Received: 6 December 2019 | Revised: 10 December 2019 | Accepted: 11 December 2019 | Published on: 19 January 2020

DOI: 10.1002/itl2.145

LETTER

WILEY

Next generation technologies for smart healthcare: challenges, vision, model, trends and future directions

Shreshth Tuli[1] | **Shikhar Tuli**[2] | **Gurleen Wander**[3] | **Praneet Wander**[4] | **Sukhpal Singh Gill**[5] | **Schahram Dustdar**[6] | **Rizos Sakellariou**[7] | **Omer Rana**[8]

[1]Department of Computer Science and Engineering, Indian Institute of Technology (IIT), Delhi, India

[2]Department of Electrical Engineering, Indian Institute of Technology (IIT), Delhi, India

[3]Chelsea and Westminster Hospital NHS trust, London, UK

[4]Department of Gastroenterology, Northshore Long Island Jewish Hospital, New York,

[5]School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK

[6]Distributed Systems Group, Vienna University of Technology, Vienna, Austria

[7]Department of Computer Science, University of Manchester, Manchester, UK

[8]School of Computer Science and Informatics, Cardiff University, Cardiff, UK

Correspondence
Shreshth Tuli, Department of Computer Science and Engineering, IIT, Delhi 110016, India.
Email: shreshthtuli@gmail.com

Modern industry employs technologies for automation that may include Internet of Things (IoT), Cloud and/or Fog Computing, 5G as well as Artificial Intelligence (AI), Machine Learning (ML), or Blockchain. Currently, a part of research for the new industrial era is in the direction of improving healthcare services. This work throws light on some of the major challenges in providing affordable, efficient, secure and reliable healthcare from the viewpoint of computer and medical sciences. We describe a vision of how a holistic model can fulfill the growing demands of healthcare industry, and explain a conceptual model that can provide a complete solution for these increasing demands. In our model, we elucidate the components and their interaction at different levels, leveraging state-of-the art technologies in IoT, Fog computing, AI, ML and Blockchain. We finally describe current trends in this field and propose future directions to explore emerging paradigms and technologies on evolution of healthcare leveraging next generation computing systems.

KEYWORDS

artificial intelligence, Blockchain, cloud computing, fog computing, healthcare, internet of things, machine learning

1 | INTRODUCTION

Cyber-physical systems, the Internet of Things (IoT), Cloud computing, Artificial Intelligence and Blockchain are the signature elements of the next industrial revolution commonly termed as Industry 4.0.[1,2] IoT aims at providing a seamless integration of various smart devices to enable the integration of different sensors, computing resources and actuators. Sensors allow perception of external environment, whereas actuators allow such system to provide physical reponse to

Abbreviations: AI, Artificial Intelligence; IoT, Internet of Things; ML, Machine Learning.

users. These sensors and actuators provide utility in different applications like healthcare, transportation, surveillance among others.[3] Cloud computing, provides the computational resources to remotely execute diverse tasks and provide results to a plethora of applications. The new paradigms of Artificial Intelligence (AI) and Machine Learning (ML) provide users with high quality services, low response times, scalability and robustness to different user needs.[4] The demands of healthcare applications have been ever increasing[5] due to modern AI applications becoming data intensive. Moreover, modern number of patients, types of analysis and response time requirements are becoming more vigorous.[6] New diseases are being discovered every day, new cures need to be tested via simulations, and most importantly, healthcare applications need to be deployed using robust and scalable frameworks that provide high quality results in minimum time.[7]

The problem of providing healthcare to all is challenging because of three major reasons. The first being that most patients need to be continuously monitored and their data analyzed at every instance.[5] This becomes challenging as the data is so immense that it requires high computational resources and efficient algorithms.[8] Moreover, large computation power is costly, which makes the affordability of healthcare for all people the second biggest challenge.[9] The third challenge is maintaining integrity and reliability of systems.[10] The healthcare data is very sensitive since it can be maliciously used to target a specific sector of people by terrorists or pharmaceutical monopolists. This requires such frameworks to be tamper-proof and hack free, preventing any fraudulent manipulation of sensitive healthcare data.[11]

As discussed in Section 1, the challenges of providing healthcare to all are difficult to solve. There have been many efforts in recent years to mitigate the problems and providing more efficient systems.[10,12-14] However, most of such systems focus on a specific problem and do not deliver a holistic framework that solves the larger issue of providing high performance, affordable, secure, robust, scalable and efficient approach for healthcare applications. Deep Learning and AI can provide high performance systems as shown in prior work.[8] Fog computing and shifting the computational resources closer to the edge of the network improves response time, allows more scalable environments and makes deployments more energy efficient and affordable.[3] Blockchain and encryption with public-private signature management are key elements for providing secure communication among patients and computational machines with high data integrity.[15] The main challenge lies in the ability to integrate all these technologies to provide a single solution that caters to all the needs and requirements of the healthcare industry. This requires expertise of different domains to be brought together, and in that effort the next section provides a conceptual model of providing a holistic solution of the problem discussed (Figure 1).

2 | MODEL

In this section we propose and describe a model that brings together all technologies that mark the Industry 4.0 revolution to provide a single end-to-end integrated solution for healthcare.

2.1 | IoT paradigm

The IoT paradigm is comprised of numerous IoT devices with associate healthcare sensors and actuators. Typical healthcare sensors in the IoT paradigm include Blood pressure sensors, Pulse Oximeters as well as Electrocardiogram, Body temperature and Airflow sensors. Such sensors are geographically distributed and perceive the external environment to make decision and providing utilities for the corresponding system. Inherently, the devices are energy constrained and perform minimal computational tasks although they may generate a large amount of data within a short period of time. Therefore, to process the IoT data and host relevant applications, smart systems employ sophisticated deep learning models which range from Convolutional Neural Networks (CNNs) to sequence models like Long-Short-Term-Memory (LSTM) networks.[16] The model also extends infrastructure, platform and software services to Edge and Cloud computing. In this case, the sensed data signals and functional requirements such as expected accuracy rate, data sensing frequency and service delivery deadlines are forwarded to computing paradigms from the IoT domain.

2.2 | Gateway level

The gateway level devices include smartphones, mobile computers like laptops and tablets acting as an interface between the IoT layer and computational resources. These devices collect data and package them into tasks to forward to the IoT-Fog broker. These devices can also be configured to manage data (to a small extent) to meet the user specifications

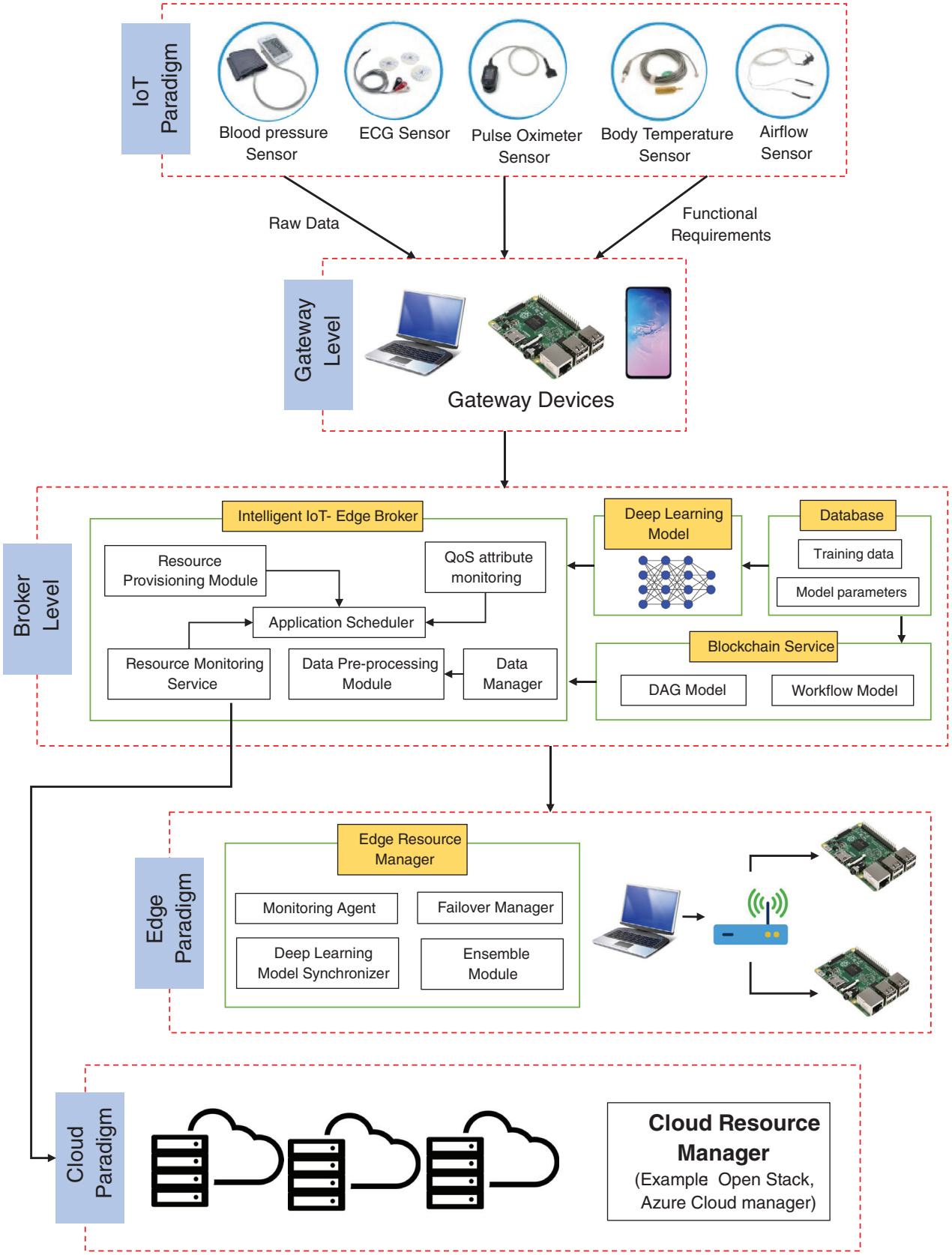

FIGURE 1 Proposed model leveraging advanced technologies of Artificial Intelligence and Blockchain for enhanced performance and seamless task execution on Fog computing Environments

or application Quality of Service (QoS) characteristics. Designing the software modules for such devices is challenging because one gateway device might be connected to multiple IoT devices or sensors and need to manage data and service requirements for each sensor or user. Further, these devices are prone to diverse security threats and malicious attacks that might steal data or sabotage one or multiple such gateway devices. Different techniques can be used to mitigate these difficulties like virtualization, encryption, blockchain based data management with close interaction with Broker and Worker nodes to allow more robust and seamless communication among the IoT devices, gateway nodes and Broker nodes.[17]

2.3 | Broker level

1. IoT-Edge Broker (IEB): This is deployed at the broker level and is the core component of the model which mediates and makes key decisions for the computational network. It consists of a set of sub-components with specialized functions. As a mediator between the IoT and Edge computing paradigms, it is responsible for perceiving the context of IoT devices and application scenario, monitoring the performance of Edge nodes, resource discovery, planning for advance resource configuration prior to application placement, provisioning resources dynamically and management of IoT application execution meeting their QoS requirements, overcoming the faults of the framework. Within IEB, the Data Manager handles interactions between the gateway node and IoT devices, QoS Attribute Monitor analyses the IoT context and state of the Edge infrastructure, predicts the demand, monitors the attainment of QoS attributes, monitors characteristics of Edge and Cloud nodes with the help of Resource Monitoring Service and facilitates application placement with fault tolerance and with the help of Resource Provisioning Module. The Application Scheduler applies policies and techniques to maintain the performance of the system by allocating jobs to the best Edge or Cloud nodes for optimal QoS and deadlines of applications with the help of prediction models and heuristics. The Data Pre-processing Module filters and converts data into required formats and forwards to the appointed worker node which might be in Edge or Cloud.
2. Deep Learning Models: These are saved in a shared repository and act as the on-the-fly learning models that adapt to the performance metrics or loss functions defined by developers to account for the user requirements and application performance. The ease of availability of the model comes with challenges like attacks from hackers that might steal the model or maliciously change it to bring down the accuracy or performance of the predictions of the model.[10] Another challenge is how to maintain the training data private and yet allow all users to access the deep learning models and utilize them without complex authentication mechanisms. Various differential privacy training models can be used and the training and cross-validation data can be kept encrypted in a secured database.[18]
3. Database: The Database (placed at gateway level or layers above based on resource availability) acts as a registry for maintaining instance sensor data and meta-data regarding applications and data flows, and IEB uses its services for resource discovery. The database also stores the deep learning model parameters and training data in encrypted format. The on-the-fly model weights and biases are stored in distributed blockchains to maintain integrity and fail-safe execution and prediction of input data.
4. Blockchain Service: This service maintains the integrity of the sensor data and the model parameters. Different services and techniques exist to maintain the same having different access speeds and overhead characteristics. Trade-offs need to be carefully analyzed so that the response time and integrity of data are not compromised. For Big-Data environments, critical care needs to be given for allocating the Edge or Cloud nodes for hashing, mining and proof-of-work calculation, considering the resource constraints and reliability of edge devices.

2.4 | Infrastructure level

Edge and Cloud Infrastructures are comprised of virtualized resources like virtual machines, containers, etc. offered by centralized datacenters and distributed Edge nodes. Both Edge and Cloud Infrastructures have their own resource managers named Edge Resource Manager (ERM) and Cloud Resource Manager (CRM) respectively. They are responsible for (a) exploring the state of the respective infrastructure, (b) predicting performance, (c) resource virtualization (virtual machines and containers), (d) pooling, (e) scaling, (f) coordination and (g) optimization (migration and consolidation). In addition, they offer (h) service backup and (i) reliability in assisting the IEB for ensuring fault tolerance during uncertain events such as node failures, resource outage and security attacks. Periodically they (j) synchronize the

deep learning model parameters and also (k) maintain majority consensus for data blocks in the blockchain network to maintain common deep learning models and sensor data.

Some of the use cases for the proposed model include data marketplace for personal data, where a user can selectively decide to sell their data to healthcare providers and insurance companies, which takes user consent into consideration (and driven through the use of blockchain based provenance tracking of data). The three pillars of next generation technologies: Artificial Intelligence, Blockchain and IoT allow us to build solutions to issues around accuracy, device calibration, enabling data security and privacy. Our model identifies how devices can be used to capture data from a variety of patient-based sensors.

3 | TRENDS AND FUTURE DIRECTIONS

Many efforts have been in the direction of enhancing service quality in Fog environments, with an aim to provide more accurate disease prediction and automated prescription generation.[12,19,20] Other works focus on developing novel algorithms to provide healthcare services with minimum Service Level Agreement (SLA) violations[21] and reducing response time of results.[8] Many research works also design new techniques to increase the security and reliability of such systems like.[10,22] Further, architecture-level optimizations have been proposed in Wireless Body Sensor Nodes (WBSNs) that exploit emerging technologies, in order to reduce energy consumption and enhance performance.[23,24]

In terms of future work, we propose to integrate other frameworks like Sensor networks,[25] Deviceless edge computing,[26] Serverless computing,[27] Data analytics like in "mySignals"[28] and bringing computation towards the sensors and wearable devices incorporating mobile computation nodes.[29] This will further improve response time and is helpful in critical settings.[30] Further, proper blockchain algorithms need to be developed that are able to work in distributed environments with computational restrictions of the devices at the Edge of the network. There is also a need to consider various machine or deep learning techniques to predict failures and maintain the required level of QoS for the cloud service. Other directions of research include exploration of paradigms like Quantum Computing, enhanced and targeted Operating Systems, Processing-in-Memory (PIM), 6G, and more.[31]

ACKNOWLEDGMENTS

We would like to thank Dr. Guiliano Casale (Department of Computing, Imperial College London) and Dr. Gurpreet Singh Wander (Hero Heart Institute, Dayanand Medical College and Hospital, Ludhiana, India) for their valuable comments, useful suggestions and discussion to improve the quality of the paper.

ORCID

Shreshth Tuli https://orcid.org/0000-0003-2960-1128
Sukhpal Singh Gill https://orcid.org/0000-0002-3913-0369

REFERENCES

1. Lasi H, Fettke P, Kemper H-G, Feld T, Hoffmann M. Industry 4.0. *Bus Inf Syst Eng*. 2014;6(4):239-242.
2. Lee J, Bagheri B, Kao H-A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf Lett*. 2015;3:18-23.
3. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): a vision, architectural elements, and future directions. *Future Generation Computer Syst*. 2013;29(7):1645-1660.
4. Singh GS, TuliS, Minxian X, et al. Transformative effects of IoT, Blockchain and artificial intelligence on cloud computing: evolution, vision, trends and open challenges. *Internet of Things*. 2019; 8:100118.
5. Ahuja Sanjay P, Sindhu M, Jesus Z. A survey of the state of cloud computing in healthcare. *Net Commun Technol*. 2012;1(2):12.
6. Garrett BM. Changing the game; some thoughts on future healthcare demands, technology, nursing and interprofessional education. *Nurse Educ Pract*. 2012;12(4):179-181.
7. Riazul ISM, Daehan K, Humaun KMD, Mahmud H, Kyung-Sup K. The internet of things for health care: a comprehensive survey. *IEEE Access*. 2015;3:678-708.
8. Shreshth T, Nipam B, Singh GS, et al. HealthFog: an ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments. *Future Generation Computer Systems*. 2020;104:187-200.
9. Amartya S. Universal healthcare: the affordable dream. *The Guardian*. 2015;6(01):2015.
10. Tuli S, Mahmud R, Tuli S, Buyya R. Fogbus: a blockchain-based lightweight framework for edge and fog computing. *J Syst Software*. 2019;154:22-36.
11. Jameel F, Javed MA, Jayakody DNK, Hassan SA. On secrecy performance of industrial internet of things. *Internet Technol Lett*. 2018;1(2):e32.

12. Ahmad M, Amin MB, Hussain S, Kang BH, Cheong T, Lee S. Health fog: a novel framework for health and wellness applications. *J Supercomput*. 2016;72(10):3677-3695.
13. Rahmani Amir M, Nguyen GT, Behailu N, et al. Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. *Future Generation Computer Syst*. 2018;78:641-658.
14. Tuli Shreshth, Basumatary Nipam, Buyya Rajkumar. EdgeLens: Deep Learning based Object Detection in Integrated IoT, Fog and Cloud Computing Environments. *Proceedings of the 4th IEEE International Conference on Information Systems and Computer Networks*. 2019.
15. Melanie S. *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media, Inc.; 2015.
16. Sepp H, Jürgen S. LSTM can solve hard long time lag problems. *Advances in Neural Information Processing Systems. Cambridge: MIT Press*; 1997:473-479.
17. Aazam Mohammad, Huh Eui-Nam. Fog Computing and Smart Gateway Based Communication For Cloud of Things. *2014 International Conference on Future Internet of Things and Cloud*. IEEE; 2014.
18. Javaid Ahmad, Niyaz Quamar, Sun Weiqing, Alam Mansoor. A Deep Learning Approach for Network Intrusion Detection System. *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering); 2016.
19. Chye KH, Gerald T, others. Data mining applications in healthcare. *J Healthcare Inf Manage*. 2011;19(2):65.
20. Raghupathi W, Raghupathi V. Big data analytics in healthcare: promise and potential. *Health Inf Sci Syst*. 2014;2(1):3.
21. Hallett S, Parr G, McClean S, McConnell A, Majeed B. Cloud-based Healthcare: Towards a SLA Compliant Network Aware Solution for Medical Image Processing. In: *Cloud Computing 2012: The Third International Conference on Cloud Computing, GRIDs, and Virtualization*. IARIA, 2012; 219–223.
22. Tuli Shreshth, Tuli Shikhar, Jain Udit, Buyya Rajkumar. APEX: Adaptive Ext4 File System for Enhanced Data Recoverability in Edge Devices. *Proceedings of the 11th IEEE International Conference on Cloud Computing Technology and Science*. 2019.
23. Braojos R, Bortolotti D, Bartolini A, Ansaloni G, Benini L, Atienza D. A synchronization-based hybrid-memory multi-Core architecture for energy-efficient biomedical signal processing. *IEEE Trans Comput*. 2017;66(4):575-585.
24. Tuli Shikhar, Rios Marco Antonio, Levisse Alexandre Sébastien Julien, Atienza Alonso David. RRAM-VAC: A Variability-Aware Controller for RRAM-Based Memory Architectures. *Proceedings of the 25th Asia and South Pacific Design Automation Conference (ASP-DAC)*. 2020.
25. Karolj S, Davor D, Enis A, Ivan S, Zorislav S. Scalable distributed computing hierarchy: cloud, fog and dew computing. *Open J Cloud Comput*. 2015;2(1):16-24.
26. Marjan G, Bojana K, Magdalena K, et al. A Deviceless edge computing approach for streaming IoT applications. *IEEE Internet Comput*. 2019;23(1):37-45.
27. Stefan N, Thomas R, Ognjen S, et al. A serverless real-time data analytics platform for edge computing. *IEEE Internet Comput*. 2017;21(4):64-71.
28. Brenda H-G. *Understanding my Signals: Help for Parents of Premature Infants*. Santa Barbara, California: Greenwood Publication Group, Vort; 1988.
29. Gerhard T. The agenda of wearable healthcare. *Yearb Med Inform*. 2005;14(01):125-138.
30. Darwish A, Hassanien AE. Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors*. 2011;11(6):5561–5595.
31. Rukmani K, Ghankuntla R, Vijay D, Anil T, Adarsh D. Future of wireless technology 6G & 7G. *Int J Electr Electron Res*. 2015;3(2):583-585.

How to cite this article: Tuli S, Tuli S, Wander G, et al. Next generation technologies for smart healthcare: challenges, vision, model, trends and future directions. *Internet Technology Letters*. 2020;3:e145. https://doi.org/10.1002/itl2.145