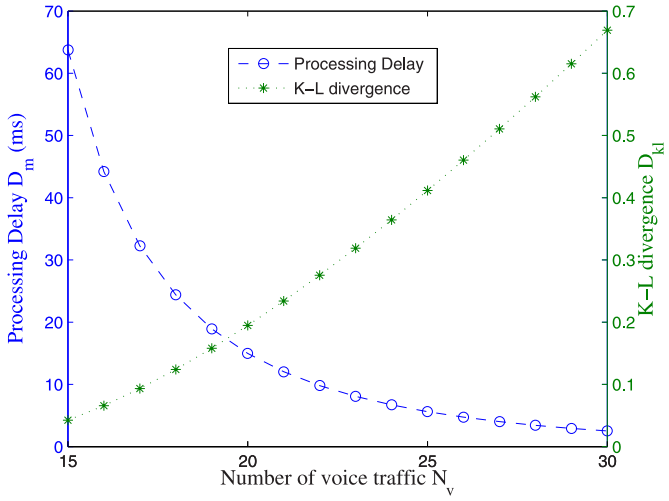

Fig. 4. Tradeoff between privacy preservation and shaping delay.

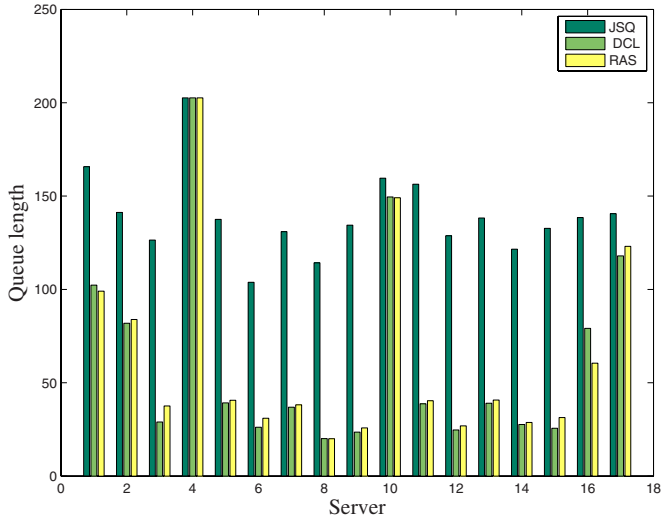

Fig. 6. Comparison of average queue length of JSR, DCL, and RAS.

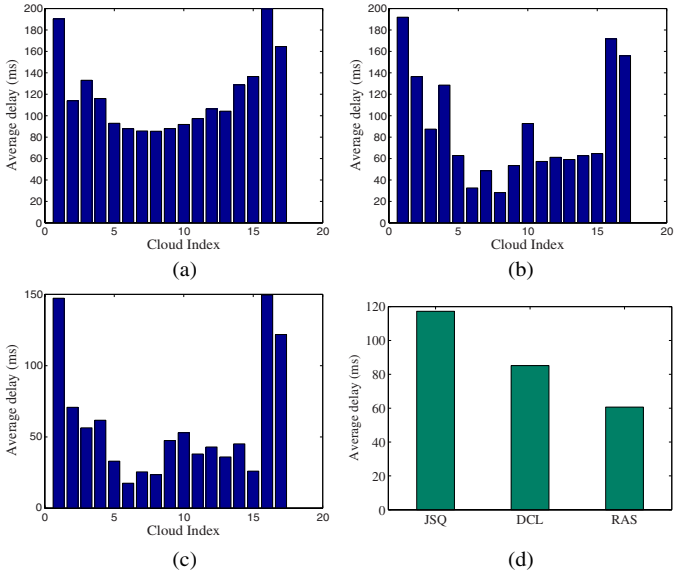

Fig. 5. Average service delay performance. (a) Delay performance of JSQ. (b) Delay performance of DCL. (c) Delay performance of RAS. (d) Average service delay comparison.

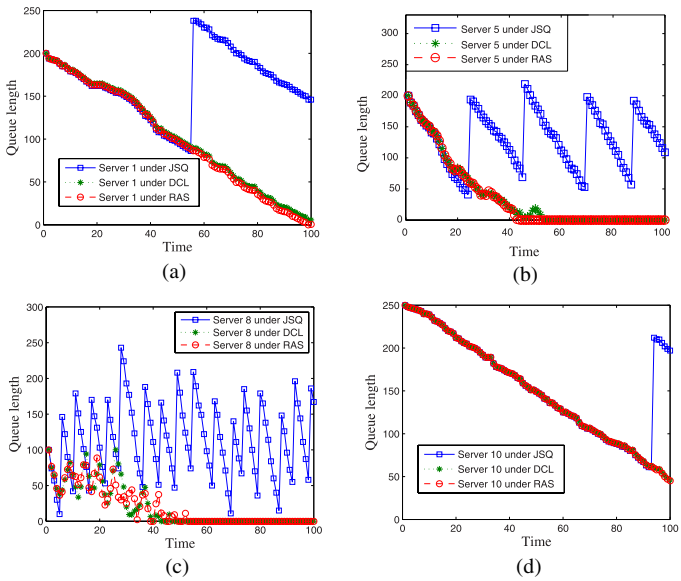

Fig. 7. Queue dynamics. (a) Server at St. John. (b) Server at Quebec. (c) Server at Toronto. (d) Server at Regina.

time, leading to a larger K-L divergence, i.e., higher privacy leakage risk.

C. Resource Allocation Scheme Evaluation

In this section, we provide simulation results to demonstrate two benefits of our proposed scheme: 1) reduce the delay suffered by traffics; and 2) achieve load balance among different servers. We use RAS denote the algorithm designed in this paper.

1) Average Service Delay: The service delay performances of three algorithms, namely JSQ, DCL, and RAS, are shown in Fig. 5. It can be seen from Fig. 5(d), the average service delay of all requests under three algorithms are 120, 87, and 56 ms, respectively. The reason why our algorithm has smaller average service delay is that, in our algorithm, the amount of requests redirected to other clouds is reciprocal to the service delay among two clouds. This method limits the number of requests to be redirected to a remote cloud server, thus introducing less delay for the requests. The average service delay suffered by the requests to each cloud under algorithm JSQ, DCL, and RAS, are shown in Fig. 5(a)–(c), respectively. As we can observe that, the average service delay for requests to each cloud under the JSQ is higher than that under DCL and RAS. The reason is that, JSQ always pours all the requests to the cloud with the smallest queue length. Thus, when the cloud with smallest queue length is far away, the delay is significantly large. In comparison, both DCL and RAS redirect requests to all other servers with the smaller queue length, thus avoid the situation to direct all requests to the remote cloud.

2) Queue Length: The average queue length for all clouds under algorithm JSQ, DCL, and RAS, are shown in Fig. 6. It can be seen that, the average queue length under JSQ is higher than that under DCL and RAS. The reason is that, JSQ is designed to maximize the throughput of the distributed clouds. So, its algorithm is designed to avoid the situation where any buffer is empty. Thus, the average queue length is the highest. We can also observe that, the average queue length under RAS is comparable to the average queue length under DCL. This proves the ability of our proposed algorithm in stabilizing the cloud networks.

The queue dynamics of all clouds under the algorithm JSQ, DCL, and RAS, are shown in Fig. 7.

The queue dynamics over each iteration for cloud at St. John, Quebec, Toronto, and Regina are shown in Fig. 7(a)–(d), respectively. In can be seen that, compared to JSQ, both DCL and RAS perform better in terms of eliminating backlogs and ensuring the stability of all clouds. And our proposed algorithm is comparable to DCL, in terms of maintaining the stability of all clouds.

VII. Conclusion and Future Works

In this paper, we have explored geo-distributed clouds to propose an e-health monitoring system with minimum service delay and privacy preservation. We have provided the numerical analysis and simulation results to demonstrate the effectiveness of the system. For our future study, we will extend this work by studying a more general and complicated case where users have random medical requests and diverse privacy preservation requirements.

References

[1] Z. Li, B. Wang, C. Yang, Q. Xie, and C.-Y. Su, "Boosting-based EMG patterns classification scheme for robustness enhancement," *IEEE J. Biomed. Health Informat.*, vol. 17, no. 3, pp. 545–552, May 2013.

[2] D. A. Nowak and G. R. Fink, "Psychogenic movement disorders: Aetiology, phenomenology, neuroanatomical correlates, and therapeutic approaches," *NeuroImage*, vol. 47, no. 3, pp. 1015–1025, 2009.

[3] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," in *Proc. IEEE Conf. Comput. Commun.*, 2012, pp. 388–396.

[4] A. Soomro and D. Cavalcanti, "Opportunities and challenges in using WPAN and WLAN technologies in medical environments," *IEEE Commun. Mag.*, vol. 45, no. 2, pp. 114–122, Feb. 2007.

[5] H. Lee, K.-J. Park, Y.-B. Ko, and C.-H. Choi, "Wireless LAN with medical-grade QoS for e-healthcare," *IEEE J. Commun. Netw.*, vol. 13, no. 2, pp. 149–159, Apr. 2011.

[6] M. Barua, X. Liang, R. Lu, and X. Shen, "Espac: Enabling security and patient-centric access control for e-health in cloud computing," *Int. J. Security Netw.*, vol. 6, no. 2/3, pp. 67–76, 2011.

[7] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[8] A. Qureshi, "Power-demand routing in massive geo-distributed systems," Ph.D. dissertation, Massachusetts Inst. Technol., Cambridge, MA, USA, 2010.

[9] Y. Wu, C. Wu, B. Li, L. Zhang, Z. Li, and F. C. M. Lau, "Scaling social media applications into geo-distributed clouds," in *Proc. IEEE Conf. Comput. Commun.*, 2012, pp. 684–692.

[10] C. J. Debono, B. W. Micallef, N. Y. Philip, A. Alinejad, R. S. H. Istepanian, and N. N. Amso, "Cross-layer design for optimized region of interest of ultrasound video data over mobile WIMAX," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1007–1014, Nov. 2012.

[11] K. P. Dyer, S. E. Coull, T. Ristenpart, and T. Shrimpton, "Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail," in *Proc. IEEE Symp. Security Privacy*, 2012, pp. 332–346.

[12] L. Buttyán and T. Holczer, "Traffic analysis attacks and countermeasures in wireless body area sensor networks," in *Proc. IEEE Int. Symp. World Wireless, Mobile, Multimedia Netw.*, 2012, pp. 1–6.

[13] C. V. Wright, S. E. Coull, and F. Monrose, "Traffic morphing: An efficient defense against statistical traffic analysis," in *Proc. 16th Netw. Distributed Security Symp.*, 2009, pp. 237–250.

[14] P. Branch and J. But, "Rapid and generalized identification of packetized voice traffic flows," in *Proc. 37th Conf. Local Comput. Netw.*, 2012, pp. 85–92.

[15] A. Assaad and D. Fayek, "General hospitals network models for the support of e-health applications," in *Proc. IEEE 10th Netw. Oper. Manage. Symp.*, 2006, pp. 1–4 .

[16] A. Ahmad, A. Riedl, W. J. Naramore, N.-Y. Chou, and M. S. Alley, "Scenario-based traffic modeling for data emanating from medical instruments in clinical environment," in *Proc. WRI World Congr. Comput. Sci. Inf. Eng.*, 2009, pp. 529–533.

[17] H. Tawfik, O. Anya, and A. K. Nagar, "Understanding clinical work practices for cross-boundary decision support in e-health," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 4, pp. 530–541, Jul. 2012.

[18] M. Masud, M. S. Hossain, and A. Alamri, "Data interoperability and multimedia content management in e-health systems," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1015–1023, Nov. 2012.

[19] L. Constantinescu, J. Kim, and D. D. Feng, "Sparkmed: A framework for dynamic integration of multimedia medical data into distributed m-health systems," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 1, pp. 40–52, Jan. 2012.

[20] S. P. Ahuja, S. Mani, and J. Zambrano, "A survey of the state of cloud computing in healthcare," *Netw. Commun. Technol.*, vol. 1, no. 2, pp. 12–19, 2012.

[21] M. Alicherry and T. V. Lakshman, "Network aware resource allocation in distributed clouds," in *Proc. IEEE Conf. Comput. Commun.*, 2012, pp. 963–971.

[22] A. Leivadeas, C. A. Papagianni, and S. Papavassiliou, "Efficient resource mapping framework over networked clouds via iterated local search-based request partitioning," *IEEE Trans. Parallel Distributed Syst.*, vol. 24, no. 6, pp. 1077–1086, Jun. 2013.

[23] S. Manfredi, F. Oliviero, and S. P. Romano, "A distributed control law for load balancing in content delivery networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 1, pp. 55–68, Feb. 2013.

[24] R. Lu, X. Lin, and X. Shen, "Spoc: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distributed Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013.

[25] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: A strong privacy-preserving scheme against global eavesdropping for e-health systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–378, May 2009.

[26] X.-B. Li and S. Sarkar, "Against classification attacks: A decision tree pruning approach to privacy protection in data mining," *Oper. Res.*, vol. 57, no. 6, pp. 1496–1509, 2009.

[27] W. Song, W. Zhuang, and Y. Cheng, "Load balancing for cellular/WLAN integrated networks," *IEEE Netw.*, vol. 21, no. 1, pp. 27–33, Jan./Feb. 2007.

[28] M. Liu and B. Liu, "A note on sum of powers of the Laplacian eigenvalues of graphs," *Elsevier Appl. Math. Lett.*, vol. 24, no. 3, pp. 249–252, 2011.

[29] B. Jansson, "Choosing a good appointment system? A study of queues of the type (D, M, 1)," *INFORMS Oper. Res.*, vol. 14, no. 2, pp. 292–312, 1966.

[30] C. Pack, "The output of a D/M/1 queue," *SIAM J. Appl. Math.*, vol. 32, no. 3, pp. 571–587, 1977.

[31] S. T. Maguluri, R. Srikant, and L. Ying, "Stochastic models of load balancing and scheduling in cloud computing clusters," in *Proc. IEEE Conf. Comput. Commun.*, 2012, pp. 702–710.

[32] D. Michie, D. J. Spiegelhalter, and C. C. Taylor, *Machine Learning, Neural and Statistical Classification*. New York, NY: Ellis Horwood, 1994.

[33] D. Barber, *Bayesian Reasoning and Machine Learning*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

Qinghua Shen (S'11) received the B.Sc. and Master's degree in electrical engineering from the Harbin Institute of Technology, Harbin, China, in 2008 and 2010, respectively. He is currently working toward the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

His research interests include resource allocation for the e-healthcare system, cloud computing, and smart grid.

Xiaohui Liang (S'10) received the Bachelor's and Master's degrees at the Department of Computer Science, Shanghai Jiao Tong University, Shanghai, China. He received the Ph.D. degree at the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada.

He is currently working as a Postdoctoral Fellow at the Broadband Communications Research Group at the University of Waterloo. His research interests include security and privacy for the e-healthcare system and mobile social networks.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree from Dalian Maritime University, Dalian, China, in 1982, the M.Sc. and Ph.D. degrees from Rutgers University, New Jersey, USA, in 1987 and 1990, all in electrical engineering.

Currently, he is a Professor and University Research Chair at the Department of Electrical and Computer Engineering, University of Waterloo, ON, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. His research interests include resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, vehicular ad hoc, and sensor networks. He is a coauthor/editor of six books, and has published more than 600 papers and book chapters in wireless communications and networks, control and filtering.

Dr. Shen served as the Technical Program Committee Chair for IEEE VTC'10 Fall, the Symposia Chair for IEEE ICC'10, the Tutorial Chair for IEEE VTC'11 Spring and IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Cochair for Chinacom'07 and QShine'06, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; an Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, COMPUTER NETWORKS, AND ACM/WIRELESS NETWORKS, etc.; and the Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, and 2010, from the University of Waterloo, the Premier's Research Excellence Award in 2003, from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society. He has been a Guest Professor of Tsinghua University, Shanghai Jiao Tong University, Zhejiang University, Beijing Jiao Tong University, Northeast University, etc.

Xiaodong Lin (S'07–M'09–SM'12) received the Ph.D. degree in information engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 1998, and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008.

He is currently an Assistant Professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON. His research interests include wireless network security, applied cryptography, computer forensics, software security, and wireless networking and mobile computing.

Dr. Lin received Natural Sciences and Engineering Research Council of Canada Graduate Scholarships Doctoral and the Best Paper Awards of the 18th International Conference on Computer Communications and Networks in 2009, the 5th International Conference on Body Area Networks in 2010, and the IEEE International Conference on Communications in 2007.

Henry Y. Luo received the Ph.D. degree in biomedical engineering from the University of Sussex, Brighton, U.K., in 1994.

He is currently an Expert Reviewer with the Canadian Natural Sciences and Engineering Research Council, Ottawa, ON, Canada. Since 2007 he has been the President and CTO of Care in Motion Technology Inc., Waterloo, ON, and a Senior Manager on DSP application of Unitron hearing, Canada, since 1998.