IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-4, Issue-04 E-ISSN: 2347-2693

Internet of Things for Remote Healthcare

P K Mishra[1*], M. R Pradhan[2] and M.Panda[3]

[1*]Department of Computer Science and Engineering, Centurion University ,Odisha,India
[2]Department of Computer Science and Engineering, GITA, Bhubaneswar,Odisha,India
3Department of Computer Science, Utkal University Odisha,India

www.ijcseonline.org

Received: Mar/22/2016 Revised: Apr/03/2016 Accepted: Apr/17/2016 Published: Apr/30/ 2016

***Abstract*—IoT is a innovative innovation which bridges interoperability challenges to radically change the way in which healthcare will be delivered, driving better outcomes, increasing efficiency and making healthcare affordable. Industry analysts predict that the ability for patients to take more responsibility of their health and the promotion of preventive measures are capable of disrupting current care delivery and will shape the future of healthcare. In this paper, we discuss today´s issues, including benefits and difficulties, as well as approaches to find a way the problems of employing and integrating Internet of Things devices in healthcare systems. It proposes few applications of IoT in rural healthcare and ways to improve primary health needs of the developing nations.**

Keywords-Internet Of Things,WSN

I. INTRODUCTION

Current technology enabled world, changes are rapid and the status-quo is constantly disrupted. Internet of Things (IoT) is one such disruption happening right now, which has the potential to change the way healthcare is delivered. There are no standard definitions for the Internet of things, As per the definition of Gartner [1], "Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment". The IERC definition [2] states that IoT is "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network " The IoT allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service [2]. The main contributor for the IoT can be attributed to the growth of smart phones and tablets. These mobile devices act as a window to the IoT world. They have the capabilities to perform the wide variety of tasks for the patient & doctors, in addition to providing mobility and connectivity.

More important though than agreeing on a definition of the overall term is to have a common understanding of the components and concepts that constitute the Internet of Things used in helth care service . First and foremost, what are the things in the Internet of Things for helth care? What is the relation to devices, resources and services? Second, what do we mean when we talk about addressing, identification and resolution? Looking at discussions at conferences and research projects, one can see that these terms are used with different meanings by different people, and that the terminology is often mixed up, leading to confusion and hindering scientific discourse. The goal of this paper is to bring some clarity of IOT healthcare service and terminologies associated with the it.

II. RELATED WORK

IoT research field works over the growing maturity of several related technologies, such as MANET, WSN, RFID devices, and so forth. The growing interest in this area is also demonstrated by several recent special issues on IoT [1], [3]. Despite the encouraging results obtained so far, most research works tend to mainly focus on specific technological issues (e.g., RFID tag reading speed, security, etc.), and only recently, a few research efforts have started to tackle IoT management issues rising from the full integration of different technologies. In the following, for the sake of briefness, we sketch a limited selection of solutions close to our envisioned approach recognize MANET and WSNs convergence as a key enabling technology for IoT smart cities scenarios. Regarding urban IoT scenarios, several successful industrial and academic research initiatives are available addressing different application domains. There are already various applications to inform car drivers willing to park at a parking area4 and similar projects to monitor free parking lots5 and 6; these projects are important and demonstrate the growing interest in this IoT domain. From an architectural perspective, and addressing a different application domain, Zorzi et al. call for a radical change "from today's Intranet of things" to the "future Internet of things" by indicating as core priorities the definition of an architectural reference model for the interoperability of IoT systems and of mechanisms for an efficient integration of

IoT architectures into the service layer of next generation future Internet networking infrastructures

III. IOT-HELTH CARE DEVICES AND COMPONENT

In the IoT network, all the devices are connected to the internet with separate IP

address.IPv4 is not enough to address the demand of internet enabled devices in the IoT space. Hence IPV6 was developed to address the demand of huge number of IP addresses. Currently major challanges addressing the requirement of IoT devices are deployment of IPV6 across the world and requirement of prolonged battery life. The other requirement is increase in the receiver sensitivity level of RF ICs and not but the least the cost. The cost of the IoT device should be less than about 5 to 6 dollar to capture the big IoT market.

As mentioned IoT network consists of front end and back end. Back end is entirely digital internet hardware and software. Front end consists of mainly sensors. Following are IoT components used in IoT device as well as for sensing applications. Fig-1 and Fig-2 Represents Devices and Components Of IOT

IoT components include Sensors, power management devices, amplifiers,signal acquisition devices,microcontrollers,processors,battery monitoring ICs, low power RF ICs and more. sensors are Usedfortemperature,motion,humidity,acceleration,tilt,pressure,shock,gas,pH,sound and infrared applications.

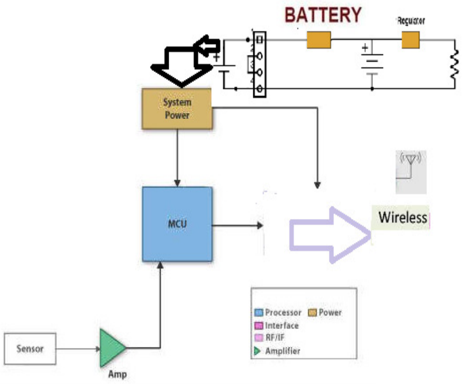

Fig-1

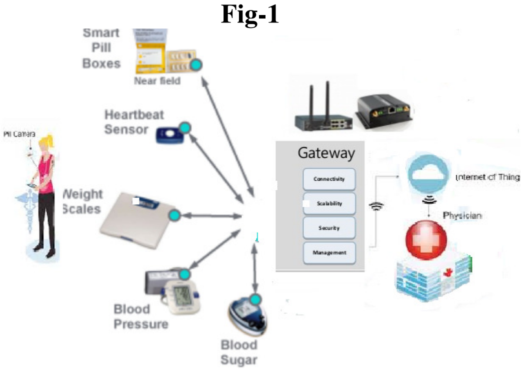

Fig-2

Processors

Companies such as Free scale,Microchip,Lattice semiconductor and Atmel are working towards providing ultra low power MCU for IoT applications. Companies are working on such process technologies so that the processors are tailored to meet IoT specifications.

Battery monitoring IC

The biggest benefit is to use battery monitoring devices so that it will turn off the device when voltage goes below the threshold limit set by the manufacturers/users. This helps conserve the power and hence life span of the IoT device. One such device is STC3115 designed by ST Microelectronics.

Regulator

Another major natural resource available is ambient light. The companies are developing devices which store the energy from the indoor light and use this power to energize the sensors and other IoT components. One such device is ADP5090 designed by Analog Devices. This devices eliminates need of battery for power source. This ultra low power regolator is the source of energy harvesting solutions.

IoT sensors

IoT sensors which are used for optical, ambient light, temperature, pressure, Inertia, humidity, proximity, gesture, touch and fingerprint sensing applications. These sensors are based on MEMS technology. MEMS is the short form of Micro Electro-Mechanical Systems.

If the sensors are digital it is straight forward to interface with microcontroller using SPI. If the sensors are analog, either Analog to Digital converter is needed as mentioned later from Analog devices. Otherwise Sigma Delta modulator can be used which converts analog data to the SPI output. It is easy to interface SPI signals with any microcontroller devices.

IoT devices Communication

IoT devices are classified into two classes based on capability and ability to communicate.

The first class of IoT devices handle the sensors/transducers. They do not communicate with the server. Data from these IoT devices can be transmitted to server using gateway devices. Bluetooth and RFID standards for communication. These class of devices are battery operated. They are portable devices. Hence they require low power wireless technologies as mentioned above. They take care of single sensors. They handle data volume of less size.

The second class of IoT devices directly communicate to central servers for data storage. It supports IPv6 protocol. This class of devices use powerful processors. They are not constrained by battery power. They also support gateway functionalities where in they support different types of communication ports such as DSL,WiFi etc. They support multiple sensor devices.

IV.TECHNOLOGICAL FRAMEWORK

Proposed SYSTEM REQUIREMENTS For IOT Helthcare

Requirements Operational	Yes/No	Description
Query management	Yes	Easy Query System for End user
Power management	yes	Power Management Dynamicaly
Authentication	Yes	Users have control how their data is exposed to other users
Data privacy	yes	A system shall provide end users with secure access to resources
Multiple patients	yes	A system built shall support time-critical message handling and delivery on a second time scale
Service	Yes	A system shall support prioritization of services And enable centralized or decentralized automated activities

Table-1

A. Diverse architectures constitute the mutually non interoperable application specific solutions that shape the market requirements for health monitoring devices. The links between the many applications in health monitoring are: • The process of gathering data from sensors. (WSNsWireless sensor networks) • Support for standard user interfaces and displays. • Network connectivity for access to infrastructural services. • In-use requirements such as low power, robustness, durability, accuracy and reliability. [8] A. Wireless Sensor Networks(WSNs) Wireless Sensor Network (WSN) is an important enabling technology of IoT. It connects a number of sensor and actuator nodes into a network through wireless communication. This integrates the network into a higher level system through a network gateway. [9] Ubiquitous Sensor Network (USN) is an extension of the WSN integrated with an application system of the IoT. Gateways are information hubs which collect sensor data, analyse it and then communicate it to the cloud through wide area network (WAN) technologies. Gateways can be designed for clinical or home settings. In home settings, they may be part of larger connectivity resource that also manages energy, entertainment and other systems. Sensors measure physical data of the parameter to be monitored. The sensor nodes are normally lightweight, inexpensive, easy to deploy and maintain.

B. Standard user interfaces , displays and in userequirements Usability is improved by enabling display devices to deliver a great deal of information with the help of graphics user interfaces(GUIs) This information can be easily accessed due to the vivid detailing done by the GUIs. Processors with high graphics-processing performance support advanced GUI development. The in-use requirements for a healthcare system based on IoT are: Interoperability: Interoperability is crucial for healthcare products based on IoTs to facilitate seamless integration of products designed by different manufacturers. This is achieved by the device manufacturers following set standards or by making sure that gateways are available to translate the identification of one device into another. Reliability: Together with interoperability, reliability is another crucial requirement for the adoption of the Internet of Things. If available IoT based healthcare systems are not reliable, or do not always provide the right information, people will move away from the technology and still rely on more trusted ways of healthcare.

V. IOT HEALTH CARE ARCHITECTURE

The medical sensor network system integrates heterogeneous devices, some wearable on the patient and some placed inside the living space. Together they inform the healthcare provider about the health status of the resident. Data is collected, aggregated, pre-processed, stored, and acted upon using a variety of sensors and devices in the architecture (pressure sensor, RFID tags, floor sensor, environmental sensor, dust sensor, etc.). Multiple body networks may be present in a single system.. The components of tharchitecture are shown in Figure3.

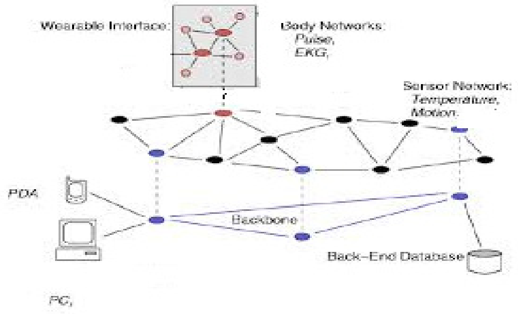

Fig-3

sensor nodes by a high-speed relay for efficient routing. The backbone may communicate wirelessly or may overlay onto an existing wired infrastructure. Nodes possess significant storage and computation capability, for query processing and location services. The number is minimized to reduce cost.

1.Cloud Databases.

One or more nodes connected to the backbone are dedicated databases for archiving and data mining. If unavailable, nodes on the backbone may serve as in-network databases.

2. Human Interfaces.

Patients and Doctor interface with the network using PDAs, PCs, Mobiles. These are used for data management, querying, object location, memory aids, and configuration, depending on who is accessing the system and for what purpose. Limited interactions are supported with the on-body sensors and control aids. Caregivers use these to specify medical sensing tasks and to view important data.

3. Body Network systems. This network comprises tiny portable devices equipped with a variety of sensors (such as heart-rate, heart-rhythm, temperature, oximeter, accelerometer), and performs biophysical monitoring, patient identification, location detection, and other desired tasks. These devices are small enough to be worn comfortably for a long time. Their energy consumption should also be optimized so that the battery is not required to be changed regularly. Actuators notify the wearer of important messages from an external entity. For example, an actuator can remind an early patient to check the oven because sensors detect an abnormally high temperature. Or indicate that it is time to take medication. The sensors and actuators in the body network are able to communicate among themselves. A node in the body network is designated as the gateway to the emplaced sensor network. Due to size and energy constraints, nodes in this network have little processing and storage capabilities. More details about the particular body networks we have developed are available [16].

4. Sensor Network. This network includes sensor devices deployed in the environment (rooms, hallways, furniture) to support sensing and monitoring, including: temperature, humidity, motion, acoustic, camera, etc. All devices are connected to a more resourceful backbone. Sensors communicate wirelessly using multi-hop routing. The sensor network interfaces to multiple body networks, seamlessly managing reported data and maintaining patient presence information.

5.i Backbone. A backbone network connects systems, such as laptop , PCs, and databases, to the sensor network. The bed sensor, developed by the Medical Automation Research Center (MARC), is based on an air bladder strip located on the bed, which measures the breathing rate, heart rate and agitation of a patient.

ii. Pulse-oximeter and EKG. These sensors were developed by Harvard University [15]. They are wearable, connecting to MicaZ and Telos devices, and collect patient vital signs. Heart rate (HR), heartbeat events, oxygen saturation (SpO2), and electrocardiogram (EKG)

VI. ID ISSUE ,RESOLUTION AND CHALENGES

The Internet of Things envisions billions of devices of our daily lives interconnected in such a way that applications that were not possible in isolation emerge from the combination of capabilities and the cooperation of such 'smart objects'. In such a vast network of interconnected objects, the issue of identification of a particular object and its addressing mechanism play a crucial role that affects all other aspects of the system, including its overall architecture, privacy characteristics, governance, etc., whose study is part of the work performed in other sub-groups The Group identified three areas whose technological developments will be relevant to reflections on public policy in Europe: object identifiers, network addresses and resolution and discovery functions. Multiple vs. Unique Identifiers: Work to define identifiers for various classes of objects (sensors, actuators, tags etc.) is currently ongoing in industry and is also part of studies in standardisation bodies both public and private (e. g. ITU, IETF). It seems unclear at this stage whether usage will drive developments towards a globally unique scheme or several distinct ID spaces with varying degree of interoperability. These alternative scenarios have very different public policy implications. If a globally unique scheme were to emerge, like the Internet IP addresses, questions similar to the critical Internet resources debate would likely need to be addressed. A higher degree of flexibility in allowing different governance models would probably be suited to the alternative scenario of multiple identifier spaces. In the latter case, the degree of interoperability would be part of the debate. With the standardization of protocols such as IPv6 and, more concretely for embedded devices, 6LoWPAN, it has been shown that it is feasible in practice to provide a unique identifier (ID) to arbitrarily small devices in an efficient way. However the issues of providing non-colliding unique addresses in a global scheme requires an infrastructure in place that supports highly dynamic devices that appear and disappear from the network at any time, move between different local and/or private networks and have the flexibility to either identify their user uniquely or hide his/her identity, thus preserving privacy as needed. Additionally, this infrastructure has to be able to retrieve information about an object as required for the interoperability and cooperation with other objects and networks and allow for the interchange of meta-data and data without compromising security and/or privacy. Identifiers vs. Network Addresses: Another issue that needs to be taken into account is the conceptual difference between the ID of an object and its network address (or addresses). In the most general case, the ID of an object and its address(es) are distinct and serve different purposes. The former provides a unique handle to the object itself whereas the latter might change depending on the physical location of the object, its logical membership in one or several networks, or the current role of the object. In cases where the ID of an object and its address are different, the ID is normally structured by different identification schemes. The Electronic Product Code (EPC) is one of the well known object identification schemes which could uniquely identify objects associated 2 with an RFID tag. Similarly the addressing schemes could be different. Objects currently connected to the Internet use the global IP addressing scheme (IPv4 or IPv6). Some other objects may not use global IP addressing, using private addressing instead. Even in the case of objects that use a private network, these might be still connected to the Internet, which will often be used to bridge one private network to another. In this case a border gateway which uses global IP addressing is needed to transport the data from one private network to another. For this particular case, the addressing scheme could be heterogeneous and a device could potentially have the capability to "speak" different addressing schemes to operate as part of different networks.

Challenges: 1. It will be nearly impossible to have one global identification scheme for all the objects in the world, since most industries have been using their own proprietary coding standards (ie. identification schemes) for a long time. For this reason, it is highly unlikely that they will move to a different object identification system. Another difficulty is that it will require consideration of a wide variety of object identification schemes to achieve a global object identification schema.

These ID's are used to disambiguate two things from each other, and depending on the context, different ID's may be used. An ID can be compared to a social security number or a key value for looking up records about the thing in a data base. Many types of different ID schemes have been proposed for IDs in the Internet of Things [15], and it is unlikely that we will have one common scheme across the globe and across industries. An address on the other hand is a technical term for accessing – "talking to" – either a device or a service. In the case of devices, the ID and the address often are the same, e.g., an IPv6 or MAC address, but in general they are not. As an example, let's have a look again at the container filled with a chemical. The container has an ID, e.g., a Serial Shipping Container Code (SSCC). This ID can be used to find in a data base information like the type of chemical currently in the container or ist current location. The sensor tag attached however might have an IPv6 address that can be used to query the sensor for the current temperature. The temperature readings could then of course be saved in the data base as properties of the entity of interest and thus become accessible also via the SSCC again, but the point is that the ID links to properties of the entity of interest, while the address is directly used for communication with the device.

Resolution-This is particularly true if the system is global and the issues of scalability, interoperability, etc. are crucial. Domain Name System (DNS) [RFC1034], the name resolution service on the Internet was basically conceived for translating "human-friendly" computer host names on a TCP/IP network into their corresponding "machine-friendly" IP addresses. Besides translating host names to IP addresses, at present DNS is used for instance by Mail transfer agents to find out where to deliver mail for a particular address, a general mechanism for locating services in a domain using SRV records, resolution of identifiers that do not have traditional host components through DNS using NAPTR resource records etc. There are overlay resolution mechanisms services such as Object Naming Service (ONS) and Object Directory Service (ODS) which use the DNS to resolve the object identifiers (their respective identification schemes) to its related digital information.

Challenges: 1. Object discovery is, for example, a trivial task in small networks of several hundreds or thousands of devices, where a broadcasting mechanism can be used easily to look for a particular device. However, using the same scheme in a network of millions of devices would impose significant performance problem on any network design.

VII. APPLICATIONS OF INTERNET OF THINGS IN HEALTHCARE

In the last approach, multiple sensor nodes can join the Internet in one From in-home monitoring devices to large hospital-based imaging systems and thin-client solutions, healthcare industry devices that are part of an intelligent system offer better care, by automating processes, facilitating collaboration and securely managing information. Intelligent systems provide clinicians with easier access to health information, streamline costs, and create operational efficiencies that help to improve the patient experience. Some examples are cited below. A. Monitor an aging family member Ultrasound-based technology already used in hospitals can be deployed as a personalized home healthcare solution to locate and track a senior resident's activity and detect falls. Emergency calls are managed by a battery operated cost effective system which is easy to install and requires only a wide area communication interface Continuous analysis of the data is done by the gateway. Relevant data is broadcast, and the built-in wireless wide area network connection is used to send out a notification for help as soon as any critical event is detected. In order to remotely monitor vital signs like: Blood pressure and weight additional devices can be used in conjunction. of such a system are rhythm monitoring to understand the cardiac role of unexplained symptoms can be understood better using a rhythm monitoring system. Other clinical applications of such a system include arrhythmia medication therapy to monitor treatment effectiveness, post ablation procedure to monitor cardiac rhythm, vitals monitoring i.e. to monitor cardiac rhythm respiration and activity remotely in the hospital or at home and discharge for heart failure to monitor rhythm and respiration.[12]

VI. CONCLUSION

As the examples in this paper make clear, the long predicted IoT revolution in healthcare is already underway. And, as new use cases are emerging, they continue to address the urgent need for affordable, accessible care. Meanwhile, the IoT building blocks of automation and machine-to-machine communication continue to be established. The addition of the service layer forms the complete IoT infrastructure. This revolution is characterised by providing end-to-end processing and connectivity solutions for IoT-driven healthcare.

VIII References

[1] L. Mainetti, L. Patrono, and A. Vilei, “Evolution of wireless sensornetworks towards the internet of things: A survey,” in Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on. IEEE, 2011, pp. 1–6.

[2] Harvard University. CodeBlue project: Wireless Sensor Networks for Medical Care. Available: http://www.eecs.harvard.edu/~mdw/proj/codeblue/

[3] I.F.Akyildiz,W.Su,Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (2002) 393– 422.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, T. Razafindralambo, A survey on facilities for experimental Internet of Things research, IEEE Communications Magazine 49 (2011) 58–67.

[5] Jayavardhana Gubbi, Rajkumar Buyyab, Slaven Marusic, Marimuthu Palaniswami. 24 February 2013. Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems 29 (2013) 1645–1660.

[6] David Niewolny. 18 Oct 2013. How the Internet of Things Is Revolutionizing Healthcare, Freescale Semic Mikhail Simonov, Riccardo Zich, Flavia Mazzitelli. Personalised healthcare communication in Internet of Things.

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

[8] O. Vermesan and P. Friess, " Internet of Things Strategic Research and Innovation Agenda," Internet of Things-. Converging technologies for smart environment and Integrated Ecosystems: River Publishers, 2013, pp. 54

[9] Zhibo Pang, "Technologies and Architectures of the Internet-ofThings (IoT) for Health and Well-being," Doctoral Thesis, KTH – Royal Institute of Technology Stockholm, Sweden, January 2013.

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

[11] Satish Ram, “Internet-of-Things(IoT) Advances Home Healthcare for Seniors ," (Embedded Intel), [online] March 26th 2013 www.preventice.com/bodyguardian/clinicalapplications/ (Accessed: 23 August 2014).

[12] L.Atzori, A.Iera, nad, G. Morabito. ”The internetOfThings“:Asurvey,”Vol.54,no.15,pp27872805,Oct. 2010”IEEECommun.Magsurvey,”Vol.49,no.11,pp30-31,Oct.2011

[13] D. Christin, A. Reinhardt, P. S.Mogre, and R. Steinmetz. Proceedings of the 8th GI/ITG KuVS Fachgespräch “Drahtlose Sensornetze” (FGSN), pages 31–34, 2009.

Authors Profile

Mr. P K Mishra pursed Bachelor of Engineering from Bijupatnaik University of Technology, Rourkel,Odisha in 2005 and Master of Tecnology from IIIT Bhubaneswar Universityin year 2010. He is currently working as Assistant Professor in Department of Computer Sciences, Cenurion University Odisha, since 2012. He has published more than 10 research papers in reputed international journals including Thomson Reuters & Web of Science and conferences and it’s also available online. His main research work focuses on IOT, Network Security, softcomputing and. He has 7 years of teaching experience

Dr. Manoranjan Pradhan holds a Ph.D degree in Computer Science from Sambalpur University. He obtained his M.Tech in Computer Science from Utkal University in 2004, MCA from Utkal University in 1999 and M.Sc from Berhampur University in 1996. He is having 14 years of teaching and research experience. He is presently working as Professor and Head, department of CSE, Gandhi Institute for technological advancement (GITA), Bhubaneswar, Odisha, India. He is a member of CSI(I), ISTE(I) and OIS(I). He has published about 15 papers in International and national journals and conferences. He has also published 2 books to his credit. He is a program committee member of various international conferences. He is acting as a member of various international journals. His active area of research includes Computer Security, Intrusion Detection System, Computational Intelligence, Mobile Adhoc Network, Cloud Computing, Social Networks etc.

Dr. Mrutyunjaya Panda holds a Ph.D degree in Computer Science from Berhampur University. He obtained his Master in Communication System Engineering from Sambalpur University, Bachelor in Electronics and Tele-Communication Engineering from Utkal University in 2002, 2009, 1997 respectively. He is having 13 years of teaching and research experience . He is presently working as Reader Computer Science in Utkal University Odisha.He was professor and Head, department of ECE, Gandhi Institute for technological advancement (GITA), Bhubaneswar, Odisha, India. He is a member of IEEE(USA), KES(Australia), IAENG(Hong Kong), ACEEE(I), IETE(I), CSI(I), ISTE(I). He has published about 45 papers in International and national journals and conferences. He has also published 5 book chapters to his credit. He is a program committee member of various international conferences. His active area of research includes Data Mining, Intrusion detection and prevention. Social networking, Mobile Communication, wireless sensor networks etc.