Themed Section : Engineering and Technology
© 2018 IJSRSET | Volume 5 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099

A Study of IoMT - An Advanced Application to the Current Health Scenario

Tharanee Shree Saravanan[1]
[1]Dept. of ECE, Velammal Institute of Technology, Chennai, Tamil Nadu, India
tharaneeshree@gmail.com[1]

ABSTRACT

The present study is an attempt to highlight in detail about the pros and cons of the Internet of Medical Things, which is the most effective and efficient application of information processing involving both computer hardware and software, that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making. The Internet of Medical Things (IoMT) is the collection of medical devices and applications that connect to healthcare IT systems through online computer networks. Many of the innovations resulting from IoMT provide a valuable platform for the evolution of healthcare and the provision of better, personalized treatment for more patients. However, for the initiatives to succeed, both healthcare professionals and patients must buy into the changes. IoT is not just meant for improving our lives, but it is transforming our lives in a big way. Healthcare is one of the most noble causes IoT can help and it's already doing it.

Keywords: Health Care, Medical Device Application, Tele Medicine, Medical Sensors For Diagnose, Electronic Health Record, Cyber Attacks

I. INTRODUCTION

Health care is conventionally regarded as an important determinant in promoting the general physical and mental health and well-being of people around the world. A well-functioning healthcare system requires a robust financing mechanism; a well-trained and adequately paid workforce; reliable information on which to base decisions and policies; and well maintained health facilities and logistics to deliver quality medicines and technologies. Healthcare can contribute to a significant part of a country's economy. In this world of hi-tech, such an important service need an effective and efficient application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making, which is popularly now known as Internet Of Medical Things (IoMT).

The Internet of Medical Things (IoMT) is the collection of medical devices and applications that connect to healthcare IT systems through online computer networks. Medical devices equipped with Wi-Fi allow the machine-to-machine communication that is the basis of IoMT. IoMT devices link to cloud platforms such as Amazon Web Services, on which captured data can be stored and analyzed. IoMT is also known as healthcare IoT.

As is the case with the larger Internet of Things (IoT), there are now more possible applications of IoMT than before because many consumer mobile

devices are built with Near Field Communication (NFC) radio frequency identification (RFID) tags that allow the devices to share information with IT systems. RFID tags can also be placed on medical equipment and supplies so that hospital staff can remain aware of the quantities they have in stock.

The practice of using IoMT devices to remotely monitor patients in their homes is also known as telemedicine. This kind of treatment spares patients from travelling to a hospital or physician's office whenever they have a medical question or change in their condition.

II. A WEARABLE MEDICAL DEVICE

The Internet of Medical Things (IoMT) is a group of wearable medical devices used to collect patient physiological data. The wearable medical devices are inter-connected with the assistance of wireless networks. Most of the medical devices are connected with the use of Wi-Fi to communicate each other. The data collected on wearable medical devices are stored on a cloud database. Now-a-days, the number of wearable medical devices generates large amounts of healthcare data, including blood pressure, heart rate, body temperature, respiratory rate, blood circulation level, body pain and blood glucose level. However, the main challenge in IoMT is how to manage with respect to critical applications, where a number of connected devices generate a large amount of medical data. This large volume of data, often called big data, cannot readily be processed by traditional data processing algorithms and applications. In general, many database clusters and additional resources are required to store big data. However, storage and retrieval are not the only problems. Obtaining meaningful patterns from big data, such as that pertaining to patient diagnostic information, is also an essential problem. Presently, a number of emerging applications are being developed for various environments. Sensors are most often used in critical applications for real-time or near future. In particular, the IoMT uses an accelerometer sensor, visual sensor, temperature sensor, carbon dioxide sensor, ECG/EEG/EMG sensor, pressure sensor, gyroscope sensor, blood oxygen saturation sensor, humidity sensor, respiration sensor and blood-pressure sensor to observe and monitor the patient's health in a continuous manner. By intelligently investigating and collecting large amounts of medical data (i.e., big data), IoMT can enhance the decision-making process and early disease diagnosis. Hence, there is a need for scalable machine learning and intelligent algorithms that lead to more interoperable solutions, and that can make effective decisions in emerging IoMT.

III. CHALLENGES TO ADOPTION

Many of the innovations resulting from IoMT provide a valuable platform for the evolution of healthcare and the provision of better, personalized treatment for more patients. However, for the initiatives to succeed, both healthcare professionals and patients must buy into the changes.

That means creating a great patient experience through simple, easy-to-use devices, and clear benefits. Doctors can play an important role in advising patients on the most suitable devices for their conditions, and providing feedback to patients to demonstrate that the devices are providing improved care.

Doctors must also increase adoption rates by recognizing the benefits IoMT can bring to their practice. IoMT suppliers must provide clear use cases that doctors can assess to review the potential for their patient group. Doctors also need to have access to an end-to-end solution that enables them to access data and insights quickly and easily and receive real-time alerts when the data indicates that action is needed.

A 2013 survey by eClinicalWorks assessed healthcare providers' interest in mobile health apps linked to electronic health records (EHRs). The results show

providers want their patient engaged, and see clear benefits in health outcomes with this connection. According to the survey, 93 percent of respondents felt a mobile health app connected to EHRs delivered value.

Ninety-three percent of respondents believed that mobile health apps can improve a patient's health outcome, and 89 percent were likely to recommend a mobile health app to a patient. Respondents felt that the top three benefits of this technology were medication adherence (65 percent), diabetes management (54 percent) and preventative care (52 percent).

IV. DRIVING A CULTURE CHANGE

In many ways, IoMT represents a culture change for both patients and doctors. But that change will only take place if both parties are confident of beneficial outcomes. And any new initiatives must overcome requirements for regulatory compliance, particularly with the Health Insurance Portability and Accountability Act (HIPAA), which protects the privacy of patients' health information.

Because IoMT promotes and enables the collection and sharing of health information by a number of different parties, doctors and healthcare providers must enforce security of data.

If IoMT can overcome these initial challenges, it could prove to be the solution to rising healthcare costs that are being driven by a rising population of people over 65, which could rise to almost 20 percent of the US population by 2030, according to Administration on Aging.

As IoMT continues to evolve, it could ultimately transform US healthcare by offering broader, more accessible, and cost-effective solutions.

V. RESOURCE MANAGEMENT

IoT solutions are now used to track the location and quantity of products as a form of automated stock control. This also has application in healthcare as hospitals use the technology to monitor stock levels of essential supplies or to locate equipment in storage or in medical wards. Administrators use RFID tags fitted to the equipment to monitor and manage it.

Using the same RFID technology, hospital administrators are now able to track patients' progress through the hospital when they are visiting for consultation or staying for operations or treatment. The information enables administrators to identify bottlenecks in the system or departments where additional resources are needed.

It can also provide patients or their families more information on ER waiting times, available dates for operations, and progress of patients in recovery. This provides a more accurate basis for planning and managing hospital resources, improving efficiency, reducing costs, and improving the patient experience.

Some hospitals are taking the process further and offering patients and their families access to doctors' notes, IoMT data and other treatment information through a secure patient portal. In addition, the same principals of shared information let patients upload data that might be useful to doctors—from their own connected devices.

VI. SUPPORTING COLLABORATION

The vast amount of data available through IoMT and the ability to share findings through the cloud support collaborative treatment. In its simplest form, doctors can share information to obtain expert opinions or treatment recommendations from a specialist.

IoMT can also form the basis for a type of crowdsourcing in healthcare. Here, professionals contribute their diagnosis or opinions on rare diseases or complex medical problems. Using a form of

scientific polling based on algorithms, the participants offer a solution that speeds diagnosis and gives patients the benefit of a wide range of expert views.

That data and its related insights are available as a knowledge base that can help specialists identify and solve complex problems in the future. Commentators note that problems of liability and payment may act as barriers to the wider adoption of this form of crowdsourcing, but the application demonstrates the potential of IoMT to deliver new kinds of healthcare.

The following are five challenges of IoT in healthcare that put it at risk of failure.

Lack of EHR system integration. While the data that is collected from IoT devices can include a patient's vital signs, physical activity or glucose levels while at home, that information does not typically travel to an EHR system and, in most cases, is not centralized or made easily available to providers. This limits the information's value since it is not always presented to the provider in a clinical context.

Some EHR systems allow patients to import data into their record, but this still remains relatively limited to a few dominant EHR players and leaves many providers uncertain of how to handle information that lives outside of their records systems.

Interoperability challenges keep IoT data in different silos. Patients are likely to collect different sets of data when using different medical devices depending on each device's purpose and, in some cases, the ordering physician. A patient with diabetes may frequently collect glucose levels and report them back to their primary care physician while also potentially capturing data related to their asthma on a separate device, which may be going to their asthma and allergy care provider. In many cases, the information that the patient captures stays within the boundaries of each of the systems and IoT vendors and is not visible to other systems. Unfortunately, with the lack of wider adoption of adequate interoperability, data from different IoT devices may remain locked in each individual system and lose its potential value to the rest of a patient's care team.

IoT data alone may not be as meaningful if it is not within the context of a full health record. Many providers support the collection of meaningful patient data between visits, but this data is only valuable if it can be incorporated and viewed within the context of a full patient chart and timeline. There are still many cases where the data collected from wearables and other medical devices stays locked in the IoT vendor repository or apps, but for a physician, that data may not provide any help unless it is visible within the context of the patient's full record.

Data security causes concerns in the implementation of IoT in healthcare. From the time that the data is collected at the device level to the point that it is transmitted over to its final destination, securing that information is critical and is required under HIPAA. But with the lack of common security standards and practices, many health IT professionals have concerns about the risks associated with IoT device tampering and data breaches.

The Food and Drug Administration (FDA) is in the process of defining a common security practice and standards for medical devices as they become more frequent in the clinical setting. Earlier in 2016, the FDA released a draft of "Postmarket Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff" to outline the steps manufacturers should take to continually address cybersecurity risks with their devices to better protect public health.

Constant changes in hardware and connectivity technology. Patients today need more than one device to capture the different health data their providers need. This can require more than one sensor that, in most cases, is used alongside a hub to which information is pushed that's designed to process the information. These hubs are not always compatible with the different sensors that are

available, and having a lack of common hardware or wireless connectivity standards -- such as Wi-Fi, Bluetooth or Z-Wave -- can cause patients to have extensive hardware in their homes, which can be overwhelming and costly.

Providers are hopeful that IoT will have a positive impact on supporting patient care and delivering valuable data. IoT applications offer the opportunity for providers to have visibility to what happens between visits and can provide some insights into patient medication adherence, activity levels and vital signs. But this emerging technology is threatened by the different challenges of IoT in healthcare defined here that, if left unaddressed, can get in the way of its success. Fortunately, there is traction around addressing many of these IoT challenges, and progress continues to be made toward resolving them and toward allowing IoT technologies to have a meaningful impact on healthcare.

VII. THREATS PRESENTED BY THE IOMT

The addition of connected devices to the healthcare industry has expanded the surface area for possible attacks. Further, many healthcare institutions lack adequate security capabilities. The combination of these two factors equates to an "easy win" in the eyes of cybercriminals.

Some of the more traditional forms of cyberattacks, like phishing schemes and DDoS, are still alive and well, but healthcare IT security is now faced with combating attacks on connected medical devices in healthcare facilities, as well as home health devices. These devices have, for the most part, not been designed with security as a top-of-mind concern, as developers are primarily focused on functionality and ease of use.

As a result, attackers are not only exploiting inadequate IT security to gain unfettered access to networks and data, but actual control of IP-enabled medical devices themselves. Vulnerable systems, valuable data and a wide-open surface are putting the industry in the attack spotlight and, as a result, have medical IT teams on edge.

[1]

VIII. DEFENDING AGAINST ATTACKS

With what we now know about the IoMT, it should come as no surprise that security budgets to defend against threats have been growing. "Gartner believes that the average security budget for IT, operational technology (OT) and IoT security requirements will respond to the growth of IoT devices across all business segments and scenarios, rising from less than one percent of annual security budgets in 2015 to 20 percent in 2020."

There are a number of different features healthcare IT professionals should look for when evaluating a security vendor's solutions and capabilities.

One critical consideration is that a vendor be able to provide internal segmentation firewalls (ISFWs) to defend against breaches, as the landscape of networks is typically wide open and flat. Because ISFWs operate inside the network instead of at the edge, they allow healthcare organizations to intelligently segment networks between patients, administrators, healthcare professionals and guests, as well as between types of devices – for example, between a patient information system and a life-saving heart monitor or infusion pump.

It can then prioritize interconnected medical devices that need the highest degrees of protection and monitoring, and inspect and monitor all traffic moving between segments, all without impacting performance.

A healthcare security vendor should also have a team in place that's dedicated to uncovering the latest threat intelligence, so real-time threat and mitigation updates can be made expeditiously, before cybercriminals take advantage of any weaknesses in connected IoT devices or the critical services they provide.

IX. FEW EXAMPLES FOR IoMT

1. OpenAPS - closed-loop insulin delivery

One of the most fascinating areas in IoT medicine is the open source initiative OpenAPS, which stands for open artificial pancreas system.

Dana Lewis and her husband Scott Leibrand have hacked Dana's CGM (continuous glucose monitor) and her insulin pump. Using the data feed from the CGM and a Raspberry Pi computer, their own software completes the loop and continuously alters the amount of insulin Dana's pump delivers. As of summer 2016, when Dana presented at OSCon in Austin, 59 people were using the open source software and hacking their own equipment.

This example shows how patients have been waiting for years for improved technology which the healthcare industry has not delivered.

Security concerns and lengthy development and testing periods mean that connected devices have taken some time to come to market.

Dana Lewis told e-patients.net that, in the view of OpenAPS, "the relative net risk of this [loop] feature is far outweighed by the net benefit of providing users the ability to control their own devices, as discussed here."
Reading the FAQs on the OpenAPS website gives an interesting insight into some of the issues in this part of the healthcare market.

2. **Pharma** is following, though, and developing its own connected systems to help diabetes sufferers. In 2016, Roche acquired distribution rights to an implantable long-term continuous glucose monitoring (CGM) system which uses a 90 day sensor below the patient's skin.

The sensor communicates with a smart transmitter which then sends blood glucose levels to a sister mobile app on the patient's phone.

3. Activity trackers during cancer treatment

The Memorial Sloan Kettering Cancer Center (MSK) and cloud research firm Medidata are testing the use of activity trackers to gather lifestyle data on patients being treated for multiple myeloma.
Patients will wear an activity tracker for up to a week prior to treatment and then continuously for several months over the course of multiple treatments.

The trackers will assist in logging activity level and fatigue, with appetite also being logged directly, and all data saved to Medidata's Patient Cloud ePRO app on their personal smart phones.

Using a variety of data gathered day-to-day through wearables or apps is a fairly obvious way that diagnosis and treatment can be improved for many conditions.

This is particularly the case for a disease such as cancer, for which the reaction to therapy plays an important and determinant part in prescribing the right treatment.

4. Connected inhalers

The most immediate use for IoT technology in healthcare is not to assist in diagnoses, though, but to ensure adherence. Adding sensors to medicines or delivery mechanisms allows doctors to keep accurate track of whether patients are sticking to their treatment plan.

This provides motivation but also clarity for patients. Devices connected to mobile apps allow for patients to receive reminders, as well as to check on their own adherence.

Novartis is undertaking connected inhaler research with both Qualcomm and Propeller Health, developing inhalers for chronic obstructive pulmonary disease (COPD).

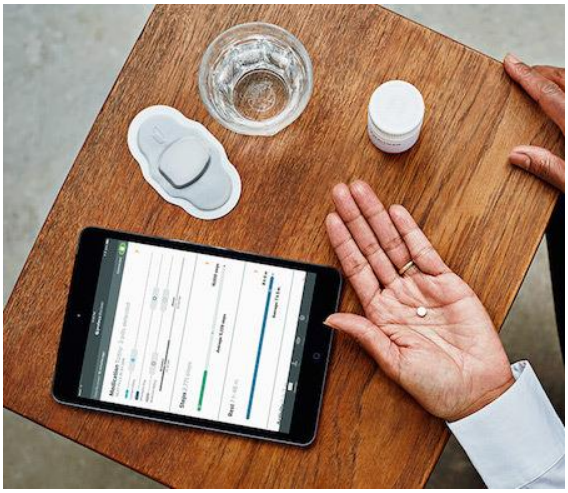
Propeller's Breezhaler device connects to its digital platform via a sensor, passively recording and transmitting usage data. Novartis' own device will likely not be released until 2019, though, showing the timescales involved in this sort of research.

5. Ingestible sensors

Proteus Digital Health and its ingestible sensors are another example of digital medicine.

Again, the chief purpose of this technology, trialled with an antipsychotic and a hypertension pill, is to monitor adherence. However, in this case, the pill dissolves in the stomach and produces a small signal which is picked up by a sensor worn on the body, which again relays the data to a smartphone app.

According to a study by the World Health Organisation in 2003, 50% of medicines are not taken as directed. Proteus' system is one effort to reduce this figure.



X. CONCLUSION

IoT is not just meant for improving our lives, but it is transforming our lives in a big way. Healthcare is on of the most noble causes IoT can help and it's already doing it. With the emergence of IoT (Internet of Things) and devices, the healthcare industry will benefit from seamless connectivity, improved data and information between healthcare professionals and patients.

IoT is changing healthcare in many different areas including equipment supplies, patient care and monitoring, drug delivery and management, remote surgeries and connectivity of doctors with patients. Healthcare applications are proving to be life changing not just fro primary treatments but also for patients with terminal illness. Experts believe that this is just the beginning, there are more applications which are ready to disrupt the future of healthcare.

Today's healthcare institutions should continue looking for new ways to improve the patient experience and save lives, without having to worry about dangerous cybercriminals breaching their systems. Which means that security should never be neglected during implementation or forgotten about after new devices have been activated.

Today's cybercriminals are smarter and more determined than ever, and the healthcare industry needs to be aware of the trends, capabilities and

possible avenues of attack that they are looking to exploit.

The next decade may well see a revolution in treatment and diagnosis of disease, as the Internet of Things (IoT) is brought to bear on medicine.

XI. REFERENCES

[1] "What is IoMT", http:/internet of things agenda. techtarget.com

[2] "How the IoMT is transforming Health Care", The VoIP Report, thevoipreport.com, August 31st ,2017

[3] "Emerging applications of Internet of Medical things", http:/www.journals.elsevier.com