A SURVEY OF HEALTHCARE APPLICATIONS BASED ON GOOGLE IOT CLOUD PLATORM

SIT792 Minor Thesis

TEAM 2

DR. MICHEAL HOBBS

Jay Vimalbhai Trivedi (218449725)

Contents

1. Abstract

Over recent years, the Internet of Things has been one of the main highlights in the advancements of technology. According to Li, Da Xu, and Zhao (2015) IoT is also considered as the Internet of the future which comprises a vast number of intelligent communicating 'things'. The future of the Internet of Things is embedded with diversified connected devices that are being used to extend the boundaries of technology with physical capabilities. It has penetrated its branches in different fields of advancements in technology among which one of the branches is discussed in this thesis that of IoT in Healthcare applications. The thesis paper highlights the security and privacy issues and challenges faced by the healthcare applications in the Internet of Things (IoT) and its application with Wireless Sensor Network (WSN) and Cloud Computing.

2. Introduction

This section gives you a deeper understanding of the Internet of Things (IoT) and its application in healthcare. Along with it, you'll also gain insights on the working of healthcare applications and its functionalities, with its different aspects such as Wireless Sensor Networks (WSN) and how actually Cloud computing plays a major role when it comes to the handling of the sensitive information of the individuals.

2.1 Entry point of the Internet of Things (IoT)

Kulkarni and Sathe (2014) have observed that throughout the years the Internet and Web have been evolved through different stages to reach the form we see today. The process of evolution compromises of four stages as shown below.

Stage 1: Significance of ARPANET

The ARPANET stands for Advanced Research Project Agency Network, which was initiated by the US Military and the Department of Defence. The primary usage of this project was for research and academic purposes are taken care of by the universities and various research institutes.

Stage 2: Gold rush for the domain names

In this era, the Hypertext Mark-up Language was being introduced which is also known as HTML. As a result, the big brand companies were rushing their way to get their domain names registered under it. The aim of doing this was the distribution of information regarding the vivid services and products by them. This process is coined as brochureware.

Stage 3 The entry of the dot com

In this phase, the internet shifted from a stable state to an online transaction state. During this phase, companies such as eBay and Amazon grounded its roots in the market by selling their goods and services online to attract more customers and stay ahead in the competition.

Stage 4 The social and web experience era

In this, the internet has become an integral part of social interactions. In which companies like Facebook, Twitter has enabled various services in which the individual can have the ability to share their daily activities and interactions on the website.

Stage 5 The Internet of Things

This is an integral part of the journey through which the world has changed its face towards the development and enhancement of the technology that we see today. To describe in a laymen's words the Internet of Things (IoT) means bridging the objects used in the everyday life such as smart-phones, televisions, sensors, automobiles, and many more to the internet. This opens the doors for new capabilities and opening of a new form of communication between things and people, and among themselves as well.

2.2 About the Internet of Things (IoT)

According to Kulkarni and Sathe (2014), Islam, Kwak, Kabir, Hossain, and Kwak (2015), the term Internet of Things was first introduced by Kevin Ashton in the year 1999. He defined the term IoT as uniquely identifiable compatible devices which are inter-connected objects with radio-frequency identification (RFID) technology. It is a mixture of certain fields such as Embedded and control systems, wireless sensor networks to provide a Device to Device (D2D) communication with the internet. In a simple language, the words "internet" and "things" can easily be described as an interconnected worldwide network that is grounded upon sensory, communication, networking, and various other information technologies that are a newer version of information and communication technology (ICT). The RFID (Radio Frequency Identification) is considered as the first essential step towards the Internet of Things (IoT).

The applications of the RFID (Radio Frequency Identification) can be further diversified into two branches such as private and business users. The private users comprise of healthcare, e-learning, and domestic are the major fields whereas, for the business users' view it includes automation and logistics which are considered as the main domains. The following points depict the branches in which the Internet of Things (IoT) is recently enhancing.

- **Ubiquitous Computing**

  Throughout the years it has been observed that the advancements of the micro-electro mechanism systems (MEMS) technology, wireless communications, and digital electronics have paved its way towards the evolution of miniature devices. The importance of having these devices is that they can easily sense, compute, and communicate wirelessly without any necessary device/medium interference. These

miniature devices are the building blocks that connect to form Wireless Sensor Networks (WSN).

- **Applications**

  With the Internet of Things (IoT), it now has been made possible to make the data gathering and analyzing process faster when the devices are connected through with they can communicate among themselves and with the cloud.

2.3 Internet of things (IoT) and Healthcare

The dependency of healthcare on IoT has been increased in the past few years for the improvement of the quality of the care given, easy access of the healthcare applications as well as reduction of the cost of care. Based on an individual's unique features such as their behavior, biological representation, and social characteristics, the prolonged well-being treatment, and patient support can be named as "Personalised healthcare" Kulkarni and Sathe (2014). As these Personalized healthcare data are being gathered from individuals, IoT (i.e. through wireless sensor networks and cloud computing) makes it possible to make the data gathering process to be easy moving which makes the healthcare dependable on IoT. The Internet of Things ensures to provide any individual's care services and manages to keep its unique digital identity. The generic definition of knowledge of healthcare for every individual is stated by the following principle stated as "the right care for the right person at the right time" which leads to better improvement in the quality of treatment of the patient thus making healthcare cost-effective (Kulkarni & Sathe, 2014). IoT holds the ability for the improvement in healthcare of the patients by various healthcare applications such as glucose level sensing, blood pressure monitoring, body temperature monitoring which are further discussed in brief in this thesis.

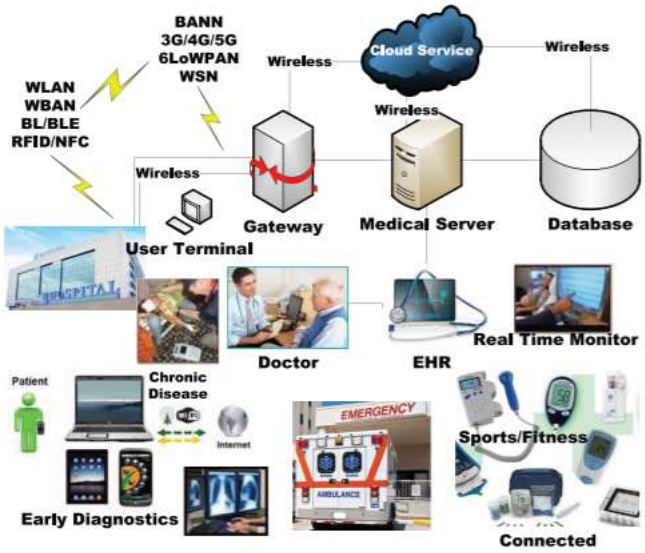

Figure 1: Healthcare trends by (Islam et al., 2015)

2.4 Application of Internet of Things (IoT) in Healthcare

By Islam et al. (2015) the IoT comes with two sub-divisions as IoT services and IoT applications in healthcare. The role of the services is that it is being used to develop and provide the application whereas the application is being used by the patient and users. As a result, the services come under developer-centric while the application is user-centric. The IoT applications are being closely examined in this thesis because these healthcare applications are in place to make a positive impact on the patient's livelihood. These applications cover a vast range of areas such as wearable devices, gadgets, and different healthcare devices through wireless sensor networks and cloud computing that are made available in the market. The paper covers different areas in which these applications are being used and its various security and privacy concerns regarding its use.

3. Background of the research area and project

In the following part, we'll be discussing various healthcare applications and wearable devices (In this case smartwatches which is considered as one of the wearable devices among many others) which are currently being used by the patients and their corresponding healthcare professionals. This section will give a detailed view of the applications and their functionalities being used. Along with it, we'll be introducing the role of cloud computing in IoT healthcare systems which are followed by different steps. The relationship between both the applications and cloud computing will provide a base for certain security threats and privacy issues that are being faced by them.

3.1 Mobile phone applications in healthcare

According to Boulos, Wheeler, Tavares, and Jones (2011), it is evident that there has been a rapid increase in the capability of mobile communication to broaden the boundaries of healthcare and clinical intervention in the community. Studies have shown that mobile communication for healthcare has landed tremendous support for the collection of data in healthcare research, medical education, and clinical practices. The intervention of smartphone communication in healthcare has its perks when it comes to in-built functionalities such as short message services (SMS), Global Positioning System (GPS), and various health monitoring systems such as Body Area Network (BAN), etc which are now used to treat patients having disabilities and/or multiple chronic diseases.

Below are discussed different domains of healthcare application given by (Islam et al., 2015) which has played a significant role in our daily lives

A. Glucose level sensing

Diabetes is a part of metabolic diseases which represents high sugar levels in the bloodstream over a prolonged period. Blood glucose monitoring keeps track of the change in the sugar level in the blood over a specific period which helps in the planning of the meals, daily activities, and duration of medication at a certain time interval. A mobile IoT configuration system has been used which senses the glucose level with real-time analysis. A sensor is being placed with the patient which keeps track of the glucose levels with time, the data is transferred to the health professional which are monitoring the levels through the sensors. The transmission device which includes a blood glucose collector, a mobile phone, and a background processor collects the data on blood glucose on various IoT networks.

B. Blood pressure monitoring

The blood pressure monitoring device collects the blood pressure data at regular intervals of time and sends it to the desired health professional over the IoT network. This device consists of a blood pressure apparatus body with an in-built communication module. The Airstrip technologies have deployed a patient monitoring system using software development tools that keeps monitoring the blood pressure (Baig, GholamHosseini, & Connolly, 2015). The software is compatible with all smartphones, tablets, and PCs. A two-sided gateway is being used when the data is transferred to the health professional for further treatment.

C. Body temperature monitoring

Body temperature monitoring plays a vital role in healthcare services because the body temperature is a vital sign to detect any affected disease in the body. In the mobile health IoT system, the body temperature sensor is embedded with the person's body which continuously transmits the body temperature and its variations as a form of signal to the authorized personnel. The e-CAALYX mobile application is one of the examples which is used by the patient having multiple chronic diseases in which it transmits the data through the sensors along with the geographic location using GPS to the health professional (Boulos et al., 2011).

D. Monitor an aging family member.

Nowadays ultra-sound technology has been used in hospitals to keep track of senior patients' activities and fall detection. This technology is now deployed for home care to monitor the elderly patient's movements and in case of any fall detection. An emergency call functionality is also embedded in this technology which is used in some serious case scenarios which use a wide-area communication interface. Another system that works well with a senior health monitoring system is a small waterproof monitoring system that can also be worn as a wristwatch. With a specific time, interval, the system is programmed to send the positioning signal of the individual to the ultrasound receiver. Upon receiving the signal by the receiver, it communicates over the wireless network connections to the homecare gateway. The gateway performs a specific analysis of the data and transmits the relevant data further. The wireless wide area network is used to send out any help signal or notification if any critical event is detected (Kulkarni & Sathe, 2014).

E. Medication management

Proper distribution of medication over a wide area of patients has been one of the challenges faced by the healthcare department. As a solution, a medication management system has been deployed to provide and delivers the medication with the help of RFID tags over the IoT networks.

F. Wheelchair management

Multiple types of research have been done to implement and deploy smart wheelchairs with full automation for elderly people. The IoT technology has made its way to implement the smart wheelchair designed with integrated WBAN's along with a peer-to-peer medical support system that controls the chair vibration and detects the status of the wheelchair user. The data is collected in the application which is linked with the WBAN of the wheelchair and is transmitted to the allocated healthcare professional.

The below image depicts various healthcare applications on smartphones

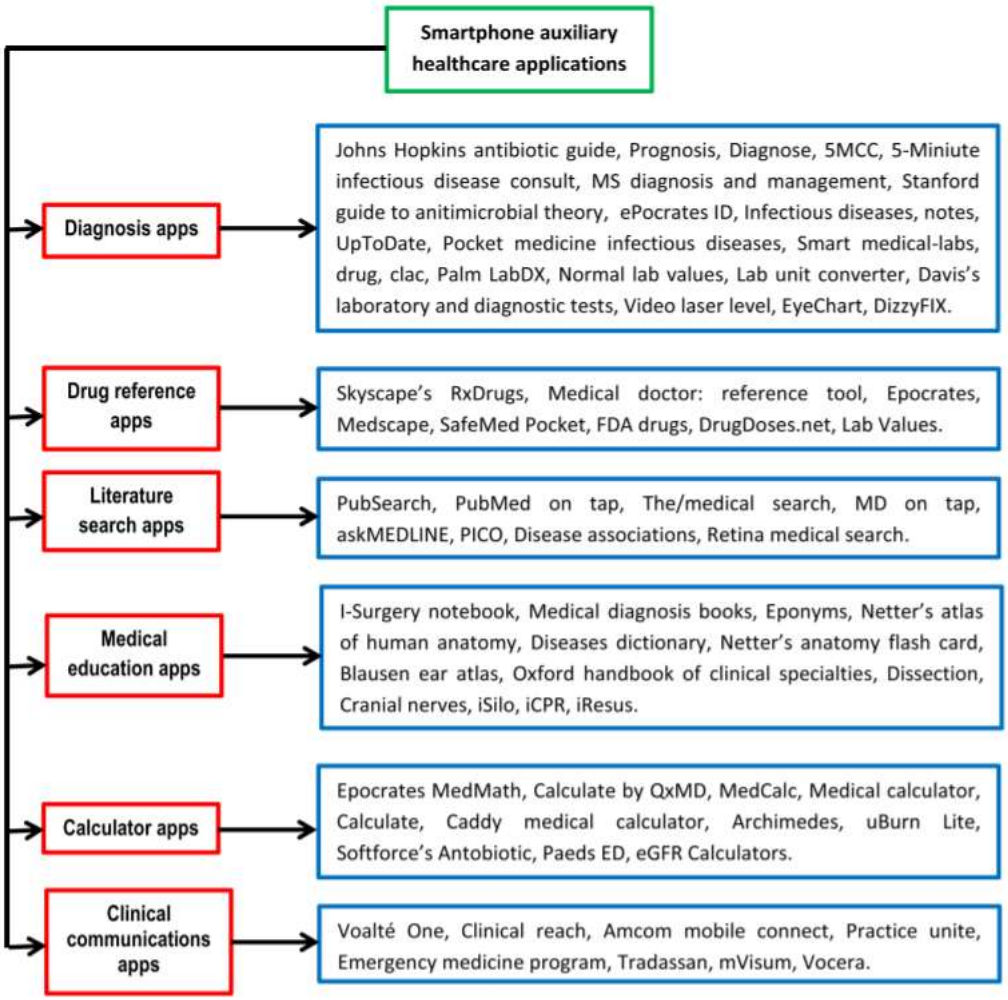

Figure 2: Health care apps for smartphones by (Islam et al., 2015)

3.2 IoT-based healthcare system

A typical IoT structure given by Alam et al. (2018), can be further diversified into four major components such as things, gateways, communication technologies, and cloud platforms. Below given is the detailed summary for each component.

- **Gateways**
  - It can also be referred to as fog nodes. The role of fog nodes is that it acts as a middleman between the device and the IoT cloud platform which provides connectivity, security, and manageability. Some of the IoT applications need immediate analysis of transmitted data. For example, the blood pressure of the patient is kept under constant observation. When the blood pressure reading is reaching its maximum threshold limit, precise measurements are taken immediately. Any kind of delay of transmission for the blood pressure readings from the device to the IoT cloud platform for processing and analyzing purposes may lead to some serious events. Therefore, keeping the analyzing process of the data gathered nearby the patient will lead to better health diagnosis and increases the survival chances of the patient. To tackle this kind of situation technologies such as fog computing is introduced which analyzes the collected data within no time. By introducing such gateways will lead to redundant stress for communication technologies.
- **Communication technologies**
  - One of the major key issues related to IoT-based applications is the sharing of information in which the deployment of proper communication technology is mandatory. Better sharing of information is the key to the improvement of the efficiency and effectiveness of the service provided by the cloud platform. When it comes to real-time information sharing reliable and secure connectivity plays an essential role in the process. A robust and easy to implement a solution for this issue is the deployment of wireless communication technologies. The term 'wireless' itself is a combination of two components namely short-range communication such as Bluetooth, Wi-Fi whereas long-range communication examples are 3G/4G cellular network or use of satellite system.
- **Cloud infrastructure**
  - The cloud infrastructure is a combination of a set of servers and storage which are linked together. To support the IoT applications, these infrastructures execute the application based on machine learning or with the help of artificial intelligence technologies that collects analyses and refines the data gathered from the device or thing to provide sensitive information that is used for decision-making purposes. The trio of

three technologies namely machine learning, big data, and artificial intelligence has made major impacts in all the industry sectors by processing and analyzing large chunks of data and turning them into useful information in no time. With the usage of these capabilities, it will result in a reduction of cost of medical treatments and optimization of the processes not only in the healthcare systems but also make a big impact on different organizations. The creation of a proactive framework based on predictive analytics is the future of the healthcare industry.

3.3 Smartwatches: A turning point of technology

As observed by Lu, Fu, Ma, Fang, and Turner (2016) with the IoT taking its lead in the enhancement in new technologies there is no doubt that wearable technologies are entering into our lives. The big brand technology companies have invested a large amount of fortune in developing wearable devices to have a strong position in the consumer market. It has been observed that only 1% to 2% of individuals in the U.S. are using wearable devices whereas the market is predicted to $25 billion by 2019 which makes 60% of the market value for smartwatches. A wearable device is stated as an electronic device like a smartphone that can be worn as an accessory under any individual's clothing. The wearable device is integrated with technologies such as biosensors and wireless data communication which allows the user to access and transmit the information to a wide field of network. A similar type of smartwatches is also known as wrist bands which possess the same functionality as a smartwatch depending upon the configuration.

It was observed by Banerjee, Hemphill, and Longstreet (2018), that wearable healthcare devices can be further distinguished as Wearable Health Monitoring Devices, Medical Wearable Devices, Medical Embedded Devices, and Stationary Medical Devices. Wearable healthcare monitoring devices fall under consumer products (i.e. Fitbit, Fuel band, etc). Medical wearable devices are mostly prescribed devices which are insulin pumps. The medically embedded devices are those which are embedded inside the body. The design of stationary medical devices is made in such a way that it can pinpoint a specific physical location. Each of these devices forecasts a set of attributes which are identification, location, sensing, and connectivity.

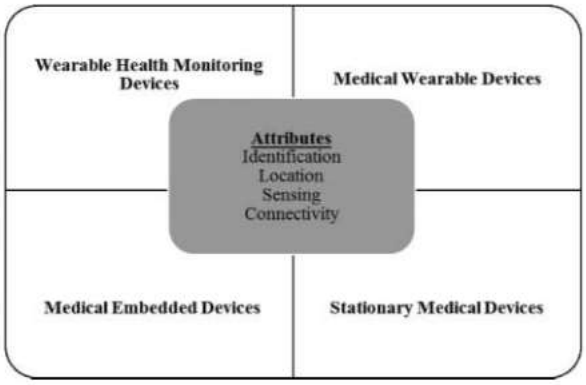

Figure 3: Healthcare IoT Topology by (Banerjee et al., 2018)

3.4 Issues regarding wireless sensor networks

This section gives a detailed summary of the threats that occur in wireless sensor networks.

Security threats

Monitoring and eavesdropping on patient vital signs

It was being observed by Kumar and Lee (2012) that this is one of the common threats occurring to the privacy of the patient. With the help of vital signs snooping any individual with malicious intent can easily find out the patient's information through communication channels. When the personnel with a receiver antenna can easily grasp the messages from the network which may contain the physical locations of the patient which allows the person to easily attack the patient to cause any damage towards them. They can also trace the messages received, phone calls, emails, and many more which endangers the privacy of the patient.

Threats to information when in transit

The wireless communication ranges are not secure hence it poses as a threat. In healthcare applications, the sensors sense and collect the data of the patient and its environment and transmit it to the respected physician or the caretaker. During the process of transmission of data, it can be attacked. Any opponent can extract the transmitted data through the wireless channels and has the capability of altering it by penetrating any false data into it. Later, it transmits the altered data to the physician or caretaker which is a threat to the patient's recovery. Message modification also causes a threat when the individual hijacks the wireless communication channel and alters the text upon passing causes serious damage to the patient (Kumar & Lee, 2012).

Masquerade and Replay attacks in WSNs

In home-based, applications the attacker can easily attack the rely points when the patient data is being transferred to a remote location. The wireless rely nodes are not secure which in return the person can easily gain unrestricted access to it which leads to masquerade. The unauthorized rely node acts as a real node to the network. This poses a threat when it delivers false alarms to the remote sites in which the response team could start their rescue operation for a dummy person. The masquerade node is a common entry point for the denial of service attacks which causes serious issues with the application operation. Hence it proves a great threat to healthcare applications(Kumar & Lee, 2012).

Location threats

Medical sensor networks have the capability to detect the patient's location for the medical staff to arrive on time in case of any emergency. Location tracking systems make use of radio signals or ultrasound technology to pinpoint the exact location of the patient by continuously monitoring it. as a result, any intruder can easily receive or access the received radio signals and analyze them which later on can have access to the patient's exact location and its privacy (Kumar & Lee, 2012).

Activity tracking threats

Any individual or attacker can gain access to the exercise data when the personnel is not aware of it while training. Depending upon the medical sensor the attacker captures the data, alters it, and sends vague exercise tips which may end in serious consequences if the patient is suffering from a chronic disease (Kumar & Lee, 2012).

Denial-of-service threats

Denial-of-service disrupts the flow of the system by over-flowing it with unnecessary information as a result it leads to the breakdown of the system and its operations. The Denial-of-service threat proves more threatening as the data in the healthcare applications must be kept under ongoing observation by the health professionals (Kumar & Lee, 2012).

Privacy issues

Individuals tend to share their data with physicians, health-coaches, insurance companies, or with family. Any breach of the data leads to various privacy issues. According to National Committee for Vital and Health Statistics (NCVHS), it has been stated that "Health information privacy is an individual's right to control the acquisitions, uses or disclosures of his/her identifiable health data" (Kumar & Lee, 2012). Every patient has the right to determine which data should be collected, used, and given further to the corresponding health professional. This leads to various privacy threats were given by Kumar and Lee (2012) are as follows

Identity threat: When a patient loses or shares personal information or identity to another which containing sensitive information it leads to financial, physical, and emotional harm to the patient. Any person from the inside can use this information for his/her cause which leads to difficult scenarios.

Access threats: In this, the patient is usually at fault as he/she is involved in access to the data or information. Upon conveying any false data to the designated health professional may lead to troublesome scenarios.

Misuse of medical information: The patient's health data is continuously transmitted onto the wireless channel which means it is an entrance for any wireless attack on it such as eavesdropping and snooping. This imposes a threat to patient privacy.

Leakage of prescriptions: it was being observed that the violation of medical prescriptions is one of the major reasons for privacy issues. The medical prescription contains all the detailed information regarding the patient such as medical number, contact information, and address. When transmitting the medical prescriptions onto the wireless medium it poses a great threat to the patient's privacy.

Eavesdropping on patient's information: The patient's medical information is continuously flowing through the wireless links over the medium which can easily be monitored. The monitoring system collects information from the medium and extracts valuable information from it for further use. The eavesdropping of the information can be easily done when the data is being transmitted to the monitoring systems. This poses a serious privacy risk for the patient.

Social implications: Social implications occur when the patient itself is not able to decide for its privacy. This usually occurs with elderly people which are unaware of the privacy threats caused.

3.5 Cloud computing in healthcare applications

In this section, we'll discuss the security issues given by Zhang and Liu (2010) of healthcare cloud computing. The common security issues that are being faced by healthcare cloud are ownership of information, authenticity, authentication, non-reputation, patient consent, authorization, integrity, and confidentiality of data.

1. **Ownership of information**

   In general, the owner can also be called the creator of the information. It is necessary to prioritize the ownership of information as it is mandatory to protect a user against any misuse of the patient's data. To define the term "owner" in a layman's words it is the person who is held responsible for the information. We can also consider the term "owner" as "creator", "author" and "manager" of information.

2. **Authenticity and authentication**

   Authenticity means how true the data is without being tampered with or without any false inputs Authentication means only the authorized user is allowed to have access to the information, any breach in the authentication may lead to serious mishaps regarding the data of the patient. Authentication poses a great threat to Man-in-the-Middle attacks when a person impersonates the identity of another individual to have access to the classified data. This results in a vast amount of sensitive data loss for those healthcare applications in which man in the middle is implemented.

3. **Non-repudiation**

   Non-repudiation means to follow one's obligation of the contract. Which means an organization cannot deny transaction nor the other organization cannot deny the transaction being transmitted.

4. **Patient consent and authorization**

   The patient has the full authority to allow or deny any sharing of sensitive information to the health professionals, practitioners, and caretakers.

5. **Integrity and confidentiality of the data**

   Integrity simply means to make sure the consistency and accuracy of the data are being kept throughout the process. Speaking in the healthcare application sector it must be made sure that the data is not being tampered with. Whereas confidentiality can be implemented by access control and various encryption techniques used in the EHR system.

6. **Availability and utility**

   The availability of information should always be kept in this scenario. The role of computing systems in this scenario is to store and process the electronic health records

of the patients, the security control is a protection layer which protects it from any harm caused, the communication channel must be working properly to access of the information. The systems with higher configurations are always available which are used to prevent any disruptions caused by the power outages, hardware failures, and system upgrades. Availability also makes sure that it protects the system from any denial-of-service attacks and makes sure the HRE data remains intact. The role of utility is to make sure that the usability of EHR data is made after performing exercises and implementing security to it.

From a detailed summary of the applications in healthcare given above we can see the role of the technologies which have submerged with our day to day lives. These applications can detect even a minute increase or drop of the illness in the human body and can alert the individual taking care of the person through wireless networks. Secondly, from the step by step stages of the cloud computing stated above highlights the importance of cloud and its infrastructure on the healthcare applications. Thirdly, we saw the various security threats and privacy issues prevailing with the wireless sensor networks which are used in any healthcare applications and wearable devices for the patient and cloud computing.

4. Motivation

We live in a world where the branch of the mobile application is on an expanding loop where new healthcare applications are being deployed in the market every day. When it comes to healthcare mobile applications it is of great importance to take care of the gathering of personal health information. With the development of smartphones, it leads to different smartphone applications in various domains such as healthcare. This industry has been on an expanding curve and is continuously going on. It was being noted that there are more than 800,000 applications created for the two of the most important operating systems, Apple iOS, and Google Android (Martínez-Pérez, De La Torre-Díez, & López-Coronado, 2015). Each of them has different medical and healthcare applications. Speaking of healthcare applications, Apple iOS' App Store has over more than 31,000 applications related to medicine, health, and fitness areas whereas Android's Google Play has over 16,000 medical and healthcare applications (Martínez-Pérez et al., 2015). These applications are a part of mobile health defined by the World Health Organization

However, in the development and in releasing phase of the applications certain things are not considered by the developers. Among them are the privacy and the security issues which play an important role in those applications which use the personal and non-transferable data, such as healthcare applications which store the patients' Electronic Health Records (EHRs) or multiple data associated with the health status of the individual. The clinicians and patients are getting their hands on the applications faster than the providers get a chance to protect the security and privacy issues, which is also one of the problems faced. According to the recent survey from the Healthcare Information and Management Systems Society (HIMMS), the mobile technology usage for data collection done by clinicians went up to 45% up from 30% last year and overall 93% of clinicians use their smartphones to access the EHR (Martínez-Pérez et al., 2015). Hence these issues are still prevalent and need various countermeasures to keep the process easy flowing.

Nowadays any wearable devices such as smartwatches or fitness bands can be considered as a miniature version of the smartphones. They provide all the similar functionalities as a smartphone such as dialling a phone number, drafting an email, access to a location through GPS, etc. They also consist of various inbuilt applications such as electrocardiograph (ECG) which monitors your vital signs, keeps track of your footsteps, and can also analyze your sleeping patterns. All the data that is gathered with the usage of the above-given

functionalities are being synced with its related application of the smartphones. As a result, of Bluetooth technology, the data is transferred into the smartphone which eradicates any tedious manual methods of data transfer. Apart from the smartwatches the healthcare applications itself also tend to gather the data with the help of various inbuilt functions of the smartphones itself through sensors. The data being gathered is then transmitted to the related IoT platforms. This leads to certain security threats and privacy issues being followed with the implementation of these wearable devices either in-body or on-body of the individual.

5. Problem statement

With the deployment of any kind of enhancements in a field there are always some loopholes need to pay attention to. This thesis is focused upon the various security threats and privacy issues facing today with the healthcare applications and any medical wearable devices which includes monitoring and eavesdropping of the patient vital signs, threats to information in transit, and many more as discussed in the above section. Secondly, these applications and wearable devices are linked to the cloud in that case it is also one of the centers of attraction to the attackers as it has various security issues such as ownership of information, authenticity, and authentication.

With the analysis of these issues and by implementing a precise research methodology we'll be seeing a precise and concise evaluation and solution for both the fields which adds a security layer that protects the patient's sensitive and valuable information from any attacks.

6. Related work

In this section, we'll be viewing the latest enhancements in healthcare applications of the Internet of Things (IoT) which are discussed by Ssegawa and Ezekia I (2015)

- **An ingestible sensor for measuring medication adherence**

  A smart pill is one of the latest enhancements used in the field of healthcare applications. By using the smart pill technology, medication ingestion and various patterns of the patients can be monitored easily. The irregularity of the medication is one of the serious issues related to the patient as it can cause some serious outcomes. This technology involves a system that keeps track of the ingestion of the tablet or capsule. The system is a summation of ingestible sensors attached to a tablet, a small wearable sensor, a mobile application that comes with a portal. Whenever the patient swallows the smart pill, it reaches the stomach and gives a signal which is received by the sensor patch that is attached to the human body. The signal that is generated goes under two processes, first, it is converted into a digital record and second, it is transmitted to the mobile device which is attached to the patient's body. After receiving the signal to the mobile device, it is then sent to the designated cloud platform where the health professionals or caretakers can access the medical data with the help of their portals. The sensor in the pill is made up of edible elements that are used in the diets of the patients on daily basis. The deployment of this technology will change the map of healthcare applications and will eradicate the complications related to medications.

  Limitations

  - The reading gathered by the smart pill is accurate hence it should be secured and should be stored in a highly secured place to prevent unauthorized users to access and use it in a harmful manner.
  - As well as the method of ingesting the smart pill might not sound comfortable to different people considering their body types.
  - The smart people must be kept affordable and should be taken under the supervision of the health professional to reduce the risk of any accidents.

- **Ambient Assisted Living**

  The increasing number of older people has led to making more advancements in technology and its services for the improvement of their quality of life. Ambient assisted living is a high-tech intelligent system deployed for elderly people to have

a better, healthier, and safer environment. This technology is a combination of two fields such as wearable devices and mobile technology which allows the health professionals and caretakers to give accurate treatment to elderly people during emergencies at home. The smartwatch is used for fall detection and sends an automatically generated message to the designated healthcare professional at times of great distress. As the smartwatch is connected with the mobile application via Bluetooth the phone can also call up the healthcare professional.

Limitations

- In the Ambient assisted living two technologies are being used the smartphone and the smartwatch, the smartwatch itself doesn't have any sort of internet connectivity to have proper functionality as a result it is synced with the smartphone via Bluetooth technology which makes it dependent for the transmitting the data into it.
- Secondly, this technology is costly as a result not all elderly people might be comfortable to afford it which is one of the drawbacks of using this technology.
- Lastly, the smartwatch should be kept in range with the smartphone because the Bluetooth connectivity varies in range with the device. Hence with the increase in the distance between them may cause communication failure and lead to misinterpretation of the data itself.

- **Smartphone medicine**

Smartphones have become one of the necessary aspects of human life where people are completely relying on smartphone technology to do the basic tasks in their day to day lives. Smartphone technology has not been used before as it is used now. The principle of smartphone medicine technology is to enhance the health and other health-related areas of people during their daily lives. There have been many wearable devices available in the market for specific usages for the patient. These devices are being connected with the smartphone or any wearable devices that can be attached to the human body. This device picks up the signal from the body in the form of sensors which is then collected and stored in the form of data which is then synced with their respected IoT cloud provider. With the process described above smartphones have enabled real-time data streaming because they act as a form of a hub that connects different wearable devices at the same time. The sensors used in the smartphones also capture the environmental data which includes weather reports, the air quality index, vital sign monitoring system, ultraviolet light

measurements. These data when gathered in real-time helps in assessing the daily risks that can be caused to the patient or the individual without them having the awareness of it. the medicalized smartphone is stepping towards the future of smartphones which supports both medical and healthcare applications. The smartwatches can measure the basic vital signs of the body whereas medicalized smartphones now can perform blood tests at certain hospitals along with it, it can store many other human body readings and measurements, stores it for the future use.

Limitations

- The smartphone medicine technology requires the pairing of other devices to provide efficient results of the body.
- Secondly, the implementation of this technology requires high costing which is its drawback.

6.1 Wireless sensor networks

Dishongh and McGrath (2010) have defined Wireless sensor networks (WSN) constitute numerous numbers of small-sized battery-powered computing devices that are scattered throughout a physical environment. Now each device senses, collects, monitors, and displays the information collected from the environment. The devices sense the values collected for temperature, vibration, humidity, or any other health-related data which can be captured. It gives the output of analyzing as blinking the LED lights, change the color on the display which makes the person aware that the data is being gathered and processed.

The usage of such wireless network devices is in industrial, environmental, and in the healthcare applications in which the data gathering process is tedious and time-consuming. A WSN device can also be called as a packaged data collecting device made up of a sensor, an actuator, a radio stack, a processor with a powered delivery mechanism (Dishongh & McGrath, 2010).

The implementation of wireless medical sensor networks (WMSN) has enhanced certain fields of healthcare such as emergency response, in-hospital communication, out-hospital monitoring to various environmental monitoring services. The below figure depicts the architecture of wireless sensor networks for healthcare applications.

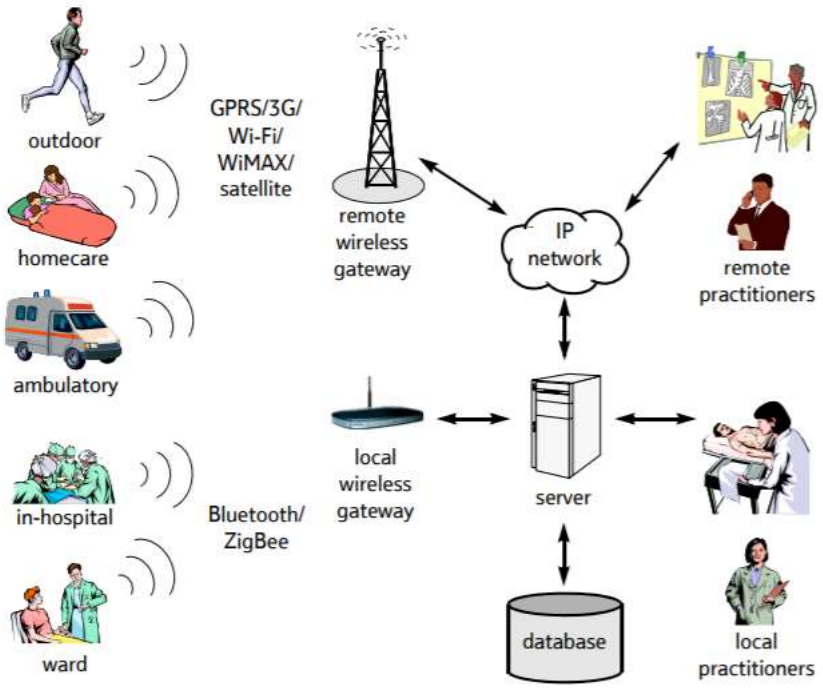

Figure 4: System architecture of wireless sensor network in healthcare application by (Ng, Sim, & Tan, 2006)

Recent applications of Wireless sensor network system in healthcare

CodeBlue technology is made up of wireless infrastructure which is deployed in emergency medical care. The configuration of this technology consists of low-power adapters, wireless vital sign monitoring sensors, personal digital assistants, and a PC-class system. It improves the response time to assess the patient on their location by making sure that a continuous transfer of data is taking place between the healthcare professional with proper allocation of the hospital resources (Ng et al., 2006).

Scalable Medical Alert Response Technology (SMART)

The system monitors and tracks the patient by location detection at the emergency site and throughout the process of transport, triage, stabilization until the patient is admitted to the healthcare facility and is assigned to the professional. The system is made up of a location-based monitoring system with a remote transition for medical sensors and information display for personal assistant data along with a detection unit. The SMART technology keeps the patient, health professionals, and various medical equipment in alignment in case of any emergencies (Ng et al., 2006).

MobiHealth technology uses mobile value-added services for healthcare applications with 2.5G and 3G technologies. Body Area Network (BAN) is being deployed in which sensors and actuators are embedded in the body. These devices continuously transmit the vital signs generated from the body with audio and video feeds to the healthcare professionals and caretakers. This technology is also used in disease prevention and diagnostics, remote assistance, para-health services, and also in sports. It can also be used by paramedics by providing remote assistance during any vehicular accidents by providing live audio and video feed of the place of incident (Ng et al., 2006).

Limitations of wireless sensor networks in healthcare are as follows (Ng et al., 2006)

- The sensor has a limited amount of power, memory, and bandwidth which makes it more vulnerable for its implementation in the healthcare applications.
- Secondly, the open environment may cause to tampering of the sensor nodes which makes it less functional.
- Thirdly, the sensor network is a combination of many mobile sensor nodes organized in flat or hierarchical representation which may lead to the overhead of the messages which affects the authentication and key changes processes.

6.2 Cloud computing in healthcare applications

Cloud can also be known as a "Data Hub" of information in which all the sensitive data is transmitted, stored, analyzed, processed, and sent to the individual. Cloud computing also proves cost-effective when it comes to storage and usage of data. Nowadays all healthcare providers as well as the insurance companies are moving towards cloud computing as a means of storing the electronic health records of the patients. The electronic health record of the patient is collected by the means of healthcare applications as well as any wearable devices. The data of the wearable devices as well as the applications are then transmitted to the cloud platform via wireless sensor networks.

All the recent applications from the enhancements of healthcare applications in IoT as well as in wireless sensor networks, the data is gathered to the IoT cloud platform. From that, all the health professionals as well as the caretakers can easily access them at their convenience.

7. Research methodology

The research methodology conducted in the thesis is a quantitative collection of information. The step-by-step process of the methodology is explained below

1) Extracting the desired content from different research papers.
2) Refining the content to narrow down the process.
3) Implementation of the refined material.

Extracting the desired content from different research paper

After investigating different fields in healthcare applications, it is important to gain meaningful and valuable information from different research papers. Not all the research papers will be having the desired content which is needed for the research as a result a precise and concise process of extraction is done from which all the necessary information was being taken to write the research paper.

Refining the content to narrow down the process

When the desired material is obtained it is necessary to refine the content to give it a final touch which allows any non-techno-savvy individual to grasp the information easily upon reading the material. With the refining process is done it keeps the path clearer by eradicating any confusion to the person reading the research paper.

Implementation of the refined material

Implementation is the final part of the process which allows all the valuable content collected, analyzed, and refined kept in a proper structural manner. With this, the individual will have a clearer idea that everything is in alignment with the result.

8. Problem analysis

The paper highlights the advances in the field of healthcare applications in the Internet of Things which has changed the view the world is seeing right now. At the beginning itself, we have seen the evolution of the web which leads towards the establishment of the Internet of Things. Upon researching further, the applications are diversified into different fields of healthcare such as the blood pressure monitoring system, body temperature monitoring system to the implementation of wireless sensor networks. The wireless sensor network is considered as one of the pillars in healthcare applications.

The major functionality of the wireless sensor networks is that these devices are a medium through which the sensitive and valuable information of the patient or any individual is transferred with the help of sensor nodes, antennas, and integrators. The wireless sensor networks work effectively in two ways 1) is the healthcare application itself which monitors the data with the in-built sensors in the smartphones and 2) are the wearable devices of any kind which are implemented in-body and on-body of the patient or any individual who wants their data to be kept safe and used further in case of any illness or emergencies. When it comes to the networks there are always its drawbacks or loopholes which should be sealed or taken care of for its successful implementation. When using the wireless sensor networks, it is a must to have a security mechanism deployed which takes care in process of transferring and analyzing the patient's data. These security mechanisms minimize and reduce various security threats as shown above as well keeps the privacy of the patient safe by keeping any unauthorized personnel or an individual with a malicious intent to cause harm to the patient or the organization accessing the data. As a result, implementing them will make the process of evaluation of data an easy flowing.

Now as described above the Cloud platform is one of the "Data hub" for all the sensitive and confidential information of the patient. When it comes to its functionalities the cloud is the center of attraction that links the healthcare applications and wireless sensor networks together and makes sure they are in alignment with various complex data processes. As a result, it makes the Cloud platform more vulnerable to different security attacks from any unauthorized personnel. In the case of Cloud platforms, certain security models can be deployed to protect it from any possible attacks. These models take the electronic health records collected from the healthcare applications and wireless sensor networks into consideration as it is the most valuable piece of information when it comes to healthcare applications. These models act like a wall which makes it hard to penetrate from the cyber-attacks from outsiders. Along with it comes the significance of the digital signature and verification which is an important layer when handling the data. It allows only the

authorized personnel handling the patient to view, modify, and transfer it to other corresponding health professionals or organizations. Hence, by embedding these models with the digital signature and verification process it keeps the security and privacy issues of the patients at bay.

9. Evaluation and existing countermeasures.

There are certain requirements to be kept in mind to deal with the security and privacy issues for the healthcare applications which are given by (Kumar & Lee, 2012)

In this section, we'll be focusing on **various security and privacy requirements** for healthcare applications along with a robust and precise solution.

1) **Data confidentiality**: The patient health data generally falls under the category of legal and ethical responsibilities of confidentiality. The health data that is being gathered from the applications via wireless sensor networks must be kept private and confidential to the health professionals and the caretakers. To keep any unauthorized individual from eavesdropping of the private data, the implementation of the confidentiality must be kept and maintained. Data eavesdropping may lead to some serious outcomes as any traitor or attacker may use it to cause any harm to the patient's information by breaching its privacy. As a result, data confidentiality is one of the major requirements to be considered for healthcare applications.
2) **Data authentication**: Data authentication will lead to an authorization which is mandatory for both medical and non-medical applications. In wireless sensor networks, it is important to have data authentication from the sensors itself to avoid any false data to be sent by an intruder who tries to cause harm to the patient's privacy and security.
3) **Strong user authentication**: One of the major problems in a wireless sensor network which makes it open for any attack is the exchange of wireless message to any unauthorized user. Hence it is highly recommended to have a strong user authentication. One of the examples is "One Time Password (OTP)" also can be called two-factor authentication which immediately alerts the health professional when someone tries to access the patient information. As a result, each user must provide a form of authenticity for accessing any kind of information of the patient.
4) **Data integrity:** Data integrity provides a form of assurance to the receiver of the data that the data has not been altered throughout the process of transmission. The wireless sensor networks have a broadcast nature that allows any individual to make changes in the data through the transmission channel. One must possess the ability to pinpoint any data alterations if done by the attacker as any mishap can lead to serious events.

5) **Key distribution**: Whenever two organizations are exchanging sensitive and valuable information through a medium, a session key must be taken in place. This key will only be accessible to the parties doing the exchange. It will provide a form of protection from any security attacks done by any individual having malicious intent. Therefore, it is mandatory to have a proper key distribution scheme in place to protect the patient's privacy.
6) **Access control**: In certain healthcare applications, the users have direct access to the patient's information which possess a great threat to their privacy. To prevent any unauthorized individual to have access to the information a role-based access control mechanism should be kept in place to avoid any serious situations.
7) **Data availability:** Data availability makes sure that all the information and services are available at all times. The medical node sensor availability makes all the data regarding the patient available to the healthcare professional and caretaker. In some situations when the sensor nodes are captured by any individual the data availability is lost as a result it is mandatory to keep the "always-on" mode of operation for the healthcare applications.
8) **Data freshness**: In healthcare applications, data confidentiality and integrity are of no use if the data freshness is not being kept. Data freshness means the data received from the patient is live and is continuously monitored without being altered by any individual. There are two types of data freshness 1) weak freshness: this includes partial message ordering without any time constraint and 2) strong freshness: it is a combination of request-response pair which allows any delay estimation.
9) **Secure localization**: One of the strong points in healthcare applications is the ability to pinpoint the live location of the patient. Any loose ends in the patient tracking system allow an attacker the ability to extract the live location of the patient to cause any harm.
10) **Forwards and backward secrecy**: In real-time healthcare applications the new medical sensors are replaced with the old ones in case of any failures, hence it is important to deploy forwards and backward secrecy. In forward secrecy, the medical sensor has not the ability to read the future messages once the message has been transmitted from the network. In backward secrecy, a sensor is attached to the network which couldn't read the previous messages that are being sent.
11) **Communication and computation cost**: The wireless sensor networks are resourceful devices in which the healthcare applications need a certain amount of

space to perform the predefined tasks allocated to them. Hence, security schemes must be effective and precise in terms of communication and computation costs.

12) **Patient permission**: Patient permission is a must when the healthcare professional is handing over their private information to other healthcare personnel. Hence, the approval to do so from the patient is a mandatory thing to do before passing it over.

9.1 Existing security mechanisms for wireless sensor networks

According to Kumar and Lee (2012) and (Martins & Guyennet, 2010), security mechanisms are collective measures taken place which is used to detect, prevent, and recover from the security threats on healthcare applications.

1) **Key establishment and trust setup**

   To set up a sensor network it is mandatory to establish cryptographic keys. Key establishment techniques should be kept in place with numerous nodes taking part in data extraction and transfer just as a single key should be there with the two parties which are exchanging sensitive information through a medium. Establishing a key environment will add a security layer against cyber threats.

2) **Secrecy and authentication**

   The sensor network application is more vulnerable to cyber threats such as eavesdropping, injection, and medication of the information. As a result, cryptography is the first line of defense that protects the network from malicious attacks by embedding into the sensor networks. When operating in point-to-point communication high-level cryptography plays a major role in security purposes.

3) **Privacy**

   Privacy is the main concern when dealing with sensitive information of the patient. The deployment of sensor networks might lead to some privacy concerns among the patients. As a result, awareness of the sensor networks should be made among the patients to tackle the network from malicious attacks.

4) **Intrusion detection**

   The wireless sensor networks are vulnerable to many forms of intrusion attacks from the cyber attackers which pose a threat to leakage of sensitive data of the patient. With this by the implementation of secure groups makes it less possible for any intrusion to occur within the network.

5) **Secure data aggregation**

One of the benefits of using the wireless sensor networks is that a big chunk of the dataset is broken down into fine granules of data which makes it less susceptible to the cyber-attacks. Because as the data is being broken down into small blocks any individual having the intent to intrude in the process will not be able to read the entire data itself.

9.2 Cloud computing security models for healthcare applications

According to Zhang and Liu (2010), there are several security models deployed for health professionals and caretakers to protect the sensitive information of the patients from the perspective of healthcare applications. In this section, we'll be discussing those models which are used by them to have a better understanding of the protection of healthcare applications.

1) **EHR secure collection and integration model**

Electronic health record (EHR) is the sensitive information which consists of valuable information regarding the patient. The first step is the secure accumulation and integration of the EHR data from the multiple EHR repositories which are handled by the care delivery organizations (CDO). This allows one CDO to share the EHR with other CDOs. One of the main important functionalities used in this is the EHR integrator which does two important processes such as it makes sure that all the EHRs that are being received by the CDO are accurate and checks for confidentiality, integrity, and data authenticity. After that it merger the data collected into a single file with a security certificate attached to it. in this way, it prevents any unauthorized individual from accessing the data by keeping it secure for a longer time duration.

2) **EHR secure storage and access management model**

The secure storage and access management model allows the health professionals to access the data restricting any unauthorized personnel from accessing it. the access control compromises of collection of role-based and attribute-based access control policies and HIPAA compliance policies which gives them authority to only the health professionals and caretakers to interact with the information. Even the decryption mechanism is accessed by authorized individuals whenever there is a case of any emergency.

3) **EHR secure usage model**

This model allows only the verified users including the health professionals and the patients as well to access the content of the EHR data. This model consists of two steps 1) Signature: once the patient has been examined thoroughly and is ready for further

treatment, the health professional creates a unique electronic medical record certificate with a signature that is only allowed to the patient and the health professional who is allotted for further treatment. Secondly, is the verification when that patient is sent further with another health professional, they verify all the details through the certificate and the signature generated by the previously authorized person.

9.3 Signature and verification

A digital signature is one of the important tactics that is being used in healthcare applications as well as it is used by the health professionals and caretakers to provide authenticity, integrity, and non-repudiation. The digital signature itself is a mark of privacy of the patient's information as it is unique for individuals. In this section, we'll be focusing on three important signatures for healthcare applications in the cloud environment.

1) **Anonymous signature (Zhang & Liu, 2010)**

   This signature scheme provides anonymity to the signer itself which protects its sensitive information from access by the unauthorized personnel. There two basic types of anonymous signature such as group signature and ring signature.

   a. Group signature: In this signature scheme, a member of the group can anonymously sign a message on behalf of the rest of the group. The members of the group will be able to sign the message with their secret keys. Now upon doing the signature, it can be easily be verified by the members who know the public key by keeping the identity of the original signer secretive. There will be a group manager of the group who can reveal the signer in case of any emergencies.

   b. Ring signature: This signature can be done by any member of the group of users. The ring signature itself is a ring-like algorithm used to perform the signature. The ring signature on the message can only be done by a particular member of the group of users and not everyone has the authority to do so. One of the best qualities of using the ring signature to sign a message is that it remains unknown that an individual's key has been used to do the signature which provides security and confidentiality. The ring signatures perform way better than group signature in two ways: it is impossible to trace back the identity of the individual who signed the message and any group of users are used as a group for the ring signature without doing any previous setup.

2) **Threshold signature (Zhang & Liu, 2010)**

A threshold signature is one of the methods used for signing the digital medical certificate. The certificate is only signed by only one health professional but also a person from the subgroup of health professionals. Int his way it is difficult to decrypt the signature and to reveal the identity of the person.

3) **Digital credential (Zhang & Liu, 2010)**

Digital credentials are a digital representation of paper-based credentials such as passports, credit cards, health-insurance cards. These credentials are assigned by the trusted organizations that provide a sense of authenticity which can be easily verified when needed. To define credentials, it is a mark of completion, clearance, or competence which is attached to the individual. In the same scenario, the digital credential relates something important to the owner. The main key point of using digital credentials is that the users are given cryptographic tokens which are unique in themselves that allows them to verify themselves with the relations to the private and public relationships towards the organizations by keeping their identity secretive.

9.4 Discussion

We live in a world where we all are surrounded by data if it's a small-sized smartwatch or a big cloud platform containing massive amounts of information. Each data is unique and sensitive to an individual. From the thesis conducted above and from a precise observation the monitoring and eavesdropping of the patient's vital sign is an important threat to look out for. As the data is sensitive, the individual eavesdropping on the data can easily monitor it and can infiltrate false data into it which leads to some serious concerns. with the false data being filtered in the treatment of the patient will be in jeopardy. From this, the data further transferred to the cloud will also be false with the eavesdropping attack in the beginning. As a result, the moment someone eavesdrops on the data signs and causes it to harm the further the chain of action will be disrupted which causes some serious issues regarding the patient.

10. Conclusion

In the thesis, we have seen the various advancements of technology in the field of healthcare by using different applications and wearable devices via wireless sensor networks. Along with it, we saw how cloud computing plays a major role when dealing with sensitive information of the individual. With these advancements in place, we observed the threats and privacy issues facing them and upon precise observation, the threat of eavesdropping on the patient's vital sign should be of more concern as it is linked with further threats. An existing countermeasure is in place which can prevent these attacks from happening. As a result, from the research, there are way more advancements to be done in the area of healthcare in the mere future and with those its countermeasures should also be kept in mind.

11. References

Aceto, G., Persico, V., & Pescapé, A. (2018). The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges. *Journal of Network and Computer Applications, 107*, 125-154.

Alam, M. M., Malik, H., Khan, M. I., Pardy, T., Kuusik, A., & Le Moullec, Y. (2018). A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE access, 6*, 36611-36631.

Baig, M. M., GholamHosseini, H., & Connolly, M. J. (2015). Mobile healthcare applications: system design review, critical issues and challenges. *Australasian physical & engineering sciences in medicine, 38*(1), 23-38.

Banerjee, S., Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *The Information Society, 34*(1), 49-57.

Boulos, M. N. K., Wheeler, S., Tavares, C., & Jones, R. (2011). How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX. *Biomedical engineering online, 10*(1), 24.

ishongh, T. J., & McGrath, M. (2010). *Wireless sensor networks for healthcare applications*: Artech House.

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2015). The internet of things for health care: a comprehensive survey. *IEEE access, 3*, 678-708.

Kulkarni, A., & Sathe, S. (2014). Healthcare applications of the Internet of Things: A Review. *International Journal of Computer Science and Information Technologies, 5*(5), 6229-6232.

Kumar, P., & Lee, H.-J. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. *sensors, 12*(1), 55-91.

Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers, 17*(2), 243-259.

Lu, T.-C., Fu, C.-M., Ma, M. H.-M., Fang, C.-C., & Turner, A. M. (2016). Healthcare applications of smart watches: a systematic review. *Applied clinical informatics, 7*(3), 850.

Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: a review and recommendations. *Journal of medical systems, 39*(1), 181.

Martins, D., & Guyennet, H. (2010). Wireless sensor network attacks and security mechanisms: A short survey. In *2010 13th International Conference on Network-Based Information Systems* (313-320).

Ng, H., Sim, M., & Tan, C. (2006). Security issues of wireless sensor networks in healthcare applications. *BT Technology Journal, 24*(2), 138-144.

Ssegawa, A. K., & Ezekia I, U. O. (2015). International Journal of Computer Science & Information Security.

Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. In *2010 IEEE 3rd International Conference on cloud Computing* (268-275).