Fog-Enabled Smart Health: Toward Cooperative and Secure Healthcare Service Provision

Wenjuan Tang, Kuan Zhang, Deyu Zhang, Ju Ren, Yaoxue Zhang, and Xuemin (Sherman) Shen

The authors investigate fog-enabled smart health toward cooperative and secure healthcare service provision. They introduce the overall infrastructure and some promising applications, including emergent healthcare service, health risk assessment, and healthcare notification. They discuss the challenges of fog-enabled smart health from the perspectives of cooperation and security.

Abstract

The rise of smart health promotes ubiquitous healthcare services with the adoption of information and communication technologies. However, increasing demands of medical services require more computing and storage resources in proximity of medical users for intelligent sensing, processing, and analysis. Fog computing emerges to enable in situ data processing and service provision for smart health in proximity of medical users, exploiting a large number of small-scale servers. In this article, we investigate fog-enabled smart health toward cooperative and secure healthcare service provision. Specifically, we first introduce the overall infrastructure and some promising applications, including emergent healthcare service, health risk assessment, and healthcare notification. We then discuss the challenges of fog-enabled smart health from the perspectives of cooperation and security. A case study is presented to demonstrate efficient and secure health data sharing through naive Bayes classification and attribute-based encryption with assistance from fog computing. Finally, by exploring interesting future directions, more attention can be attracted to this emerging area.

Introduction

With the adoption of information and communication technologies in the healthcare sector, the concept of smart health has been formed to promote ubiquitous healthcare services by using the context-aware network and sensing infrastructure in smart cities [1]. Benefiting from pervasive healthcare devices (e.g., wearable devices and body area network sensors), various kinds of data can be collected, which are then analyzed by a remote cloud server with powerful computing capabilities. However, serving medical users with emergent healthcare requests solely by the remote cloud server introduces severe latencies. For example, a solitary elderly person falls down and requires immediate healthcare service. The health information may not be promptly received and processed by the cloud server, causing the failure of significant help from medical service [2]. Meanwhile, the remote cloud server can hardly provide healthcare services that are tightly connected to geographical location due to already congested core networks. Consider the case of an infectious disease outbreak propagating in a local area. It is cumbersome to coordinate the local network or physical resources with the remote cloud server for controlling the geographical diffusion of a communicable disease. As a result, the emergent and location-sensitive healthcare services require more computing and storage resources in proximity of medical users to participate in smart health.

As a decentralized computing paradigm, fog computing [3] is attractive for smart health service provision by exploiting distributed network resources of small-scale server nodes with limited computing capabilities (e.g., gateways, cloudlet servers, and routers) residing in close proximity to users. Fog computing is promising to provide services with location awareness, low latency, quality of service assurance, and immediate notification services for real-time applications [3–5]. Through meeting the aforementioned increasing medical service requirements, such as providing emergent healthcare service when elderly people fall, and harmonizing the local resources for infectious disease control, fog computing can significantly benefit smart health. Playing as local servers, fog nodes exploit the close proximity to rapidly process the health data and quickly respond to the service requirements. Meanwhile, in the middle layer between healthcare devices and the cloud server [6], fog nodes enable sensed health data aggregation and duplication to save network resources. In addition, by extending the capability of the centralized cloud server to the network edge [7], fog nodes can provide preliminary in situ health data processing to improve data analysis efficiency. Through involving originally disengaged network resources to string the healthcare devices and the cloud server together, fog computing enables smart health to provide high-quality healthcare services.

Although fog-enabled smart health can significantly benefit medical service provision, its success still hinges on how we address cooperation and security challenges. To provide comprehensive healthcare services, fog-enabled smart health calls for extensive cooperation among healthcare devices, fog nodes, and the cloud server. However, how to distribute data processing tasks among the high-

Wenjuan Tang, Deyu Zhang (corresponding author), Ju Ren , and Yaoxue Zhang are with Central South University, China; Kuan Zhang is with the University of Nebraska-Lincoln; Xuemin (Sherman) Shen is with the University of Waterloo; Yaoxue Zhang is also with Tsinghua University and Jiangxi University of Finance and Economics.

Digital Object Identifier:
10.1109/MCOM.2019.1800234

0163-6804/19/$25.00 © 2019 IEEE

ly heterogeneous computing entities introduces a challenging issue in fog-enabled smart health systems. In fact, at the network edge, the data transmitted through a single fog node is limited, and the computation performed by a single fog node is constrained, causing the single fog node to make incomplete and biased medical decisions.

In terms of security concerns, heterogenous fog nodes may not be fully trusted, and they may be compromised by adversaries. Compromised fog nodes introduce security threats by illegally accessing health information during data storage and transmission, broadcasting incorrect health service instructions in the local area, or even colluding with other malicious devices for evil behaviors. Fog nodes play as storage and computation components in the middle layer, where data confidentiality, valid authentication, and access control should be guaranteed during entity interaction and data exchange with both healthcare devices and the cloud server. Without properly supporting security, fog-enabled smart health will hardly encourage medical users to participate in the system. In summary, efficient cooperation and security solutions are required to drive the development of fog-enabled smart health.

The emerging trends motivate us to investigate fog-enabled smart health toward providing secure and cooperative healthcare services. In this article, we first introduce architecture and applications of fog-enabled smart health. Then we discuss several challenges that must be addressed for improving fog-enabled smart health. A case study is presented to demonstrate how fog computing can be integrated with smart health for efficient and secure service provision. Finally, we present several open research directions and expect the flourish of fog-enabled smart health. We list the contributions of this work as follows:.

- We design a fog-enabled smart health structure with three layers: multi-source data layer, heterogenous fog network layer, and healthcare service layer. Through incorporating multi-source data, heterogenous information communication, and smart service provision, we propose emergent health care service, health risk pre-assessment, and healthcare information notification.
- We analyze efficient cooperation and security challenges in fog-enabled smart health. How to bring healthcare devices, fog nodes, and a cloud server to cooperate efficiently to achieve low computation, communication, and storage cost with maximum system performance is a critical challenge. Meanwhile, how to guarantee the system security and preserve data privacy should be addressed.
- We propose a fog-assisted health data sharing scheme in a case study. The proposed scheme employs fog nodes to pre-process and re-encrypt the shared data, leading to efficient data access and encryption burden reduction for healthcare devices.
- We discuss some open research directions about using software defined networking (SDN) technologies to enable heterogenous fog nodes to cooperate for resource allocation and distributed machine learning (e.g., federated learning) to improve data process efficiency on fog nodes for smart health.

Fog-Enabled Smart Health Architecture and Applications

Fog-Enabled Smart Health Architecture

Fog-enabled smart health incorporates the multi-source data layer, heterogenous fog network layer, and healthcare service layer, as shown in Fig. 1.

Multi-Source Data Layer: Benefiting from the ubiquitous sensing infrastructure of smart cities, smart health exploits pervasive sensing devices to collect healthcare related data from wearable devices (e.g., ECG sensor and blood pressure sensor) worn on human bodies, as well as context-aware environmental information (e.g., air pollution, water quality, and allergen information) related to healthcare [8]. Benefiting from fog computing with distributed network resources, the supplemental data source of fog-enabled smart health can be health records from local care centers, health guidance from family doctors, and health information from mobile social networks. Medical users, local care service providers, as well as government departments and companies can enrich data sources in this layer.

Heterogeneous Fog Network Layer: The heterogeneous fog network layer combines distributed small-scale network resources (e.g., gateways, cloudlet servers, and routers) with heterogenous communication technologies. Resource-limited healthcare devices (e.g., wearable health watches) use energy-efficient communication solutions (e.g., Bluetooth and ZigBee) in the fog network layer. Smartphones or other stronger data collection devices and entities utilize cellular network or WiFi access points to interact with fog nodes. To provide various kinds of services from healthcare devices, fog nodes allocate their computation, communication, and storage resources flexibly to achieve location awareness and low latency. To cooperate with the remote cloud server for complex data analysis, fog nodes pre-process the collected data and send the pre-analysis results to the remote cloud server.

Healthcare Service Layer: Based on multi-source data collection and heterogenous communication technologies, fog nodes and the cloud server process and analyze data in the healthcare service layer, and coordinate the healthcare resources for ubiquitous service provision (e.g., emergency processing, disease control, health guidance, smart home health monitoring, and healthcare consultation). By analyzing the health data stored on the fog nodes or the cloud server, different service providers (e.g., hospitals, care centers, pharmaceutical manufacturers, research organizations, insurance companies, and the government) can also contribute their professional knowledge to participate in fog-enabled smart health and provide nursing, physiotherapy, and corporate wellness services for individuals, families, and communities.

Fog-Enabled Smart Health Applications

Through incorporating multi-source data, heterogenous information communication, and smart service provision, several promising applications emerge for fog-enabled smart health, as seen in Fig. 2.

To provide various kinds of services from healthcare devices, fog nodes allocate their computation, communication, and storage resources flexibly to achieve location awareness and low latency. To cooperate with the remote cloud server for complex data analysis, fog nodes pre-process the collected data and send the pre-analysis results to the remote cloud server.

Although fog computing is expected to assist smart health through improving service provision, fog-enabled smart health raises a series of challenges in terms of the efficient cooperation among healthcare devices, fog nodes, and the cloud server, as well as security and privacy issues.

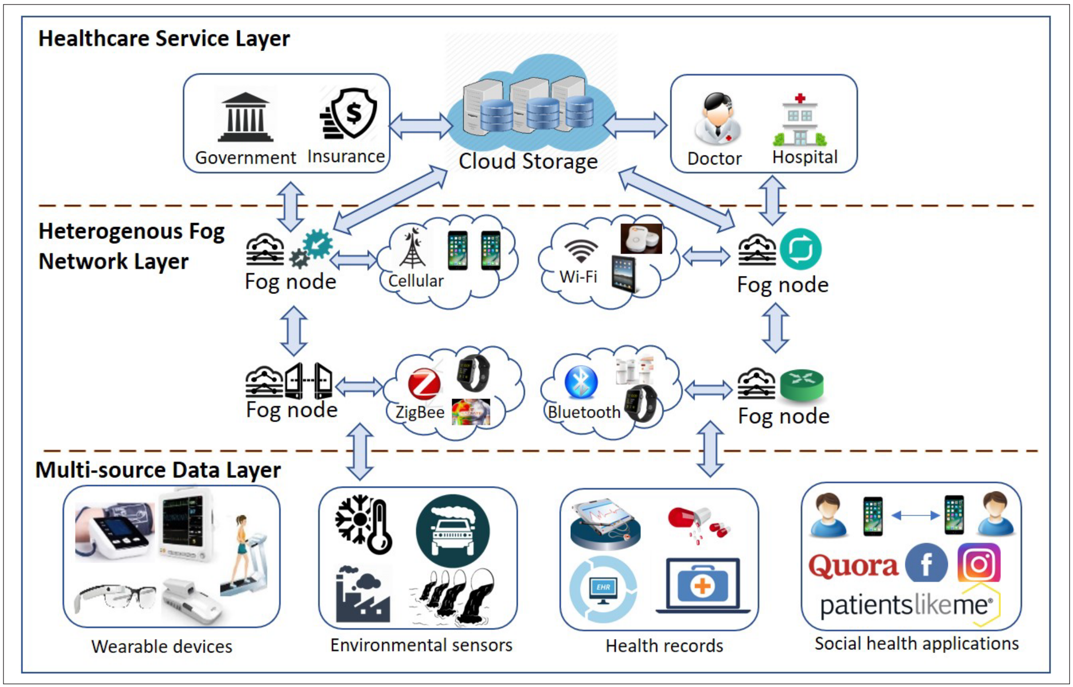


Figure 1. Architecture for fog-enabled smart health: multi-source data, heterogenous fog network, and healthcare services.

Emergent Healthcare Service: In fog-enabled smart health, the health data can be transmitted to the fog node quickly, and the health response can be delivered in real time due to the low latency. In this application, medical users are equipped with wearable healthcare devices and social healthcare applications for monitoring their daily activities. When the fog node receives an emergency call from sensors or the social networks, such as when an elderly person falls downstairs and faces risk of life, the fog node cooperates with the closest ambulance through the fastest route to help him, and the ambulance transports the patient to the most resourceful hospital and saves the patient from a calamitous condition.

Health Risk Pre-Assessment: To save precious and limited healthcare resources as well as expensive cost for medical users, it is necessary for medical users to learn their health risks ahead of some specific professional medical treatments. For example, sensitive medical users may prefer to seek help from well-known hospitals when they feel uncomfortable, which may lead to unnecessary medical resource occupation and financial resource waste since they could stay healthy by several simple treatments, such as taking exercise and changing diet. In this application, the fog node (e.g., smart home health monitor) analyzes the health data and predicts general health risks for medical users, as well as providing health guidance. In this way, medical users can evaluate their health situation in advance, and consult for health guidance to decide whether to order healthcare services from specialists or just go to the pharmacy for medicine. Health risk pre-assessment through data pre-processing by the fog node can manage suitable healthcare resources to effectively flow to different medical users with various kinds of health risks.

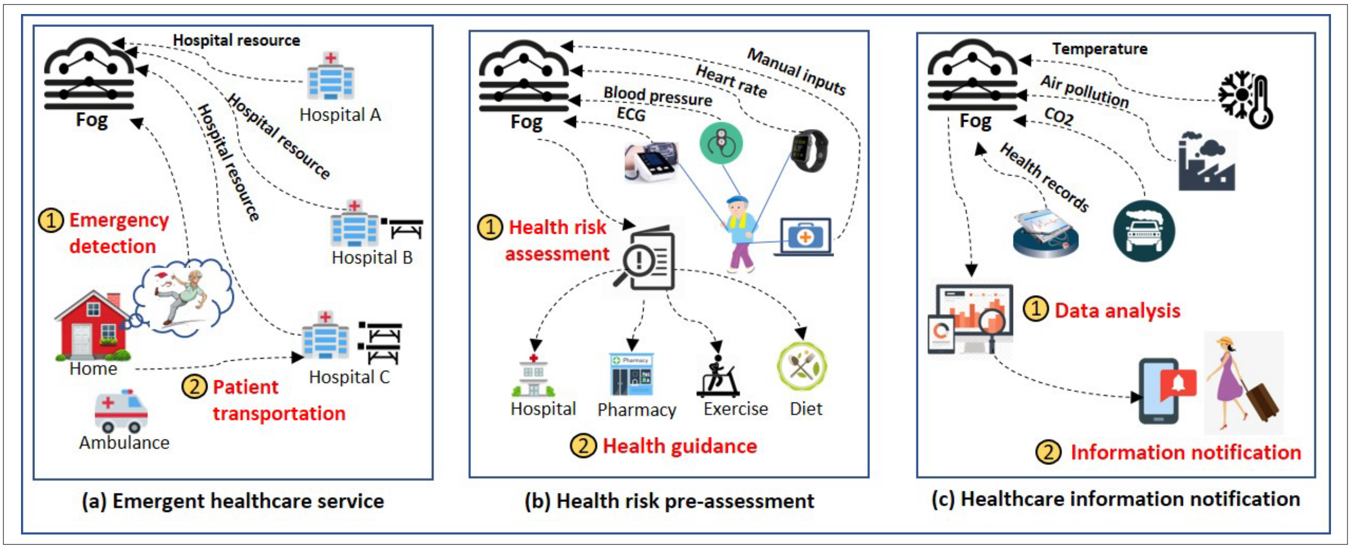
Healthcare Information Notification: In fog-enabled smart health, medical users can not only obtain healthcare services corresponding to their medical requests, but also subscribe to health notifications for health guidance. The fog node can analyze context-aware information (e.g., air quality and influenza rate) of the local region, and then push notifications to subscribed medical users. Specifically, the fog node can combine and analyze context-aware information with individual historical health records, and provide personalized suggestions for specific users (e.g., the fog node sends notifications to susceptible people when they enter into a location area where allergens are detected). Additionally, the local health department can propagandize health knowledge through fog-enabled smart health for the public.

Challenges in Fog-Enabled Smart Health

Although fog computing is expected to assist smart health through improving service provision, fog-enabled smart health raises a series of challenges in terms of efficient cooperation among healthcare devices, fog nodes, and the cloud server, as well as security and privacy issues.

Efficient Cooperation among Healthcare Devices, Fog Nodes, and the Cloud Server

In fog-enabled smart health, healthcare devices, fog nodes, and the cloud server perform different levels of data processing for efficient healthcare service provision. The healthcare devices perform basic data processing operations, but are too resource-limited to perform complex data analysis. The centralized cloud server, which remotely stores the data, can provide excellent data processing and analysis, but would meet the backhaul bottleneck limitations. As the middle-layer devices between healthcare devices and the cloud server, fog nodes can complement a portion of computation and storage tasks for both of them. Without



(a) Emergent healthcare service

(b) Health risk pre-assessment

(c) Healthcare information notification

Figure 2. Applications of fog-enabled smart health.

any one entity, the other two components can hardly operate smart health efficiently for comprehensive services provision. Toward this aim, they should collaborate with each other through efficient data exchange and computation allocation [9]. However, for a specific data processing task, which parts should be allocated to healthcare devices, fog nodes, and the cloud server for maximum performance with minimum resources?

In terms of cooperation between fog nodes, how to manage data exchange, resource allocation, and task execution is still a remaining challenge. Fog-enabled smart health involves abundant edge network resources, among which the computation, communication, and storage resources vary heterogeneously. For achieving efficient service provision at different time periods and location areas, fog-enabled smart health should meet varying medical requirements in terms of varying demands of computation, communication, and storage resources [10]. Some compute-intensive tasks do not leverage data communication but heavily hinge upon real-time computing resources. Some data transmission demanding tasks involve energy-efficient communication ability instead of exquisite computing resources. Generally, the data transmitted through a single fog node is limited, and the function operation performed by a single fog node is generally constrained, such that the single fog node may make incomplete and biased service provision. Additionally, task switching from one fog node to its neighboring fog nodes is required when medical users update their medical requirements in a mobile scenario. As a result, cooperation challenges on choosing proper task allocation and data exchange among heterogenous entities for varying medical requirements should be addressed for fog-enabled smart health.

Security and Privacy Challenges

Due to the openness of the network environment and the privacy sensitivity of personal health data, security and privacy challenges in fog-enabled smart health should be addressed. Adversaries may attack the healthcare devices (e.g., bio-sensors and wearable devices) and send incorrect biometric data to fog nodes such that they can affect the sensed health data or even blackmail medical users that are equipped with healthcare devices. Since the health data and instruction information transmitted between medical users and service providers might be eavesdropped or tampered, medical users' treatments may be affected, which results in their lives being in danger. During the service provision through data access and analysis, personal health related information might be disclosed to unauthorized users, such that private information of medical users might be utilized for illegal money in the black market [11]. To protect health information from being illegally accessed, tampered, and disclosed, it is imperative for fog-enabled smart health to have valid authentication, data confidentiality, and data access control mechanisms [12].

Since abundant originally disengaged edge resources are involved as fog nodes for efficient service provision, security risks may concurrently sneak around the smart health systems due to increasing entity interactions and data exchange frequency. The basis of the health data can be securely relayed, processed, and analyzed by a fog node on condition that the fog node can be securely controlled. However, if the fog node itself is attacked or tampered by adversaries, the data processing meets increasing security risks and privacy leakage challenges. More seriously, the collusion of fog nodes that store the fragmented data may reveal all of the data and private health information. To address the above challenges, security and privacy schemes for fog-enabled smart health should be proposed.

Case Study

In this section, we present a case study of a specific fog-assisted health data sharing scheme to demonstrate how fog computing can cooperate with healthcare devices to efficiently and securely improve data sharing. In this scheme, the shared health data can be accessed by authorized service providers with efficient resource consumption on the condition of privacy preservation.

In this case study, we propose a privacy-preserving and efficient health data sharing scheme

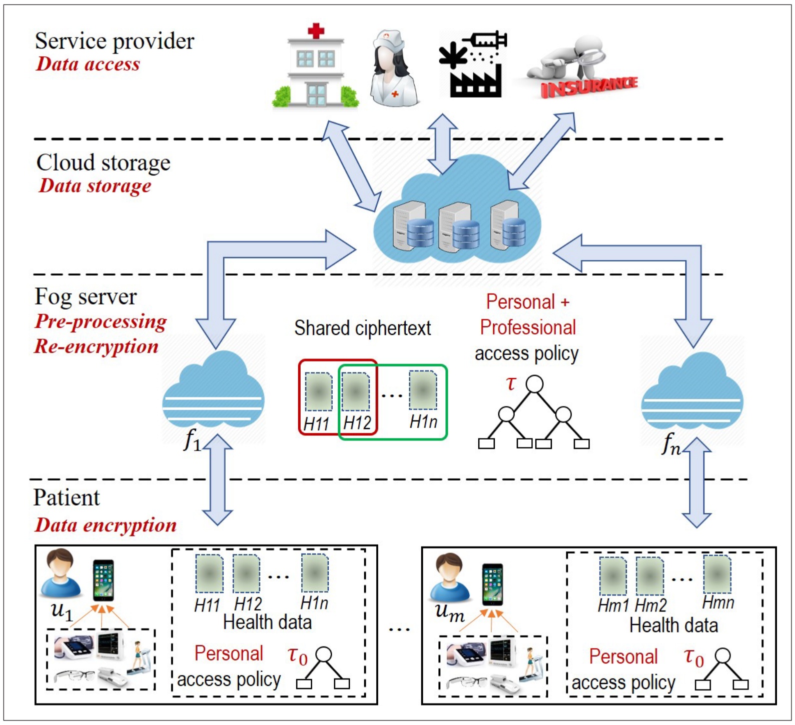


Figure 3. Fog-assisted health data sharing process.

with the assistance of fog computing. This scheme consists of four entities: patient, fog node, cloud server, and service provider. The transmission channel between patient, fog node, and cloud server is secure. The patient is trusted and aims to prevent unauthorized entities from obtaining the shared plaintext. The fog node and cloud server are *honest but curious*. The fog node provides data pre-processing services, and the cloud server performs data storage, but both of them are curious about the shared plaintext. Unauthorized service providers may obtain the shared health data to spread advertisements and drug promotions. The fog node, cloud server, and unauthorized service providers may collude with each other and intend to learn the shared plaintext.

The scheme process is shown in Fig. 3. First, the patient encrypts the shared data with his/her personal access policy. Second, to enable the shared data to be accessed more efficiently, a fog node is employed to classify the shared data into different disease risks and index the corresponding shared health items; also, to reduce the encryption burden on the patient, a fog node is employed to re-encrypt the shared data with a professional access policy according to the disease risks. Finally, the service provider with authorized attributes can access and decrypt the ciphertext for healthcare service provision.

We illustrate the theoretical details of the proposed scheme. The trusted authority initializes the system, and generates public keys and system master keys, as well as private keys for service providers.

The patient chooses a random secret element to encrypt his/her shared data. The secret element is divided into two sub-elements, s_1 and s_2, by using Shamir's Secret Sharing. For personalized health data sharing and access control, the patient defines a personal access policy with personal attributes to hide s_1 according to his/her interests and experiences. The personal access policy can be expressed with an access tree A_{tree}, as seen in Fig. 4a. Meanwhile, the patient encrypts s_2 with the fog node's public key and sends the ciphertext to the fog node.

The fog node receives the ciphertext, and decrypts s_2 with its secret key. For efficient data access by service providers, the fog node categorizes the heterogenous kinds of raw health data. Through analyzing the encrypted health ciphertext based on naive Bayes classification, the fog node computes the *top* – *k* possible disease risks SID_1, SID_2, ..., SID_k. Meanwhile, for every disease risk, the fog node indexes the related health items to classify the shared health data into *k* categories as seen in Fig. 5, where ID_i represents the health item. Additionally, the fog node defines a professional access policy according to the *top* – *k* possible disease risks, and hides s_2 in the professional access policy. The professional access policy can be expressed with an access tree B_{tree} as seen in Fig. 4b. The fog node transmits the ciphertext to the cloud server for storage.

The service provider's private key can use his/her privacy keys to access the shared encrypted data. Only if the service provider has sufficient attributes that satisfy both the personal access policy and the professional access policy can the service provider obtain the shared plaintext *M*.

We analyze whether the proposed scheme can keep data confidential; since the shared data is encrypted on the patient side, the fog node and cloud server cannot learn the shared ciphertext, so data confidentiality is guaranteed. The proposed scheme can provide patient-centric access control for the patient. Only the service provider with attributes that satisfy the personal access policy A_{tree} has a probability to decrypt the shared data, such that the patient can decide whether his/her shared data to be accessed by the service provider satisfy his/her own specific requirements. The proposed scheme can resist collusion attacks. The fog node cannot learn the information of secret element s_1 so that it cannot learn the encrypted health information *M* only by using s_2. Additionally, although the fog node can learn s_2, it cannot compute the corresponding decryption element without the random encryption number from data users, so collusion of fog nodes and malicious data users cannot decrypt the health plaintext *M*.

In the performance evaluation, we demonstrate that the proposed scheme is cost-efficient in terms of encryption time, ciphertext storage, and energy consumption. The experimental platform is a mobile phone with ARM Cortex-A9 CPU and 1 GB RAM, and the energy consumption is monitored by PowerTutor through using built-in battery voltage sensors and knowledge of battery discharge behavior. We compare the proposed scheme with general CP-ABE [13], which encrypts the shared data on healthcare devices and then transmits the ciphertext to the cloud server. We find that the encryption time, ciphertext storage, and energy consumption on the patient is linearly increasing with the number of attributes. When the whole attribute number is set, there are more professional attributes, and the encryption time and storage ciphertext on the patient side are

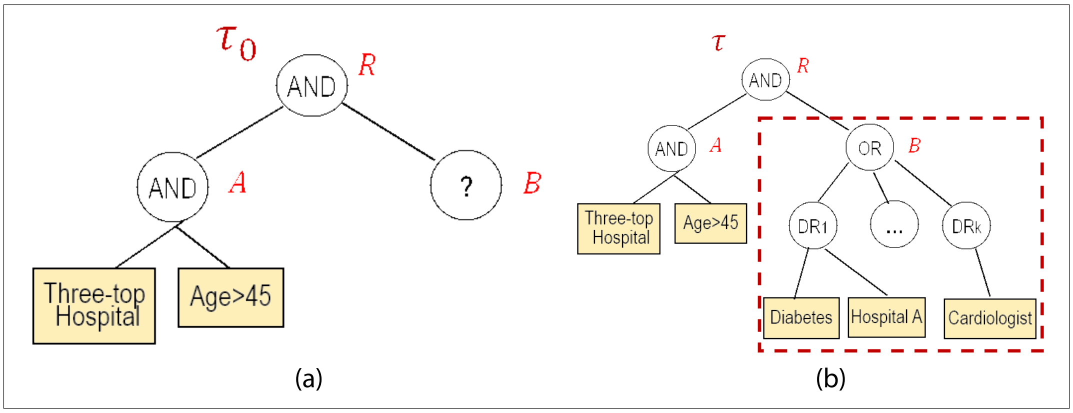


Figure 4. Access tree construction: a) access tree on patient; b) access tree on fog server.

reduced more. Specifically, we demonstrate the energy consumption on the patient as seen in Fig. 6. *R* is the ratio of the attribute number of personal access policy defined by the patient in the whole access policy. From Fig. 6, we can demonstrate that when *R* varies from 1/2 to 1/4, the energy cost decreases on the patient side because more encryption burden is offloaded from the patient to the fog node. When the attribute number is 30 and *R* = 1/4, the energy consumption of CP-ABE is near 15 J, while the energy consumption of our scheme is near 5 J. In summary, we demonstrate that a fog-assisted health data sharing scheme can achieve efficient data sharing service with privacy preservation.

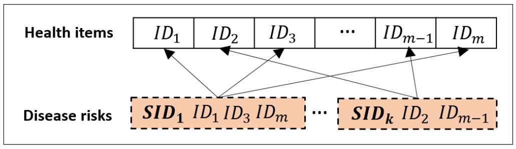


Figure 5. Top-*k* disease risks and related health items.

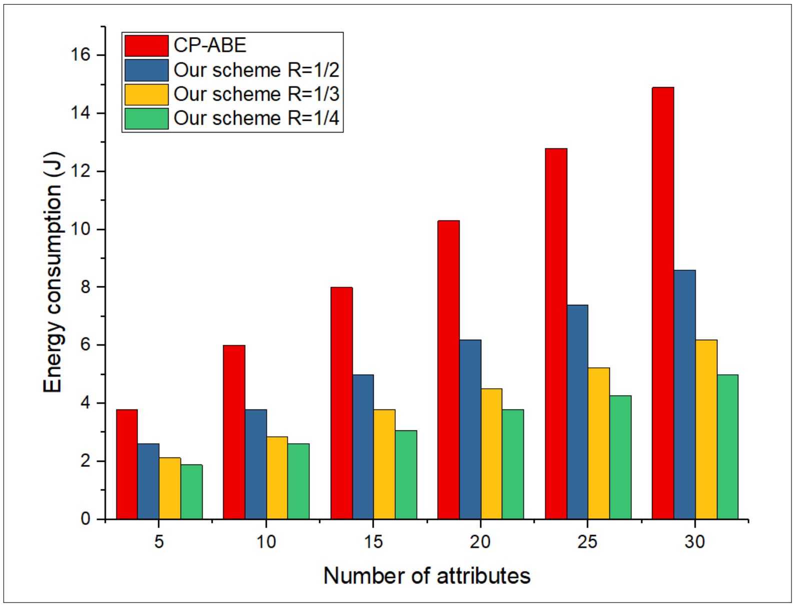


Figure 6. Encryption energy consumption on a mobile phone.

Open Research Directions

Since the research of fog-enabled smart health is still in its early stage, some off-the-shelf research solutions may not address all of the challenges in fog-enabled smart health. We discuss several open research directions below.

Fog Cooperation through SDN Approach

SDN, characterized by the decoupled control plane and data plane, provides fine-grained network control service. Based on real-time global information, the SDN controller can have a global view of the network via a programmable control plane, and is able to make informed management decisions [14]. Consequently, SDN is promising to combine fog computing for dynamic network deployment, agile network management, fast application innovation, and efficient resource utilization. With the coordination of SDN in fog-enabled smart health, local network information is continuously shared among fog nodes, leading to a logic controller with group intelligence so that multiple fog nodes can cooperate. The SDN controllers evaluate resources of fog nodes and the health service requirements, then make corresponding task execution, data exchange, and resource allocation for efficient cooperation between healthcare devices, fog nodes, and the remote cloud server.

Distributed Machine Learning for Smart Health

To meet the increasing consistent healthcare service demands in smart health, efficient and high-intensity data processing and analysis are desired. Benefiting from data mining and machine learning, healthcare services (e.g., health risk prediction and abnormal health condition detection) can be processed efficiently, which saves human resources. However, in some critical healthcare scenarios (e.g., emergency evaluation), it is not desirable to run machine-learning-based analysis on a cloud server due to concerns about latency, connectivity, and security. An insight into intelligent and efficient service provision for smart health is to develop resource-efficient and distributed machine learning algorithms that can run on fog nodes or even on resource-constrained healthcare devices [15]. If the learning model can be trained on the remote cloud server that has a global information view, while the decision making can be realized on fog nodes nearby the healthcare devices, the performance of the health data classification, disease prediction, medical decisions, and other medical services may be improved due to the low latency and local aware-

If the learning model can be trained on the remote cloud server that has a global information view, while the decision making can be realized on fog nodes nearby the healthcare devices, the performance of the health data classification, disease prediction, medical decision and other medical services may be improved due to the low latency and local awareness.

ness. Federated learning can be implemented to perform distributed learning of models from several clients. In federated learning, clients do not share their training data but rather train a local model on distributed fog nodes, such that the data security and privacy can be preserved within the local area. Additionally, security protection based on distributed machine learning can be developed for detecting false data injection and insider attackers to improve system security and privacy preservation for fog-enabled smart health.

Conclusion

In this article, we investigate fog-enabled smart health to provide efficient healthcare services. We introduce a three-layer architecture that incorporates multi-source data, a heterogenous fog network, and healthcare services for fog-enabled smart health, and present some interesting applications. We discuss fog cooperation and security challenges for fog-enabled smart health to flourish. A privacy-preserving fog-assisted health data sharing case study is presented to demonstrate that efficient healthcare service can be achieved with the assistance from fog computing. Several open research directions are also discussed for fog-enabled smart health.

References

[1] A. Solanas *et al.*, "Smart Health: A Context-Aware Health Paradigm within Smart Cities," *IEEE Commun. Mag.*, vol. 52, no. 8, Aug. 2014, pp. 74–81.

[2] X. Liang *et al.*, "Enabling Pervasive Healthcare through Continuous Remote Health Monitoring," *IEEE Wireless Commun.*, vol. 19, no. 6, Dec. 2012.

[3] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet of Things J.*, vol. 3, no. 6, 2016, pp. 854–64.

[4] N. Chen *et al.*, "Fog as a Service Technology," *IEEE Commun. Mag.*, vol. 56, no. 11, Nov. 2018, pp. 95–101.

[5] F. Bonomi *et al.*, "Fog Computing and its Role in the Internet of Things," *Proc. ACM MCC*, 2012, pp. 13–16.

[6] J. Ren *et al.*, "Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing," *IEEE Network*, vol. 31, no. 5, Sept./Oct. 2017, pp. 96–105.

[7] D. Zhang *et al.*, "Delay-Optimal Proactive Service Framework for Block-Stream as a Service," *IEEE Wireless Commun. Letters*, vol. 7, no. 4, 2018, pp. 598–601.

[8] K. Zhang *et al.*, "Security and Privacy in Smart City Applications: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, Jan. 2017, pp. 122–29.

[9] X. Masip-Bruin *et al.*, "Foggy Clouds and Cloudy Fogs: A Real Need for Coordinated Management of Fog-to-Cloud Computing Systems," *IEEE Wireless Commun.*, vol. 23, no. 5, Oct. 2016, pp. 120–28.

[10] X. Chen *et al.*, "Efficient Multi-User Computation Offloading for Mobile-Edge Cloud Computing," *IEEE/ACM Trans. Networking*, vol. 24, no. 5, 2016, pp. 2795–2808.

[11] W. Tang *et al.*, "Flexible and Efficient Authenticated Key Agreement Scheme for Bans Based on Physiological Features," *IEEE Trans. Mobile Computing*, 2018. DOI: 10.1109/TMC.2018.2848644.

[12] I. Stojmenovic and S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues," *Proc. FedCSIS*, 2014, pp. 1–8.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attributebased Encryption," *Proc. IEEE S&P*, 2007, pp. 321–34.

[14] S. Tomovic et al., "Software-Defined Fog Network Architecture for IoT," *Wireless Personal Commun.*, vol. 92, no. 1, 2017, pp. 181–96.

[15] M. Abadi et al., "Tensorflow: A System for Large-Scale Machine Learning," *Proc. OSDI*, 2016, pp. 265–83.

Biographies

Wenjuan Tang [S'17](wenjuantang@csu.edu.cn) received her B.E. degree from Central South University, Changsha, China, in 2012. She is working toward a Ph.D. degree in computer science in the Department of Information Science and Engineering, Central South University. From August 2016 to September 2018, she was a visiting Ph.D. student in the Department of Electrical and Computer Engineering, University of Waterloo, Canada. Her research interests include applied cryptography and information security, with current focus on e-healthcare systems, fog/edge computing, transparent computing, and the Internet of Things.

Kuan Zhang [S'13, M'17] (kzhang22@unl.edu) has been an assistant professor in the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln, since September 2017. He received his B.Sc. degree in communication engineering and his M.Sc. degree in computer applied technology from Northeastern University, China, in 2009 and 2011, respectively. He received his Ph.D. degree in electrical and computer engineering from the University of Waterloo in 2016. He was also a postdoctoral fellow with the Broadband Communications Research (BBCR) group, Department of Electrical and Computer Engineering, University of Waterloo from 2016 to 2017. His research interests include security and privacy for mobile social networks, e-healthcare systems, cloud/edge computing, and cyber physical systems.

Deyu Zhang [S'14, M'17] (zdy876@csu.edu.cn) (corresponding author) received his B.Sc. degree (2005) in communication engineering from PLA Information Engineering University, China, and his M.Sc. degree (2012) from Central South University, also in communication engineering. He received his Ph.D. degree in computer science from Central South University in 2016. He is now an assistant professor with the School of Software and a postdoctoral fellow with the Transparent Computing Lab in the School of Information Science and Engineering, Central South University. He was a visiting scholar with the Department of Electrical and Computer Engineering, University of Waterloo from 2014 to 2016. His research interests include stochastic resource allocation transparent computing, edge computing, and IoT. He is a member of CCF.

Ju Ren [S'13, M'16] (renju@csu.edu.cn) received his B.Sc. (2009), M.Sc. (2012), and Ph.D. (2016) degrees, all in computer science, from Central South University. From August 2013 to September 2015, he was a visiting Ph.D. student in the Department of Electrical and Computer Engineering, University of Waterloo. Currently, he is a professor with the School of Information Science and Engineering, Central South University. His research interests include the Internet of Things, wireless communication, transparent computing, and cloud computing. In these related research areas, he has published over 40 papers in prestigious international journals and conferences, including IEEE TIFS, TWC, TVT, TII, IEEE INFOCOM, and so on. He serves/has served as an Associate Editor for *Peer-to-Peer Networking and Applications*, a leading Guest Editor for *IEEE Network*, and a Technical Program Committee member of many international conferences including IEEE INFOCOM '18, IEEE GLOBECOM '17, WCNC '17, WCSP '16, and so on.

Yaoxue Zhang (zyx@csu.edu.cn) received his B.S. degree from Northwest Institute of Telecommunication Engineering, China, in 1982, and his Ph.D. degree in computer networking from Tohoku University, Japan, in 1989. Currently, he is a professor in the Department of Computer Science at Central South University and also a professor in the Department of Computer Science and Technology at Tsinghua University, China. He is also with the School of Information Technology, Jiangxi University of Finance and Economics, China. His research interests include computer networking, operating systems, ubiquitous/pervasive computing, transparent computing, and big data. He has published over 200 technical papers in international journals and conferences, as well as 9 monographs and textbooks. He is a Fellow of the Chinese Academy of Engineering and the president of Central South University.

Xuemin (Sherman) Shen [M'97, SM'02, F'09] received Ph.D. degrees (1990) from Rutgers University, New Jersey. He is a University Professor, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, social networks, smart grid, and vehicular ad hoc and sensor networks. He served as the Technical Program Committee Chair/Co-Chair for IEEE GLOBECOM '16, INFOCOM '14, IEEE VTC-Fall '10, and GLOBECOM '07, and Symposia Chair for IEEE ICC '10. He also serves as the Editor-in-Chief of the *IEEE Internet of Things Journal*, *Peer-to-Peer Networking and Applications*, and *IET Communications*; and is a Founding Area Editor for *IEEE Transactions on Wireless Communications*. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.