**IoT Based Health Care Monitoring System**

1\***Dr. S. Suresh Kumar**, 2Dr. S. Prasad Jone Christydass, 3S. Saranya

1,2Associate Professor, 3Assistant Professor

1,2 ECE, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India.

3EEE, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India.

1\*sureshkumar.67014@gmail.com, [2prasadjones.ece@gmail.com](mailto:2prasadjones.ece@gmail.com), 3[charanyasuccess@gmail.com](mailto:charanyasuccess@gmail.com)

**Abstract**

This chapter extensively examines literature pertaining to remote health monitoring through IoT technology. It extracts valuable insights and identifies critical research gaps. IoT facilitates seamless connectivity, allowing the integration of physical entities with digital systems using wearable devices, sensors, RFID, and NFC technology. Numerous IoT-driven healthcare concepts are present in the literature, primarily theoretical. However, these conceptual frameworks offer valuable ideas for improving healthcare accessibility, particularly for rural populations lacking affordable medical services. This thesis addresses shortcomings in existing architectures: the absence of a practical smart bed framework linking village primary healthcare centers to patients with wearable devices for remote vital sign monitoring, the need for practical implementation, and the imperative of end-to-end security and privacy for sensitive healthcare data. Subsequent chapters delve deeper into the research conducted.

**2. Introduction**

People from all areas of life are being influenced by the development of new technology. The Internet of Things (IoT) is a collection of many cross-disciplinary technologies that made it possible to integrate the physical and digital worlds. There are numerous use cases that have the potential to actually change the world. However, one of the IoT integration use cases that has the greatest influence on people is the healthcare sector. For the people who cannot afford the time or money for healthcare services, remote health monitoring is highly wanted. This chapter's study of the literature on various aspects of the development of healthcare units with IoT integration for the provision of remote health monitoring services was centred on this context. It sheds light on the functions of mobile computing, RFID and NFC-type technologies, ECG signal analysis, SOA-based IoT messaging, the benefits of the cloud, potential IoT applications in the healthcare sector, IoT and robotics, cyber-physical systems, and security and privacy issues related to healthcare systems.

**2.1 SUITABILITY OF THE INTERNET OF THINGS FOR HEALTHCARE UNITS**

Healthcare organisations require immediate access to patient health data. Therefore, in addition to specific identifying technologies like RFID and NCS, they require a form of technology that supports 24x7 availability, sensing, Internet, and communication. Important characteristics of IoT technology include connections at any time, anywhere, and with anything. Thus, in addition to delivering availability and scalability, it enables healthcare apps to access live patient health information without regard to time or location. Technology also makes it possible for many items to communicate with one another. It facilitates communication between PCs, Things to Things (T2T), Humans to Things (H2T), and Humans to Humans (H2H), for example. This hypothesis is depicted according to [1]. The Internet of Things (IoT) technology and its quick advancements assist in linking intelligent items via the Internet to offer interoperable services in a scattered setting. According the usage of IoT in the healthcare industry and other sectors leads to an exponential growth of data [4].

It is difficult to manage big data and have ubiquitous data access. Additionally, having access methods in the presence of many data formats is tiresome. Boyi Xu and colleagues investigate the resource-based data accessing technique known as UDA-IoT in the healthcare industry. In order to exploit data acquired from various IoT sources, they investigated "the methods and means to have integrated approach in healthcare information system. For the purpose of storing and interpreting IoT data, they created a semantic data model. Stakeholders get quick access to data on emergency medical services thanks to the UDA-IoT. In a case study titled emergency medical DSS (Decision Support System). "The medical DSS is used to handle emergency medical events with the DSS," they wrote. Real-world entities, alternative alternatives, entity- and transition-oriented models, persistency, an execution engine, and cloud IoT data access services are all included in the implementation. In order to make educated judgements, doctors and system managers in the healthcare industry can leverage IoT data sources.

As part of the IoT, concentrated on gateways that are used to connect sensor networks and the Internet [5]. These gateways are used to offer services like embedded data mining, local real-time data processing, and higher level local storage. In addition, Gateway may deal with a variety of difficulties, including energy efficiency, scalability, and dependability. They found that "IoT based health monitoring in hospitals can bring about reliability, security, interoperability, performance, and energy efficiency" after doing study with a suggested design. IoT-aware smart architecture was suggested by [3] for autonomously monitoring and tracking hospital equipment, patients, and staff. RFID, Wireless Sensor Networks (WSN), and smart phones all have significant roles to play in its architecture. In order to have secure remote access to the healthcare infrastructure, a virtual private network (VPN) is used. The future potential of IoT was highlighted by [2]. "Schematic overview of IoT that is used for sensing, analytics, and visualisation tools" was supplied. [6] completed similar work. To illustrate the necessity of IoT. offered a case study. In order to monitor food contamination and related challenges for human health, suggested an architecture for the Internet of Things [6]. Different IoT implementations and their semantic interoperability were explored by [7]. They also looked into "the need for ontology" in order to effectively implement IoT. They provide details on "health ontologies" that represent the representation of medical knowledge.

The Internet of Things (IoT) can bring together business owners, government officials, common people, medical experts, smart homes, smart transportation, community and national installations like defence, remote sensing, smart grid, infrastructure, and other utilities. Big data, according to Mohak Shah, is inextricably linked to the Internet of Things since the latter generates vast amounts of data that must be handled [8]. IoT was described by as a tool for sharing information, providing support, and making strategic decisions. In order to reduce health difficulties, found that rural health can benefit from QoS and QoE [9]. The "importance of education in the area of healthcare and emerging technologies" that can be used to improve human life quality was emphasised.

An IoT-based m-Health scenario was proposed by [10]. The phrase "an architecture based on mobile devices and healthcare infrastructure to form an intelligent personal assistant (IPA)" is used. The introduction and widespread use of mobile devices opened the door for IPA applications in the real world. These programmes are primarily related to the healthcare industry. "Autonomous collection of data related to location of the patient, fall detection, heart rate, and so on" is made possible by this method.

"Meta heuristic algorithms pertaining to healthcare, including challenges and issues therein" was the topic of. They looked into the usage of support vector machines (SVM), ant colony optimisation (ACO), genetic algorithms (GA), and particle swarm optimisation (PSO) in healthcare systems. Additionally, they offered a framework for big data analysis in the context of the healthcare industry.

People need to be educated about IoT, according to [11]. According to [12], "wearable devices are growing every year. To service patients in healthcare facilities, they have sensors. They promoted the use of wearable technology for health-related purposes. The topic of "Health Internet of Things (HIoT)" was the focus of. "Wrist-worn devices, heart rate monitors, pulse oximeters, glucose monitors, and stethoscopes" are some of the relevant technologies mentioned for the implementation of HIoT. The integration of "Bluetooth, Wi-Fi, and RFID" is present in all of these gadgets. They also offered views on the expenses of data transfer associated with IoT integration in healthcare. They provided indicators for gauging the effectiveness of data transport.

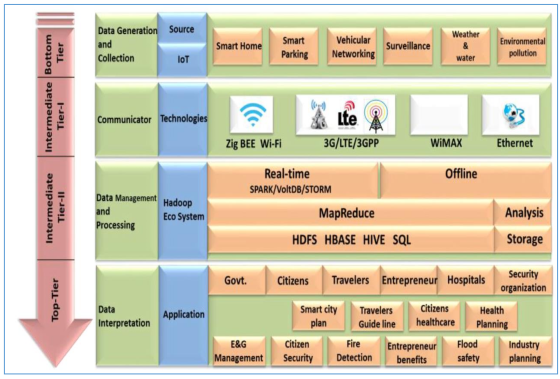
Health information technology (HIT) and electronic medical records (EMR) should be in place when healthcare units are integrated with IoT, according to[10]. An overview of IoT integration with health infrastructure for monitoring was presented by [11]. IoT can only be realised with the help of five technologies, according to Lee & Lee [13]. RFID, Wireless Sensor Network (WSN), Internet of Things Middleware, Cloud Computing, and IoT Application Software are a few of them. Noted the need of the semantic web in addressing IoT and WoT needs. They said that semantic technologies offer advantages such simple interconnection, new knowledge deduction, and interoperability. On the other side, present difficulties in such integrated systems [12]. The difficulties include interoperability, digital divide, security and privacy, and knowledge empowerment [14]. Healthcare organisations can benefit greatly from the Internet of Things (IoT). Healthcare is one of the several domains for which Dijkman. suggested a business model framework using IoT [15]. The framework encourages creative thinking in new IoT-based business models.

**2.2 MOBILE CLOUD COMPUTING (MCC)'S IMPACT ON REALISING THE INTERNET OF THINGS IN HEALTHCARE UNITS**

Cloud computing, wireless networks, network operators, mobile consumers, and cloud service providers are just a few of the components that make up mobile cloud computing. The use of MCC in healthcare services was investigated by [16]. Wearable devices can access patient health information in real time thanks to the integration of MCC with body area networks, according to their statement. Furthermore, since they can outsource storage and calculations to the cloud, devices involved in MCC do not require substantial resources in terms of memory capacity and CPU performance. Many benefits, including a rich user experience and features, effective performance, patient-centric services, and increased reliability, are offered when MCC is linked with wearable device networks. Mobile devices and patient-used body sensor nodes build a network inside the hospital. Such a network then uses access points or base stations to connect to the Internet. The healthcare network can then use the Internet to access cloud and mobile application servers. Patients' vital signs can be saved on servers that store data, and they can be processed for diagnosis using the appropriate algorithms. Physicians can then use the information they have about their patients to provide real-time care. In line with Hiremath. Due to its support for outsourcing storage and processing to the cloud [17], MCC can lessen the load on smartphones.

The significance of "MCC in the context of IoT and healthcare integration" was examined by MCC has drawbacks in terms of privacy, security, connectivity, performance, and latency [17]. For the integration of smart cities, IoT, and big data analytics,. presented an IoT-based system [18]. IoT applications for healthcare facilities were given particular attention. "Urban development, big data analytics, and smart city development" are all included in their proposal. They developed a 4-tier architecture, which is shown in Figure 2.1.

To meet the demands of IoT integration with various applications, there are three and four layers. Among the technologies employed are those for communication, data generating, data collection, data administration, data processing, and data interpretation. In order to raise people's quality of life, they investigated the effects of big data analytics on health organisations [19]. The necessity for lean in healthcare was noted by [20].



**Figure 2.1 shows a 4-tiered Internet of Things system for use in healthcare and other applications.**

**2.3 RFID, EPC, AND BARCODE PLAY IMPORTANT ROLES IN IoT-BASED HEALTHCARE UNITS**

According to [15], RFID and RFID readers are crucial components of the hardware abstraction of smart e-Health gateway design. "RFID is a low-power and low-cost technology that includes devices, referred to as tags, for participating in computations by sending information to RFID readers," claim [15]. RFID tags are appropriate for Internet of Things applications since they don't use any energy and have a long lifespan. Ultra-High-Frequency (UHF) RFID is a different variety of RFID with extra features, such as computing and sensing. The monitoring and transmission of patients' vital signs to doctors is simple, zero-energy, and inexpensive when using RFID enabled sensing in healthcare facilities. RFID tags are used to merge sensing and computational capabilities. RFID tags function within the reader's range of coverage. RFID technology is only used for monitoring medical equipment or patients.

According to Fernandez and Pallis, IEEE 802 standards, ZigBee, Bluetooth, Ultra Wide Band (UWB) networks, RFID networks, WPAN, and standards for cellular networks like GSM, GPRS, LTE, HSPA, and UMTS all play a significant role in wireless technology.

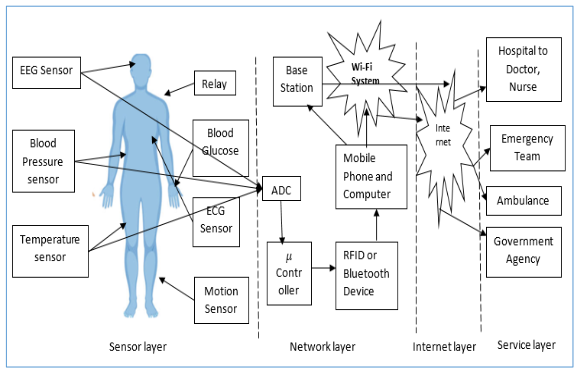
IoT integration with healthcare infrastructure has been made possible [14]. In addition to examining e-Health technology, [15] also shed light on RFID technology. They believed that RFID played a significant role in the development of IoT and its integration with the healthcare infrastructure. RFID is actually required to identify any physical object that participates in computers, including medical equipment. A complex RFID system requires several parts. They comprise the antenna, host computer or device, RFID tag, RFID reader with RF module, and antenna.

Objects are identified via tags. In addition, tags offer details such object position, physical data changes, and data transmission to an antenna. There are three different kinds of tags: passive, active, and semi-passive. While passive tags lack their own power supply and have a smaller read range, active tags have an inbuilt power supply and a longer read range.

**2.4. RFID-BASED REMOTE HEALTH MONITORING SYSTEM**

One method for identifying objects and devices in an IoT integrated system is Radio Frequency Identification (RFID). Figure 2.2 illustrates the remote health monitoring method that [17] suggested. RFID is a technology that uses radio waves to uniquely identify items. The technology at the very least has an antenna, an RFID tag, and an RFID reader. Reader uses an antenna to transmit a signal of interrogation to the tag. The RFID tag then replies with the data it contains. RFID tags can be either active or passive, depending on the availability of a power supply. Power and space are required for active RFID tags, and they can support a range of up to 100 metres. Numerous real-time sectors can benefit from the long range. Active RFID tags, for instance, can aid with logistics and asset location. On the other hand, passive RFID tags rely on the electromagnetic energy of RFID readers instead of having a power source. Passive RFID tags can only operate at a 25-meter range due to power limitations.

The three frequency bands where passive RFID tags function are as follows. They have the abbreviations Ultra High Frequency (UHF), High Frequency (HF), and Low Frequency (LF), with a frequency range of 125 kHz to 960 MHz, respectively. NFC is operated on the protocols and standards that are based on RFID as stated in the ISO/IEC 14443. NFC devices operate with 13.56 MHz, which is similar to the HF RFID. As a result, RFID proximity cards use these standards. As a more precise form of HF RFID, NFC benefits from the frequency's short read range disadvantages. The distance between NFC devices must be a few millimetres or less. Because of this, NFC is now widely used for private communication between mobile devices like smartphones.



**Figure 2.2 shows an integrated IoT system for remote health monitoring.**

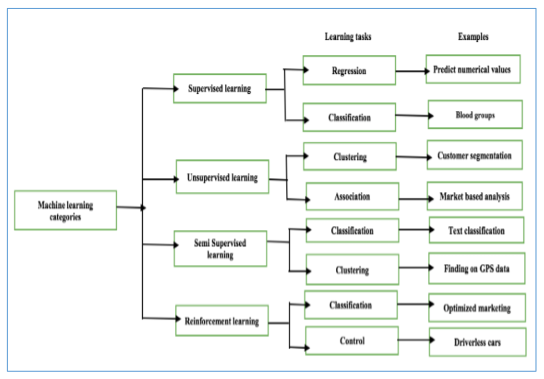
NFC differs from RFID devices in that it permits peer-to-peer communication. It does imply that an NFC gadget can serve as both a reader and a tag. NFC consequently gained popularity for contactless payments. Due to this, numerous players now. The mobile industry will concentrate on NFC use in the newest devices. When two smartphones are tapped together, NFC-enabled devices can also offer quicker and more convenient communication. NFC is also being used by smart posters in the advertising sectors. NFC devices can scan passive NFC tags. Additionally, some NFC devices may be created in a fashion that allows them to read passive HF RFID tags that are compliant with ISO 15693. Additionally, NFC tags may contain commands that launch specific mobile applications. Increased use of HF RFID tags and NFC tags in many contexts, such as posters, signs, and adverts, makes it possible to effectively inform consumers. To recap, NFC is based on HF RFID, and the latter's range restrictions have been transformed into a distinct benefit for near-field communication. Because of the NFC's distance restrictions, RFID is preferred in this work for the empirical study.

The system depicted in Figure 2.2 includes a number of sensors, including EEG, blood pressure, temperature, relay, blood glucose, ECG, and motion sensors. Analogue to Digital Converter (ADC) is used to convert analogue signals from the sensors into digital signals. The base station will get the sensed data. Different stakeholders, including government organisations, ambulance services, emergency response teams, and physicians, can access it via the base station over the Internet. The system is composed of four layers. The sensor layer, network layer, internet layer, and service layer are some of their names. The system has various benefits, including time savings for patients, real-time health monitoring, and cost savings. The proposed system is discussed conceptually. However, it does not offer security measures and does not have any empirical research.

**2.5 WEARABLE SENSORS AND MACHINE LEARNING IN HEALTHCARE**

In the healthcare sector, wearable sensors have gained a lot of popularity. They can gather vital signs from patients and give doctors the data they need to make wise judgments. IoT and cloud computing are combined in the healthcare management system that. [18] suggested. Wearable sensors are used to gather data from the human body, and data analytics are used by the system to deliver a clinical diagnostic or prognosis. Figure illustrates the system.

In order to achieve better results with data analytics, the system uses both historical data and current data. The cloud-based diagnosis system is the one that uses machine learning methods. Artificial intelligence (AI) and the newly growing area of data science both include machine learning methods. They are employed to address various issues in the actual world. Prediction of heart disease is not an exception. Various algorithms have been reported to be effective in the literature for heart disease prediction. They are, however, data-driven strategies. For classification algorithms to be improved, feature extraction, feature selection, and feature optimisation are crucial. Based on the training that has been given to them, classification algorithms are capable of performing prediction tasks. They are referred to as supervised machine learning algorithms as a result.



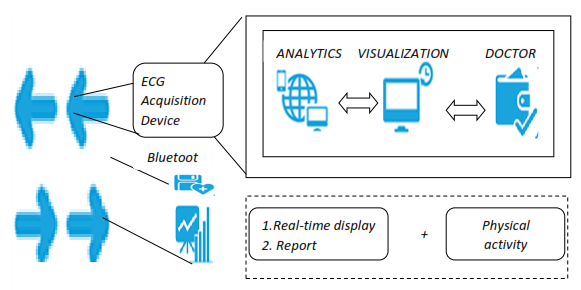
**Figure 2.3 shows various machine learning methods**

The categories of machine learning include supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning, as shown in Figure 2.3. Regression and classification are two data mining tasks that can be completed using supervised learning techniques. While classification is used to make predictions or divide a sample into classes, regression is used to forecast the connection between dependent and independent variables. Association mining and clustering are examples of unsupervised learning problems. The former is utilised to cluster or group related things. One illustration of the same is customer segmentation. On the other side, association rule mining can be used to examine and comprehend data trends that suggest potential client behaviour. Classification and clustering are two examples of semi-supervised learning. Examples include text classification and locating GPS data, respectively. On the other hand, classification and controlling are used in reinforcement learning. An example of control is a driverless car, while an example of classification in terms of reinforcement learning is optimised marketing. These ML techniques are frequently applied in medical applications. Regression is applied to the patient's medical records, previously sensed data from wearable body sensors, and recently sensed data or classification is required to establish a connection between the dependent and independent variables and to finish the diagnosis.

**2.6 ECG SIGNAL ANALYSIS FOR REMOTE HEALTH MONITORING**

IoT can link the analogue and digital worlds. A new IoT subtype known as Wearable IoT (WIoT) has emerged with the rise of wearable medical equipment. This kind of network can help medical practitioners track patient health data so they can offer individualised wellness and healthcare. The WIoT architecture was presented by [14]. There are three main parts that make up the WIoT. Wearable body area sensors, Internet-connected gateways, cloud and big data support are some of them. Medical infrastructure is connected to body-worn devices. Therapeutic sensors, on-body contact sensors, health and wellness sensors, behavioural sensors, and rehabilitation sensors are the several types of body area sensors. Sensors used in rehabilitation encourage language learning and assistive technologies for the blind. Behaviour sensors keep an eye on things like fall, sleep, and exercise, as well as feelings like tension, worry, and despair. They also keep an eye on things like calorie intake and eating patterns. Fitness and wellness sensors track movement, including calorie intake and physical activity, as well as location, including indoor localization and GPS data. Therapeutic sensors keep an eye on emergency situations like defibrillators, drug distribution, and stimulation for chronic pain treatment.

ECG is a crucial factor in determining heart health. It is frequently employed in the healthcare sector. However, it takes time, requires effort, and costs money to transport a patient to the hospital. It is feasible to obtain a patient's ECG in real time from a distance using IoT connectivity. He examine this idea, as seen in Figure 2.4 [18]. The patient's ECG data is acquired utilising an ECG acquisition equipment and an IoT-integrated application. When the data is brought into a system for data analytics, a doctor is shown the results visually.



**Figure 2.4: ECG signals used for remote health monitoring**

The patient, who is located in a remote area, provides the real-time data. The data is then used for analytics, leading to a diagnosis. This type of system is highly technological, and IoT is required to realise the system that offers real-time reports and displays. It can occasionally be used to determine a patient's level of physical activity. Physiological measurements like ECG, EMG, and EEG, chemical measurements like perspiration, saliva, and glucose, and visual measurements like oximetry are all handled by monitoring sensors. In the future, personalised healthcare services will be crucial. The potential for individualised health care in smart homes was raised by [15]. They put out an architecture to deliver individualised medical treatment. "Sensor devices, M2K gateway, communication technologies, cloud storage, and access control mechanisms" are all part of the design. Google cloud messaging uses push notifications to enable real-time messaging.

**2.7 SYSTEM FOR REMOTE HEALTH MONITORING USING RASPBERRY PI**

The technology that connects IoT, health monitoring, and smart homes is Raspberry Pi. Saha and colleagues explore this claim. It is a cloud-based solution that makes use of numerous wearable sensors. The sensors are an IR sensor, an accelerometer sensor, a blood pressure sensor, a respiration sensor, and a temperature sensor. These sensors are coupled with Raspberry Pi technology, which transmits the collected data to the cloud. Wherein data may be studied from, the results of which can be transmitted to the appropriate authority in the form of an SMS text message, email, or web application.

Applications for remote health monitoring can be integrated with smart homes using a straightforward architecture. Home telehealth is "the process of utilising telecommunication technologies by patients and healthcare service providers to have fair exchange of information related to healthcare," according to the definition. They investigated the potential application of IoT to achieve home telehealth [15]. They suggested a system called CogSense for enabling real-time healthcare services with teamwork between patients, carers, and doctors. Their system consists of sensors that track patient health, communication technology, and data processing that aids in better decision-making. It is feasible to have realisable services with customised data storage and retrieval using a cloud-enabled strategy. According to [21]., "IoT can help to obtain embedded intelligence for medical services" [22].

**2.8 SMART IOT MODULAR APPLICATION FOR REMOTE HEALTH MONITORING**

If heterogeneity in data and devices as well as insufficient worldwide standards are addressed, Fernandez and Pallis' study of the opportunities and constraints of IoT integration with healthcare units revealed that IoT provides the way for increasing QoS in healthcare services [24]. Regarding emphasising opportunities and problems in IoT-based healthcare systems. have done similar work [23]. In light of this, they made use of IoT architecture to implement a modular healthcare application [24]. The system is made up of a variety of modules. They are referred to as the interface module, the main module, and the sensor module. The purpose of the first module is to collect data from patients whose health is being tracked. Information from the patient is collected using a variety of wearable sensors. After basic processing, the data is transmitted to the main module. The primary module does data analysis, and the output is saved in the cloud. Data from the cloud can be obtained by stakeholders after proper authentication. The system has been conceptualised and is realised in theory. To be evaluated, it requires empirical research, though.

**2.9 IoT MESSAGING BASED ON SOA**

An architecture called Service Oriented Architecture (SOA) facilitates the interchange and integration of diverse applications. This technology comes highly recommended for implementing IoT in distributed environments. The "Shortest Processing Time (SPT) for optimal scheduling of IoT messages" technique was a suggestion made by Jenq Leu [25]. A queue is used in the scheduling, which stabilises the messaging task. They took into account Internet-connected IoT devices that are accessed by distant IoT clients. An Internet of Things (IoT) device includes a variety of components, including sensor nodes, RFID cardiographs, Bluetooth blood pressure (BP) monitors, and others. The components are broken down into actuator, broker, adapter, and sensor categories. A sensor is used to gather environmental data. Actuator puts controller-issued instructions into effect based on user requests or information picked up by sensors. Broker acts as a liaison between the sensor and the actuator. Applications and devices can be seamlessly integrated with the aid of SOA and AJAX technologies.

**2.10 CLOUD MIDDLE-WARE SERVICES FOR IoT WITH HEALTHCARE INTEGRATION**

Regarding cloud computing, middleware servers are located online and provide good service to end users. Cloud middleware services can assist many businesses that operate in related industries to collaborate for organic growth. Cloud-based middleware services can be coupled with many healthcare platforms. Cloud middleware services were examined by [23]. Cloud middleware is used to integrate several healthcare platforms. By combining heterogeneous service technologies, he proposed a method for creating IoT middleware [22]. The authors claimed that "Service Oriented Computing (SOC) and RFID play important role in realising IoT services and middleware". They concentrated particularly on SOC and its advantages when used to construct middleware for IoT. Because SOC permits interoperability, it is feasible to develop middleware that can meet the requirements of the heterogeneous IoT environment.

The "functionality of middleware used for IoT" was researched by [23]. They claimed that it functions as interoperable services to interconnect heterogeneous applications [16]. Different IoT middleware, including UBIWARE, SOCRADES, UBISOAP, ISMB, and WHEREX, were compared. The characteristics that are compared between them are context awareness, security and privacy, interoperability, and portable platform. The IoT uses the ZigBee, Bluetooth, sensor, RFID, and WIFI interface protocols.

**2.11 POTENTIAL INTERNET OF THINGS (IOT) APPLICATIONS IN HEALTHCARE UNITS**

When IoT is connected with health infrastructure, healthcare units can use a variety of apps to serve patients in a stylish manner. Potential uses of the Internet of Things in the healthcare industry, according to Nomusa, include "ambient-assisted living, chronic medication management, telemedicine, disease surveillance, oral health management, baby care, sport and fitness, emergency services, community and health-based care, mental health, nutrition, occupational health, environmental health, heart disease care, and diabetes management" [13].

An architecture called "CloudIoT for integration of cloud computing and IoT" [16] was proposed. It was discovered that the integration of cloud computing with IoT was insufficient and required more investigation. As a result, they suggested "CloudIoT for realisation of the integration". Nomu shed light on potential uses of IoT and associated technologies in South African healthcare systems [13]. Diabetes management, heart disease management, occupational health, nutrition, mental health, home and community-based healthcare, emergency services, sports and fitness, baby care, oral health, disease surveillance, telemedicine, chronic medical management, and ambient-assisted living for the elderly are among the applications.

**Assisted Ambient Living**

As life expectancies have increased, there are more elderly individuals in many nations. To live an autonomous and independent life as adults, they require particular care. Ambient-assisted living can be achieved with IoT technologies in healthcare facilities. IoT and healthcare infrastructure, in particular for elderly people, offer services that can raise adults' quality of life. One of the platforms for ambient assisted living is Caalyx-MV. It provides provisions for offering adult population healthcare services. The home system uses a variety of computing equipment to accomplish this.

The ambient-assisted living platform has several devices or components for elderly persons. Among them are a smart T-shirt, a weight bridge, a blood pressure cuff, a video camera, a TV, a data logger, WiFi, a set-top box, and a modem for mobile devices. UMTS, the internet, and surveillance. Healthcare services, professional care services, and assistance to family and friends are among the care services offered to elderly. The services are delivered online [9].

Another system for promoting "ambient-assisted living" is CONFIDENCE. It utilised body-mounted radio tags. The technology has the capacity to track patients, rebuild their posture, and identify any anomalies. It can recognise falling and being ignored. It is aimed at persons over 65 who are elderly. Elderly individuals can live comfortably and with confidence if CONFIDENCE is in place [9].

**Managing Chronic Medication**

Patients needing long-term pharmaceutical management are those with chronic illnesses. If the patient doesn't comply in this way, it could have fatal repercussions. Additionally, it raises the price of additional medical services and prescription drugs. Chronic medication tracking is achievable with IoT connection. RFID can be used to connect to medical devices and monitor movement. In this instance, "automatic information acquisition" uses both RFID and EPC. It is feasible to assist patients with chronic diseases in receiving the best medication as prescribed by doctors with the use of these technologies as part of the Internet of Things. Using "supply chain of medicine and monitoring" as a visual aid can enhance the quality of services provided for managing chronic medication use.

**Telemedicine**

Telemedicine, in the words of the World Health Organisation, is "the practise of medical care using audio visual interactions and data communications that includes finding the cause of the problem, education, transfer of medical data, diagnosis, and treatment" [10]. Various healthcare organisations' divisions offer telemedicine. Typically, patients call from home using the Internet. Services providers answer these calls. Then, service providers take the initiative to involve a qualified doctor in analysing, diagnosing, and resolving patient problems. The "predominant in this kind of application where patients can interact with service providers and get advice from experts without leaving the comfort of home" is voice-based communication. Along with saving time and money, this can boost their confidence and morale.

**Monitoring of diseases**

Strategies to stop disease outbreaks can be made better with the aid of disease surveillance. Governments and healthcare organisations can leverage IoT-enabled healthcare services for disease surveillance. Google Flu Trends is a programme that tracks online activity and keeps an eye out for influenza epidemics. When compared to experts in healthcare systems, Twitter can promptly identify "cholera outbreaks" in the same way. An application called Health Map can track global disease trends [17]. It can offer information on epidemics in the user's current location or any other location they might be interested in. It gives consumers timely warnings about various ailments and their severity. These services can become real-time and more accurate and high-quality with IoT integration. The Health Map application makes use of GIS, GPS, and RFID technologies.

**Management of Dental Health**

This is connected to dental illnesses and oral health. Given the connection between conditions including diabetes, respiratory illnesses, cardiovascular diseases, and pregnancy difficulties, preventive dental care is crucial. Management of oral health is made simpler by technology in place and IoT connection with healthcare infrastructure [13].

**Child Care**

As a baby develops into an adult, providing for their needs is crucial in every culture. In order to shield infants from diseases, efforts are required. To name a few, "measles, tuberculosis, and polio" are only a few of the diseases for which "immunisation and vaccination" are crucial. RFID tags and sensors can enhance the standard of newborn care. For the purpose of providing neonates with immediate care, it is crucial to monitor body temperature and other vital signs. Baby's quality of life can be enhanced by location-based services and transportation. This makes use of IoT in healthcare facilities [13].

**Exercise and Sports**

With IoT-enabled healthcare services, it is feasible to monitor one's health and lifestyle. Nomusa examined how mobile programmes like "EndoMondo Sports Tracker" can assist athletes in having mobile programmes connected to sensors to track their activity. The programmes may monitor not just actions but also the amount of time spent, speed, and other factors. Additionally, Google Maps is integrated into the application. An additional Android smart phone software called "CardioTrainer" uses GPS tracking to record athletes' fitness activities. IoT-related devices and software alert athletes in real time via voice messages regarding time, cycles, and other information.

**Crisis Services**

The distance between the healthcare facility and the patients' homes frequently causes medical services to be delayed. Arriving at the hospital takes longer than expected. Involvement also involves time and money. If there is no backup plan in place, the same thing may happen in an emergency as well. To solve this issue, healthcare-related IoT applications can be modified to enable real-time patient monitoring from either the patient's home or while they are travelling. Even before a patient arrives at the hospital, care can begin. The sensor technology, IoT mobile nodes, and healthcare infrastructure all work together to provide real-time communication between various stakeholders. Real-time delivery of the patient's vital signs is made feasible via machine-to-machine interaction. Healthcare services are significantly impacted by this [13].

**Community-based healthcare**

People who are connected to communities have a higher quality of life thanks to community-based healthcare services. When patients are not advised to move for whatever reason, these services are given at home. Patients with chronic illnesses and those who are physically disabled, for example, can use these services. With the development of technology, "NFS-enabled devices" now provide patients an easy-to-use interface. These technologies can be employed to guarantee better healthcare services because NFS and RFID are compatible [13].

**Mental Wellness**

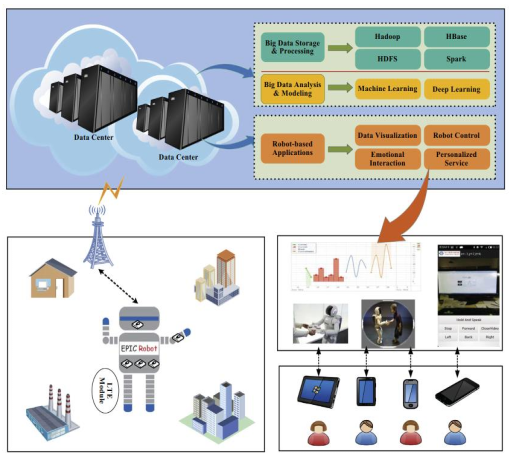
The care of mental health is frequently neglected. In other words, it goes undiagnosed and is ignored. According to [13], integration of IoT applications with healthcare can alleviate this issue. Some mental health conditions, including "Generalised Anxiety Disorder" (GAD), result in long-term problems for people. To treat such illnesses, behavioural, cognitive, and physical techniques are required. The use of biofeedback, educating patients through various programmes, and bringing their awareness of their own responses to circumstances all contribute to a great deal of issue solving.

**Nutrition**

Another crucial component of healthcare services is nutrition. When it is ignored, it causes a variety of illnesses. IoT-based techniques with healthcare facilities can offer information and prompt counselling to ensure that people's nutritional issues are addressed. With IoT applications connected to healthcare infrastructure and patient wearable devices, it is possible to address nutrition-based allergies and their impacts [13].

**2.12 HEALTHCARE UNITS USE IOT AND ROBOTICS**

Robotic systems based on "Long Term Evolution" (LTE) approaches were studied by [14]. They discovered that robotics is appropriate for applications requiring a lot of bandwidth in order to improve Quality of Service (QoS) and Quality of Experience (QoE). The use of robotics in healthcare facilities has several benefits, including improved communication and increased intelligence. Robots powered by LTE can gather physiological data and offer real-time or emergency reaction with video communications. The potential for extended intelligence increases with wearable sensor devices or any sensor device connected to a healthcare unit can gather data and send it to the cloud, which offers endless storage and processing options. Sensors and cameras can be included into healthcare robots to provide stakeholders with real-time data. Figure 2.5 depicts the LTE-based mobile robot system suggested.



**Figure 2.5. LTE-based mobile robot framework**

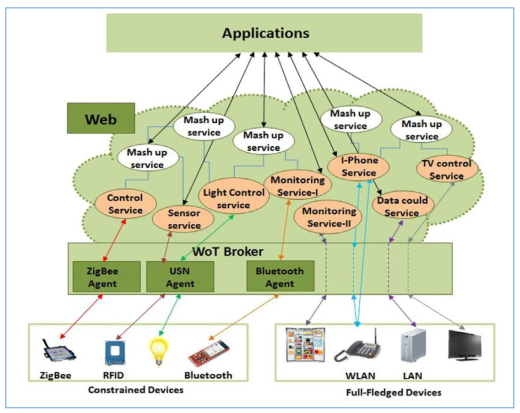
The robot framework, as depicted in Figure 2.11, comprises robots and other intelligent devices connected as a network and they are managed by an application. The data from the robot's many sensors is stored on the cloud. Analytics and decision support systems can exploit this data.

**2.13 IOT-ENABLED CYBER-PHYSICAL SYSTEM**

IoT integrates the physical and digital worlds to create a smart cyber society. The idea of a smart cyber society was put up. as a platform with many communication levels [15]. To create a smart cyber society, the Internet of Things (IoT), Cloud Platform System (CPS), and Web of Things (WoT) are used. They looked into the system while keeping in mind several factors, such as emergencies, healthcare, safety, and security. They believed that the suggested system could enhance medical care. Additionally, they discovered that technologies like Web Services facilitate Machine to Machine (M2M) communication. When connected with CPS, they could also define the function of wearable technology in healthcare.

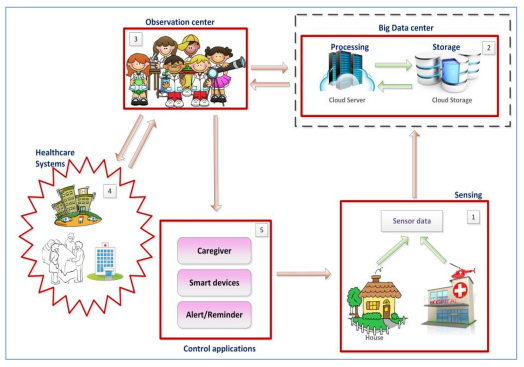
The smart cyber society architecture consists of "applications, sensor devices, and smart devices" utilised in many domains, such as healthcare units, to have integration with the web, the cloud, and other governmental organisations. To create a smart cyber society, various real-world societies, virtual communication platforms, and CPS are combined. Additionally, suggested an architecture for WoT that integrates IoT and, ultimately, a smart cyber society.

The layers of the WoT architecture are depicted in Figure 2.6. Applications are created by integrating limited devices that use technologies like "Bluetooth, RFID, and ZigBee" with fully functional devices like LAN and WLAN. The "World Wide Web Consortium" (W3C) provides a variety of web standards that are utilised in the architecture. A network of this type can provide remote patient monitoring services via WoT and IoT integration CPS.



**Figure 2.6 WoT's architecture**

Human body can use different wearable devices that provide provisions to monitor “blood pH, levels of glucose, dissolved oxygen, carbon dioxide and temperature”. With this architecture, it is possible to realize smart homes and smart cyber society. They proposed a learning system based on CPS and big data [18]. The learning system they proposed is called Topic-Oriented Learning Assistance (TOLA). The system is better than Massive Open Online Courses (MOOC) with CPS and IoT integration. they proposed a CPS for comprehensive data analytics and healthcare monitoring. In the context of big data produced by healthcare integrated IoT systems, their study assumes importance [16]. They focus on “big data analytics, IoT, cloud computing, and sensing technologies”. Their CPS for healthcare monitoring is as shown in Figure 2.7.



**Figure 2.7 CPS for healthcare monitoring**

As presented in Figure 2.7, it is evident that sensed data is sent to big data centre where data is stored. Observation systems interact with control applications and healthcare systems. The control applications are care giver application, smart device applications, and alert/remainder applications. Sensing devices are used as part of healthcare infrastructure. Big data centre is for storing huge amount of data produced by sensors. Observation centre is used by clinicians to obtain healthcare data and process it in order to gain intelligence. Clinicians may interact with other healthcare systems based on the kind of alerts generated. The observation centre sends control information to control applications which provide intended services. Yan et al. studied “the need for trust management in the context of IoT that is integrated with surveillance and healthcare domain” [16]. They studied IoT and preened it as data-centric IoT with provision for M2M and machine to human interactions.

**2.14 SECURITY FOR IOT INTEGRATED HEALTHCARE UNITS**

It is essential for IoT integrated healthcare units to have end-to-end security measures. They focused on “mobility enabled healthcare IoT for providing a scheme to enable end-to-end security” [16]. The scheme contains different aspects such as end user authentication and authorization procedures, mobility – aware healthcare network, and secures communication from sensor devices. The overview of healthcare IoT with end-to-end security.

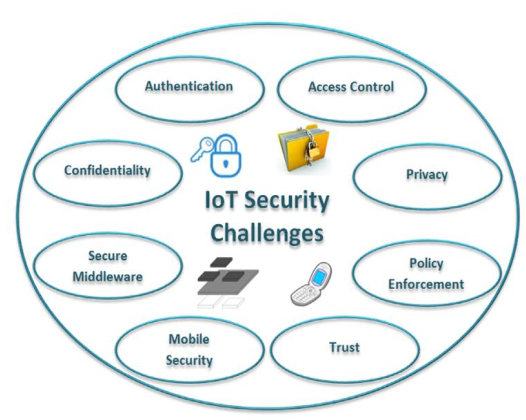
There are different layers found in the architecture. They include device layer, fog layer, and cloud layer. These layers are integrated with service providers of healthcare. Sensor devices are presented in the device layer. Smart gateways are used in fog layer while cloud services are provided by cloud layer. Elliptic Curve Diffie- Hellman (ECDH) public key encryption, digital certificates and Elliptic Curve Digital Signature Authentication (ECDSA) are used to provide end-to-end security.

They explored security related issues such as hacking, loss of boundary, messy complexity and hyper connectivity in case of smart cities involved in IoT integrated healthcare [16]. They also identified some problems such as inadequate configuration of smart devices, unattended devices, and non protection to sensitive data, spam, and social engineering. They discussed data protection and consumer laws in the wake of IoT, cloud and emerging integration of them with healthcare [17]. The intersection of both IoT and cloud are known as Clouds of Things (CoT) that reflect M2M communications. They proposed a framework known as “Health Share” which is meant for “sharing healthcare data through social media related to healthcare domain or Health Social Networks” (HSNs) [12]. Their architecture has an attribute trusted authority that provides relevant access permissions to doctors and patients in healthcare units.

Attribute oriented authentication and authorization are performed in their system. The concepts of signing and verification with respect to security are used in their system. Charlotte Garrett investigated data access problems in healthcare domain [12]. They proposed a framework for proper accessing of primary healthcare data among healthcare units. Roman et al. opined that distributed nature of IoT and related technologies throws privacy and security challenges [13]. In the process, they examined different architectures of IoT in distributed environment.

It is evident that three are different distributed approaches in which IoT can operate. In all these approaches there are challenges pertaining to privacy and challenges. The architectures are broadly classified into centralized ones and distributed ones. Different architectures for IoT include centralized IoT, collaborative IoT, connected IoT and distributed IoT. These IoT architectures are compared in terms of openness, viability, reliability, scalability, interoperability, and data management. They opined that protocols and network security services are yet to be improved to cope with IoT usage in healthcare and other domains with end-to-end security. They also found the need for good identity management mechanisms. They identified data deluge as big threat to privacy o f data. They focused on external attacks on IoT and the need for a framework to provide secure communications [14]. They presented a framework for enforcing security policies in the context of IoT.

Security framework for IoT is presented. The framework provides provision for Networked Smart Objects (NSO) with security policies and policy engine. The NSOs are integrated as part of IoT and there is security provided as shown in the framework. Administrator takes care of NOS configurations pertaining to security policies. The architecture includes provision for data API, data normalization, Message Queue Telemetry Transport (MQTT), security analyzer, HTTPS/SSL. They investigated privacy and security challenges in healthcare integrated IoT system [14]. They found that traditional security policies are not sufficient for IoT integrated healthcare units. And they proposed a flexible architecture to promote scalability, privacy and security of such systems. The main security issues identified by them are presented in Figure 2.7. These security challenges are to be overcome to have sustainable IoT integration with healthcare infrastructure.



**Figure 2.7 Security challenges in IoT**

IoT security challenges include “authentication, access control, privacy, policy enforcement, trust, mobile security, secure middleware, and confidentiality”. They opined that sustainable spreading of IoT is possible when these issues are resolved with customized security and privacy levels. They emphasised on the need for mobile security as increased number of mobile devices are participating in IoT in critical applications. They investigated “security mechanisms with constrained devices” when they are connected to IoT [16]. They evaluated different cryptographic primitives such as “block ciphers, privacy enhancing schemes, digital signature schemes, asymmetric primitives, random number generators, and hash functions”. They emphasized on the usage of attribute-based schemes, group signatures, and homomorphic encryption schemes for leveraging privacy and security with IoT. They studied the privacy issues related to individuals when IoT is realized [16]. They found that as of now legislations are not adequate to handle issues with IoT integration. They also said that “future legislations should consider security and privacy of IoT services in the wake of their global reach and ubiquity”.

studied data breaches in healthcare domain. Data breaches are related to misuse of health information which leads to identity theft, fake health insurance, financial identity theft, medical identity fraud, and privacy violations [14]. These breaches can cause issues such as “loss of employment, loss of insurance, stigmatization, discrimination, and serious reputational harm”. Kevin Fu provided many recommendations to improve security in IoT and healthcare infrastructure integration [16]. Need for building security into IoT devices, improving password strength, aware of connectedness with counter measures, considering big picture of IoT and take security measures, avoiding risk to human safety by providing end to end security in IoT, better cyber security mechanisms, improving the count of security professionals, having an independent body for national cyber security. IoT and its security concerns are also studied by [17]. They listed top 10 vulnerabilities of IoT such as “poor physical security, insecure software, insecure configuration, insecure mobile interface, insecure cloud interface, privacy concerns, lack of transport encryption, insecure network services, authentication inefficiency, authorization inefficiency, and insecure web interface”.

**2.15 PRIVACY AND SECURITY IN IoT-AWARE HEALTHCARE SYSTEMS**

With the invent of e-Healthcare, healthcare services are provided efficiently using electronic devices. This can help remote monitoring of patients. It is further leveraged with IoT usage. This kind of service can help to have quality healthcare services for reduced cost. In this context, it is important to look into privacy and security issues as well for sustainable growth of IoT in healthcare units. They studied privacy and security issues in such IoT applications employed for e-Healthcare [14]. Privacy refers to non-disclosure of sensitive data pertaining to patient while security refers to allowing access to healthcare data with authentication. The universal access to healthcare data sources causes security and privacy challenges that are to be overcome for sustainable services. Health information of individuals needs to be kept confidential. However, the transmission of sensitive data over wireless networks makes it vulnerable. Therefore, proper security is to be enforced besides preserving privacy of sensitive data. It is challenging to provide global access and at the same time protect privacy of patients’ data. Achieving right to access to healthcare data and preventing disclosure of sensitive data is challenging. They focused on information technologies that work for healthcare services [25]. The improvements include “electronic medical record (EMR), electronic health record (EHR) and Personal Health Record (PHR)”. They proposed a roadmap to have smart cities with e-government and cloud computing initiatives [14].

They studied privacy and security in IoT applications [24]. They proposed a reference architecture that can be used to build cloud-based IoT applications in the real world. They opined that “privacy and security” play vital role for sustainable IoT growth in healthcare sector. “Healthcare applications and integration of IoT” also should be compliant with prevailing laws and insurance requirements like “Health Insurance Portability and Accountability Act (HIPAA)”. IoT applications and service layers of IoT need to ensure security and privacy requirements such as “availability, privacy, nonrepudiation, integrity and authorization”. Improving privacy and security in IoT applications is done using informed consent from users, control over privacy settings, vendor regulations, and access to user data without lock-in, and user identification and authentication. In addition to this IoT also needs physical security.

**2.16 SUMMARY**

This chapter has reviewed literature on different aspects associated with remote health monitoring using IoT technology. From the literature, the valuable insights are ascertained. They, along with important research gap, are provided here. IoT technology enabled any time, any place and anything connectivity. It paves way for humans (physical objects) to be integrated with digital systems with the help of wearable devices and sensors besides technologies like RFID and NFC. Many IoT integrated healthcare architectures are found in the literature. The common thread in all of them is that most of them are conceptual and theoretical in nature. However, the ideas presented in those architecture are very valuable. The idea behind remote health monitoring is to help rural people who cannot afford costly medical services. Towards this end there are architectures proposed. However, they suffer from the following problems. First, they lack in the realization of a framework that is based on smart bed associated with village PHC with patient having wearable devices in order to collect his/her vital signs remotely and provide real time monitoring. Second, instead of theatrical perspective, there is need for practical aspect that investigates the components towards realization of such application. Third, there is need for end to end security and privacy is to be preserved since healthcare data is sensitive in nature. These problems are addressed in the thesis and the subsequent chapters provide more details on the research carried out.

**REFERENCES**

1 T. Bhattasali, N. Chaki, “Exploring Security as a Service for IoT Enabled Remote Application Framework”, In: Proceedings of 14th ACM International Conference on Mobile Systems, Applications, and Services Companion, ACM Mobisys (2016).

2 T. Bhattasali, R. Chaki, N. Chaki, K. Saeed, “Securing Service in Remote Healthcare”, Advanced Computing and Systems for Security, Springer, Advances in Intelligent Systems and Computing, Volume 395 (2016).

3 T. Bhattasali, R. Chaki, N. Chaki, K. Saeed, “An Adaptation of Context And Trust Aware Workflow Oriented Access Control For Remote Healthcare”, International Journal of Software engineering and Knowledge Engineering (IJSEKE), June (2018).

4 S. H. Kim, W. Whitt, “Statistical analysis with Little's Law”, Oper. Res., 61(4) (2013).

5 T. Bhattasali, “A New Interaction Model for Mapping Cloud Flow to Virtual Machine”, International Journal for Research in Engineering Application & Management (IJREAM), Special Issue, November 2018.

6 Y. Wang, G-Y. Du,F-X. Sun, “A Model for User Authentication Based On Manner of Keystroke And Principal Component Analysis”, In: Proceedings of International Conference on Machine Learning and Cybernetics (2006).

7 K.S. Balagani, V.V. A. Phoha, S. Phoha, “On the discriminability of Keystroke Feature Vectors Used In Fixed Text Keystroke Authentication”, 32(7) (2011).

8 D.Gunetti, C. Picardi, M. Karnan, M. Akila, N. Krishnaraj, “Biometric Personal Authentication Using Keystroke Dynamics: A Review”, Elsevier Journal of Applied Soft Computing ,11(2) (2011).

9 D. Gunetti, C. Picardi, “Keystroke Analysis of Free Text”, ACM Transactions on Information and System Security, 8(3) (2005).

10 A. Ahmed, I. Traore, “Biometric Recognition Based on Free-Text Keystroke Dynamics”, IEEE Transactions on Cybernetics, 44(4)(2014).

11 T. Bhattasali, K. Saeed, “Two Factor Remote Authentication in Healthcare”, In:Proceedings of IEEE International Conference on Advances in Computing, Communications and Informatics, (2014).

12 T. Bhattasali, R. Chaki, K. Saeed, N. Chaki, “Typing Signature Classification Model for User Identity Verification”, Advanced Computing and Systems for Security,Springer, Advances in Intelligent Systems and Computing,Volume 666, 2018.

13 S. Haykin, “Neural Networks: a Comprehensive Foundation. Prentice HallPTR(1998).

14 S. Giroux, R. Smolikova, M.P. Wachowiak, “Keystroke Based Authentication byKey Press Intervals as a Complementary Behavioral Biometric Systems”, In: Proceedings of IEEE International Conference on Man and Cybernetics (2009).

15 Z. Syed, S. Banerjee, B. C. Leveraging, “Variations in Event Sequences inKeystroke-dynamics Authentication Systems”. In: Proceedings of IEEE International Symposium on High-Assurance Systems Engineering (2014).

16 T. Shimshon, R. Moskovitch, L. Rokach, Y. Elovici, “Clustering Di-Graphs forContinuously Verifying Users According to their Typing Patterns”, In: Proceedings of IEEE Convention of Electrical and Electronics Engineers in Israel(2010).

17 M. Karnan, N. Krishnaraj, “Bio Password Keystroke Dynamic Approach To SecureMobile Devices. In: Proceedings of IEEE International Conference on Computational Intelligence and Computing Research (2010).

18 J. Hu, D. Gingrich, A. Sentosa, “A K-Nearest Neighbor Approach for User Authentication Through Biometric Keystroke Dynamics”, In: Proceedings of IEEE International Conference on Communications(2008).

19 K. S.Killourhy, R.A Maxion, “Comparing Anomaly-Detection Algorithms forKeystroke Dynamics”. In: Proceedings of IEEE/IFIP International Conference Dependable Systems & Networks (2009).

20 L.C. F. Araujo, L. H. R. Jr.Sucupira, M.G.Lizarraga, L. L. Ling, J.B.T. YabuUti, “ User Authentication Through Typing Biometrics Features”, IEEE Transaction on Signal Processing 53(2)(2005).

21 K. S. Killourhy, S. Kevin, R. A.Maxion, A. Roy, “Free vs. Transcribed Textfor Keystroke- Dynamics Evaluations”, In: Proceedings of Workshop: Learning fromAuthoritative Security Experiment Results (2012).

22 T. Bhattasali, K. Saeed, N. Chaki, R. Chaki, “Bio-Authentication For LayeredRemote Health

Monitor Framework”, Journal of Medical Informatics and Technologies, 23(2014).

23 K. Jain, A. Ross, S. Pankanti, “Biometrics: A Tool for Information Security”, IEEE Transactions on Information Forensics and Security, 1(2)(2001).

24 Q.Y. Xie, Y. Cheng, “ K-Centers Min-Max Clustering Algorithm Over Heterogeneous Wireless Sensor Networks”., In: Proceedings of IEEE Wireless Telecommunications Symposium (2013)..

25 B. Kao, S.D. Lee, P.K.F.Lee, D. W.Cheung, W. S. Ho, “Clustering Uncertain Data using Voronoi Diagrams and R-Tree Index”, IEEE Transactions On Knowledgeand Data Engineering, 22(9)(2010).