Smart Healthcare System: A Primer

[1]Jackson Akpojaro, *[2]Rotimi-Williams Bello
[1, 2]Department of Mathematical Sciences, University of Africa, Toru-Orua, Bayelsa State, Nigeria
Email address: [1]jakpojaro@yahoo.com, [2]sirbrw@yahoo.com

Abstract: *Smart healthcare system also known as Internet of Things (IoT)-based healthcare system is the abbreviation for Self-directed, Motivated, Adaptive, Resource-enriched, and Technologies-embedded (SMART) healthcare. This smart healthcare system is not smart device healthcare, but rather a medical paradigm shift for digital natives. IoT and cloud-based healthcare services promote patients' monitoring and good healthcare delivery which are important to the 21st century healthcare services. But many healthcare institutions do not understand how germane the application of these technologies is to the healthcare delivery to promote patients' monitoring and good healthcare delivery which are important to the 21st century healthcare services. The only option left to face the challenges confronting monitoring and delivering of ideal medical services in the 21st century by healthcare providers is the application of these technologies. The understanding of the use of these devices, applications, and services do not only help patients know how to manage their health and life for good purpose but assists healthcare providers to reduce emergency cases, track patients, staff, and inventory; enhance drug management for the overall control of epidemics. Also, the understanding of the use of these technologies helps in simultaneous reporting and monitoring, end-to-end connectivity and affordability, data assortment and analysis, remote medical assistance, tracking and alerts. Devices involving hardware and software technologies for smart healthcare system are revealed to enhance medical service delivery to both in-patients and out-patients. Findings show that cell phone with radio-frequency identification (RFID)-sensor capabilities can serve as a platform for ideal healthcare delivery. Healthcare data insecurity and privacy through multiple devices and protocols are the major limitations of IoT applications in healthcare delivery noticed in the course of this study. This is a serious issue as vital information about patient which is in the cloud can only be accessible through IoT multiple devices and protocols.*

Key Words: *Smart, Healthcare, IoT, Patient, System, RFID.*

1. INTRODUCTION:

Communication gap and poor coordination of care among primary care, secondary care, tertiary care, and specialty care providers lead to major inefficiencies in healthcare delivery. In resource constrained settings, these inefficiencies exacerbate mismatches between the demand and supply for specialist services. The overall sufferers are the patients. Healthcare is the maintenance or improvement of health via the prevention, diagnosis, and treatment of disease, illness, injury, and other physical and mental impairments in human beings. Healthcare is delivered by health professionals (providers or practitioners) in allied health professions, physicians, physician associates, dentistry, midwifery, nursing, medicine, optometry, audiology, pharmacy, psychology, and other health professions. It includes the work done in providing primary care, secondary care, and tertiary care, as well as in public health. Access to healthcare may vary across countries, groups, and individuals, largely influenced by social and economic conditions as well as the health policies and plans in relation to the personal and population-based healthcare goals within their societies. Healthcare systems are organizations established to meet the health needs of target populations. Their exact configuration varies between national and sub national entities.

In all cases, according to the World Health Organization (WHO), 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 [1]. Therefore, smart healthcare system is to the rescue. Internet of Things (IoT) can change the hospital-centric routine method of medical delivery to home-centric. IoT-based healthcare will yield unparallel benefits which could improve the quality of treatments receive by the patients. IoT embedded medical devices and techniques can immensely help in the monitoring of patients with both serious and mild diseases. This technology can also benefit clinicians by allowing them concentrate on more important tasks as they would not be conducting frequent ward rounds and consultation. The demand for medical attention by patients from doctors and nurses is extremely high. Apparently, a solution is required to reduce the pressure; which is the main objective of this study.

2. ENGINES OF INTERNET OF THINGS (IoT):

The term IoT generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange

and consume data with minimal human interventions. There is, however, no single, universal definition. The concept of combining computers, sensors, and networks to monitor and control devices has existed for decades. IoT can be compared to cyber-physical system; a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities. The ability to have a networked of physical devices embedded with electronics, software, sensors, actuators and connectivity which enables the physical devices to connect and exchange data, creating opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions is a key technological debate. The recent confluence of several technology market trends, however, is bringing the IoT closer to widespread reality. These include ubiquitous connectivity, widespread adoption of IP-based networking, computing economics, miniaturization, advances in data analytics, and the rise of cloud computing. IoT implementations use different technical communications models such as device-to-device, device-to-cloud, device-to-gateway, and back-end data-sharing.

These models highlight the flexibility in the ways that IoT devices can connect and provide value to the user, each with its own characteristics. Despite a shared belief in the potential of IoT, industry leaders and consumers are facing barriers to adopt IoT technology more widely. Among the barriers is the desire to have IoT hardware and software components that are highly interoperable, dependable, reconfigurable, and in many applications, certifiable. The basic communications models of IoT demonstrate the underlying design strategies used to allow IoT devices to communicate. Aside from some technical considerations, the use of these models is largely influenced by the open versus proprietary nature of the IoT devices being networked. And in the case of the device-to-gateway model, its primary feature is its ability to overcome proprietary device restrictions in connecting IoT devices. This means that device interoperability and open standards are key considerations in the design and development of internetworked IoT systems. From a general user perspective, these communication models help illustrate the ability of networked devices to add value to the end user. By enabling the user to achieve better access to an IoT device and its data, the overall value of the device is amplified. Often, however these devices use protocols like Bluetooth, Z-Wave, or ZigBee to establish direct device-to-device communications. Some of the communication models enabling technologies that made smart healthcare system possible are: addressability, short-range wireless, medium-range wireless, long-range wireless, and wired.

2.1 Addressability:

The original idea of the Auto-ID Center is based on RFID-tags and unique identification through the Electronic Product Code; however, this has evolved into objects having an IP address or URI. An alternative view, from the world of the Semantic Web [2] focuses instead on making all things addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralized servers acting for their human owners. Integration with the Internet implies that devices will use an IP address as a unique identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IoT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required [3], [4], [5]. IoT devices additionally will benefit from the stateless address auto-configuration present in IPv6 [19], as it reduces the configuration overhead on the hosts, and the IETF 6LoWPAN header compression. To a large extent, the future of the IoT will not be possible without the support of IPv6; and consequently, the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future [5].

2.2 Short-range Wireless:

Bluetooth mesh networking–specification providing a mesh networking variant to Bluetooth low energy (BLE) with increased number of nodes and standardized application layer (Models). (a) Light-Fidelity (Li-Fi)–Wireless communication technology similar to the Wi-Fi standard, but using visible light communication for increased bandwidth. (b) Near-field communication (NFC)–Communication protocols enabling two electronic devices to communicate within a 4 cm range. (c) QR codes and barcodes–Machine-readable optical tags that store information about the item to which they are attached. (d) Radio-frequency identification (RFID)–Technology using electromagnetic fields to read data stored in tags embedded in other items. (e) Thread–Network protocol based on the IEEE 802.15.4 standard, similar to ZigBee, providing IPv6 addressing. (f) Transport Layer Security–Network security protocol. (g) Wi-Fi–technology for local area networking based on the IEEE 802.11 standard, where devices may communicate through a shared access point or directly between individual devices. (h) Z-Wave–Communication protocol providing short-range, low-latency data transfer at rates and power consumption lower than Wi-Fi. Used primarily for home automation. (i) ZigBee–Communication protocols for personal area networking based on the IEEE 802.15.4 standard, providing low power consumption, low data rate, low cost, and high throughput.

2.3. Medium-range Wireless:

(a) HaLow–Variant of the Wi-Fi standard providing extended range for low-power communication at a lower data rate. (b) LTE-Advanced–High-speed communication specification for mobile networks. It provides enhancements to the LTE standard with extended coverage, higher throughput, and lower latency.

2.4. Long-range Wireless:

(a) Low-power wide-area networking (LPWAN)–Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission. Available LPWAN technologies and protocols: LoRaWan, Sigfox, NB-IoT, Weightless. (b) Very small aperture terminal (VSAT)–Satellite communication technology using small dish antennas for narrowband and broadband data. (c) Long-range Wi-Fi connectivity.

2.5. Wired:

(a) Ethernet–general purpose networking standard using twisted pair and fiber optic links in conjunction with hubs or switches. (b) Multimedia over Coax Alliance (MoCA)–Specification enabling whole-home distribution of high definition video and content over existing coaxial cabling. (c) Power-line communication (PLC)–Communication technology using electrical wiring to carry power and data. Specifications such as HomePlug or G.hn utilize PLC for networking IoT devices.

2.6 Device-to-device Networks:

Device-to-device networks as shown in Fig. 1, allow devices that adhere to a particular communication protocol to communicate and exchange messages to achieve their function. This communication model is commonly used in applications like home automation systems, which typically use small data packets of information to communicate between devices with relatively low data rate requirements. Residential IoT devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other in a home automation scenario. This device-to-device communication approach illustrates many of the interoperability challenges. These devices often have a direct relationship, they usually have built-in security and trust mechanisms, but they also use device-specific data models that require redundant development efforts by device manufacturers [7]. This means that the device manufacturers need to invest in development efforts to implement device-specific data formats rather than open approaches that enable use of standard data formats.

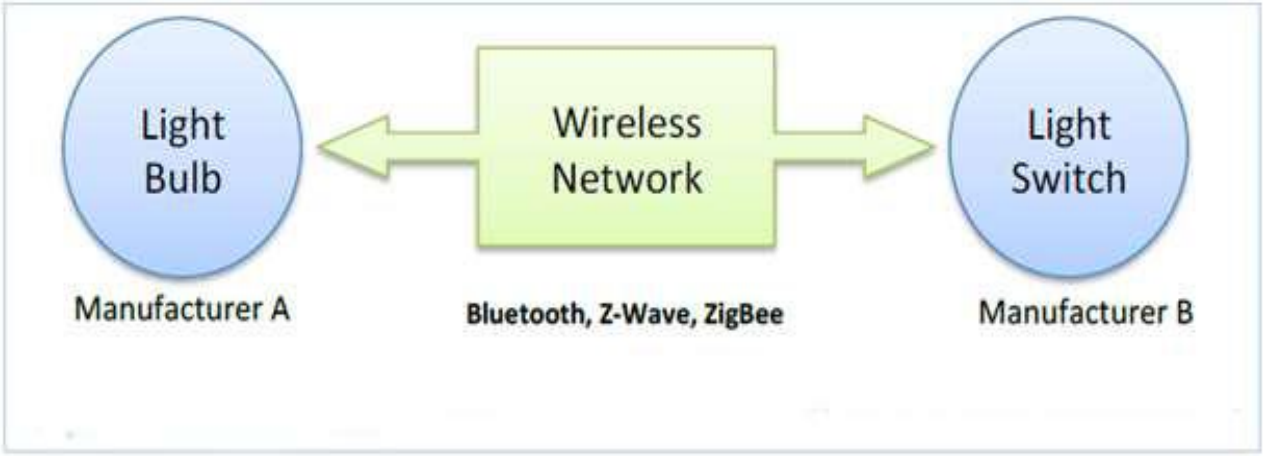

Fig. 1: Device-to-device communications model
Source: https://www.kernelsphere.com/four-internet-things-communications-models/

2.7 Device-to-cloud Networks:

In a device-to-cloud communication model as shown in Fig.2, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service. This communication model is employed by some popular consumer IoT devices like the Nest Labs Learning Thermostat and the Samsung smart-electronic. In the case of the Nest Learning Thermostat, the device transmits data to a cloud database where the data can be used to analyze energy consumption. The device-to-cloud model adds value to the end user by extending the capabilities of the device beyond its native features. However, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. Frequently, the device and cloud service are from the same vendor. If proprietary data protocols are used between the device and the cloud service, the device owner or user may be tied to a specific cloud service, limiting or preventing the use of alternative service providers. This is commonly referred to as "vendor lock-in'', a term that encompasses other facets of the relationship with the provider such as ownership of and access to the data. At the same time, users can generally have confidence that devices designed for the specific platform can be integrated.

Fig. 2: Device-to-cloud communications model
Source: https://www.kernelsphere.com/four-internet-things-communications-models/

2.8 Device-to-gateway Networks:

In the device-to-gateway model, or more typically, the device-to application-layer gateway (ALG) model; the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation. The model is shown in Fig 3. Several forms of this model are found in consumer devices. In many cases, the local gateway device is a smart phone running an app to communicate with a device and relay data to a cloud service. This is often the model employed with popular consumer items like personal fitness trackers. These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on smart phone app software to serve as an intermediary gateway to connect the fitness device to the cloud. The other form of this device-to-gateway model is the emergence of "hub" devices in home automation applications.

These are devices that serve as a local gateway between individual IoT devices and a cloud service, but they can also bridge the interoperability gap between devices themselves. For example, the Smart Things hub is a stand-alone gateway device that has Z-Wave and Zigbee transceivers installed to communicate with both families of devices. It then connects to the Smart Things cloud service, allowing the user to gain access to the devices using a smart phone app and an Internet connection. This communication model is used in situations where the smart objects require interoperability with non-IP (Internet Protocol) devices. Sometimes this approach is taken for integrating IPv6-only devices, which means a gateway is necessary for legacy IPv4-only devices and services. In other words, this communications model is frequently used to integrate new smart devices into a legacy system with devices that are not natively interoperable with them. A downside of this approach is that the necessary development of the application-layer gateway software and system adds complexity and cost to the overall system.

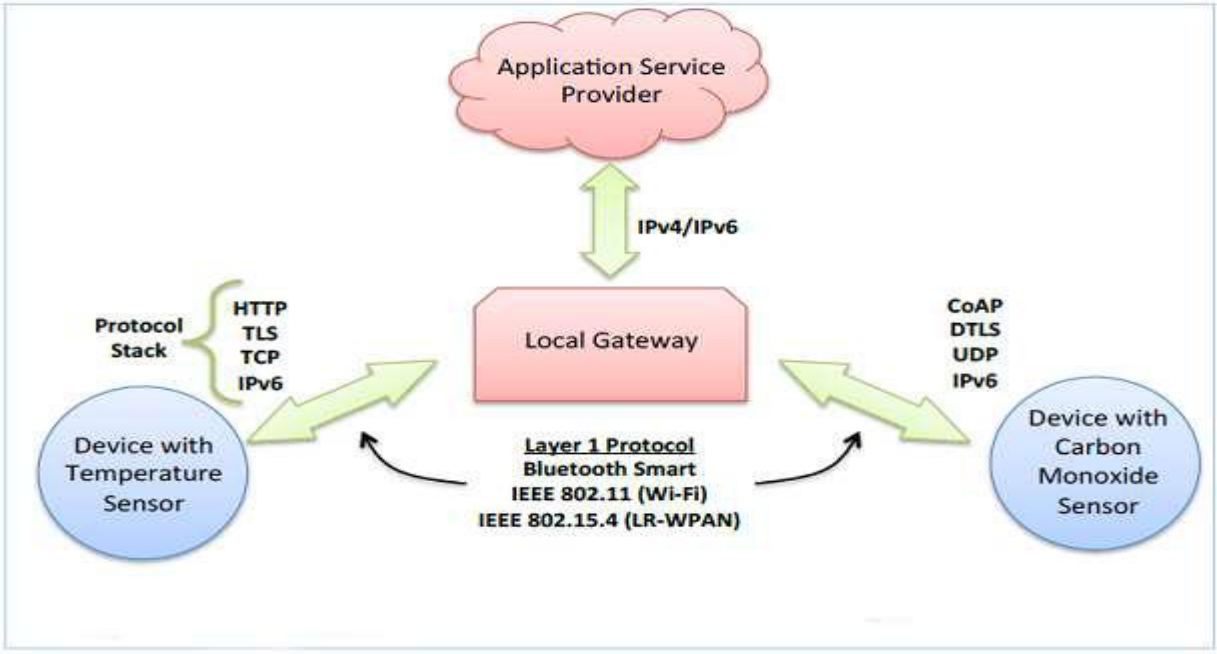

Fig. 3: Device-to-gateway communications model
Source: https://www.kernelsphere.com/four-internet-things-communications-models/

2.9 Back-end data-sharing Networks:

The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. This architecture supports "the user's desire for granting access to the uploaded sensor data to third parties". This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where "IoT devices upload data only to a single application service provider''. A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed as shown in Fig. 4. Effective back-end data-sharing architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers. The back-end data-sharing model suggests a federated cloud services approach or cloud applications programmer interfaces (APIs) are needed to achieve interoperability of smart device data hosted in the cloud. This architecture model is an approach to achieve interoperability among these back-end systems. "Standard protocols can help but are not sufficient to eliminate data silos because common information models are needed between the vendors." In other words, this communication model is only as effective as the underlying IoT system designs. Back-end data sharing architectures cannot fully overcome closed system designs.

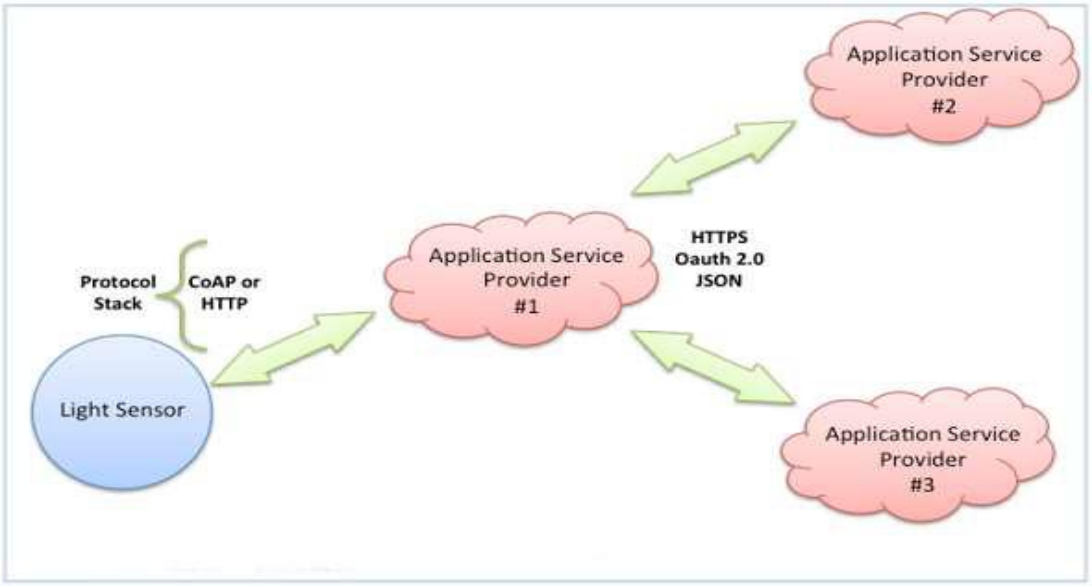

Fig. 4: Back-end data-sharing communications model

Source: https://www.kernelsphere.com/four-internet-things-communications-models/

3. SMART HEALTHCARE SYSTEM FRAMEWORK:

[8] recommend the use of environmental or vision based sensors around the home. However, this restricts the usefulness of the system to one physical location. It would be preferable to implement all essential sensors as small, portable, and externally wearable nodes. This would provide patients with a non-intrusive and comfortable solution that is capable of monitoring their health wherever they go. This would make patients more receptive to using health monitoring technology than they would be if implantable sensors or cameras were required. Additionally, repairing or replacing externally wearable nodes would be simple when compared to implanted sensors or vision-based sensors installed in the home [9].

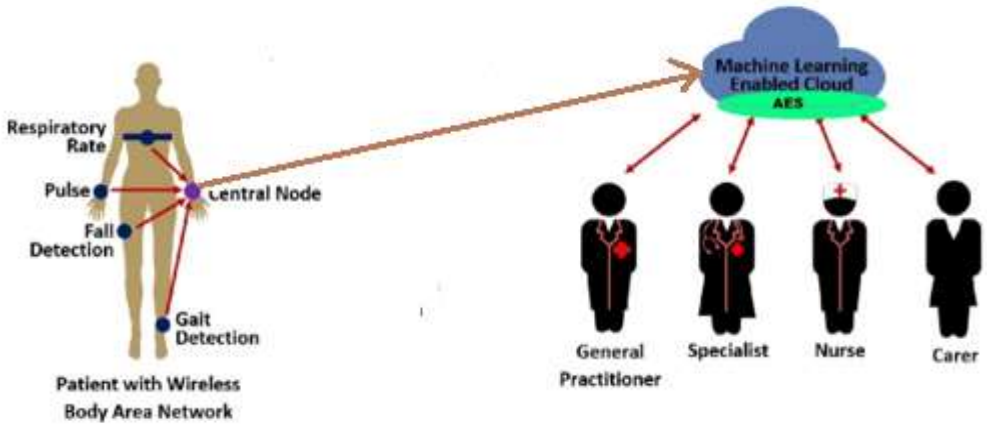

Fig. 3.1: Smart Healthcare System Framework.

Existing models in [10] and [11] recommend short-range communications, such as Bluetooth, for transferring sensor data to a smartphone to be processed. Long-range communications such as LTE can then be used to transfer the processed information from the patient to the healthcare provider, typically a doctor, through SMS or the Internet. The key limitation of this is that smartphone typically have limited battery life, requiring frequent recharging; a patient with a flat battery would be a patient disconnected from healthcare providers. A low-powered node designed specifically for managing healthcare information would be preferable [9].

Previous works by [12] and [13] also propound the use of cloud for storing the high volume of data that will be accumulated and processed over time by the healthcare system. Using the big data that will rapidly form and continue to grow in cloud storage, machine learning algorithms can be implemented in the high-computing environment of the cloud. These algorithms could be designed to search through the large amount of data, identify previously unknown disease trends, and provide diagnostics, treatment plans, and much more as shown in Fig 3.1.

3.1 Sensor and Central Nodes:

These are wearable sensors that measure physiological conditions of the body. The sensors suggested are those that would determine important signs like body temperature, pulse rate, respiratory rate. Blood oxygen and pressure sensors could be added further. The sensor node sends data to the central node for processing which then forward the information to an outside location. A dedicated central node is preferred that would perform only one function in other to reduce the amount of power consumption.

3.2 Communication and Transmission:

The various sensors placed on the body communicate and transmit data to the central node through a short range communication method using low powered Bluetooth or Zigbee. The central node further transmits the aggregate data obtained from the nodes to the cloud through internet connectivity where relevant parties like the practitioners, nurses and specialist can access. When selecting either short or long range communication method, several factors will be considered that include security, robustness and high availability. Other issues relating to effect on human body should be considered as in the case of the short range communication.

3.3 Cloud Storage:

The cloud would be suitable for keeping of patient's biomedical information for a long term basis and at the same time assisting the health professionals with diagnostic information. However, providing accessibility for healthcare professionals without compromising security is a key concern that should be addressed by researchers developing healthcare IoT systems. The cloud storage architectures should be designed to support the implementation of machine learning on big data sets. Machine learning offers the potential to identify trends in medical data that were previously unknown, provide treatment plans and diagnostics, and give recommendations to healthcare professionals that are specific to individual patients [9].

3.4 Advance Encryption Standard (AES):

Patients medical details need to be properly secured so as the prevent intruder from having access to sensitive information of patients which ought to be treated with utmost confidentiality (Fig. 3.1). Most of the previous works on applications of IoT in healthcare delivery did not take into consideration the importance of safeguarding the patients' medical details available on cloud from vulnerabilities. Advanced Encryption Standard (AES), is a symmetric block cipher used to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

4. LIMITATIONS OF SMART HEALTHCARE SYSTEM:

Smart healthcare system is faced with numerous challenges; among which are:

a) Funding: One of the major problems facing smart healthcare system is funding. IoT infrastructures are not easy to acquire; they are costly, thereby making its implementation very difficult. The maintenance of smart healthcare system is also costly.
b) Bureaucracy: Bureaucracy and lack of clear communication channels and collaboration culture are some of the difficulties confronting smart healthcare system. Organizational and cultural changes often are more difficult than technological changes [14].
c) Lack of computer knowledge among health practitioners: Many of the health practitioners have little or no knowledge of computer. This in no small measure has negatively contributed to the backwardness experienced implementing smart healthcare system.
d) Epileptic Power Supply: Epileptic power supply can hinder the success of the remote healthcare delivery project.

e) Security and Privacy: Data insecurity and infringement of privacy through multiple devices and protocols are the major limitations of IoT applications in healthcare delivery. This is a serious issue as vital information about patient which is in the cloud can only be accessible through IoT multiple devices and protocols.

5. CONCLUSION:

Put together in this paper is a primer of smart healthcare system. The paper sequentially introduced the problems confronting healthcare delivery and the need for smart healthcare system; among are communication gap and poor coordination of care among primary care, secondary care, tertiary care, and specialty care providers that lead to major inefficiencies in healthcare delivery. In resource constrained settings, these inefficiencies exacerbate mismatches between the demand and supply for specialist services. The overall sufferers are the patients.

Some of the communication models enabling technologies such as addressability, short-range wireless, medium-range wireless, long-range wireless, and wired technologies that made smart healthcare possible were discussed. Some of the factors mitigating the implementation of smart healthcare system were also pointed out. Because of costly IoT infrastructures, smart healthcare system needs to be funded. Bureaucracy can endanger implementation of smart healthcare system; therefore, good policies must be put in place that gives room for technological change.

For smart healthcare system implementation and deployment to be realized, the awareness of computer appreciation among health practitioners for healthcare delivery must be put in place. There is need for stable power supply in an environment where smart healthcare system is being operated. Finally, data insecurity and infringement of privacy through multiple devices and protocols are issues that must be addressed by manufacturers and users of IoT devices. Vital information about patient is kept in the cloud and can only be accessible through IoT multiple devices and protocols; therefore, these devices and protocols must be guarded against vulnerabilities.

REFERENCES:

1. "Health Topics: Health systems" WHO World Health Organization. Retrieved: 2013-11-24. www.who.int.
2. Hassan, Q.F. Internet of Things A to Z: Technologies and Applications. John Wiley and Sons. pp. 27–8, 2018.
3. Sheng, M.; Qun, Y.; Yao, L. and Benatallah, B. Managing the Web of Things: Linking the Real World to the Web. Morgan Kaufmann. pp. 256–8, 2017.
4. Waldner, Jean-Baptiste. Nano computers and Swarm Intelligence, London: ISTE. pp. 227–231, 2008.
5. Kushalnagar, N.; Montenegro, G. and Schumacher, C. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. IETF, RFC 4919, 2007.
6. Sun, Charles C. "Stop using Internet Protocol Version 4!". Computerworld, 2014.
7. Duffy Marsan, Carolyn. (2015) "IAB Releases Guidelines for Internet-of-Things Developers." Internet Engineering Task Force, IETF Journal 11.1: 6-8.
8. Pasluosta, C. F., Gassner, H., Winkler, J., Klucken, J., and Eskofier, B. M. (2015). An Emerging Era in the Management of Parkinson's disease: Wearable Technologies and the Internet of Things. IEEE J. Biomedical and Health Informatics, 19(6), 1873-1881.
9. Baker, S. B., Xiang, W., and Atkinson, I. (2017). Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. IEEE Access, 5, 26521-26544.
10. Poon, C. C., Lo, B. P., Yuce, M. R., Alomainy, A., and Hao, Y. (2015). Body sensor networks: In the era of big data and beyond. IEEE reviews in biomedical engineering, 8, 4-16.
11. Chang, S., Chiang, R., and Wu, S. (2016). A context-aware, interactive m-health system for diabetics. IT Prof. 18 (3), 14–22.
12. Dimitrov, D. V. (2016). Medical internet of things and big data in healthcare. Healthcare informatics research, 22(3), 156-163.
13. Xu, B., Da Xu, L., Cai, H., Xie, C., Hu, J., and Bu, F. (2014). Ubiquitous data accessing method in IoT based information system for emergency medical services. IEEE Trans. Industrial Informatics, 10(2), 1578-1586.
14. Adewale, O. S. (2004). An Internet-based telemedicine system in Nigeria. International Journal of Information Management, 24(3), 221-234.