IJIRMET
ISSN (Online): 2456-0448
International Journal Of Innovative Research
In Management, Engineering And Technology
Available online

AN ARCHITECTURAL INFERENCE SYSTEM FOR HEALTH MONITORING

Based on IOT

[1] *Agarsha Merin John*
M tech in Network Engineering, Rajagiri School of Engineering And Technology, Kochi, India.
agarshamerin@gmail.com
[2] *Divya James*
Assistant Professor, Rajagiri School of Engineering& Technology, Kochi, India.
divyaj@rajagiritech.edu.in

To access & cite this article
Website: www.ijirmet.com

ABSTRACT

Network security is designed to protect the usability and integrity of different network and data. It makes efficient and effective access to the system. It finds a variety of threats and stops them from entering or spreading on our web. A body sensor network (BSN), is a wireless network of wearable devices. A human health monitoring platform designed and developed under the application of the body sensor network. Internet of Things (IoT) is a new concept that is to allow users to connect various sensors and smart devices to collect real-time data from surroundings. This paper presents a novel approach for data transmission, security, and reliability and proposed architecture based on the cognitive model to realise coaching system for daily life activities. Also, it introduces a structural health monitoring framework, used to collect data from multiple data sensors to make intelligent and reliable monitoring. This paper also proposes a secure and reliable body-sensor network based on the Internet of Things. It is a new model introduced to the overall health of the patient. It stimulated and implemented through strong pro activities of the patient and realised using mobile devices. Visions for future health-care IoT and some future research methods are proposed.

KEYWORDS: Iot, health system, security, body sensor network.

I. INTRODUCTION :

Internet of things is recently received and makes proper attention due to its potential and capacity. Wearable devices have become popular and innovative devices in the Internet of Things. In recent decades the ageing of the population has led to a change in the health field with particular attention to the issue of home care and e-health. Health care is one of the fastest growing in the internet of things. Integrating IoT features into medical devices can improve the quality and effectiveness of good health. Object connected to the internet is mobile phones, cameras, home appliances, city infrastructures, medical instruments, plants and so on. This concept associated with IoT. A wireless sensor network considered as one of the critical technologies in IoT. The objective is to provide different types of health care services to the patient's home rather than in hospital and so to improve the quality of life of patients by allowing them to stay in their environment. A new paradigm leads to a coaching system to collect data sets and information available to us. The primary objective of coaching systems is to increase the comfort and autonomy of life of the people. The automatic recognition of human activities is a process by which the behaviour of an actor and the environment in which it located are monitored and analysed to infer its operations. This research field is a subject of increasing interest and presenting a significant challenge for the realisation of pervasive systems. The proposed method gives an architecture, framework, inference system and secure and reliable health monitoring system based on IoT. The inference system includes collecting and analysing the data in multiple phases, like nature of the data, the current situation of the user, processing and action to take, transmission. The architecture defines the cognitive model. It tells about how to simulate the structure and divided into different categories which correspondence of long term research. The modules included in this architecture are the goal, imaginable, perceptual-motor and so on. The idea behind in this paper is to collect data from multiple sensors and installed on different structures to process and extract useful information about the current state of the structure for maintenance and safety purposes. It based on the integration of the wireless sensor network and the internet of things. Based on the architecture, framework and inference system we are implementing a secure and reliable health monitoring system based on IoT. Example of the health monitoring system is blood pressure, heart rate, implants and so on. The proposed paper gives a secure and reliable IoT system for health care. Treated topics are requirements for IoT in health care, architectures and applications for IoT in health care, analysis of data from IoT health care systems in the framework, development methodologies for health care IoT applications and services, security, reliability issues related to IoT devices and visions and methods for future research related to health care based on IoT.

II. LITERATURE SURVEY :

Being mobile and using open network environments, data collection and transfer must be kept private as well as strict secure must be applied[1]. The body sensor network is one of the most important technologies used in IoT based modern health care system. It is a collection of low-power and lightweight wireless sensor nodes that are used to monitor the human body functions and surroundings[2].An overview of the security solutions for IoT systems proposed by the Internet Engineering Task Force in which coap and in particular Datagram Transport Layer Security examined. It will consider in future work. Based on BSN, which consist of lightweight crypto-modules, such as one way hash function random number generic function that is to pursue system efficiency and secure robustness[3]. Patient Monitoring System which consequently needs a real-time recording and notification of vital signs of the patient. In modern bio-instrumentation, computers and telecommunication technologies, PMS will acquire data, display and transmit the physiological data from the patient's body to remote location at any time. There are two subsystems are designed that is a sensor system and a display system. The first one consists of two thermometers and a wireless transmitter, and an ios mobile device. Security is attainable by transmitting the data through the password protected global system for mobile communication module that is encrypted and then the user/doctor will access the data through logging to the HTML web page. At the time of emergency an alert message will be sent to the doctor through the GSM module, and then, the proper medication will be quickly pre-

scribed [4]. Sensor body technology is the fundamental technologies for the improvement of IoT in the health care system, in which all ill person can be examined using a collection of light nodes and wireless sensors light. And they look out for significant security requirements in the modern health care system [2], [3], [4].To implement a coaching system for cognitive people, we need to identify the main task to perform. The functionalities behind in the proposed architecture are emergency and safety, communication, health monitoring, training [5]. Patient data provided via IoT enabled health care application increasingly created and stored electronically. It offers a vast wealth of information that can be utilised to make evidence-based decisions that can significantly affect how health care is delivered [6]. IoT applications involve a wide range of areas such as security and surveillance, environmental monitoring, medical and health care, SHM, manufacturing [7]. The proposed inference system to assess the user's health condition using multiple sensors to monitor the heart rate, respiration rate, blood pressure, body temperature [8].

III. SYSTEM DESIGNS :

COGNITIVE ARCHITECTURE.

This work concentrates on the utilisation of frameworks that allow for designing a cognitive architecture. This kind of model is a crucial role in the research debate, cognitive science. They have to set some useful constraints that are to recognise models for the explanation of human behaviour. A cognitive architecture is computer software that implements psychological theories on the functioning of our mental processes and used for the creation of intelligent agents. They can be numerous and of a different kind but the agent knowledge defines agent working. It depends on both the task that the architectural structure. The architecture must be independent of any work. According to cognitive architecture, specifies the underlying infrastructure for an intelligent system. The architecture includes a cognitive agent that is constant over time and across different application domains. It includes short-term and long-term memories that store content about the agent's beliefs, goals, and knowledge, and representation of elements contained in these memories and their organisation into larger-scale mental structures and the functional processes that operate on structures, including performance mechanisms that utilise and the learning mechanisms that alter. The primary objective of cognitive architecture is decision making and interaction with the environment. The first one refers to the ability to make decisions based on knowledge. It is entirely related to any task. Anything that an agent knows what to do to act in a given time composes his procedural knowledge. It must be able to learn, encode and use information. Interaction with the environment refers to the ability to interact with the inputs and outputs that the environment around the agent provides and can interpret.

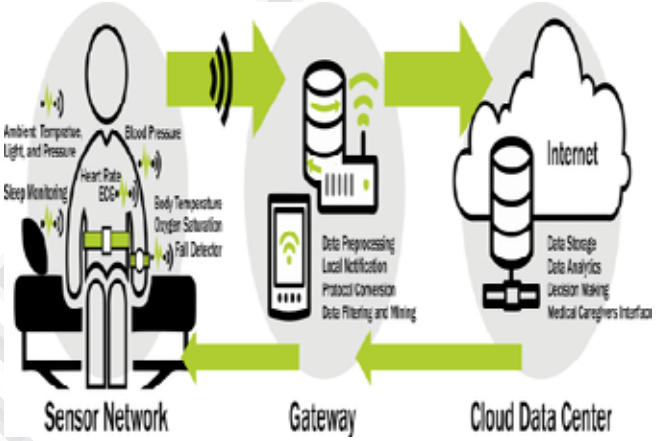

Fig a. Cognitive architecture

TYPE OF SENSORS

B.1 Temperature Sensor

The precision centigrade sensor which is the precision integrated-circuit temperature sensor. It is used to measure the temperature. The user does not subtract a large constant voltage from its output to obtain convenient Centigrade scaling. This sensor does not need any external setting or trimming to provide typical accuracy at room temperature.

B.2 ECG Sensor

ECG is used to record the charging activity of the heart over a specific period. The electrodes are placed on the patient's body to show whether or not the heart is working regularly. These electrodes will detect the tiny electrical changes on the surface that arise from the heart muscle's electrophysiologic pat-

tern of depolarising during each heartbeat.

B.3) Heartbeat sensor

Heartbeat is a very vital health parameter that is directly related to the soundness of the human cardio systems. The Heartbeat sensor is used to measure the heartbeat rate. The signal can be amplified further for the microcontroller to count the frequency of fluctuation, which is the heart rate.

B.4) Pressure sensor

The pressure sensor measures the temperature in ranges split into an absolute pressure sensor and a gauge pressure sensor. A smart piezoresistive pressure sensor can be interfaced with the microcontroller to ensure temperature compensation and linearization of the sensor. To compensate for the sensor's imperfection, an approximation of the sensor inverse response function by a second-order polynomial in terms of pressure used. The maximum measurement error concerning the full measurement range lies within a certain range compared to the ideal sensor response function within the temperature range.

B.5 Pulse Oximeter sensor.

The idea of Pulse Oximeter is based on red and infrared light to monitor pulse rate and the oxygenation of a patient's blood. The body scatters and absorbs visible light significantly and allows infra-red lightto pass through. A typical pulse Oximeter consists of light emitting diodes. It shines through a reasonably translucent site mounted in a clip. Then it is attached across a finger, toe or earlobe as the light produced by the light emitting diode travels through the body it is absorbed by a photodetector which is responsible for receiving the light that passes through the measuring site. The amount consumed also allows the pulse Oximeter to determine the blood oxygen saturation.

C. CLOUD DATA CENTRE AND GATEWAY

C.1 cloud data centre

A datais a facility used to house computer systems and associated components, such as telecommunications and storage systems. It includes redundant or backup components and infrastructure for power supply, data communications connections, environmental controls and various security devices. A large data centre in an industrial-scale operation used as much electricity as a small town.The data centre is often the engine that drives the growth of the enterprise, and energy efficiency is the key. Health care provider systems leveraging cloud-based computing and cloud services offer an array of benefits in comparison to in-house client-server systems; including economic, operational and functional advantages. The economic benefits of cloud computing can be significant. Since cloud computing provides cost flexibility and the potential for reduced costs. Also, the value of staff resources required to migrate and maintain IT resources included in the price of cloud computing. Therefore, the need for additional health care provider will reduce when using cloud services like IaaS, PaaS, and SaaS platforms. From an operational perspective, cloud services offer scalability and the ability to adjust to demand rapidly. Cloud services can be better security and privacy for health data and health systems. Cloud service provider and data centres are highly secure and well protected against intruder and threats inside the network using administrative, physical and technical methods designed and maintained by expert professional. Cloud services offer sophisticated security controls, including data encryption and access controls and access logging. Medical systems can be built using cloud services. The need for IT security skills within the health care organisation also is minimised. Cloud service providers typically operate on a scale that they have all the necessary computer skills, with the costs of those skills spread across many customers. Health care functionality can be enhanced by cloud-based health care IT systems that offer the potential for Interoperability and integration. Health care cloud services are Internet-based and used for standard protocols, so connecting them to other systems and applications is typically straightforward. Cloud services are enabled from remote areas to get forms and data via the Internet using wired and wireless networks. Internet connectivity established from anywhere at any time. Support from mobile devices is often a feature supported by health care. Cloud

services access to a much larger ecosystem of health care provider; all of which increase the potential for a wide range of services to health care provider organisations.

C.2 GATEWAY

A gateway is a mediator between the application and wireless nodes. All information received from the wireless nodes is aggregated/manipulated by the gateway and forwarded to the form. This application may run on a local computer or a networked computer. In reverse direction, when a command issued to a wireless node, the gateway groups the information to the wireless sensor network. All gateways can perform different protocol conversion to enable the wireless network to work with other industry or non-standard protocols.

D. INFERENCE SYSTEM

An inference system embedded in the sensor itself to make a decision how best to transmit sensed data through discerning situations and optimising data. The existing system refers to an alarm notification in our inference system. The output of the inferring process is to adjust a personal range of average values for each attribute and compare it with generic information. It is a novel approach in comparison to use separate sensor devices such as multiple axis accelerometers to monitor the activity or the status of human motion without analysing with other data. And so that by control the frequency of transactions can save power consumption significantly. Critical information transmits over non-prioritized requests. They are Unstable, inconsistent and fluctuating sensed data. And also the number of transmissions is efficiently reduced that means efficient get reduced. We need to overcome this situation so that a secure IoT based Bsn network proposed.

I am inferring the nature of the data requestor, e.g. registered or unregistered.

I am inferring the current situation of the user, e.g. walking, running, sleeping…..etc.

I am inferring the process and action to take, e.g. discarding the request, transmitting data.

I am inferring the transmission of the message, e.g. immediate, delay, frequency, interval, QoS.

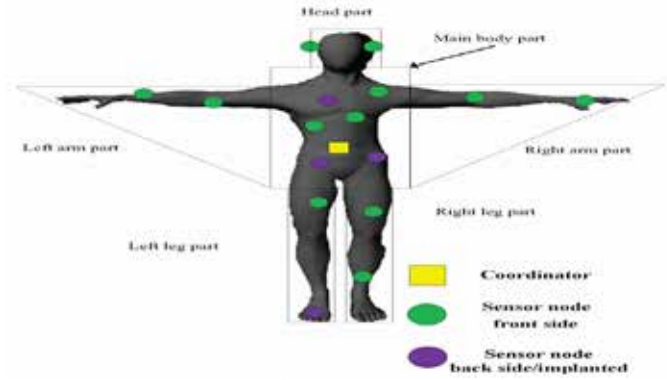

Fig b. I am inferring body sensor network.

E. SECURING HEALTH SYSTEM

To guarantee the safety and privacy of persons monitored and sometimes even controlled by IoT health care systems the IoT devices, all end-to-end communication with these devices, and all data collected by and sent to these devices must be protected against security attacks. Standard security solutions consist of access control, cryptography and obfuscation. The protection service implements defence against security attacks based on data received from the detection and reaction services. The detection service recognises security threats, attacks, and vulnerabilities trigger the protection and reaction services and receive feedback from the reaction service. The reaction service eliminates vulnerabilities, implements necessary recovery after security incidents, and sends data about executed actions to the protection and detection services. Network nodes communicating with IoT devices must be protected against intrusion by authentication schemes and Intrusion Detection Systems, and sending data to, and reception of data from IoT devices must be controlled by authorisation schemes to prevent sending of corrupted or unauthorised data and corruption of received data. If cloud services are used to store data sent from IoT devices, then the data must be stored encrypted with access permissions only to authorised users. Now, communication in sensor network applications in health care is mostly wireless. This result in various security threats to these systems. These are

the security issues cloud pose severe problems to the wireless sensor devices. In this section, we describe the critical security requirements in IoT based health care system using BSN. The security requirements are Data Privacy, data integrity, data freshness, authentication, anonymity and secure localisation.

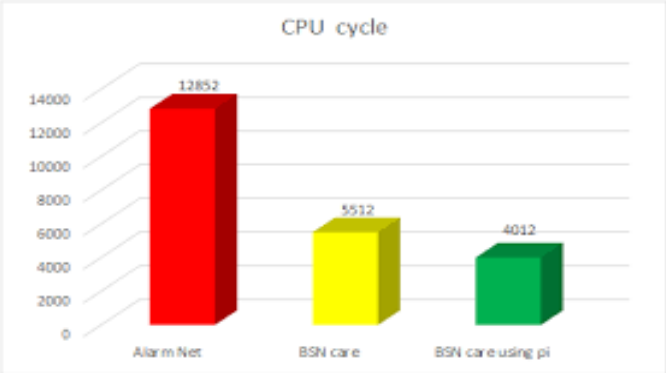

Fig c. CPU cycle for securing the system.

E.1 SECURITY THREATS

Data Interception

In today's scenario, eavesdroppers capture the data sent over Wi-Fi. Now all Wi-Fi certified products support data encryption and data integrity. Some products only support the Temporal Key Integrity Protocol. And WLANs accepts both AES and Temporal Key Integrity Protocol. But TKIP is vulnerable to attacks, so it allows a limited set of spoofed frames.

Denial of Service

Wireless LAN is inherently susceptible to the denial of service. Everyone has the same unlicensed frequencies, making competition inevitable in populated areas. The good news: As enterprise Wireless LAN migrates to long distance, they can use channels in the larger, less-crowded bandwidth, reducing accidental DOS. Moreover, simultaneous access points can auto-adjust channels to circumvent interference. But that still leaves.

DOS attacks

Phoney messages sent to disconnect users, consume AP resources, and keep channels busy. To neutralise common DOS attack methods like Death Floods, look for newer products that support management frame protection.

Wireless Intruders

Wireless IPS products like Motorola Air Defense, Air Magnet, and Airtight can also detect malicious Wi-Fi clients operating in or near business airspace. However, genuinely useful defence requires current, properly deployed WIPS sensors. In particular, sensors must be updated to monitor new channels protocols, and look for further attacks. Because, clients can connect from farther away, Wireless IPS sensor can be placed to satisfy both prevention and detection requirements.

V. MISCONFIGURED ACCESS POINTS :

When standalone Access points managed individually, configuration errors create security threats. But add a slew of relatively complex configures options, the consequences of which depend on Wi-Fi client capabilities. Prioritisation and segmentation for multimedia further complicate configuration. The answer is to combine sound, centralised management practices with education and planning to reduce operator error.

Ad Hocs and software-enabled access point

Wi-Fi laptops have peer-to-peer communication ad hoc connections that pose a risk because they circumvent network security policies. The ad has been so hard to configure that few bothered to use them. Unfortunately, the barrier is being lifted by soft APs in Windows and new laptops with Intel and Wi-Fi cards. Those virtual APs can provide secure and direct connections to other users, bypassing network security and routing traffic into the enterprise network.

Misbehaving Clients

Misbehaving of clients corporate high data risk due to unauthorized clients from Wi-Fi connections and all. Some of them use Group Policy Objects to configure authorised Wi-Fi connections and prevent end-user changes. Others will use host-resident agents to monitor client activity and disconnect

high-risk connections. Many businesses still depend on end-users to connect only to known, authorised wireless APs. Given deployment, longer reach, and broader consumer electronics integration, accidental or inappropriate Wi-Fi connections have never been easier.

Endpoint Attacks

Numerous exploits published to take advantage of buggy Wi-Fi drivers, using buffer overflows to execute arbitrary commands. Automated attack tools can be used to launch Wi-Fi endpoint exploits with minimal effort. Although vendors do patch these bugs once discovered, Wi-Fi automatically updates. Protect your workforce, track Wi-Fi endpoint vulnerabilities and keep your Wi-Fi drivers up-to-date.

Wireless attacks

In wireless attacks, hackers continue to develop new methods to phish Wi-Fi users. It is possible to attack the client cache so that the attacker can go into the past Web session such as open hot spot. Once poisoned, clients redirected to phishing sites long after leaving the hot spot, even it is connected to a wired network. There is one technique to mitigate this threat is to clear your browser's cache. Another possibility is to route all hot spot traffic through a trusted VPN gateway.

E.2 SECURITY REQUIREMENTS

Privacy of Data

Like WSNs, the confidentiality of data is considered to be the most critical issue in the body sensor network.BSN should not leak patient's vital information to external or neighbouring systems. In IoT-based health care application, the sensor nodes collect and forwards sensitive data to a central unit. A competitor can eavesdrop on the communication and can overhear important information. This eavesdropping may cause severe damage to the patient since the adversary can use the acquired data for any illegal purposes.

Data Integrity

Keeping data confidential does not protect it from external modifications. An adversary can always alter the data by adding some fragments or by manipulating the data within a packet. Lack of integrity mechanism is sometimes hazardous especially in the case of life-critical. Loss of data can also occur due to the lousy communication environment.

Data Freshness

The adversary may sometimes capture data in transit and replay them later using the old key to confuse the coordinator. Data freshness implies that data is fresh and no one can replay the old message.

Authentication

It is one of the essential requirements in any IoT based health care system using BSN, which can efficiently deal with the impersonating attacks. In BSN based health care system, all the sensor nodes send their data to a coordinator. Then the coordinator sends periodic updates of the patient to a server. In this context, it is highly imperative to ensure both the identity of the coordinator and the server. Authentication helps to localisation each other.

Secure Localization

Most applications require accurate estimation of the patient location. Lack of tracking mechanism allows an adversary to send incorrect reports about the patient location by reporting fault signal strengths. To ensure a secure IoT-based health care system using BSN, it is highly imperative that the system should pose all security requirements. And eventually can resist various security threats and attacks like data modification, impersonation, eavesdropping, replaying etc.

E.3 SECURITY SOLUTIONS

The wireless security look at external and internal policies and security design. It offers high levels of security and the flexibility to adapt to changing threats. These policies will help to determine how to

access to your wireless network and decide how to keep authorised users safe and secure, and unauthorised users blocked.

Firewalls

With a good quality firewall, your company can establish a strong security foundation to prevent anonymous threats and offer security. Firewall is like security staple in all safe networking environments, wired and wireless.

Detectionof Intruders

Intruder detection and prevention software, also found in wired and wireless networks, protect your system from direct attacks, threats, worms, viruses and more.

Content Filtering

Content filtering is just as necessary as the first two solutions in all network environments because it helps protect you from an internal activity. Filtering and monitoring software prevent your employees from accessing content via the Internet that could potentially be harmful to your operations.

Authentication of Data

Authentication of data and identification methods protect your data network. For the password protection, solutions such as key fobs and biometric authentication ensure with proper authority to access your data and so keeping your wireless network safe.

Data Encryption

Data encryption transforms data from one format to another. So authorised people can access it using secret key or password. Encrypted data is commonly referred to as cypher text, while encryption data is called plain text. Generally, encryption is one of the most popular and effective data security methods used by different organisations.

VI. FUTURE WORKS

Important future research directions for health-care IoT are security and reliability solutions which are sufficiently lightweight for applications using wearable technology, and which utilise the tamper resilience of blockchain technology. Interoperability requires generally accepted standards for lightweight cryptographic algorithms. Blockchains used to secure firmware updates and reliability enhancing maintenance of IoT devices. The role of platforms in Internet-related enterprises is becoming evident. A significant problem for health care has been in how data is shared, stored, accessed, rectified, and removed. New decentralised platforms utilising blockchain for handling secure personal data developed. These techniques should provide lightweight solutions in handling and transferring personal data, and also offer a transparent way to comply with the GDPR. The two main goals of future health care are control and prevention. People have the options of being tracked and monitored by specialists even both patient and doctor are not in the same place. Tracing peoples' health history is another aspect of IoT-and makes e-health very versatile. Business applications have the possibility of medical services not only to patients but also doctors, who need information to proceed in their medical evaluation. In this, IoT makes human interaction much more efficient because it permits not only localisation but also tracking and monitoring of patients. The primary vision is to enable the deployment of patient and context-aware networked medical systems in all environments, ranging from homes and general hospitals and so on. Heterogeneous devices in each health care environment would effectively share data efficiently, safely and securely to reduce preventable errors that are often induced unknowingly by human operators. As medical devices move between different care environments or from patient to patient, they would securely discover other tools that they need to interoperate with, and then verify and execute safe, authorised and compliant operational profiles. To realise this standardised vision architectures that balance utility, reliability and safety requirements with those of security and privacy should develop. The capability to practice effective evidence-based health care will face new challenges by the increasing amount of medical information from various new data sources and devices such as IoT enabled wearable patient technologies and applications. Even though all these developments show great promise and potential, it is

vital that the processes of evidence-based health care are taken into account and applied to ensure quality in health care.

V. CONCLUSION :

An architectural inference system for health monitoring based on the Internet Of Things is mainly intended to secure IoT based health systems. It provides security solutions for protecting private data on the mobile phones of patients. It satisfies major security requirements like data confidentiality, data integrity, data freshness, data availability and secure localisation. When using cognitive computing architecture, there is a potential to improve the quality of life and life expectancy of people. The interaction between health care IoT devices and software component requires widely accepted standards for IoT architecture and security solutions. The principal concept of IoT is low power consumption. It provides a long lifetime for the network. An IoT solution makes an intelligent and reliable monitoring system. The system is proposed to implement intelligence on body sensors by applying an inference system which reduces unnecessary transactions and helps to save resources. From the comparative study, the cognitive architecture performs better security, and it is affordable for the local users.

VI. REFERENCES :

1. Ilya Nikolaevskiy, Dmitry Korzun, Andrei Gurtov," Security for Medical Sensor Networks in Mobile Health Systems", Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, IEEE, October 2014.
2. Prosanta Gope, Tzonelih Hwang," BSN-Care: A Secure IoT-based Modern Health care System Using Body Sensor Network", IEEE Sensors Journal Volume: 16, Issue: 5, IEEE, March 2015.
3. Kuo-Hui Yeh, Senior Member, IEEE."A secure IoT based Health care System with Body Sensor Networks." IEEE Access Volume: 4, 10288 – 10299 December 2016.
4. Hesham A. El Zouka "An authentication scheme for wireless healthcare monitoring sensor network" 2017 14th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT, IEEE, November 2017.
5. Alba Amato, Antonio Coronato "An IoT-Aware Architecture for Smart Health care Coaching Systems" 2017 IEEE 31st ICAINA, IEEE, May 2017.
6. Dr. S. Rabiyathul Basariya, and Dr. Ramyar Rzgar Ahmed, 2019. "The Influence of 'Adventure Tourism Activities' in promoting tourism business in mountain stations", African Journal of Hospitality, Tourism and Leisure, Volume 8 (2).
7. Dr. S. Rabiyathul Basariya, and Dr. Ramyar Rzgar Ahmed, Nov 2018. "A Study On consumer satisfaction and preference of colour TV brands in Chennai city", International Research Journal of Management and Commerce, Volume4, Issue 10.
8. Dr. S. Rabiyathul Basariya, and Dr. Ramyar Rzgar Ahmed, "A Study on Attrition: Turnover intentions of employees", Jan 2019. International Journal of Civil Engineering and Technology (IJCIET), Volume 10, Issue 9.
9. Dr. S. Rabiyathul Basariya, and Dr. Nabaz Nawzad Abdullah, Dec 2018. "A STUDY ON CUSTOMER'S SATISFACTION TOWARDS E-BANKING", International Research Journal of Management and Commerce, Volume 5, Issue 12,
10. Vasanthi S.,Basariya S. Rabiyathul," Impact of cross training on career planning and progression", Indian Journal of Public Health Research & Development, 2019, Volume : 10, Issue : 3, pp 1081-1085.
11. Göran Pulkkis, Magnus Westerlund & Jonny Karlsson, Jonas Tana," Secure and Reliable Internet of Things Systems for Health care", 2017 IEEE 5th International Conference on Future Internet of Things and Cloud, IEEE, November 2017.
12. C. Jr. Arcadius Tokognon, Bin Gao, Senior Member, IEEE, Gui Yun Tian, Senior Member, IEEE, and Yan," Structural Health Monitoring Framework Based on Internet of Things: A Survey", IEEE INTERNET OF THINGS JOURNAL, VOL. 4, NO. 3, JUNE 2017.
13. James Jin Kang, Tom H.Luan, Henry Larkin," Inference System of Body Sensor Networks", ACM, November 2016.