EasyChair Preprint

№ 2290

Performance of Internet of Things Based Healthcare Secure Services and Its Importance: Issue and Challenges

Divya Sharma and R. C. Tripathi

January 1, 2020

Performance of Internet of Things Based Healthcare Secure Services and Its Importance: Issue and Challenges

Divya Sharma[a], Dr. R.C Tripathi[a]
[a]Department of Computer Science, Lingaya's Vidyapeeth University, India

Abstract:
The IoT has a variety of application domains, including medical assistance. The IoT revolution is redesigning modern medical care with promising technological, economic and social prospects. This article shared short advances in IoT-based healthcare technologies and reviewed cutting-edge networking architectures / platforms, industrial applications and trends in IoT-based healthcare solutions. In addition, this article has analyzed other features in addition to the security and privacy of the IoT, including security requirements, threat models and attack taxonomies from the point of view of medical care. Furthermore, this article also proposed a smart collaborative security model to minimize security risk; will discuss different innovations, such as the widespread use of big data, artificial intelligence in the context of medical care, various IoT and e-Health policies and regulations have been addressed worldwide to determine how economies and societies can facilitate sustainable development terms and provides some avenues for future research on health care based on the IoT based on a series of open problems and challenges.

Performance of Internet Of Things Based Healthcare Secure Services And Its Importance: Issue And Challenges

1. Overview

The Internet of Things (IoT) is a concept that reflects a connected whole of any person, anything, anytime, anywhere, any service and any network. IoT is a mega trend in next-generation technologies that can affect the entire spectrum of the heart and can be considered as the interconnection of intelligent objects and devices that can only be identified with the current Internet infrastructure with extensive advantages. The advantages generally include the advanced connectivity of these devices, systems and services that goes beyond machine-to-machine (M2M) scenarios [1]. Therefore, the introduction of automation is conceivable in almost all fields. The IoT offers appropriate solutions for a wide range of applications, such as smart cities, traffic congestion, waste management, structural health, security, emergency services, logistics, retail sales, industrial control and medical care. The interested reader is called for a deeper understanding of the IoT [1] - [6].

It should be noted that research and development activities in the area of health services based on the wireless sensor network (WSN) [7], [8] can be considered as initial efforts based on research in the health sector in IoT. However, the current trend is to move away from recorded standards and adopt IP-based sensor networks using the emerging network of low-power wireless IPv6-based personal area. If the WSNs become a central part of the Internet, careful analysis is required. To better understand the evolution of the WSN towards the IoT and, therefore, its fundamental differences, reference is made to the reader [9] - [11].

IoT Healthcare Applications

In addition to IoT services, IoT healthcare applications require a lot of attention. Keep in mind that applications require services, but are used by patients. Therefore, applications focus on the user. This section describes the different applications of IoT-based medical care, which include grouped and unique applications.

Glucose level detection: diabetes is a metabolic disease that increases the level of glucose in the blood for a certain period of time. Glucose monitoring exposes changes in blood patterns, activity and food formation.

Electrocardiogram monitoring: “an electrocardiogram (ECG) monitors the electric movement of the human heart, determining the rhythm and heart rate, QT intervals, myocardial ischemia and the diagnosis of arrhythmias.

Blood pressure monitoring: monitoring and control of arterial pressure in developing countries as an environment where telemedicine would be a valuable tool.

Body temperature monitoring: body temperature monitoring is a vital measure of medical services, as it can be considered a vital indication of homeostasis conservation. The m-IoT strategy that uses body temperature sensors located on TelosB.

2. Objectives Of The Study

To explore an extensive survey of IoT-based health care services and important applications

To study the extensive insights into security and privacy issues surrounding IoT healthcare solutions and proposing a security model

To discuss the new challenges and open issues that must be addressed to make IoT-based health care technologies and future prospects

IOT Based Medical Care Services: Secure And Privacy

Medical care and medical care represent one of the most interesting areas of application for the IoT [5]. IoT has the potential to give rise to many medical applications, such as remote health monitoring, fitness programs, chronic diseases and elderly care. Respect for care and medicines at home and by healthcare professionals is another important potential application.

Therefore, various medical devices, sensors and diagnostic and imaging devices can be seen as intelligent devices or objects that form a central part of the IoT. IoT-based health services should reduce costs, increase quality of life and enrich the user experience. From the point of view of health care providers, the IoT has the potential to reduce device downtime through remote delivery.

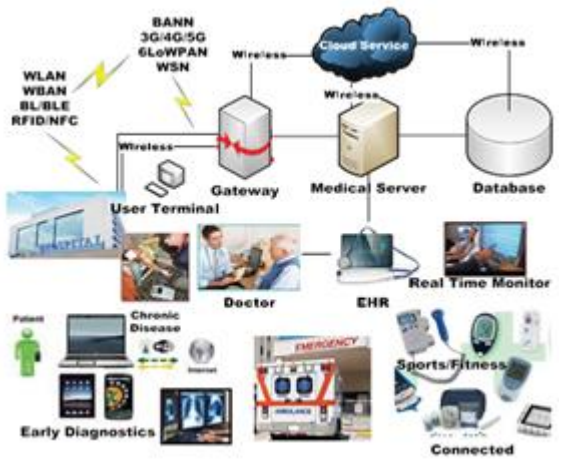

Figure 1 Healthcare trends

Moreover, the IoT is able to correctly identify the optimal times to reconstitute the supplies of various devices for continuous and trouble-free operation. Moreover, the IoT offers an effective programming of limited resources ensuring the best use and service to more patients. Figure 1 illustrates recent health trends [6]. The ease of profitable interactions through secure and seamless connectivity between individual patients, clinics and healthcare organizations is an important trend. Updated healthcare networks based on wireless technologies should support chronic diseases, early diagnosis, real-time monitoring and medical emergencies. Gateways, medical servers and health databases play a vital role in creating medical records and providing health services on request to authorized interested parties.

The IoT should facilitate a wide range of intelligent health services. These services individually provide a positioning of healthcare solutions. Each service can be considered a platform for a wide range of applications and solutions. IoT-based protocols and services require minor adjustments to work properly in healthcare. These services consist of connection protocols, resource sharing services, notification services and interconnection services and the Internet. This section describes different types of IoT-based health services. M-Health Things m-health Internet is the combination of medical sensors, mobile and communication technologies for health centers. Implementation OF problems, Internet architecture m-health Things (m-IoT) and non-invasive challenges for the detection of glucose level.

Adverse drug reactions: an adverse drug reaction refers to the damage caused by the use of drugs. This damage may occur after prolonged administration or a single dose of a drug or as a result of a change in its administration.

Community medical assistance: community medical assistance refers to the creation of a network capable of covering an area such as a residential or a local community. A cooperative community based on the IoT platform for rural medical assistance.

Information on children's health: it is essential to raise awareness and improve the education of children with mental and emotional problems and their needs among the general public and their families.

4. Security and Privacy (S&P)

The number of devices (things) connected to the Internet (Internet of Things: IoT) is growing and the achievement of strong security and privacy (S&P) is becoming increasingly challenging. With the intensive use of medical things (MT), the S&P in the medical field poses a serious problem that continues to grow. Because of the criticality and sensitivity of data in the health sector, guaranteeing the S & P of the Internet of Medical Things (IoMT) makes things even more problematic. The lack of an adequate S&P in the IoMT will not only put patients 'privacy at risk, but can also put patients' lives at risk. The wide variety of TM in health care introduces new avenues of attack on health systems. This is attributed to the following reasons:

(1) MT is mainly exchanging sensitive patient data.
(2) The problems of complexity and incompatibility derive from the interaction of a large number of heterogeneous devices and networks that connect them.
(3) As an emerging industry, health care manufacturers quickly adopt IoT solutions without regard to security. For this reason, new security issues related to confidentiality, integrity and availability (CIA) arise.
(4) Since most IoT components transmit and receive data wirelessly, this puts the IoMT in danger of security breaches in the wireless sensor network (WSN).
(5) Furthermore, IoMT solutions cover applications to manage, monitor and control them. Application risks, such as authentication and authorization violations, as well as general security and application availability, also become a problem.
(6) Some safety calculations consume a significant fraction of the computing resources. Due to the limited capacities (or processing and power) of wireless sensors, many of these

sensors do not have built-in encryption. This lack of secure MT encryption leaves devices open to be discovered and exploited by malicious parties.

Therefore, IoMT S&P has become a topic of the utmost importance to the health sector. Depending on the critical importance of the healthcare environment, these S&P risks have catastrophic consequences, including improper treatment, loss of life, bad reputation and financial loss. Therefore, it is urgently necessary to identify and assess the risks of the IoMT to better support the decision-making process when adopting or designing a safe and reliable IoMT.

5. IOT Healthcare Security

The IoT is growing exponentially. In the coming years, it is expected that the health area will see the full adoption of IoT technology and will flourish as a result of modern IoT e-Health applications and devices. These IoT-based healthcare applications and devices are expected to contain important information, including personal health care information. Furthermore, these types of devices can be connected to the global information network: access will be available everywhere, at any time. However, this makes the IoT-based medical care a target for hackers. It is essential and extremely valuable to analyze and recognize the different characteristics of privacy and security of the IoT, vulnerabilities, countermeasures and security requirements from the point of view of medical assistance to allow the IoT to adapt to these challenges.

6. Current Issues And Security Challenges

Since the security needs of the IoT cannot be certified through traditional security schemes, innovative schemes are needed to solve the new problems encountered in the IoT. Several challenges for IoT-based health services are discussed here.

Computational limitations: IoT-based healthcare devices normally contain low-speed processing units. The core of these devices (the central processing unit [CPU]) is not very influential in terms of performance and speed and does not perform expensive computational operations.

Memory limitations: most devices have less integrated memory and can be activated with an integrated operating system (SO).

Energy and mobility limitations: IoT-based healthcare devices are dynamic and equipped with small sanitary devices and batteries. Since different networks have different configurations and configurations, a security algorithm for mobility and complement is required.

Current Issues and Challenges in IoT based Healthcare and its solution

Several researchers have focused on implementing and designing different IoT healthcare frameworks and on resolving numerous architectural complications related to these frameworks. However, there are still numerous open research problems and challenges that need to be adequately addressed. This section describes some of these challenges."

Cost analysis: researchers should consider creating low-cost prototypes of IoT-enabled drug solutions; However, to date, no study has considered this problem.

Continuous monitoring: in some conditions long-term monitoring of patient health is required. To achieve this, continuous registration and monitoring is essential.

Identification: healthcare organizations and hospitals often deal with a large number of patients, with multiple support personnel performing various tasks. Accurate identification of patients and staff is required to achieve proper data management in these situations.

Mobility: IoT healthcare solutions must be able to help patient mobility because they are connected at any time and in any place. Mobility specifications are used to connect different patients to different networks.

7. Conclusion

This article would take into consideration the trends in IoT-based health research and discover several problems that need to be addressed to transform health technologies through IoT innovation.

The Internet of medical things (IoMT), also known as IoT for medical care, refers to the collection of medical devices and applications connected through networks. Many healthcare professionals use IoMT applications to improve treatments, control diseases, reduce errors, improve patient experience, administer drugs and reduce costs. According to market research, the IoT health care market segment is ready to reach $ 117 billion by 2020.

In recent years, this sector has attracted great attention from researchers to address the potential of IoT in the field of health by considering several practical challenges. As a result, there are now numerous applications, services and prototypes in the field. The research trends in the health sector based on the IoT include network architectures and platforms, new services and applications, interoperability and security, among others.

Furthermore, policies and guidelines have been developed to implement

IoT technology in the medical field in many countries and organizations around the world. However, the IoT remains at the beginning in the health field. At this stage, it is expected that a thorough understanding of current IoT research in the context of medical care is useful for different stakeholders interested in conducting further research.

New challenges related to the policies and regulations on electronic health and the IoT for the benefit of different stakeholders interested in the evaluation of health technologies based on the IoT. In summary, the upcoming results of this survey should be useful for researchers, engineers, health professionals and policy makers working in the IoT and health technology field. This is an exciting area of research and is open to researchers to investigate. With this work, we hope to help adopt and produce IoMT insurance so that patients and healthcare professionals can get great benefits with minimal risks.

REFERENCES

G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, (2010). ‘‘Smart objects as building blocks for the Internet of Things,’’ IEEE Internet Comput., 14(1), 44–51.

K. Romer, B. Ostermaier, F. Mattern, M. Fahrmair, and W. Kellerer, (2010). ‘‘Real-time search for real-world entities: A survey,’’ Proc. IEEE, 98(11) 1887–1902.

D. Guinard, V. Trifa, and E. Wilde, (2010). ‘‘A resource oriented architecture for the Web of Things,’’ in Proc. Internet Things (IOT), 1–8.

L. Tan and N. Wang, (2010). ‘‘Future Internet: The Internet of Things,’’ in Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE), 5, V5-376–V5-380.

Z. Pang, (2013). ‘‘Technologies and architectures of the Internet-of-Things (IoT) for health and well-being,’’ M.S. thesis, Dept. Electron. Comput. Syst., KTH-Roy. Inst. Technol.;Stockholm, Sweden.

J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, (2010). ‘‘Wireless sensor networks for healthcare,’’ Proc. IEEE, 98(11), 1947–1960.

H. Alemdar and C. Ersoy, (2010). ‘‘Wireless sensor networks for healthcare: A survey,’’ Comput. Netw., 54(15), 2688–2710.

L. Mainetti, L. Patrono, and A. Vilei, (2011). ‘‘Evolution of wireless sensor networks towards the Internet of Things: A survey,’’ in Proc. 19th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM), 1–6.

D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, (2009). ‘‘Wireless sensor networks and the Internet of Things: Selected challenges,’’ in Proc. 8th GI/ITG KuVS Fachgespräch ‘Drahtlose Sensornetze’, 31–34.

C. Alcaraz, P. Najera, J. Lopez, and R. Roman, (2010).. ‘‘Wireless sensor networks and the Internet of Things: Do we need a complete integration?’’ in Proc. 1st Int. Workshop Security Internet Things (SecIoT).

Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, Dec. (2010). ‘‘IOT gateway: Bridging wireless sensor networks into Internet of Things,’’ in Proc. IEEE/IFIP 8th Int. Conf. Embedded Ubiquitous Comput. (EUC), 347–352.