ISSN No:-2456-2165

# A Proposed Healthcare Architecture using Cloud Computing in WSN Environment with a Case Study

[1.] Bello Mohammed Suleiman
Department of Cyber Security
Nigerian Army University Biu (Naub)
Borno, Nigeria

[2.] Mohammed Aliyu Mahmud
Department of Computer Science
Modibbo Adama University (MAUTech)
Yola, Nigeria

[3.] Kasimu Samaila Ahmad
Department of information system
Nigerian Army University Biu (Naub)
Borno, Nigeria

**Abstract:- Internet of Things (IoT) considers a future that can connect something/someone/ any service with appropriate information communication technology that it brings innovation in the fields of home, smart home, medical system, article surveillance, and logistics. Because of this inclination, this paper develops a trailblazer: Internet of Things-aware, intelligent architecture, that can be used to monitor and track patients and other related computing devices personnel, and within hospitals premises. In line with the IoT vision, we propose IoT based healthcare architecture dependent on different but complementary technologies, especially the WSN, RFID, and smart mobile, all interacting via a Constrained Application Protocol (CoAP) over low-power wireless personal area network (6LoWPAN) framework. The framework possesses the capability to gather data instantaneously in natural status and in physical conditions of patients after which it gets processed for analysis, thereby providing services to the user. The proposed model also focuses on the security aspect in the network of the healthcare system. The security model proposes IoT based medical services which comprises three security services: protection, detection and reaction services which help to detect and analyze the network. Finally, we suggested a use case scenario to refine the application framework.**

***Keywords:-*** *Internet of Things, Wireless Sensor Network, Healthcare system, Security.*

## I. INTRODUCTION

Wireless Sensor Network (WSN) technology possesses the capability to develop and transform the way of life in various fields such as entertainment, industry, retail, travel, healthcare, employee care, and emergency management. Wireless Sensor Networks, artificial intelligence research, and pervasive computing, have built multifaceted concepts of environmental intelligence to subdue the difficulties which we come across in our daily lives [1]. Notably, one of the world's biggest issues over the past few decades was the ever-increasing population of the elderly in advanced nations countries. The population reference station [2] predicts the population of more than 65 years of advanced nations could reach close to 20% of the total population in the next 20 years. Therefore, the necessity to provide quality care to the aging population quickly and reduce medical expenses is of much importance. A reassuring use in the field is the incorporation of detection and end user electronics technology that allow for people to be monitored continuously [3].

The medical Internet of Things is a difficult area because of diverse and possibly bound network traffic patterns and network devices. A feature of electronic medicine is the ability to compress information temporally and remote access to images, and to quickly share information in geographical areas. Cost-effective communication is facilitated through secure connections between patients, hospitals, and medical institutions. Medical care networks using cordless technology such as Wi-Fi, are presumed to assist analysis and live monitoring.

Many experiments are taking place worldwide, starting from the possibilities of IoT-based medical technology. The results obtained are promising in different areas ranging services, to and prototypes, and applications. It also includes network framework and platform, interoperability and security. Wireless Sensor Network (WSN) is being studied as an initial IoT-based medical technology. An IP-based sensor network using IPv6-based low-power wireless personal area network (6LoWPAN) is adopted [4]. Heterogeneous computing grid collects important medical parameters such as Blood Pressure (BP), body temperature, electrocardiogram (ECG), oxygen saturation [5]. The IoT network is formed on the hybrid computing grid while converting heterogeneous computing and storage functions of static and mobile electronic devices such as medical terminals.

The coalition of Internet of Things (IoT), sensor technology and Cloud Computing is aimed at addressing resource limitations as it allows various networks to cover large topographical areas so that they can be linked and used by many users at the same time when required [6]. additionally, the recent surfacing of Cloud Computing and sensor awareness of infrastructure-architecture methods, service-oriented architecture, software delivery and development models [7] are also providing factors to a smart environment. In order to supply timely healthcare informatics, hospitals need some monitoring framework to follow objects and medical devices

in which security, efficiency, and safety are ensured, with reduced job-related risks.

Research work related to cloud computing will have a direct effect on a various issue in existing technologies. Based on the challenges and issues in the healthcare system, we proposed an IoT based method architecture using cloud computing in WSN environment. It amid to provide scalability, availability a global access disaster recovery facility that help for betterment of healthcare system.

The remainder of this paper is comprised of the following: in Chapter 2, related research work of healthcare system is discussed; Chapter 3 discusses proposed architecture healthcare system; in Chapter 4, we discuss use case scenario based on the proposed system. Finally, we conclude our research work in Chapter 5.

## II. RELATED WORK

The IoT-based medical system is utilized in various areas including areas dealing with the young and the old care patients to expand their insight of a broad spectrum of topics.

### *A. WSN in healthcare and cloud computing*

Due to technological advances in poor network systems and medical sensors, medical care has seen some development in recent years—take for instance the advent of Wireless Sensor Networks (WSN). These WSNs is renowned for realizing promises to greatly strengthen and expand the quality of care in a various fields and different parts of the population. An example: early system prototypes of the WSNs observed to show the possibility of early detection of clinical deterioration through hospital real-time patient monitoring [8] [9]. In cases of massive disasters by automatic electronic triage, first aid enables massive (on-the-spot) investigation of human decorum and perennial diseases [11] to improve the quality of life for the old [12].

The application of medical sensing in medicine and public health has a long-standing history [13]. Sensors incorporated in various medical devices for use in clinics, hospitals, and homes, are used on patients and their healthcare regarding physiological and physical health conditions monitoring. This is important for disease detection, diagnosis, treatment and management. Contemporary medicine is cost-effective, but always almost impossible without sensors such as thermometers, blood pressure monitors, glucose monitors, EKG, EEG, PPG, and various forms of imaging sensors.

Medical sensors combine transducers to detect other signals of electrical, thermal, optical, chemical, and physiological origin with signal processing algorithms to calculate features indicative of human health status. Sensors ahead of those that directly measure health status are also used in medicine practice [14]. For instance, it can be used for negative environmental factors such as improved patient care and workflow efficiency at hospitals, tracking the spread of diseases by public health agencies [16], monitoring people's health-related behaviors (e.g. activity level) Exposure is included.

### *B. IoT privacy and security issues in healthcare*

System Security is among the extremely significant elements of any system. There is a difference in perspectives on security with regards to people, hence defined in so many ways. Generally, security is a notion much the same to the safeness of the entire system.

Concerns about privacy and security have been investigated by several authors. Usually, focuses on security problems of common wireless sensor networks. However, the general problem of application scenarios from a medical care standpoint has thus far not been dealt with thoroughly [17]. Many authors suggest this problem is important. The authors of [18] deliberated a number of the problems for private health observations. It is discovered that majority of the publicized studies handles security problems in (sensor) network applications. This includes authors' works such as [19]. The security problem is a huge issue brought up by quite a number of the authors. Privacy issues and distinct societal impacts have not been thoroughly discussed here [20].

### *C. Cloud Computing for Healthcare Applications*

By using cloud computing, it provides users with various benefits, including reducing the waste of both information system resources and electricity, increasing the efficiency and availability of data centers, and reducing operational costs. Healthcare applications based on cloud computing utilize cloud computing environments and offer the following benefits for patients and caregivers [21].

Patient privacy and security: Cloud service provider expertise provided highly confidential medical data and increased security (Private Cloud) to avoid process leakage.

Dynamic Sensor Data (DSD) Rate: The cloud structure is very much adaptable, hence enabling a range of equivocal data flow gathering.

Global Access and Availability: The cloud deployment model provides globalized access to the system’s reliability, disaster recovery, and redundancy: a superfluous cloud architecture ensures data security and process reliability.

Scalability: Dynamic data flow resources are guaranteed in real time at any time by the elasticity of the cloud.

The most important advantage of cloud computing is that cost and time are significantly reduced compared to traditional methods. For example, large enterprises use server farms; clouds provide economies of scale and service providers be also responsible, eliminating the need to keep user information secure. Cloud computing systems provide accessibility for running programs on many connected computers and can access organizational data from anywhere, anytime, through a variety of devices including mobile phones. Cloud computing oversees the continuity of service-critical services within an organization. The main disadvantage of cloud computing is that it is essential for users to have personal backup facilities/servers just in case, to protect their data because information can be lost due to a connection failure or power outage [22].

ISSN No:-2456-2165

*D. IoT Healthcare security*

IoT is growing rapidly. In the coming years, medical departments are expected to witness the spread of IoT and to boost new e - Health IoT devices and applications. Medical devices and applications are expected to process important personal data, e.g., personal medical data. Additionally, such smart devices can connect to the global information network for access at all times regardless of their location. Therefore, IoT's medical domain can be the target of an attacker. As shown in Figure 1, and from the viewpoint of medical needs, to promote the complete introduction of IoT in the medical field, it goes without saying that it is crucial to recognize and scrutinize individual functions of IoT privacy and security. In addition to that, security regulations, weaknesses, risk assessments, and incidence response should also be identified.

Security violation in sensor network medical applications is a major concern. Because the sensor network healthcare application is about the same with the WSN application interface, many security problems are likewise comparable. Security problems can be split into two major classes: system security and information security. Many researchers have distinguished threats and attacks into two most distinct classes: passive and active. Passive attacks may arise when forwarding data packets in the system. Attackers may influence the route of packets or their final cause. An attacker can hack and steal health data by spying on a wireless communication medium. In terms of adverse effects, active threats are more destructive when compared with inactive equivalents. A criminal can find the location of the user by eavesdropping. This can lead to life threatening situations.

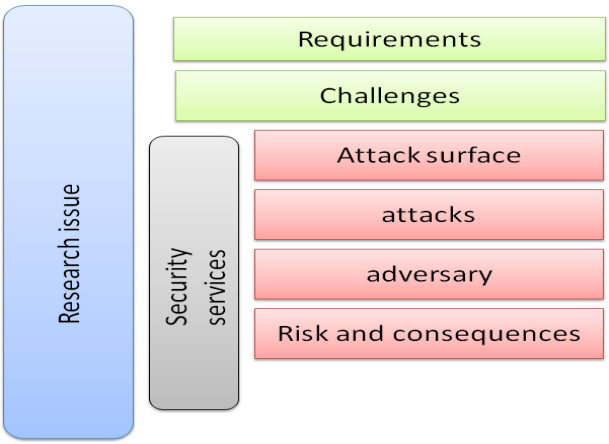


Fig 1. Security issues and challenges in healthcare

*E. Existing researches*

A. Janaki and Dr. G. Shanmugasundaram surveyed cloud-based health monitoring system for hospital management [23]. The authors surveyed all medical institutions that show that cloud computing assistance is necessary to store PHI in patients and use cloud-based virtual servers to obtain emergency help. The cloud here, represents a virtual server and stores patient' data on another server, say, a third-party sever. This server poses a serious threat to security and privacy. The Healthcare Center includes a variety of approaches that are applied to monitor medical information adapted from cloud environments. The paper discussed the healthcare monitoring systems in respect to various methods and categories of Cloud Computing techniques currently used in hospitals. Furthermore, authors discussed the merits and demerits of the healthcare monitoring system approaches.

The fusion of promising possibilities of cloud computing with technologies such as wireless networking, sensor technology, etc. will enable the creation and provison of newer varieties of cloud services. Pankaj Deep Kaur and Inderveer Chana advocated the use of cloud computing for creating and managing cloud-based medical services. As a typical case study, the authors design a Cloud-Based Intelligent Healthcare Service (CBIHCS) that monitors user's health data in real time for the diagnosis of chronic diseases such as heart diseases. The enhanced body sensor component collects distinct user health data and store it in a cloud-based storage repository for further analysis and classification. Furthermore, an infrastructure level mechanism for providing dynamic resource elasticity of CBIHCS has been proposed [24].

Spatially dispersed sensor hubs may be utilized to observe information systems, human situations, etc., in an extensive variety of use ranges. The system of body sensors in the group of individuals produces a ton of setting information. This context data demands a flexible strategy for storing and handling. One of the elements of cloud computing is that it provides a formidable and extensible storage and handling infrastructure that can carry out analog and digital assessments, and burrowing mass sensor data streams. Authors introduced a cloud computing-based system architecture called the Body-Cloud, in view of distributed computing for overseeing and observing the body sensor data stream. It fuses key ideas, for example, asset versatility and adaptability, heterogeneity of sensors, dynamic organization and administration of clients and group applications [25].

Farrukh Aslam Khan et al. proposed a highly secure cloud-based mobile healthcare framework using Wireless Body Area Network (WBAN) [26]. The exploration exhibited here has two perspectives. To start with, we endeavor to secure correspondence between sensors utilizing various biometric-based key era conspires in WBAN. Second, the electronic medicinal record (EMR) is securely put away in the healing center group cloud, and the protection of the patient's information is ensured. Assessment and investigation demonstrate that the proposed multi-biometric based system gives vital safety efforts because of its profoundly productive key era instrument.

Mohammad Mehdi Hassan et al. proposed an efficient network model that combines WBAN and Cloud for valid data sharing [27]. The proposed network architecture is designed as four layers: the perceptual layer, the network layer, the cloud computing layer, and the application layer. In the network, the integration of TCP / IP and Zigbee to the coordinator device is used. As a result, the WBAN coordinator is compatible with numerous networks, e.g., as Wi-Fi network and supports greatly, users' movability.

ISSN No:-2456-2165

## III. PROPOSED ARCHITECTURE

### A. Design overview

Figure 2 shows the proposed model of healthcare system architecture. In the model, the data is collected from different hospital wireless sensor network which accumulates and uploaded to the cloud infrastructure. The use of smart gateway is to collect and process the data and also control the system operation. Network management and security analysis monitor the network and detect anomalies which present in the network. At the user interface level, the model provides man services such as ambulatory services, some recommendation, emergency services, and location-based services.

Smart devices can be connected to the smart healthcare framework network to observe medical personnel constantly, all day long, gathering, and compiling data. The developed framework may also be utilized for security intents, and as smart services for collecting data through the Internet and from several applications including education, commerce, etc. In healthcare environments, it may be utilized to produce an improved and low-cost smart patient care and can provide access to information by patients about their personal treatment. Additionally, the smart healthcare framework supports patients' capacity to interconnect with medical staff.

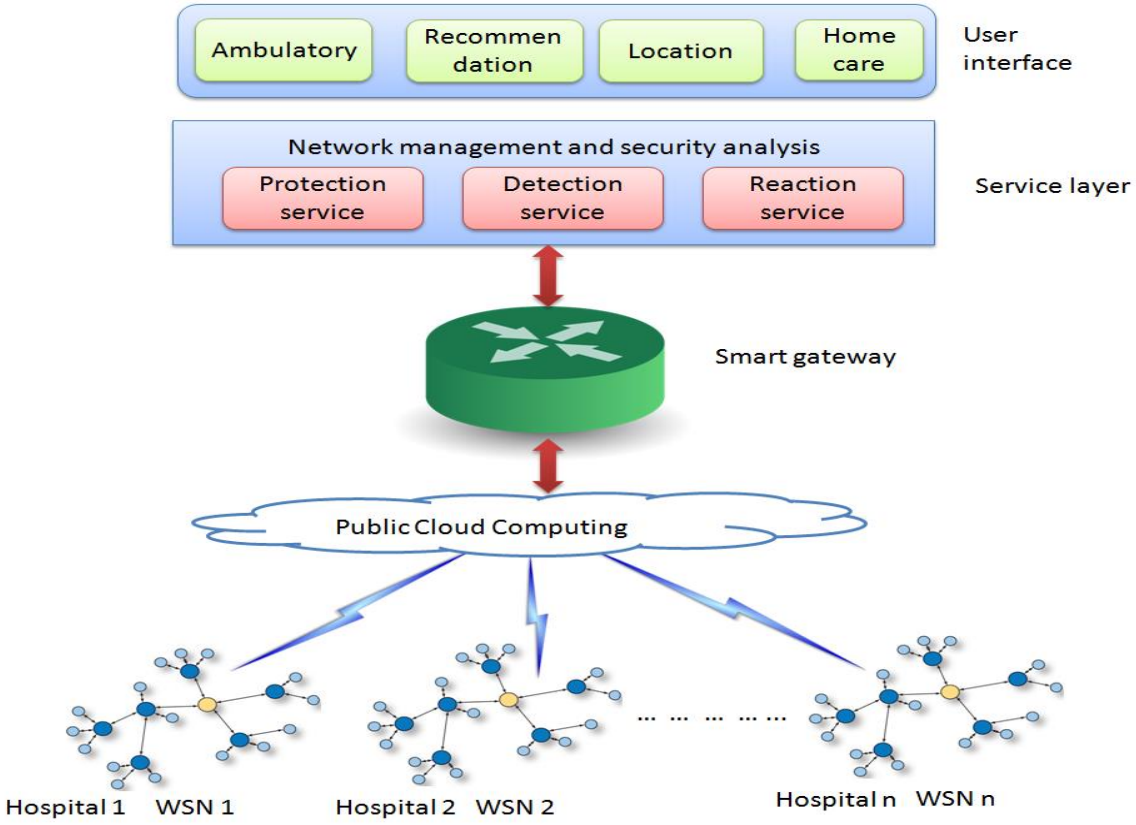


Fig 2. Proposed healthcare system architecture

### B. Smart gateway

Essentially, the method we used allowed us to bring together both the environmental conditions and the patient's physiological parameters in real time, which enabled us to send the data to the control center. Only then, would the advanced Monitoring Application (MA) analyze all data received and give feedback. In cases of emergency, the MA would send an alert through text. The IoT Smart Gateway is responsible for collecting and processing data, managing the system, and service execution. Therefore, it controls the entire system operation. Various components of the Internet of Things Smart Gateway are shown in Figure 3 and further described below:

1) Two-Way Proxy: the two-way Proxy allow for clear-cut connection and transmission with the CoAP device. It can listen to HTTP requests coming from a user interface (like in a mobile or web application) and MA, and in turn converts the requests into CoAP messages or the other way round. Particularly, the bi-directional Proxy can collect the process and reply to requests from the MA and user interface in JSON format. It was developed by applying the Spring Framework. The spring framework gets implemented on the Jetty application server previously installed on the IoT Smart Gateway. After this, the proxy logic is expanded by the caching service supports multiple requests through the same source, and limits the number of traffic introduced into the IoT peripheral network. This feature is especially essential for nodes with constraints that cannot manage requests from multiple clients concurrently. In addition, in order to easily comprehend the handling of the network automatically, the bidirectional proxy incorporates a directory namely the Resource Directory (RD).

ISSN No:-2456-2165

This directory retains a set of properties and equivalent computer contact information, and the rest of the system's information. With RD, the new device can uncover portrayals of accessible assets and CoAP customers (like as MA) and discover assets that meet particular criteria, for example, particular resource type.

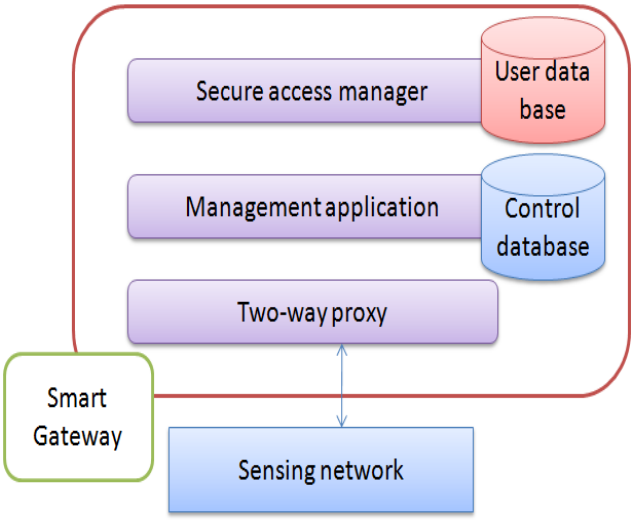


Fig 3. Smart gateway system

2) Management Application and Control DB: The MA being the standalone Java application, can be easily setup and accessed through the user interfaces. It carries out two sets of tasks: enabling hospital environmental conditions control by network operators; observing the patients' health status and alerting doctors in the event of critical conditions. For these reasons, the MA stores the data recovered from the Health Services North (HSN) hubs on a designated (MySQL) database identified as 'control DB'. The availability of this database dissociates information accumulation from information handling and representation, with the goal that specialists and administrators do not have to straightforwardly cross examine HSN hubs amid the typical mode of operation. This method is especially helpful for battery-worked gadgets given that it enables HT hubs to remain more often than not in rest mode, for instance, the IEEE UHF handset with 803.12.4 frequency is always turned OFF and wakes up in the event of crisis. With a specific end goal to screen healing center's natural conditions, the MA additionally watches essential ecological variables (e.g., the emergency unit temperature) checking if it keeps up particular control rules characterized by the system administrators. A typical example could be: if the temperature transcends 28-degree centigrade, the aeration and cooling system gets turned ON).

3) Secure Access Manager and User DB: Secure Access Manager (SAM) applications guarantees data privacy and security. This conducts interaction between the user and the IoT smart portal and provides accessibility information in the database, limited to authenticate users only, such as users registered in the user DB.

*C. Role of Cloud Computing*

Research developments towards cloud computing will have a direct effect to a number of issues in existing technologies. various methods are necessary to successfully address those issues. Research efforts in cloud computing has identified services that can be delivered over the cloud. Below we list some of those services: including Software as a Service (SaaS), Data storage, Sales force automation, Supply chain management, hosted infrastructure (services, network capability), Hosted services (fully operational IT environment). Services delivered through the cloud are dependent on other factors that affect cloud computing. further research will have to be carryout to find ways to deal with these factors. Some of the aspects that will be affected by cloud computing are listed below: -

The volume of traffic in the network: increased bandwidth will be required to enable fast connection to the Internet. Security Aspects: a secure way to access services through the Internet must be ensured. Business Models: the way business is conducted will have to change to suit the cloud computing paradigm. Accessibility: a reliable IT infrastructure must be in place to enable access to services.

*D. Security analysis*

The IoT medical paradigm is hitherto strong but continues to grow. For that reason, it can be very hard to recognize and forecast all possible weaknesses, dangers, and attacks related to the medical field of the IoT. However, as experts in security strive to discover a provisional solution to safeguard this for obvious and expected issues, those kind of security designs has not yet revealed invisible or unexpected problems that have not yet appeared. We should have the ability to mitigate. In order to realize this security goal, security solutions must be engineered with proactive properties. In other words, based on experience and knowledge, we need the ability to make decisions about unnoticed problems.

Consider a scenario that includes a service whose security scheme can find and avoid two sets of attacks against message integrity. Nonetheless, in respect to the development of medical networks, systems, and applications, etc., we assume that attackers may instigate novel forms of attack that endangers the integrity of health data. Under these circumstances, current security solutions can use attacks based on dynamic algorithms or artificial intelligence to identify at least this new type of attack. In order to solve this problem, this research purports a security model of IoT-based medical service.

ISSN No:-2456-2165

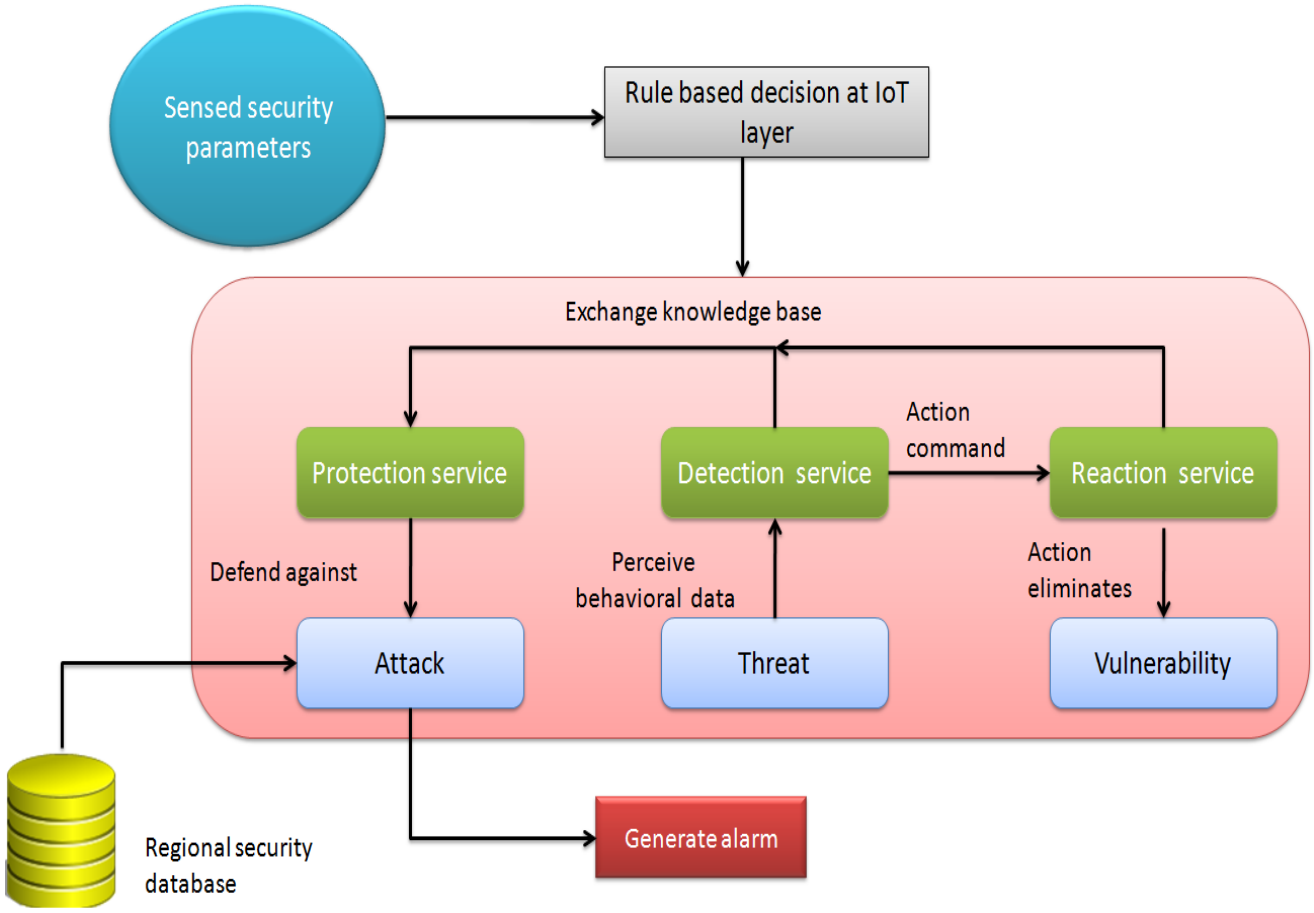


Fig 4. Security flow diagram in healthcare system

This astute security framework fundamentally combines and uses the latest information base. Figure 4 shows the cooperation strategy of the three security solutions as follows: protection services geared towards mitigating attacks; detection service obtains data activity from medical networks, devices, and applications, thereby assessing acquired health data, eventually discovering irregularities; the response service initially reinforced by a defense system, supports health institutions withstand all attacks. These security services are designed using flexible algorithms, and currently, there is a strong linkage between these services to defend against possible and invisible attacks. Upon detection of an intrusion, the discovery service issues an action command to the response service and shares the experience of anomaly detection with the protected service, minimizing further attacks. Response service responds to action commands from the discovery service, eliminating the risk of system malfunction and sharing Behavioral experiences with both detection and protection services. In this way, cooperation between services is realized.

## IV. USE CASE SCENARIO

The proposed architecture is described in a detailed manner. To refine the application framework, we analyzed the process of the proposed system through a use case scenario. Figure 5 presents a use case scenario in which a patient straps a sensing device around him. This device gathers patient's physical data and sleeping activities. Sensor /RFID could be used as monitoring devices which are put on a said subject's body. These Sensor /RFID markers could be easily patched on the flesh, concealed in human garments, footwears, or watches. These tags are creating wearable sensor network that typically capable of sensing processing and communicating among the physiological signals.

ISSN No:-2456-2165

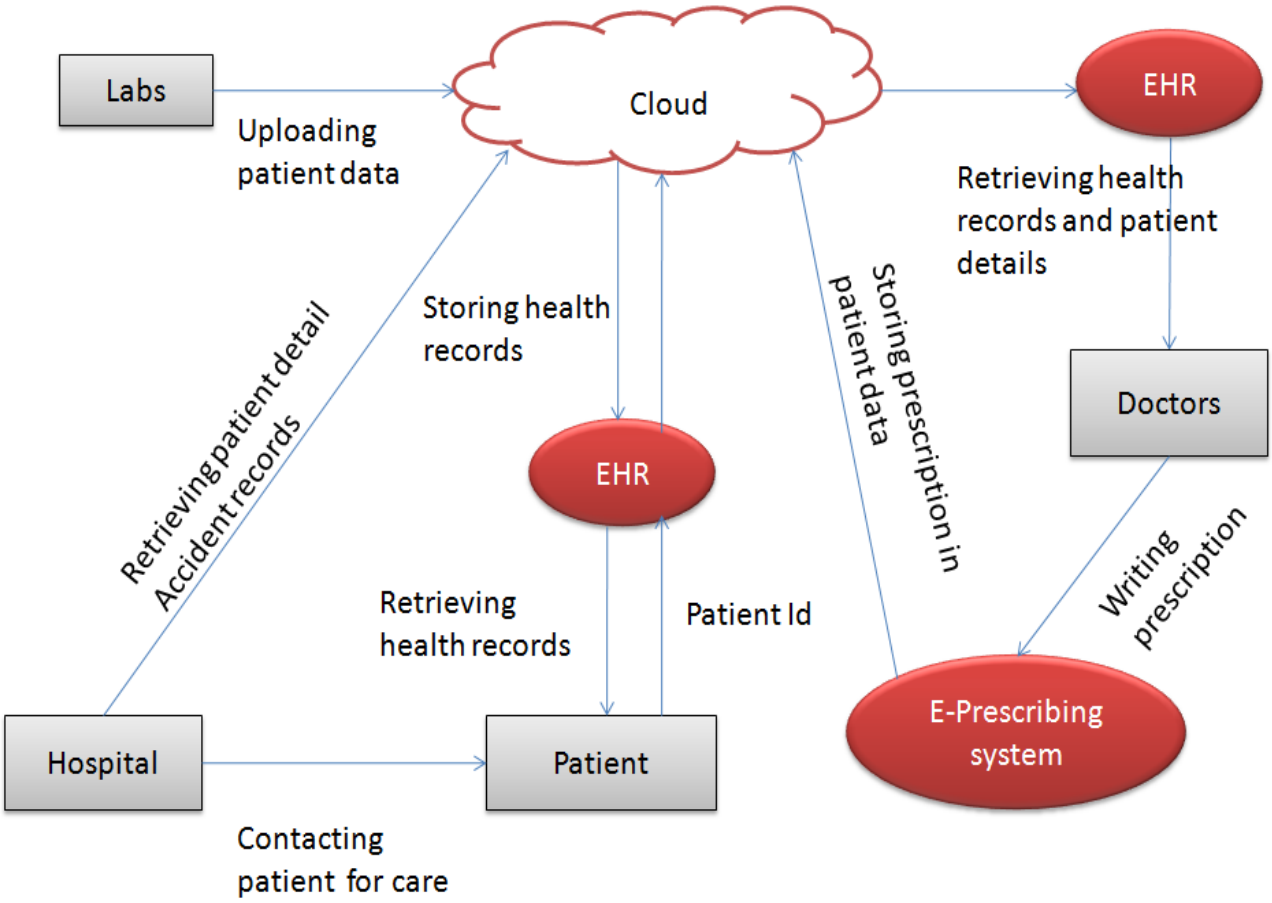


Fig 5. Use case Scenario in Healthcare system

In addition, these tags help to identify the user locations, discriminating the user's states like as user is in sitting mode, laying, running or in other physical activity mode. All the user activity data are uploaded from IoT device via Electronic Health Record (HER) system to users' view or the front-end. The front-end projects users' view and all data are uploaded manually. Then after this, the hosting of data in cloud's HER server or the back end will be carried out, and the data would be stored in patients' health profiles. These collected users' or patient data can be viewed by the hospitals on request. Laboratories and patients may also upload Magnetic Resonance Imaging (MRI) scans or Computer Tomography (CT) scan in health E-profile of the patient based on a common agreement and it would be viewed through cloud platform. A specialist can share and access these data anywhere in the world in a real time which helps to enable diagnosis and recommendation as soon as possible. Sometimes people are traveling and fell ill they could provide local doctors and access their health records shared by the cloud system. A pharmacist could also be able to check up a person's allergies through patient medical profiles.

The patients digitalized data such as medical histories, scan images, medical research labs reports, blood reports and other kinds of medical information have been processed analyzed and shared by IoT- cloud collaboration in the real time. This information can freely flow throughout the world, easily accessed (through some security checks and validation) and simply translated by medical experts. The system enables medical experts to assess patients scanned images and reports instantaneously, any location, point to point care to see more patients' categories. The solution can save more cost, save time and also provide facilities to private and government hospital network across the countries.

## V. DISCUSSION

Researchers all over the world are beginning to explore various technical solutions to mobilize the possibilities of IoT and complement existing services in order to strengthen medical provision. In addition, there are many typical applications in the medical field and many cases of the threats and challenges to be introduced in the wireless sensor network from the necessity to ensure the required reliability level and the privacy and security of medical data.

These challenges are exacerbated by resource shortages inherent in wireless sensor network platforms. Cloud computing and wireless sensor technologies in the medical setting has been suggested in our proposed healthcare system. This system aims to enforce constantly increasing sensor data to populace-centered sensing applications from the various hospitals that may be used as up-to-date services in the cloud. A number of functions are provided in this framework that can automatically and wirelessly send and receive data to numerous users. Due to the dynamic nature of the whole network, it can be utilized for exchange of information, recognition of smart IDs, placement of objects, and monitoring and tracking of

objects. The cloud service model provides provisioning and use of economic resources.

In some cases, this framework may be useful for patients who need more regular medical examinations, or for patients who cannot come to a doctor or need medical assistance at home. Because health care workers can monitor medical, such as exercise, weight, blood pressure, without going to a patient's hospital, it is necessary to consider smart health technology. Applying the IoT environment is a flexible way to link the latest measurement instruments, and you can build a smart network at home anytime anyplace.

## VI. CONCLUSION

The purpose of this paper was to assess the medical environment with regards to the application of cloud computing, the employment of wireless sensor technology, and Internet integration. The employment of wireless sensor technology has emerged as an important characteristic of advanced healthcare services in real time. This paper proposed a system architecture which is supposed to collect both the environmental conditions and the patient's physiological parameters in real time and be able to send them to the control center. The IoT Smart Gateway is responsible for collecting and processing data, managing the system, and service execution. Therefore, it controls monitor, analyzes, continuously detect the overall system operation. The proposed system also focuses on security level which provides three security services i.e., protection services, detection service and reaction services which helps to detect and monitor the WSN network.

## REFERENCES

[1]. D.J. Cook, J.C. Augusto, V.R. Jakkula, Ambient intelligence: technologies, applications, and opportunities, Pervasive and Mobile Computing 5 (August) (2009) 277–298.
[2]. K. Kinsella, D.R. Phillips, Global aging: the challenge of success, Population Bulletin 60 (2005).
[3]. Rashid, B., & Rehmani, M. H. (2016). Applications of wireless sensor networks for urban areas: A survey. Journal of Network and Computer Applications, 60, 192-219.
[4]. L.Mainetti, L.Patrono, A.Vilei, "Evolutional wireless sensor networks towards the Internet of Things: A survey", in Proc. Soft-Com 2011.
[5]. H.Viswanathan, E.K.Lee, D.pompili, "Mobile grid computing for data and patient-centric ubiquitous healthcare", in Proc. IEEE Workshop ETSIoT, Jan. 2012.
[6]. S. Madria, V. Kumar, and R. Dalvi, "Sensor Cloud: A Cloud of Virtual Sensors," IEEE Softw., vol. 31, no. 2, Jan. 2013, pp. 70–77.
[7]. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, March. 2012, pp. 583–592.
[8]. Chipara, C. Lu, T. C. Bailey, and G.-C. Roman. Reliable patient monitoring: A clinical study in a step-down hospital unit. Technical Report WUCSE-2009-82, Department of Computer Science and Engineering, Washington University at St. Louis, Dec 2009.
[9]. JeongGil Ko, JongHyun Lim, Yin Chen, Razvan Musaloiu-E., Andreas Terzis, Gerald Masson, Tia Gao, Walt Destler, Leo Selavo, and Richard Dutton. MEDiSN: Medical Emergency Detection in Sensor Networks. ACM Transactions on Embedded Computing Systems (TECS), Special Issue on Wireless Health Systems, 2010
[10]. Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems, 36(1), 93-101.
[11]. Fernández-Caballero, A., Latorre, J. M., Pastor, J. M., & Fernández-Sotos, A. (2014, December). Improvement of the elderly quality of life and care through smart emotion regulation. In International Workshop on Ambient Assisted Living (pp. 348-355). Springer, Cham.
[12]. Bousquet, J., Anto, J. M., Sterk, P. J., Adcock, I. M., Chung, K. F., Roca, J., ... & Abdelhak, S. (2011). Systems medicine and integrated care to combat chronic noncommunicable diseases. Genome medicine, 3(7), 43.
[13]. Mishra, V., Singh, N., Tiwari, U., & Kapur, P. (2011). Fiber grating sensors in medicine: Current and emerging applications. Sensors and Actuators A: Physical, 167(2), 279-290.
[14]. Khuri-Yakub, B. T., & Oralkan, Ö. (2011). Capacitive micromachined ultrasonic transducers for medical imaging and therapy. Journal of micromechanics and microengineering, 21(5), 054004.
[15]. Najera, P., Lopez, J., & Roman, R. (2011). Real-time location and inpatient care systems based on passive RFID. Journal of Network and Computer Applications, 34(3), 980-989.
[16]. Wallace, R. G., Bergmann, L., Kock, R., Gilbert, M., Hogerwerf, L., Wallace, R., & Holmberg, M. (2015). The dawn of structural one health: a new science tracking disease emergence along circuits of capital. Social Science & Medicine, 129, 68-77.
[17]. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. IEEE Access, 3, 678-708.
[18]. Milenkovic, A., Otto, C., and Jovanov, E., Wireless sensor network for personal health monitoring: issues and an implementation. Comput. Commun. 29:2521–2533, 2006.
[19]. Ng, H. S., Sim, M. L., and Tan, C. M., Security issues of wireless sensor networks in healthcare applications. BT Technol. J. 24 (2):138–144, 2006.
[20]. Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems, 36(1), 93-101.
[21]. R. Aiswarya, R. Divya, D. Sangeetha, and V. Vaidehi, "Harnessing healthcare data security in cloud," in 2013 International Conference on Recent Trends in Information Technology (ICRTIT), 2013, pp. 482–488.

[22]. Alharbe, N., Atkins, A. S., & Champion, J. (2015). Use of Cloud Computing with Wireless Sensor Networks in an Internet of Things Environment for a Smart Hospital Network. In procceding 7th International Conference on eHealth, Telemedicine, and Social Medicine.
[23]. Shanmugasundaram, G., Thiyagarajan, P., & Janaki, A. (2017). A Survey of Cloud Based Healthcare Monitoring System for Hospital Management. In Proceedings of the International Conference on Data Engineering and Communication Technology (pp. 549-557). Springer Singapore.
[24]. Kaur, P. D., &Chana, I. (2014). Cloud based intelligent system for delivering health care as a service. Computer methods and programs in biomedicine, 113(1), 346-359.
[25]. Fortino, G., Pathan, M., & Di Fatta, G. (2012, December). Bodycloud: Integration of cloud computing and body sensor networks. In Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on (pp. 851-856). IEEE.
[26]. Khan, F. A., Ali, A., Abbas, H., & Haldar, N. A. H. (2014). A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. Procedia Computer Science, 34, 511-517.
[27]. Hassan, M. M., Lin, K., Yue, X., & Wan, J. (2017). A multimedia healthcare data sharing approach through cloud-based body area network. Future Generation Computer Systems, 66, 48-58.