# A

# Technical Seminar Report

# On

# **Internet Of Things For Health Care**

Submitted in partial fulfillment for the award of the degree of

# **BACHELOR OF TECHNOLOGY**

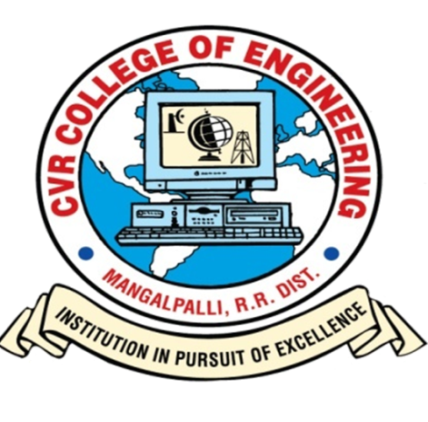
In

# **INFORMATION TECHNOLOGY (2016-17)** Submitted by

**L.Varun (13B81A12B0)**

Under the esteemed guidance of

**Mr. B. Vikranth**

****Associate Professor

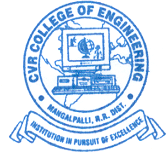
**CVR COLLEGE OF ENGINEERING**

**(UGC Autonomous)**

ACCREDITED BY NBA, AICTE, NAAC with ‘A’ Grade & Affiliated to JNTU-H

Vastunagar, Mangalpalli (V), Ibrahimpatnam(M), R.R District, PIN-501510

**2016-2017**



## CVR College of Engineering

An Autonomous Institution

ACCREDITED BY NATIONAL BOARD OF ACCREDITATION, AICTE

(Approved by A.I.C.T.E. & Govt. of Andhra Pradesh and Affiliated to JNTUniversity)

**Vastunagar,** Mangalpalli (V), Ibrahimpatnam (M), R.R. District, PIN – 501 510

Web: <http://cvr.ac.in>, email: [info@cvr.ac.in](mailto:info@cvr.ac.in)

Phones: Code within A.P.: 958414; Code from Outside: 08414

General: 252222, 252369 Office Telefax: 252396, Principal: 252396 (O)

# **DEPARTMENT OF INFORMATION TECHNOLOGY**

**CERTIFICATE**

This is to certify that the technical seminar report titled **‘Internet Of Things For HealthCare’** that is being submitted by **Mr. L.Varun (13B81A12B0)** in partial fulfillment for the award of the degree of the Bachelor of Technology in Information Technology to the Jawaharlal Nehru Technological University is a record of bona fide work carried out by him under my guidance and supervision. The results in this technical seminar report have not been submitted to any other university or institute for the award of any degree or any diploma.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**INTERNAL GUIDE SEMINAR COORDINATOR**

Mr. B. Vikranth, Dr. R. Seetharamiah,

Associate.Professor. Professor of IT.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**HEAD OF THE DEPARTMENT**

Dr. Bipin Bihari Jayasingh

Professor of IT.

# **ACKNOWLEDGEMENT**

The satisfaction that accompanies the successful completion of any task would be incomplete without the people who made it possible and whose encouragement and guidance has been a source of inspiration throughout the course of the preparation of this technical seminar report on **Internet Of Things for Health Care.**

I feel a great pleasure to express my deep sense of gratitude to all those who have helped me to carry out this report successfully. I express my profound gratitude for their valuable guidance and support.

I owe my sincere gratitude to **Dr. Bipin Bihari Jayasingh**, Head of the Department, IT, for allowing me to give seminar in the college and providing required facilities.

I am thankful to **Dr. R. Seetharamaiah,** Technical Seminar Coordinator, Department of Information Technology, CVR College of Engineering for his supportive guidelines and for having provided the necessary forward this seminar without any obstacles and hindrances.

**L.Varun (13B81A12B0)**

**ABSTRACT**

The Internet of Things (IoT) makes smart objects the ultimate building blocks in the development of cyber-physical smart pervasive frameworks. The IoT has a variety of application domains, including health care. The IoT revolution is redesigning modern health care with promising technological, economic, and social prospects. This report talks about the IoT-based health care technologies and reviews the state-of-the-art network architectures/platforms, applications, and industrial trends in IoT-based health care solutions. In addition, this paper analyzes distinct IoT security and privacy features, including security requirements, threat models, and attack taxonomies from the health care perspective. Further, this paper proposes an intelligent collaborative security model to minimize security risk; discusses how different innovations such as big data, ambient intelligence, and wearables can be leveraged in a health care context; addresses various IoT and eHealth policies and regulations across the world to determine how they can facilitate economies and societies in terms of sustainable development; and provides some avenues for future research on IoT-based health care based on a set of open issues and challenges.

# 

# **TABLE OF CONTENTS**

**Title Page No**

1. **Introduction** 6
2. **IOT Networks** 8
   1. **IOT Topology** 9
3. **IoT Network Architecture** 10
   1. **6LowPAN Protocol Stack** 11
   2. **OSI model v/s 6LowPAN model** 12
4. **IoT HealthCare Services and Applications** 16
5. **IoT HealthCare Security**  18
   1. **A Proposed Security Model** 19
6. **Conclusion** 21
7. **References** 22

# **1.** **INTRODUCTION**

The Internet of Things (IoT) is a concept of a connected set of anyone, anything, anytime, anyplace, any service, and any network. The IoT is a megatrend in next-generation technologies that can impact the whole business spectrum and can be thought of as the interconnection of uniquely identifiable smart objects and devices within today's internet infrastructure with extended benefits. Benefits typically include the advanced connectivity of these devices, systems, and services that goes beyond machine-to- machine (M2M) scenarios [1]. Therefore, introducing automation is conceivable in nearly every field. The IoT provides appropriate solutions for a wide range of applications such as smart cities, traffic congestion, waste management, structural health, security, emergency services, logistics, retails, industrial control, and health care. The interested reader is referred to [1] and[5] for a deeper understanding of the IoT.Medical care and health care represent one of the most attractive application areas for the IoT [6]. The IoT has the potential to give rise to many medical applications such as remote health monitoring, fitness programs, chronic diseases, and elderly care. Compliance with treatment and medication at home and by healthcare providers is another important potential application. Therefore, various medical devices, sensors, and diagnostic and imaging devices can be viewed as smart devices or objects constituting a core part of the IoT. IoT-based healthcare services are expected to reduce costs, increase the quality of life, and enrich the user's experience. From the perspective of healthcare providers, the IoT has the potential to reduce device downtime through remote provision. In addition, the IoT can correctly identify optimum times for replenishing supplies for various devices for their smooth and continuous operation. Further, the IoT provides for the efficient scheduling of limited resources by ensuring their best use and service of more patients. Fig. 1 illustrates recent healthcare trends [7]. Ease of cost-effective interactions through seamless and secure connectivity across individual patients, clinics, and healthcare organizations is an important trend.

This paper examines the trends in IoT-based healthcare research and uncovers various issues that must be addressed to transform healthcare technologies through the IoT innovation. In this regard, this paper contributes by

* Classifying existing IoT-based healthcare network studies into three trends and presenting a summary of each.
* Providing an extensive survey of IoT-based healthcare services and applications.
* Highlighting various industrial efforts to embrace IoT-compatible healthcare products and prototypes. Providing extensive insights into security and privacy issues surrounding IoT healthcare solutions and proposing a security model.
* Discussing core technologies that can reshape healthcare

# 

# **2.** **IOT NETWORKS**

The IoT healthcare network or the IoT network for health care (hereafter ``the IoThNet'') is one of the vital elements of the IoT in health care. It supports access to the IoT backbone, facilitates the transmission and reception of medical data, and enables the use of healthcare-tailored communications. As shown in Fig. 2, this section discusses the IoThNet topology, architecture, and platform. However, it should be mentioned that the proposed architectures in [13] and [14] can be considered as a good starting point for developing insights into the IoT network.

**2.1 THE IoThNet TOPOLOGY**

The IoThNet topology refers to the arrangement of different elements of an IoT healthcare network and indicates representative scenarios of seamless healthcare environments. Fig describes how a heterogeneous computing grid collects enormous amounts of vital signs and sensor data such as blood pressure (BP), body temperature, electrocardiograms (ECG), and oxygen saturation and forms a typical IoThNet topology. It transforms the heterogeneous computing and storage capability of static and mobile electronic devices such as laptops, smartphones, and medical terminals into hybrid computing grids [15]. Fig 1. visualizes a scenario of types of topologies and vitals are captured using portable medical devices and sensors attached to his or her body. Captured data are then analyzed and stored, and stored data from various sensors and machines become useful for aggregation. Based on analyses and aggregation, caregivers can monitor patients from any location and respond accordingly. In addition **.** Remote monitoring in wearables and personalized health care. topology includes a required network structure for supporting the streaming of medical videos. For example, the topology in Fig. supports the streaming of ultrasound videos through an interconnected network with worldwide interoperability for microwave access (WiMAX), an internet protocol (IP) network, and a global system for a mobile (GSM) network as well as usual gateways and access service networks. Similar conceptual structures are found in [16] and [19].

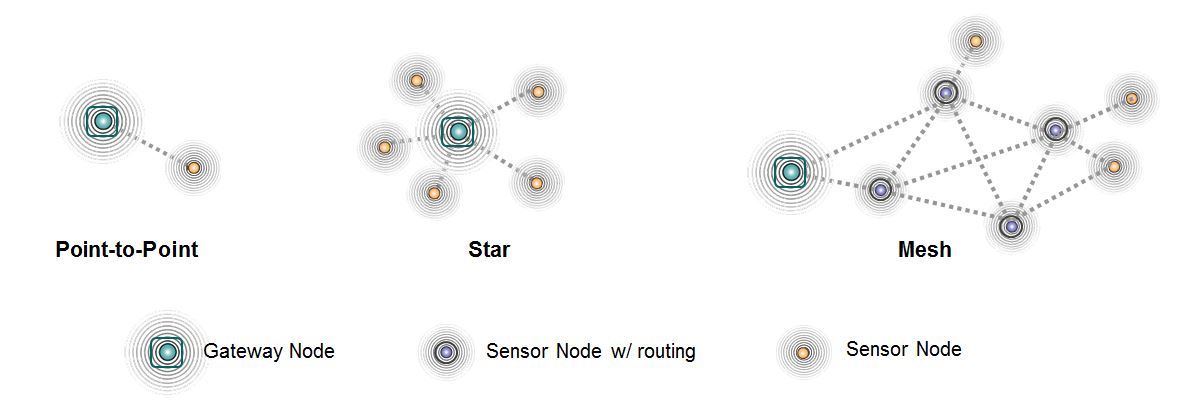


Fig1. IOT Network Topology

The above Fig 1. presents an IoThNet topology showing the role of a gateway. Here intelligent pharmaceutical packaging (iMedPack) is nothing but an IoT device that manages the problem of medicine misuse, thereby ensuring pharmaceutical compliance. The intelligent medicine box (iMedBox) is considered a healthcare gateway with an array of various required sensors and interfaces of multiple wireless standards. Various wearable sensors and IoT devices are wirelessly connected to healthcare gateways connecting the patient's environment to the health-IoT cloud, a heterogeneous network (HetNet) that enables clinical diagnosis and other analyses.

# **3.** **IOT NETWORK ARCHITECTURE**

The IoThNet architecture refers to an outline for the specification of the IoThNet's physical elements, their functional organization, and its working principles and techniques. To start, the basic reference architecture in Fig. 2 is presented for the telehealth and ambient assisted living systems recommended by Continua Health Alliance. The key issues have been identified for this architecture [25]: the interoperability of the IoT gateway and the wireless local area network (WLAN)/wireless personal area network (WPAN), multimedia streaming, and secure communications between IoT gateways and caregivers. Many studies [18], [21], [23], [26] and [30] have justified that the IPv6-based 6LoWPAN is the basis of the IoThNet.**.**

As designed in [30], Fig. 2 shows the layer structure of the 6LoWLAN. According to the IoThNet concept, sensors and wearables use IPv6 and 6LoWPAN systems for data transmission over the 802.15.4 protocol. Data are then replied back by sensor nodes with the help of the user datagram protocol (UDP). However, the 6LoWPAN is limited in that it does not support mobile IPv6 (MIPv6), a subset of the IPv6 protocol with mobility. To introduce mobility provision to the 6LoWPAN, a protocol for exchanging messages

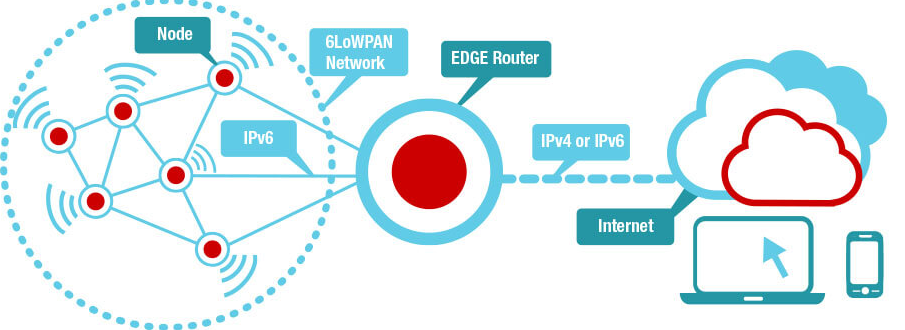
****

Fig 2. IOT network architecture

between mobile patient nodes, base networks, and visited networks is proposed in [26].To address mobility, four alternative procedures are considered in [29], including soliciting routers, waiting for a new directed acyclic graph (DAG) information object (DIO), attaching to other available parent nodes, and sending DAG information solicitation (DIS) messages. Among these,

soliciting routers and sending DIS messages represent the fastest methods because they are initiated by the mobile node itself. A typical gateway protocol stack for community medical services is described in [30]. This stack explicitly describes how periodic traffic, abnormal traffic, and query driven traffic can be managed within the HetNet. A complex eHealth service delivery method consisting of three phases has been proposed in [30], including composition, signalization, and data transmission. Signalization protocols serve mainly as the basis of complex service composition, quality-of-service (QoS) negotiation, and resource allocation procedures in the IoThNet and the state encountered in the QoS negotiation procedure, which is nothing but the creation of a connection to expected QoS values.

**3.1 6LoWPAN PROTOCOL STACK**

**6LoWPAN** is an acronym of  *Ipv6 over Low power Wireless Personal Area Networks* 6LoWPAN is the name of a concluded working group in the Internet area of the IETF.

The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices, and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things.

The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks as mentioned in Fig 3. IPv4 and IPv6 are the work horses for data delivery for local-area networks, metropolitan area networks, and wide-area networks such as the Internet. Likewise, IEEE 802.15.4 devices provide sensing communication-ability in the wireless domain. The inherent natures of the two networks though, are different.

The target for IP networking for low-power radio communication is applications that need wireless internet connectivity at lower data rates for devices with very limited form factor. An example is automation and entertainment applications in home, office and factory environments. The header compression mechanisms standardized in RFC6282 can be used to provide header compression of IPv6 packets over such networks.

IPv6 is also in use on the smart grid enabling smart meters and other devices to build a micro mesh network before sending the data back to the billing system using the IPv6 backbone. Some of these networks run over IEEE 802.15.4 radios, and therefore use the header compression and fragmentation as specified by RFC6282.

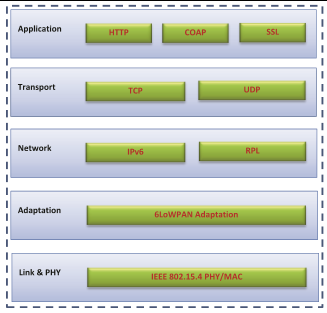
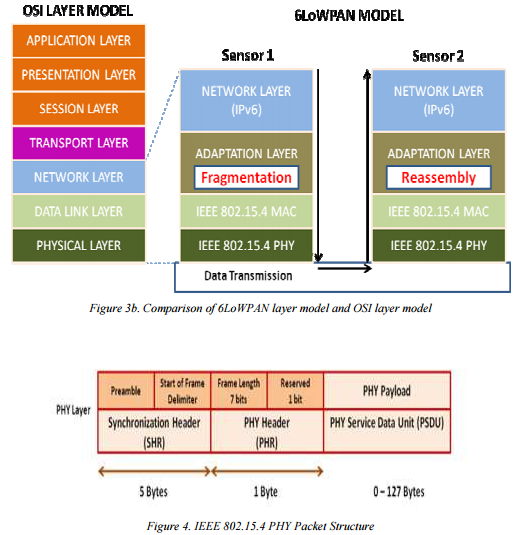
****

Fig 3. 6LoWPAN Protocol Stack

**3.2 OSI model v/s 6LowPAN model**

6LoWPAN radically changes the IoT landscape. As discussed, up until now a complex application layer gateway was needed to make devices such as ZigBee, Bluetooth and proprietary systems connect to the Internet. 6LoWPAN solves this dilemma by introducing an adaptation layer between the IP stack’s link and network layers to enable transmission of IPv6 datagrams over IEEE 802.15.4 radio links. All communications systems use a set of rules or standards to format data and control the exchange. The most common model in data communication systems is the Open Systems Interconnect (OSI) model, which in a simplified model, breaks the communication into five fundamental layers. Fig 3 shows this simplified OSI model alongside two typical examples of stacks used in IoT devices. One is a device running the Wi-Fi stack, the other device is an IoT-connected device based on 6LoWPAN.



The physical layer converts data bits into signals that are transmitted and received over the air. In the 6LoWPAN example, IEEE 802.15.4 is used. In addition to the well-rounded 2006 version of the standard, two important amendments exist: e and g. IEEE 802.15.4e is a MAC amendment and provides enhancements such as time slotted channel hopping (TSCH) and coordinated sampled listening (CSL). Both enhancements aim to further lower the power consumption and make the interface more robust. The IEEE 802.15.4g is a PHY (or physical layer) amendment and aims to provide an additional range of radio frequency bands to enable worldwide use even in the Sub-1 GHz frequency bands. The data link layer provides a reliable link between two directly connected nodes by detecting and correcting errors that may occur in the physical layer during transmission and receiving. The data link layer includes the media access layer (MAC) which provides access to the media, using features like carrier sense multiple access – collision avoidance (CSMA-CA) where the radio listens that no one else is transmitting before actually sending data over the air. This layer also handles data framing. In the 6LoWPAN example, the MAC layer is IEEE 802.15.4. The 6LoWPAN adaptation layer, providing adaptation from IPv6 to IEEE 802.15.4, also resides in the link layer as mentioned in the Fig 4.

The network layer addresses and routes data through the network, if needed over several hops. IP (or Internet Protocol) is the networking protocol used to provide all devices with an IP address to transport packets from one device to another.

The transport layer generates communication sessions between applications running on end devices. The transport layer allows multiple applications on each device to have their own communications channel. TCP is the dominant transport protocol on the Internet. However, TCP is a connection-based protocol (including packet ordering) with large overhead and therefore not always suitable for devices demanding ultra-low power consumption. For those types of systems, UDP, a lower overhead, connectionless protocol, can be a better option. Secure transport layers examples include TLS (transport layer security) running atop TCP and DTLS, which is based on UDP. Finally, the application layer is responsible for data formatting. It also makes sure that data is transported in application-optimal schemes. A broadly used application layer on the Internet is HTTP running over TCP. HTTP uses XML, which is a text-based language with a large overhead. Therefore, it is not optimal to use HTTP in many 6LoWPAN systems. However, HTTP can still be very useful for communications between 6LoWPAN and the Internet. For this reason, the industry and community have developed alternative application layer protocols, such as the constrained application protocol (COAP), a message protocol running over UDP with a bit-optimized REST mechanism very similar to HTTP. COAP is defined by IETF in RFC 7252 and defines retransmissions, confirmable and non-confirmable messages, support for sleepy devices, block transfers, subscription support and resource discovery. COAP is also easy to map to HTTP via proxies. Another application layer protocol that should be mentioned is message queue telemetry transport (MQTT), an open-source protocol that was invented by IBM. MQTT is a publish/subscribe type of protocol running over TCP. Data is not transported directly between end points. Instead a broker (i.e., server) is used to relay messages. MQTT introduces the “topic” entity; devices can publish and subscribe to different topics. Once a topic is updated that a specific device has subscribed to, the device will get notified and receive the data via the broker. Devices can use wildcards like # and \* to subscribe to a hierarchy of topics. MQTT supports several layers of quality of service (QoS) making sure that messages are delivered. The broker can run both locally in an IP intranet and on the Internet and multiple brokers are supported interacting in the same system. Several public brokers are available and many of the cloud service providers provide MQTT access. There are many more application layer protocols available that can run over the TCP/ UDP. Those listed here specifically target low-power IoT applications.

# 

**4. IOT Healthcare Services and Applications**

The IoT is anticipated to enable a variety of healthcare services in which each service provides a set of healthcare solutions. In the context of healthcare, there is no standard definition of IoT services. However, there may be some cases in which a service cannot be objectively differentiated from a particular solution or application. As mentioned in Fig 5 This paper proposes that a service is by some means generic in nature and has the potential to be a building block for a set of solutions or applications. In addition, it should be noted that general services and protocols required for IoT frameworks may require slight modifications for their proper functioning in healthcare scenarios. These include notification services, resource sharing services, internet services, cross-connectivity protocols for heterogeneous devices, and link protocols for major connectivity. The easy, fast, secure, and low-power discovery of devices and services can be added to this list. However, a discussion on such generalized IoT services is beyond the scope of this survey. The interested reader is referred to the literature for a more comprehensive understanding of this topic. The following subsections include various types of IoT healthcare services.

As mentioned in Fig 5 , In addition to IoT services, IoT applications deserve closer attention. It can be noted that services are used to develop applications, whereas applications are directly used by users and patients. Therefore, services are developer-centric, whereas applications, user-centric. In addition to applications covered in this section, various gadgets, wearables, and other healthcare devices currently available in the market are discussed. These products can be viewed as IoT innovations that can lead to various healthcare solutions. The next subsections address various IoT-based healthcare applications, including both single- and clustered-condition applications.

However, many challenges remain, including computational complexity, power consumption, and noisy environments around smartphones, which should be easy to solve. In addition, there are many health and fitness accessories suitable for smartphones that can help individuals achieve their best shape. For example, Fitbit Flex, a fitness tracking wristband, keeps track of steps taken, the distance travelled, and calories burned. A separate section of this paper provides a more detailed discussion on existing commercial healthcare products that can be viewed as a foundation of IoT healthcare devices.

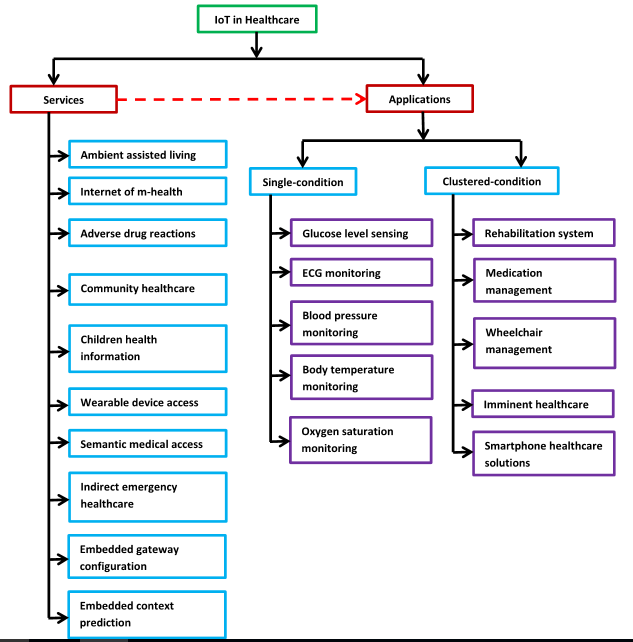


Fig 5 IOT in Healthcare applications and Services.

**5. IOT HealthCare Security**

The IoT is growing rapidly. In the next several years, the medical sector is expected to witness the widespread adoption of the IoT and flourish through new eHealth IoT devices and applications. Healthcare devices and applications are expected to deal with vital private information such as personal healthcare data. In addition, such smart devices may be connected to global information networks for their access anytime, anywhere. Therefore, the IoT healthcare

domain may be a target of attackers. To facilitate the full adoption of the IoT in the healthcare domain, it is critical to identify and analyze distinct features of IoT security and privacy, including security requirements, vulnerabilities, threat models, and countermeasures, from the healthcare perspective .

In IoT the smart devices may be connected to global information networks for their access anytime, anywhere. Therefore, the IoT healthcare domain may be a target of attackers.

Therefore in order to achieve secure services, there is a need to focus on the following security requirements:

* Confidentiality: confidentiality ensure the inaccessibility of medical information for unauthorized users.
* Integrity: Integrity ensures the received medical data are not altered during transmitting of data.
* Authentication: It enables an IoT health device to ensure the identity of the peer with which it is communicating.
* Availability: It ensures the survivability of IoT healthcare services (either local or global/cloud services ) to authorized parties when needed even under denial of service attacks.
* Data freshness: It ensures that each message or data sent is fresh. Data freshness basically implies that each data is recent and ensures that no adversary replays old messages.
* Non-Repudiation: Non-repudiation indicates that a node cannot deny sending a message sent earlier.
* Fault Tolerance: A security scheme where respective service should continue even in the presence of a fault (eg. A software glitch, a device compromise, and a device failure)

**5.1 A PROPOSED SECURITY MODEL**

IoT medical paradigms are not yet robust but continue to develop. Therefore, it is difficult to identify and predict all possible vulnerabilities, threats, and attacks associated with the IoT medical domain. Nonetheless, when security specialists work to and tentative security solutions for apparent and predictable problems, such security schemes should have the capability to mitigate unseen or unpredictable issues that have yet to emerge. The Fig 6 describes how to achieve this security goal, security services should be designed with dynamic properties. That is, they should have the ability to reach decisions on unnoticed problems based on experience and knowledge. Consider a scenario in which a security scheme includes services that can detect and evade two types of attacks on message integrity. However, now suppose that, with the expansion of health devices, networks, and applications, an attacker initiates a new type of attack that also threatens medical information integrity. In this case, existing security services are expected to be capable of at least identifying this new type of attack by using dynamic algorithms or those based on artificial intelligence. To address this issue, this paper proposes a security model for IoT-based healthcare services. This intelligent security model is collaborative in nature and uses the most recent knowledge base. Fig. 6 presents the collaboration scheme for the following three security services: Protection services are designed to reduce attacks. Detection services receive activity data from healthcare applications, devices, and networks and are analyzed.

To achieve a security goal, security services should be designed with dynamic properties. i.e, they should have the ability to reach decisions on unnoticed problems based on experience and knowledge.

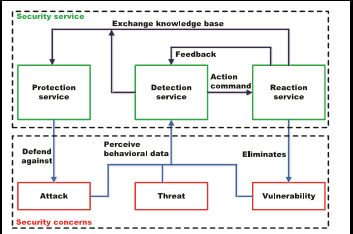


Fig 6 . IOT HealthCare Security Model.

The above figure presents the collaboration scheme for the following three security services:

* Protection services are designed to reduce attacks.
* Detection services receive activity data from health-care applications, devices, and networks and analyze captured eventually detecting any anomaly.
* With aid of defense mechanisms, reaction services help health entities survive all attacks

1. **Conclusion**

Researchers across the world have started to explore various technological solutions to enhance healthcare provision in a manner that complements existing services by mobilizing the potential of the IoT. This document describes diverse aspects of IoT-based healthcare technologies and presents various healthcare network architectures and platforms that support access to the IoT backbone and facilitate medical data transmission and reception. Substantial R&D efforts have been made in IoT-driven healthcare services and applications. In addition, the paper provides detailed research activities concerning how the IoT can address pediatric and elderly care, chronic disease supervision, private health, and fitness management. For deeper insights into industry trends and enabling technologies, the paper offers a broad view on how recent and ongoing advances in sensors, devices, internet applications, and other technologies have motivated affordable healthcare gadgets and connected health services to limitlessly expand the potential of IoT-based healthcare services for further developments.

1. **REFERENCES**

[1] J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, *From Machine-to-Machine to the Internet of Things: Introduction* *to a New Age of Intelligence*. Amsterdam, The Netherlands: Elsevier, 2014.

[2] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, “Smart objects as building blocks for the Internet of Things,'' *IEEE Internet Comput.*, vol. 14, no. 1, pp. 44\_51, Jan./Feb. 2010.

[3] K. Romer, B. Ostermaier, F. Mattern, M. Fahrmair, and W. Kellerer, ``Real-time search for real-world entities: A survey,'' *Proc. IEEE*, vol. 98, no. 11, pp. 1887\_1902, Nov. 2010.

[4] D. Guinard, V. Trifa, and E. Wilde, ``A resource oriented architecture for the Web of Things,'' in *Proc. Internet Things (IOT)*, Nov./Dec. 2010, pp. 1\_8.

[5] L. Tan and N. Wang, ``Future Internet: The Internet of Things,'' in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5. Aug. 2010,pp. V5-376\_V5-380.

[6] Z. Pang, ``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, Jan. 2013.

[7] K. Vasanth and J. Sbert. Creating solutions for health through technology innovation. Texas Instruments. [Online]. Available: http://www.ti.com/lit/wp/sszy006/sszy006.pdf, accessed Dec. 7, 2014.

[8] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, ``Wireless sensor networks for healthcare,'' *Proc. IEEE*, vol. 98, no. 11, pp. 1947\_1960, Nov. 2010.

[9] H. Alemdar and C. Ersoy, ``Wireless sensor networks for healthcare: A survey,'' *Comput. Netw.*, vol. 54, no. 15, pp. 2688\_2710, Oct. 2010.

[10] L. Mainetti, L. Patrono, and A. Vilei, ``Evolution of wireless sensor networks towards the Internet of Things: A survey,'' in *Proc. 19th* *Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2011, pp. 1\_6.

[11] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, ``Wireless sensor networks and the Internet of Things: Selected challenges,'' in *Proc.* *8th GI/ITG KuVS Fachgespräch `Drahtlose Sensornetze'*, Aug. 2009, pp. 31\_34.

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

[13] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, ``IOT gateway: Bridging wireless sensor networks into Internet of Things,'' in *Proc. IEEE/IFIP* *8th Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Dec. 2010, pp. 347\_352.

[14] I. Gronbaek, ``Architecture for the Internet of Things (IoT): API and interconnect,'' in *Proc. Int. Conf. Sensor Technol. Appl.*, Aug. 2008, pp. 802\_807.

[15] H. Viswanathan, E. K. Lee, and D. Pompili, ``Mobile grid computing for data- and patient-centric ubiquitous healthcare,'' in *Proc. 1st IEEE* *Workshop Enabling Technol. Smartphone Internet Things (ETSIoT)*, Jun. 2012, pp. 36\_41.

[16] W. Zhao,W. Chaowei, and Y. Nakahira, ``Medical application on Internet of Things,'' in *Proc. IET Int. Conf. Commun. Technol. Appl. (ICCTA)*, Oct. 2011, pp. 660\_665.

[17] N. Yang, X. Zhao, and H. Zhang, ``A non-contact health monitoring model based on the Internet of Things,'' in *Proc. 8th Int. Conf. Natural* *Comput. (ICNC)*, May 2012, pp. 506\_510.

[18] S. Imadali, A. Karanasiou, A. Petrescu, I. Sifniadis, V. Veque, and P. Angelidis, ``eHealth service support in IPv6 vehicular networks,'' in *Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw.* *Commun. (WiMob)*, Oct. 2012, pp. 579\_585.

[19] R. S. H. Istepanian, ``The potential of Internet of Things (IoT) for assisted living applications,'' in *Proc. IET Seminar Assist. Living*, Apr. 2011, pp. 1\_40.

[20] G. Yang *et al.*, ``A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box,'' *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2180\_2191, Nov. 2014.

[21] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, ``Knowledge acquisition and management architecture for mobile and personal health environments based on the Internet of Things,'' in *Proc. IEEE Int.* *Conf. Trust, Security Privacy Comput. Commun. (TrustCom)*, Jun. 2012,

pp. 1811\_1818.

[22] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, ``Ubiquitous data accessing method in IoT-based information system for emergency medical services,'' *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1578\_1586, May 2014.

[23] C. Doukas and I. Maglogiannis, ``Bringing IoT and cloud computing towards pervasive healthcare,'' in *Proc. Int. Conf. Innov. Mobile Internet* *Services Ubiquitous Comput. (IMIS)*, Jul. 2012, pp. 922\_926.

[24] G. Zhang, C. Li, Y. Zhang, C. Xing, and J. Yang, ``SemanMedical: A kind of semantic medical monitoring system model based on the IoT sensors,'' in *Proc. IEEE Int. Conf. eHealth Netw., Appl. Services (Healthcom)*, Oct. 2012, pp. 238\_243.

[25] X. M. Zhang and N. Zhang, ``An open, secure and \_exible platform based on Internet of Things and cloud computing for ambient aiding living and telemedicine,'' in *Proc. Int. Conf. Comput. Manage. (CAMAN)*, May 2011, pp. 1\_4.

[26] M. S. Shahamabadi, B. B. M. Ali, P. Varahram, and A. J. Jara, ``A network mobility solution based on 6LoWPAN hospital wireless sensor network (NEMO-HWSN),'' in *Proc. 7th Int. Conf. Innov. Mobile Internet Services* *Ubiquitous Comput. (IMIS)*, Jul. 2013, pp. 433\_438.

[27] A. J. Jara, A. F. Alcolea, M. A. Zamora, A. F. J. Skarmeta, and M. Alsaedy, ``Drugs interaction checker based on IoT,'' in *Proc. Internet Things (IOT)*, Nov./Dec. 2010, pp. 1\_8.

[28] R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, ``The potential of Internet of m-health Things `m-IoT' for non-invasive glucose level sensing,'' in *Proc. IEEE Annu. Int. Conf. Eng. Med. Biol. Soc. (EMBC)*, Aug./Sep. 2011, pp. 5264\_5266.

[29] N. Bui, N. Bressan, and M. Zorzi, ``Interconnection of body area networks to a communications infrastructure: An architectural study,'' in *Proc. 18th Eur. Wireless Conf. Eur. Wireless*, Apr. 2012,

[30] P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, ``Survey of Internet of Things technologies for clinical environments,'' in *Proc. 27th Int. Conf.* *Adv. Inf. Netw. Appl. Workshops (WAINA)*, Mar. 2013, pp. 1349\_1354.