Research on evolved security threats and solutions for Healthcare IoT (IoMT)

MINT-709
Capstone Project Report

Presented by
Sukhpreet Kaur Khalsa

University of Alberta
Master of Science in Internetworking
Department of Electrical and Computer Engineering

Supervisor
Sandeep Kaur

ABSTRACT

In March 1876, Alexander Graham Bell made the first practical telephone call, and the concept of communication using the telephone had been evolved. Initially, mobile phones were considered a luxury item, but nowadays, they include people's daily necessities. The goal of different features behind mobile communication has increased since the last decade. Availability of multitasking smartphones and other applications for various purposes with high capabilities has become a trend.

Integration of IoT with mobile applications is the hot trend, which boosts the power of mobile communication. Researchers of every field like engineering, medical, science, arts are accepting the fundamental of IoT. The Internet of Medical Things has grown to be a prominent feature of Information Technology, where healthcare services integrate with IoT technologies. Real-time support, independent care for the elderly, tele-auscultation, remote monitoring, and patient treatment using IoMT has been increasing day by day. Now, there is a need to enable secure mobile broadband service everywhere and at any time.

For conducting robotic surgery, a high data rate is needed. Moreover, there is a requirement to tackle the present challenges like: - direct attacks against connected surgical robots and indirect attacks against ambient devices to design a reliable and cost-effective but secure communication setup for remote/robotic surgery applications.

The research report mainly focuses on evolved security threats and solutions for healthcare IoT (IoMT), where robotic or remote surgery has been selected for deep study. In the research report, IoT communication protocols used in applications of IoMT have been classified, and the main characteristics of IoT communication protocols have been evaluated, which are used at the perception, network, and application layer of medical devices. In the next step, an examination of the evolved security threats is figured out. Based on realistic attacks, the list of the available mitigation controls that may be applied to secure IoMT communications has been defined. The research report has included all aspects of 5G compared with previous standards, which would be helpful to cope with the selected security threat for robotic or remote surgery.

ACKNOWLEDGEMENT

Before I start writing anything, I would like to be thankful **THE ALMIGHTY** for everything that He gave me till now. Secondly, I am thankful to my teacher **SRI GURU GRANTH SAHIB JI**, who always shows me the right path to follow. After that, I love to write my husband's name **Sardar Satwant Singh**, who supported me financially and mentally, during my MINT program. I am grateful to all **Gursikhs** (especially **S. Bharpoor Singh** and **S. Harbans Singh**), who assisted me in various situations.

I'm delighted to thank my mentor **MSc. Sandeep Kaur**. She always supported and guided me and gave me valuable inspiration and suggestions in my research for knowledge. She gave me the freedom to study my project while still making sure that I did not diverge from the core of my subject. The project would not have been possible without her knowing guidance.

I would also like to express my sincere thankfulness to **Mr. Shahnawaz Mir** for providing me with such a great opportunity and for allowing me to opt for a project of my interest.

I am proud to acknowledge my gratitude to **Dr. Mike McGregor**, who allowed me to start this project.

I would also like to express my sincere thanks to my In-laws' family **(Sardarni Jarnail Kaur**, **Sardar Balwant Singh**), Veer **Gurdarshan Singh**, Veer **Satinderpal Singh**, my friend Engr. **Ranjodh Kaur**, my brother Engr. **Harpreet Singh**, Engr. **Manvir Singh,** Engr. **Gurbir Singh,** all the **instructors, professors, seniors, classmates,** and the entire **University of Alberta** who helped me directly or indirectly in this study and has been helpful and cooperative in giving their support in every situation to help me achieve my goal.

In the end, I would like to mention the name of my village (**V.P.O. Husner, Tehsil Gidderbaha, District Sri Muktsar Sahib**) from where I came here in Canada to acquire knowledge in the stream of Internetworking with the blessing of my parent (**SI. Balkar Singh, Mrs. Manjit Kaur**)**,** and grandparents (**Late Mr. Malkit Singh, Mrs. Nihal Kaur**).

Table of Contents

List of Tables

……

List of Figures

1 INTRODUCTION

Healthcare IoT (IoMT) discovered major changes in the healthcare industry. Before IoT, Patients were limited to visit, call or text for communicating with the doctor. Specialists or emergency clinics could not screen patients' wellbeing consistently and make recommendations appropriately. Nowadays, it is possible to monitor a patient's condition remotely, including other features like remote treatment using robotic surgeries and tele-auscultation.

For conducting robotic surgery, a high data rate is needed, and various security threats are present, which can be divided into a direct attack against connected surgical robots and indirect attacks against ambient devices [1]. The operator needs to be within the remote site's proximity to reduce or mitigate the performance degradation resulting from large latencies [2]. 5G networks would carry a significantly higher volume of data while maintaining reliability and reducing the latency problems, improving access to mobile robotic surgery [3]. The demands for remote surgery, which were not reached by the 4G/Long-term evolution (LTE) mobile communication standard, could meet by 5G [4].

1.1 RESEARCH METHODOLOGY

Overall, research is divided into three phases. The process of all phases follows the various features from the approach described in [5] and answers the predefined research questions.

Phase 1:- To research about 5G technology and compare 5G with the previous technologies. It is based on the following research question:-

- RQ1:- What is the technical overview, history, system standard, key features of previous network technologies, and 5G?
- RQ2:- Why 5G is better than other technologies for IoMT in the future?

Phase 2:- To elaborate on the benefits of IoT, the research includes the major applications of IoT in all sectors. IoMT in the Healthcare sector is elaborated in detail and focuses on remote and robotic surgery. Based on the following research questions, the research is addressed the various security threats of remote or robotic surgery:-

- RQ3:- Which IoT protocols are used in the context of remote or robotic surgery using IoMT?
- RQ4:- What are the security threats available at the current stage of remote or robotic surgery?

Phase 3:- To find the solution and conclude the research, the result of phase 1 and phase 2 will be analyzed. The following research questions are answered in the report:-

- RQ5:- What features of 5G can become a solution to the present problem?
- RQ6:- What other solutions are available and can be integrated with 5G while doing remote surgery using IoMT?

1.2 MOBILE COMMUNICATION EVOLUTION

In 1946, the first public Mobile (car-based) Telephone System (push-to-talk system) was introduced. It used analog frequency modulation and high power BS tower to cover 50 miles radius. In 1960, an improved mobile telephone system (IMTS) was developed, which was able to provide full-duplex services and direct dialing by using 23 FM channels with 25-30 kHz bandwidth [6]. The first handheld mobile phone was demonstrated in 1973 by Motorola employee Martin Cooper. He made a call by using the world's first commercial cell phone known as Motorola DynaTAC 8000x from New York City to the headquarters of Bell Labs in New Jersey. It had happened nearly three decades after the introduction of the first mobile phone service MTS [7].

Hence, before the early 1980, wired communication was a very popular way of communication, but after that, there was an invention of a new technology known as mobile communication or wireless communication, which allows people to communicate with each other in different locations without using any wire or cable connection. The following figure shows the evolution flow of wireless communication.

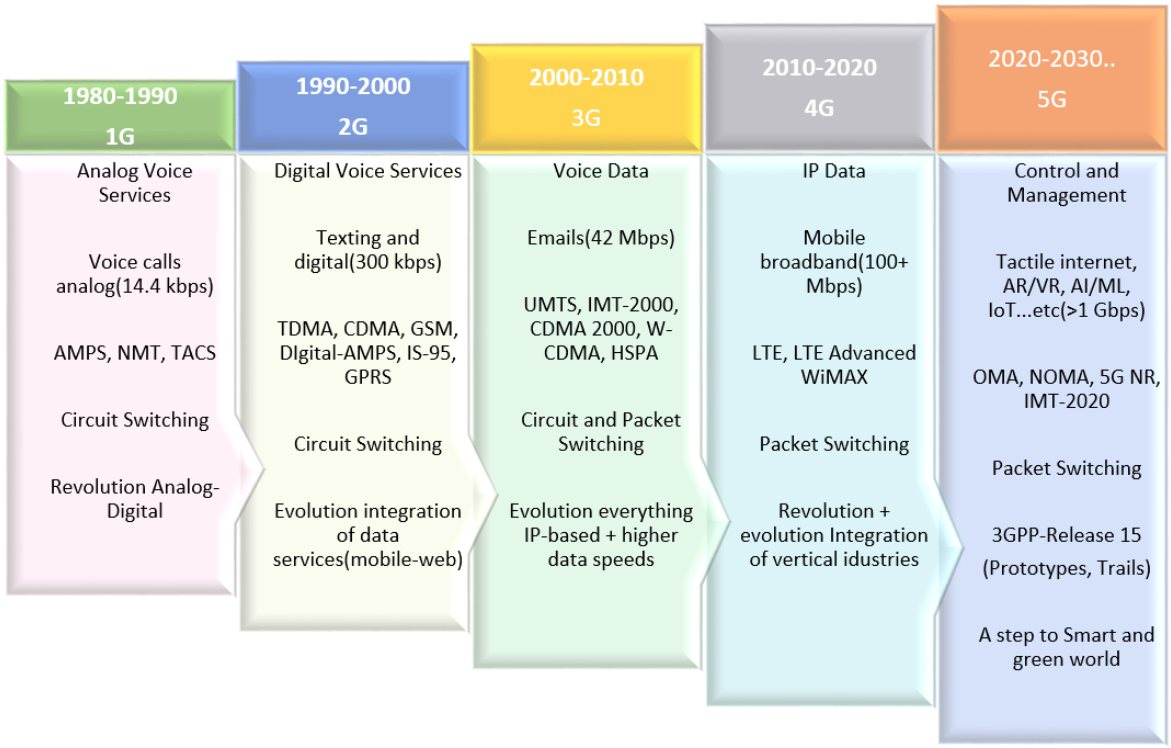

Figure 1: - Evolution of Wireless Communication

The above figure shows the evolving generations of wireless technologies in terms of services, data rate, technology, and revolution or evolution in a specific period. With the growth of wireless technologies, services, data rate, mobility, and efficiency is increasing. It also shows that 1G and 2G technologies use circuit switching, 3G use both circuit and packet switching, while 4G and 5G use Packet Switching only.

1.2.1 FIRST GENERATION

In the 1970s, private companies have begun fostering their systems to advance the current system further. Analogue Mobile Phone System (AMPS) is known as private systems, used in America; Total Access Communication System (TACS) and Nordic Mobile Telephone (NMT), utilized in parts of Europe; J-TACS, used in Japan and Hong Kong.

Independently developed systems are known as 1st generation communication. Bell Labs introduced these systems in 1982. It was popularly known as Advanced Mobile Phone System (AMPS). The key idea here was to divide isolated geological regions into cells. Every cell was served by a base station so that frequency could be recycled. AMPS could support 5 to 10 times more users than IMTS.

1.2.1.1 AMPS Technology

All 1G cellular systems depend on analog frequency modulation for voice and data transmission. In-band signaling is used to move control data among terminals and the network's remainder during a call. The architecture of AMPS is consists of the following main components: -

- Mobile Station (MS)
- Base Transceiver Stations (BTS)
- Mobile Telecommunication Switching Office (MTSO)

MS is a user handset that was used by a mobile user to communicate with another user. Each cell has BS, and it includes an antenna, controller, transceiver, which is further controlled by a small office. AMPS works on the principle of Frequency Division Multiple Access (FDMA), where every user is assigned with their frequencies, and it separates the user channels within the given spectrum. The following image depicts the AMPS architecture. [8]

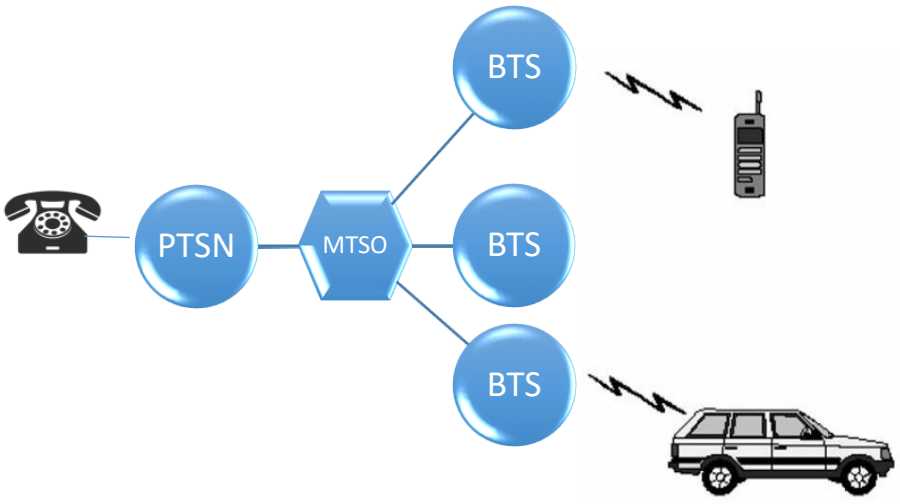

Figure 2: - AMPS Architecture

Figure 2 shows that the MTSO (currently known as Mobile Switching Center (MSC)) is a central part of the whole communication system. MTSO was performing the following functions: -

- Interconnecting calls within the Cellular network and to other PSTNs as well
- Registration and authentication
- location updating
- Call routing
- Compiling billing information

MTSO consists of databases such as Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and Authentication Center (AUC). HLR stores the documentation of the mobile subscribers of the network, whereas VLR performs temporary caching of the details of subscribed users. EIR is used to keep the record of blacklisted mobile phones and AUC to authenticate every mobile user and encrypt the mobile communications between phone and network. The MS and the BS provided Air Interface. The MS could change its operating frequency to those diagnosed by the MSC and also its output power level if instructed. BS works as an interface between the MSC and MS. It received both signals and instructions from MSC. The Base Transceiver Station (BTS) was retained in DAMPS and GSM as well. PSTN acts as an edge gateway to route the calls within the same area code, and it mainly consists of transmission, switching, signaling, and intelligent networks. [8]

1.2.1.2 Disadvantages of 1G

First-generation has various disadvantages such as weak security on the air interface, inferior voice associations, unwanted eavesdropping by third parties during a call, full analog mode of communication, and no roaming. Even though the data about the number being dialed could be encoded, the serious issue was transmitted through the air, as signals could easily be received by using any FM receiver since the transmission used frequency modulation [9].

1.2.2 SECOND GENERATION

To implement the roaming system, Individual organizations started working under one umbrella known as European Telecommunications Standards Institute (ETSI) and developed a 2G system. In 1991, second-generation cellular telecom networks were commercially launched. It was based on Global System for Mobile Communication (GSM) standards and able to deliver data at the rate of up to 9.6 Kbps. CDMA (to carry radio transmission) and IS-95 were included as other key technologies [10]. In 2G, the digital modulation scheme was implemented rather than analog signal-based communication. Due to this change, overall performance rapidly improved. Because of multiplexing techniques TDMA and CDMA, several users could use a single channel.

1.2.2.1 Global System for Mobile Communication Architecture

GSM architecture mainly consists of three components: -

- Mobile Station (MS): - It is a combination of two parts known as Mobile Equipment (ME) and Subscriber Identity Module (SIM).
- Base Station Subsystem (BSS)
- Network Subsystem (NSS)

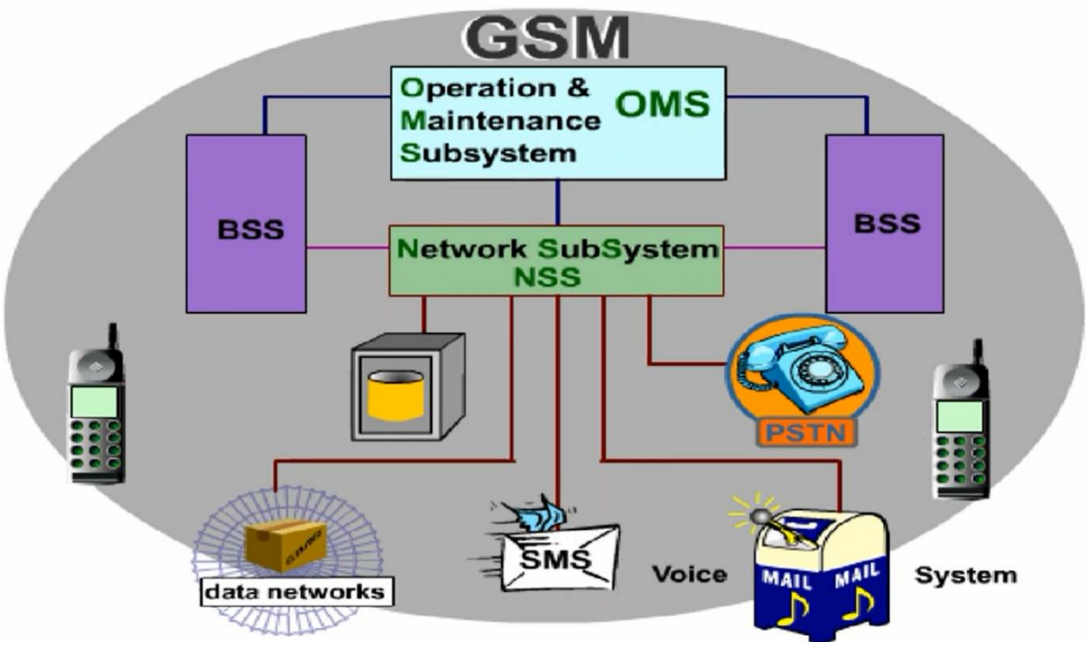

Figure 3: - GSM's basic Architecture [11]

Figure 3 shows that BSS provides the connection between the MS and the NSS. The NSS forwards user signals to other Mobile through a BSS or subscribers in the Public Switch Telephone Network (PSTN) and provides necessary customer data. The OMS monitors the performance of BSS and NSS. It remotely debugs occurring faults in the network elements as well. There are some additional components, such as interface elements to the data network, the Short Message Service (SMS) center, and Voice Mail System (VMS), which complete the GSM system architecture.

Mobile Station communicates with a BTS through the wireless interface in the same cell in which the mobile equipment is located. MS is a combination of two elements that is ME and SIM. The ME is the physical device, which consists of a transceiver, digital signal processors, and an antenna. The SIM card is a unique component of the GSM system.

Base Station Subsystem (BSS) ensures the network coverage, and it includes a large number of structurally organized radio cells. It consists of the following elements: -

- Base Transceiver Station (BTS)
- Base Station Controller (BSC)
- Transcoder (TC)

BTS is known as **transmitting and receiving unit**. Figure 1.4 shows the elements of BTS. BTS **makes the connection to the MS** via the air interface and controls the Transceiver (TRX). The

TRX is the central functional unit of BTS, and it **maintains calls to a maximum of eight mobile stations through one frequency pair each**.

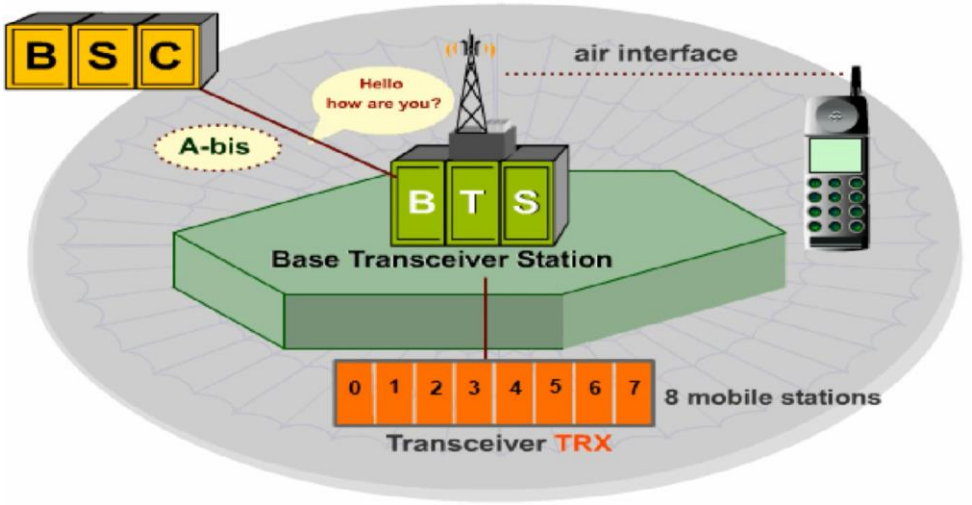

Figure 4: - BSS's component Base Transceiver Station (BTS) [11]

The BTS is also responsible for the different functions like **monitoring of the signal quality, encoding, and modulation of useful signals** through the A-bis interface to BSC. It **forwards calls signals and control information** to the base station controller BSC, which is destined for the OMS and the NSS.

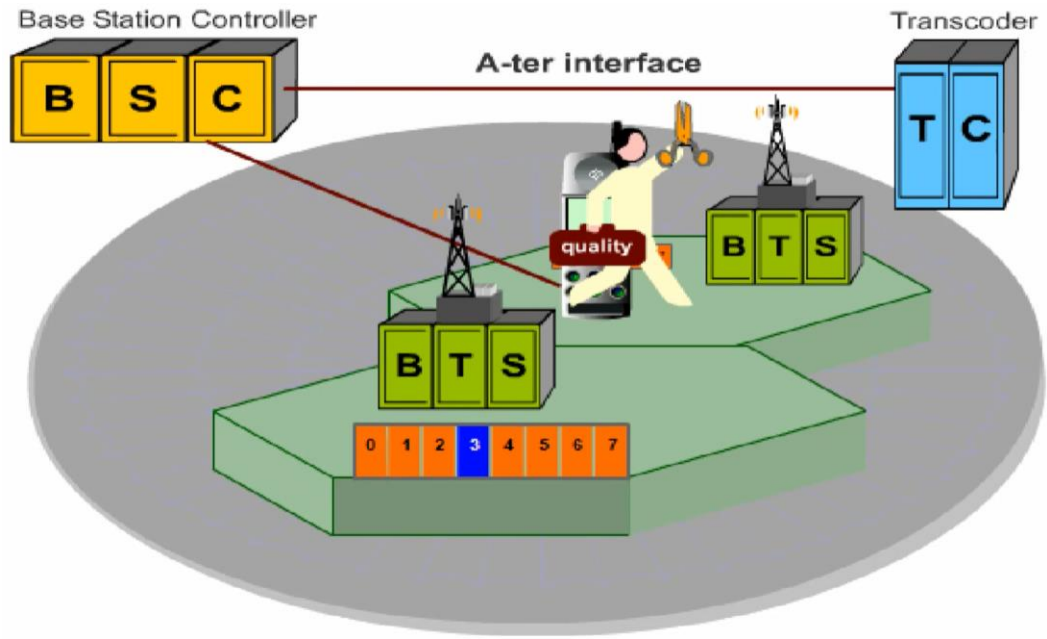

Figure 5: - BSS's component Base Station Controller (BSC) [11]

As shown in Figure 5, **BSC** is connected with BTS and TC as well. The major functions of BSC are as follows: -

- It controls several BTSs
- It assigns free radio channels in the TRX for the link to MS
- Controls necessary output power for TRX and MS
- It monitors the present radio link to and from the MS
- If neighboring radio cells are under its control, it controls handover between them
- During an existing radio connection, BSC monitors its quality
- Controls the disconnection of the radio link when the call is over
- Responsible for communicating with the Transcoder (TC) via the A-ter interface

TC is the third element in the BSS and is needed to convert 64 kbps original speech into a 16 kbps signal of speech description parameters.

To ensure a spectrum efficient modulation (the information rate that can be transmitted over a given bandwidth in a specific communication system) on the air interface, BTS, BSC, and TC together form the BSS.

Network Subsystem (NSS) is the third basic element of GSM. BSS forwards the signals to NSS. NSS controls and forwards the speech and circuits switched data to other networks if necessary. The NSS offers relevant data to security and mobility as well. It controls handoffs amongst cells in dissimilar BSSs, validates the users, and authenticates their accounts. It enables worldwide roaming of mobile subscribers as well. Mobile Switching Center (MSC) is the main component of NSS.

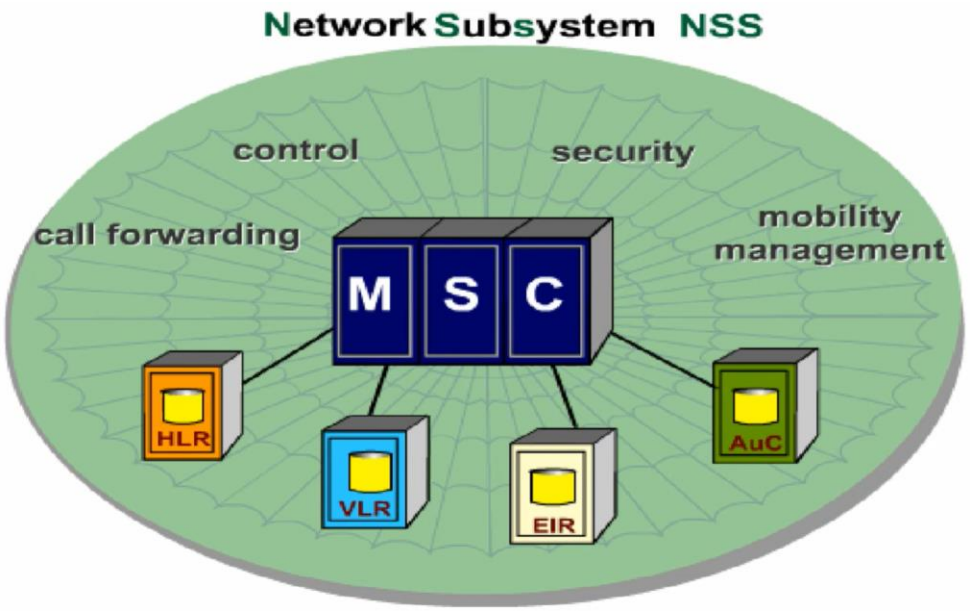

Figure 6: - NSS's Architecture [11]

Mobile Switching Center (MSC): - BSS's element TC processed the speech signals and reached MSC via A-interface. MSC serves as a digital exchange for the forwarding of messages or circuit-switched data. It connects mobile subscribers or subscribers in other networks such as PSTN, ISDN, or data networks. It is responsible for the following duties: -

- It forwards incoming and outgoing calls
- In the same mobile radio network, it makes a connection to other MSCs
- Makes connections with other mobile radio networks
- Calls Monitoring and controlling
- Responsible for call data acquisition and the forwarding of signaling information to connected registers or databases

For monitoring route and control of mobile telephone calls in GSM networks, the following registers are connected to the MSC: -

- **Visitor Location Register (VLR)**: - VLR is a database, and it is designed as a dynamic subscriber file with dedicated geographical areas of responsibility that are called **location areas**. The VLR **acquires the temporary data of all GSM customers** in its areas and is always well informed of their whereabouts. With subscriber information**,** It assists the MSC in getting hold of **charge-relevant data**. The bills are prepared from these data in the billing center by MSC.

- **Home Location Register (HLR): -** HLR database stores and manages user subscriptions. It keeps information of permanent subscribers, including their service profile, location information, and activity status. VLR gets customer data from GSM customer data acquisition from HLR. HLR data contain information on access rights about: -
  - Roaming
  - Voice Services
  - Fax Services
  - Data Services
  - Additional Subscribe Services

- **Authentication Center (AUC):** - The customer data is necessary to protect from unauthorized access and is most integral to the HLR. To do so, AUC perform the following duties: -
  - It checks the information stored on a SIM card. It is used for correspondence with his register.
  - Data must be identical to get the authentication of the subscriber. In case of no match, the network is disabled very easily by AUC.
  - It provides the essential information to cipher the air interface.

- **Equipment Identity Register (EIR):** The EIR is a database that stores information about the identity of mobile equipment. It permits the detection of stolen terminal equipment used in GSM networks by checking the International Mobile Equipment Identity (IMEI). IMEI reveals the details about the manufacturer, country of production, and device type. It is used to prevent calls from being misused, to prevent unauthorized MSs, and to report stolen mobile phones.

1.2.2.2 Advantages

The major benefits of 2G networks over their ancestors were as follows:-

- More efficient on the spectrum
- Digital encryption of phone conversations
- Allowed a far greater mobile phone penetration level
- Improved privacy using an encryption algorithm
- 2G cellphones were smaller than 1G, so they used less radio power, and the battery life lasted longer as well

1.2.2.3 Disadvantages

Major disadvantages of 2G were as follows: -

- GSM does not support a high data rate
- Unable to handle complex data
- Weaker digital signal
- Inefficient usage of bandwidth and resources

1.2.3 2.5 GENERATION

2.5G is known as 2nd generation cellular system converged with General Packet Radio Services (GPRS). A 2.5G system, for the most part, utilized 2G system frameworks. However, it applied packet switching along with circuit switching. Data rate had increased in 2.5G up to 144kbps.

1.2.4 2.75 GENERATION

When 8PSK encoding was introduced, the GSM network evolved to Enhanced Data Rates for GSM Evolution (EDGE) network. While the symbol rate stayed the same at 270.833 samples per second but each symbol rate carried 3 bits instead of one. As a result, EDGE was significantly faster, with a download speed of up to 384Kbps.

1.2.5 THIRD GENERATION

3G introduced services like video, audio, and graphics applications. It could present video communication and video streaming as well through cellular network correspondence. CDMA 2000 (Code Division Multiple Access 2000) and UMTS (Universal Mobile Telecommunications Systems), W-CDMA (Wideband Code Division Multiple Access), HSPA (High-Speed Packet Access) went under the 3G umbrella. 3G used circuit and packet switching both. The maximum data rate has been supported by 3g was: -

- 2.05 Mbps for stationary devices
- 384 Kbps for slow-moving devices
- 128 Kbps for high-speed devices

1.2.5.1 3GPP

For developing the truly global standards, the collaboration for both GSM and UMTS was expanded further from ETSI (from Europe) to encompass regional Standards Development Organizations. It includes ARIB and TTC from Japan, TTA from Korea, ATIS from North America, and CCSA from China. The successful creation of such a large and complex system specification required a well-structured organization. This gave birth to **3GPP (3rd Generation Partnership Project)** and which worked under the observation of ITU-R. **ITU-R** is one of the sectors of ITU, and its functions are: -

- Manages the international radio-frequency spectrum
- It ensures the effective use of the spectrum.
- Defines technology families and allocate spectrum
- Propose requirements for radio technology.

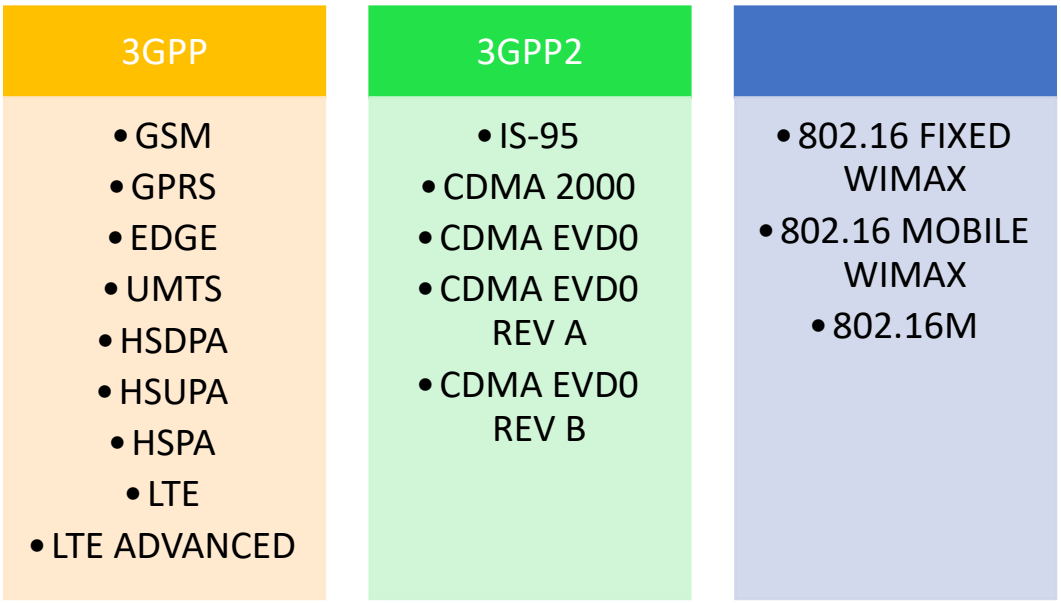

Figure 7: - Evolution of 3GPP, 3GPP2, and IEEE

The organization, which started developing standards to meet the requirements proposed by ITU-R, is known as 3GPP, 3GPP2, IEEE. Figure 7 shows the evolution of 3GPP, 3GPP2, and IEEE. 3GPP was dominated and widely accepted. 3GPP UMTS succeeded EDGE in 1999. The goal of UMTS or 3G wireless systems was to provide a minimum data rate for stationary, walking users, and moving vehicles. 3GPP designated it as **Release 99**. After that, the upgrades and additional facilities were introduced in different releases of the 3GPP standard.
Release 4: Efficient use of IP was the purpose of release 4.
Release 5: It includes a core of HSDPA. It provided reduced delays for the downlink packet and provided a data rate of 14 Mbps.
Release 6: It included the core of HSUPA with a reduction in uplink delay. It enhanced the data rate to 5.74 Mbps in uplink raw. MBMS has also been included for broadcasting services.

Release 7: Downlink MIMO operation, as well as support for higher-order modulation of up to 64-QAM, has been added in this release. MIMO or 64-QAM could be operated at a time. Data rates up to 28 Mbit/s in the downlink and 11 Mbit/s in the uplink have been provided by evolved HSPA. It brings the world to the most awaited part known as the 4G system LTE. [10]

1.2.5.2 UMTS Architecture

The architecture of Universal Mobile Telecommunications Systems (UMTS) consists of User Equipment (UE), Universal Terrestrial Radio Access Network (UTRAN), and Core Network.

User Equipment (UE): - User Equipment (UE), shown in Figure 8, is a mobile, unlike GSM, where it's called the Mobile Station. Multi-Radio Access Technology (**Multi RAT**) is known as the alternative name of UE because UMTS devices support multiple technologies. For example, it can connect to UMTS, and it can also connect to GSM/GPRS. UE consists of two items: -

- Mobile Equipment (ME)
- Universal Subscriber Identity Module (USIM)

The phone/UE connects with the Radio Access Network (RAN) with the help of an air interface. The air interface is known as the User UMTS (**Uu**) interface in UMTS.

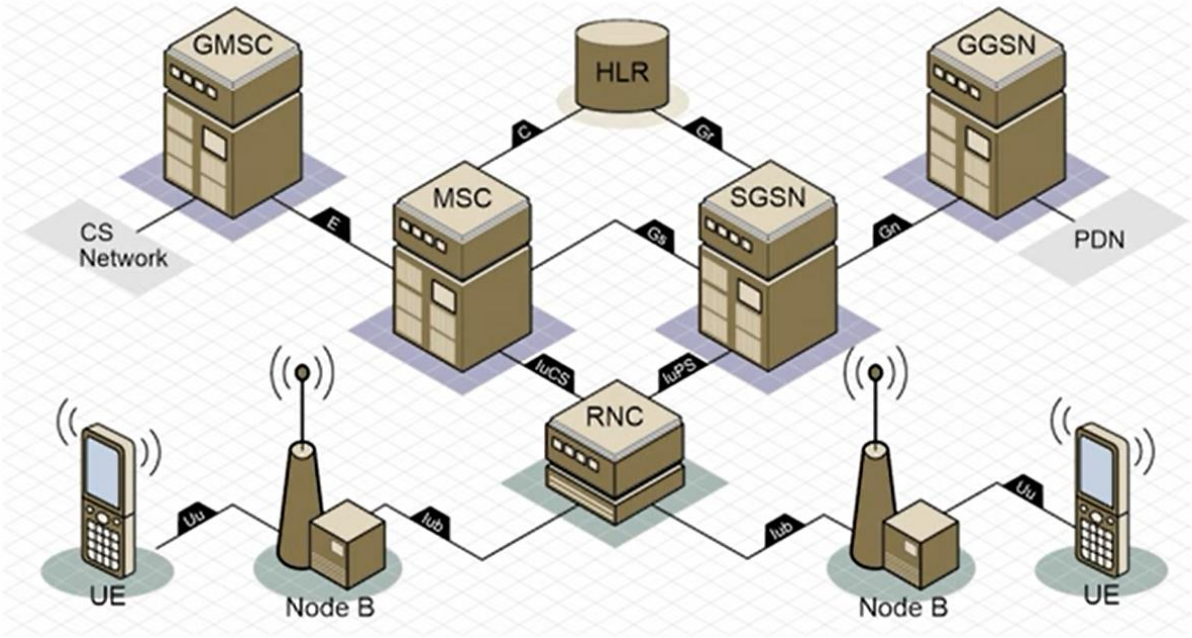

Figure 8: - UMTS Architecture [12]

Universal Terrestrial Radio Access Network (UTRAN): - The Radio Access Network (RAN) in Europe is known as Universal Terrestrial Radio Access Network (UTRAN). UTRAN is consists of base stations (**Node B**) and a Radio Network Controller (**RNC**), which bridges the gap between Mobile Station and Core Network. Moreover, UTRAN controls and manages the air interface for

the whole network. Multiple base stations **(Node B)** can connect with **RNC** by using the **IuB** interface. There are the following major functions of RNC and Node B: -

Radio Network Controller (RNC): -

- Located in centralized sites
- Manage several Node-Bs

Base Station (Node B): -

- Distributed across the country
- Provide voice and data coverage to the mobiles

CN (Core Network): - CN processes and manages the subsystems. UMTS integrates GSM with some enhancements in core network elements. It separates voice and data with circuit-switched and packet-switched domains, respectively. Hence, CN is divided into two parts known as CSCN (Circuit Switched Core Network) and PSCN (Packet Switched Core Network).

- **CSCN (Circuit Switched Core Network): -** UTRAN connects with the CSCN interface known as **IuCS** (Interface UMTS Circuit Switched). It provides a dedicated link or channel for a specific time slot for a set of users. It consists of MSC and GMSC.

    - **MSC (Mobile Switching Centre): -** It manages circuit-switched calls. Home Location Register (HLR) connects with the MSC using the **C** interface, and it helps in downloading the user's profile at VLR in MSC.
    - **GMSC (Gateway Mobile Switching Centre): -** It provides a connection to other Network Service Providers (NSP). NSP can be mobile or fixed.

- **PSCN (Packet Switched Core Network):** - It supports data aspects. - UTRAN connects with the PSCN interface known as **IuPS** (Interface UMTS Packet Switched). PSCN uses the IP network in which IPs transmit and receive data between two or more devices. **Gn** (GPRS Node) interface connects the SGSN and GGSN. **Gr** (GPRS Register) provides a signaling connection between SGSNs and HLR. It helps in downloading packet subscription information from HLR to SGSN.

    - **SGSN (Serving GPRS Support Node): -** It is used to set up and manage data connections between the UE and Packet Data Network (for instance, the internet). It also tracks the location of UE and data services.
    - **GGSN (Gateway GPRS Support Node): -** It provides a connection to External Data Networks (EDN) like the internet or intranets.

Gs is an interface to connect SGSN with MSC to provide a combined procedure to try and reduce signaling on the air interface. [12]

1.2.5.3 Advantages

Major benefits of 3G networks over their predecessors are as follows:-

- Due to the base station's (Node B) adaptive antenna array, it became easy to adjust the power, decreased the system's self-interference and enhanced receiver sensitivity, and increased the system capacity.
- Supports multimedia applications and mobile television, video conference
- Provides mobile internet access at high speed
- Increased data rate and downlink transmission

1.2.5.4 Disadvantages

3G has the following disadvantages: -

- 3G compatible handsets were required.
- Upgrade cost was high.
- High power consumption.
- Requires more expensive and closer base stations

1.2.6 3.75 GENERATION

In 3G, HSPA was used, but in 3.75G, it has been enhanced HSPA+. It evolved HSPA – MIMO. Because of this technology, the uplink and downlink speed, in theory, has been increased from 5.76Mbps to 22Mbps and 14.4Mbps to 168Mbps, respectively. At that time, the symbol of the network was changed to H+ from H.

1.2.7 FOURTH GENERATION

The initial goal of telecommunication was mobility and global connectivity, but as the technology evolved, the services started expanding. At this stage, the services were not restricted to voice and SMS. Multimedia services were evolved. 4G is known as full packet switched-based technology, where the concept of circuit-switched had been eliminated. This generation is based on Long Term Evolution (LTE). The main goal of 4G was to achieve a high data rate. It aimed: -

- 1Gbps for stationary users
- 100Mbps for High mobility users

The 4G offered progressively upgraded adaptations of similar headways guaranteed via 3G, for instance: - improved multimedia, video streaming, worldwide access, and transportability through a wide range of gadgets. Furthermore, to confirm the aim mentioned at an earlier stage, a speed of 4G was identified by ITU (International Telecommunication Union), which was 100Mbps for high mobility users and 1Gbps for every second for stationary clients, which encourages gaming and administrations HD recordings [13].

Rather than upgrading 2G or 3G's network architecture, the new architecture had been evolved. It is known as SAE (System Architecture Evolution). The requirement of SAE was high mobility, and to achieve it, the architecture should be simple. Hence, the architecture of 4G had been divided into new radio and core network parts which are a combination of E-UTRAN, E-PC, and E-UE.

1.2.7.1 4G Network Architecture

For developing a Long Term Evolution (LTE), various terms have been evolved. A major change in LTE was the adoption of all IP-based core networks, which means switching to VOIP (Voice over IP) or VOLTE (Voice over LTE), even when the capacity limits are reached, QoS (Quality of Services) on every interface guarantees that bandwidth and other requirements of voice calls can be met.

1.2.7.1.1 Techniques used in LTE

In LTE, **full-duplex** had been implemented by using FDD or TDD.

- **Frequency Division Duplexing (FDD): -** FDD is a method to establish a full-duplex communications link that uses two different radio carrier frequencies. One for transmitting uplink and the other for receiving downlink. Both the channels are separated by a defined offset frequency, which is also known as "Guard Band." It was used to stop the interference between an uplink channel and a downlink channel.
- **Time Division Duplex (TDD): -** TDD is used to carry Uplink and the Downlink transmissions over the same frequency by using synchronized time intervals.

The following Table 1 defines the factors which help an operator to decide whether to use FDD or TDD before rolling out a full-fledged system: -

Table 1: - Factors of FDD and TDD

Factor	FDD	TDD
Low Latency	FDD offers very low latency since transmit (TX) and receive (RX) functions operate simultaneously and continuously.	TDD switch between TX to RX, which leads to high latency.
Equipment Costs	The diplexer is required since UL and DL frequencies are different. It increases the device cost.	No need for a diplexer because UL and DL have the same frequency. Hence, the device cost is minimum.
Distance Prefer-ability	Transmission takes place at the same time, so efficiency is unaffected as compared to TDD	Guard period proportional to distance. Hence, efficiency reduced

Unbalanced Traffic	Less efficient because the capacity is normally balanced in both direction	Highly efficient in the real-life network because the Volume consumed in DL is much higher than in UL. In TDD, it is possible to Dynamically adjust the capacity by utilizing more time slots for DL than in UL.
Spectral Efficiency	Using different frequencies leads to low spectral efficiency	Using single frequency leads to high spectral efficiency
MAC Layer Complexity	Fixed frequencies are allocated in UL and DL	Difficult to achieve accurate time synchronization

LTE is defined to support both the Frequency Division Duplex (paired spectrum) and Time Division Duplex (unpaired spectrum). LTE market is mainly based on FDD Technology. TDD was expected to see increased adoption in the US, China, Australia, Middle East, Northern and Eastern Europe, and Southwest Asia to gain a more pronounced position in the global LTE market. [14]

Multiple Access: - In LTE, OFDMA/SC-FDMA has been used rather than traditional techniques like FDMA, TDMA, or CDMA. In OFDMA, subcarriers overlap in the frequency domain and there is a presence of negative frequencies. Data is in OFDMA over parallel subcarriers of 15-kilo hertz. OFDMA consumed high power for signal generation, and handheld devices have limited power capacity, so OFDMA became unfavorable for uplink transmission. To overcome this, LTE started using SC-FDMA (Single-Carrier Frequency Division Multiple Access) in the UL direction.

MIMO Technique: - Traditional MIMO system was based on 2, 4, or 8 antennas. It introduces additional robustness to the radio link by spatial diversity (where the same information is sent or received across independent channels to **combat fading**) or to increase the link data capacity by spatial multiplexing (where multiple antennas are used in transmitting and receiving. Each spatial channel carries independent information, in result, the data rate of the system is increased). When the number of antennas used in a communication terminal is more than 10s or100s, then it is called a Massive MIMO system. It increased the data rate, signal-to-noise ratio, and channel hardening. CoMP (Coordinate Multi-Point), Hetnet were also used to increase the throughput. [15]

1.2.7.1.2 LTE Architecture

In LTE architecture, the mobile device is referred to as **UE** (User equipment), same as UMTS. The elements of UE are similar to those in the previous generation. Figure 9 shows the internal architecture of UE.

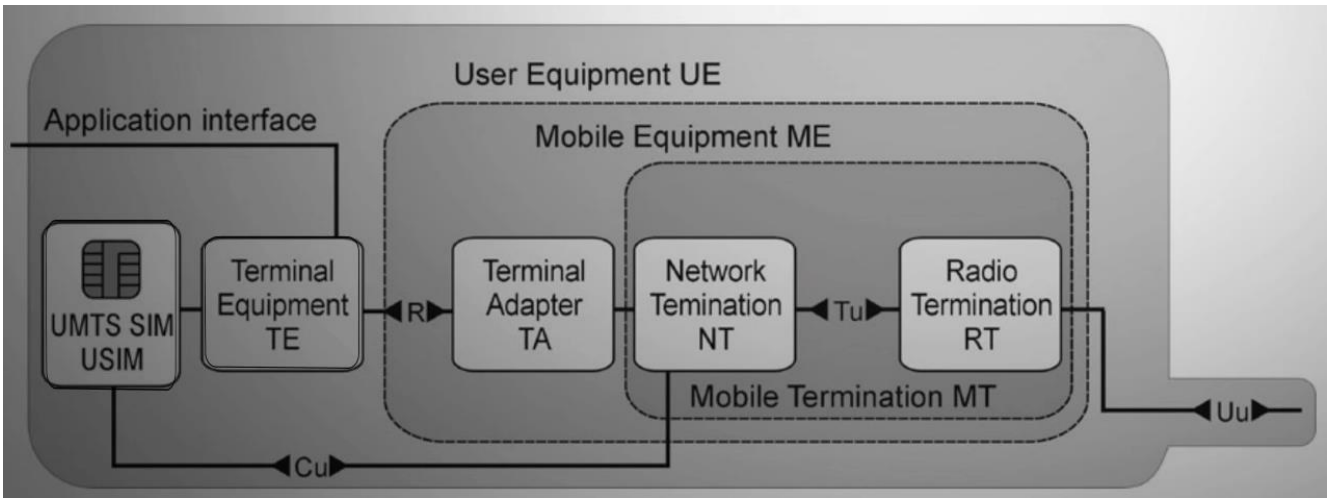

Figure 9: - UE Architecture [16]

Evolved UMTS Terrestrial Radio Access Network (eUTRAN):- 2G's concept of BS and 3G's concept of RNC was eliminated in 4G. RAN of LTE is known as Evolved UMTS Terrestrial Radio Access Network (eUTRAN), where eNB (Evolved Node B) is equal to RNC + Node B or BTS + BSC. eNode-B is the most complex node in the LTE network and its architecture is shown in Figure 10.

eNode-B: - There are two major elements of every eNB: -

- **RRU (Remote Radio Unit): -** RRU consists of antennas. It is also called a remote radio head, which is the most visible part of a mobile network. RRUs are also responsible for the Modulation and Demodulation of all signals transmitted or received on the air interface.
- **BBU (Base Band Unit): -** It consists of digital modules that process all signals transmitted on the interface and act as an interface to the core network over a high-speed backhaul connection.

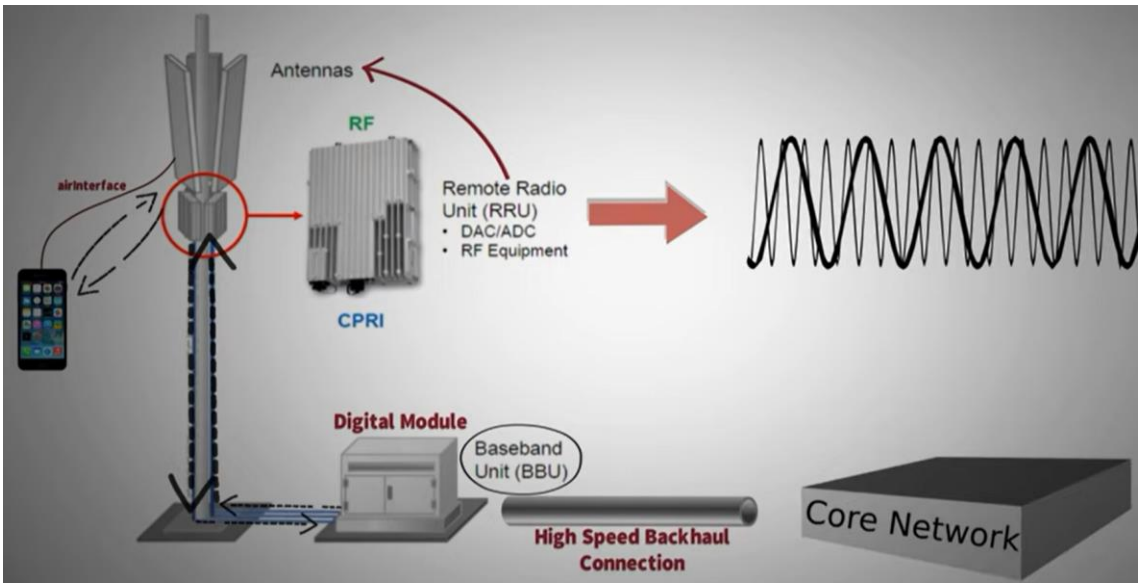

Figure 10: - eNodeB Architecture [16]

In 4G, eNodeB is not only responsible for the air interface but the following as well: -

- Radio Resource Management includes: -
  - Radio Bearer Control
  - Radio Admission Control
  - Connection Mobility Control
  - Scheduling (Dynamic allocation of resources to UEs in uplink/downlink)
- IP header compression of the user data stream
- IP header encryption of the user data stream
- It is responsible for the selection of an MME (Mobility Management Entity) at UE attachment in case no routing towards MME is found through the information provided by the UE
- Routing of User Plane data takes place towards Serving Gateway
- Scheduling and transmission includes the responsibility of: -
  - Paging messages (initiated from the MME)
  - Broadcast information (initiated from the MME or O&M)

X2 interface was introduced to avoid data loss during handover. In LTE, eNodeBs can communicate directly with each other over the X2 interface for the following purposes: -

- Handovers are controlled by eNBs themselves through X2
- Interface coordination

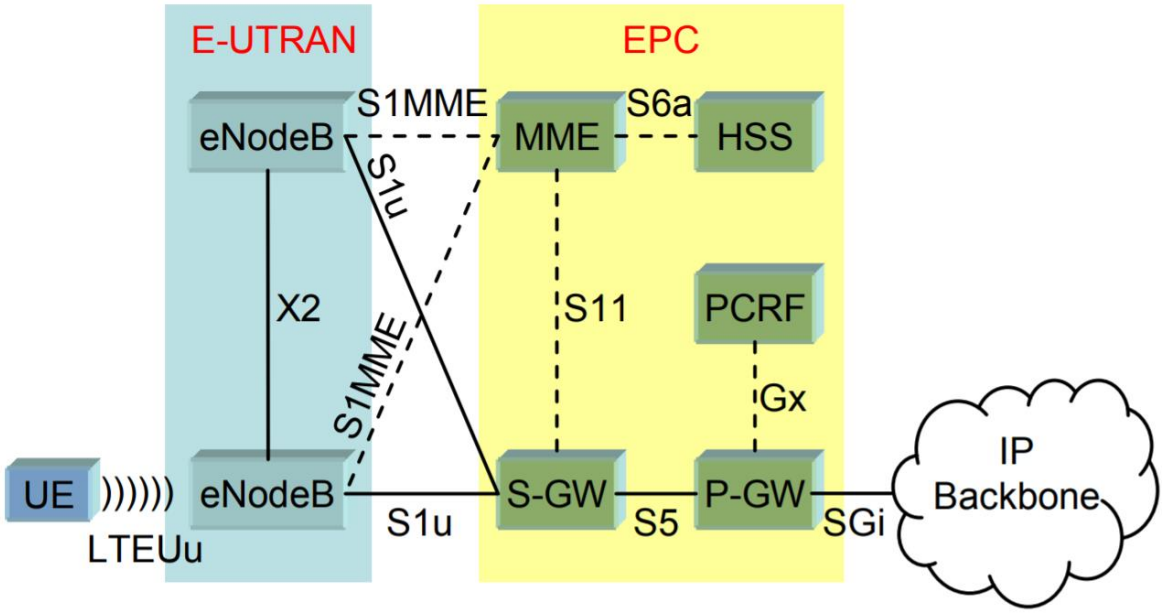

Figure 11: - 4G Architecture [17]

S1 is referred to as an interface between the base station and the core network. S1 can be carried either over a high-speed copper or fiber cable or over a high-speed microwave link. It splits into two logical parts: -

- User data is transported over the S1-U (S1 User Plane) part of the interface
- IP packets from UE are encapsulated inside GTP (GPRS Tunneling Protocol) and transferred over S1-U towards SGW.

S1 Control Plane (S1-CP) protocol) is required for the following purposes: -

- The eNode-B uses S1-CP to interact with the core network to make itself known to the network, to send status and connection keep-alive information, and for receiving configuration information from the core network.
- Used for transferring signaling messages that concern the users of the system. i.e. S1-CP used to maintain the connection, to organize a handover of the connection to another LTE, UMTS, or GSM base station as required. [16]

Evolved Packet Core (EPC):- EPC is the other important component of the SAE. It connects and communicates with internal and external PDNs and IP Multimedia Subsystem (IMS). It is consists of the following functional entities: -

- **Mobility Management Entity (MME): -** MME is known as EPC's main signaling node and part of a control plane. MME initiates the paging and authentication of the mobile device. It keeps the location information for each user at the level of the tracking area and during the initial registration process, select the appropriate gateway. **S1-MME** interface connects the MME with eNodeB and connects via the **S11** interface to the S-GW. In a pool, **multiple MMEs can be grouped** to meet the increased signaling load in the network. MME also plays an important role in the transmission of signals between LTE and the 2G/3G network. The major functions of MME are: -

  - Mobility Management
  - Mobility handling in idle state
  - EPS bearer control
  - Tracking area list management
  - NAS signaling and its security
  - PDN GW and SGW selection
  - Session Management
  - Roaming and authentication

- **Home Subscriber Server (HSS): -** HSS works under the control plane. It stores all the information about every network operator's subscribers in a central database. It is an updated version of legacy HLR and Its functions are as follow: -

  - Subscriber Management
  - Authentication

- **Serving Gateway (S-GW): -** S-GW is the part of a user plane. SGW is responsible for transferring data to neighboring eNodeB, including data transfers in all packets throughout the user plane. In other words, S-GW is an IP router with support for a mobile-specific tunneling protocol (GTP) and charging functionality. The key points of S-GW are: -

  - A single UE can be served by only one S-GW at any one time
  - Receive instructions from MME to set up and tear down sessions for a UE
  - Act as an interface for signaling between the P-GW and the MME
  - Handles user IP packets between the P-GW and eNodeB

- **Packet data network Gateway (P-GW): -** S-GW is also a part of a user plane. Functionally, P-GW provides access to external PDNs. It is an IP router with support for mobile-specific tunneling and signaling protocols. Other features of P-GW are as follows: -

  - If the UE has multiple data sessions to multiple PDNs, the UE can be connected to multiple P-GWs.
  - It is responsible for dictating QoS and bandwidth parameters for the subscriber's session.
  - Do User-based packet filtering and Lawful interception
  - Go for inter-operator charging and Packet screening as well

- **Policy and Charging Rule Function (PCRF): -** PCRF is the control plane node and it is responsible for controlling flow-based charging in the Policy Control Enforcement Function (PCEF) and policy control decision making.

1.2.7.2 3GPP next Release

As explained earlier under 1.2.5.1., the release7 had been completed and brought LTE in the market. To fulfill the further requirements proposed by ITU-R, a study group had been formed and LTE standardization began in 2004.

Release 8: - Large number of telecom companies collaborated to achieve their common vision. In June 2005, Release 8 was finally formed after lots of refining. Some of the significant characteristics of Release 8 were: -

- Delays were reduced for connection establishment and transmission latency
- user data throughput increased
- Cell-edge bit-rate has been increased
- Reduced cost per bit
- Simplified network architecture
- Implied improved spectral efficiency
- Seamless mobility and power consumption efficiency

These requirements were fulfilled by advancements in radio technology. Three fundamental technologies that shaped the LTE radio interface design were: -

- Multicarrier technology
- MIMO (multiple-antenna technology)
- Application of packet-switching at the radio interface

The specifications for Release 8 were completed by December 2007. In northern Europe by the end of 2009**,** the **first commercial deployment** has taken place. In the subsequent releases, various services such as Multi-Cell HSDPA, Coordinate Multipoint, HETNET, Carrier Aggregation, Massive MIMO, and many more were targeted. It was the time to move from services to multi-services, in other words from LTE advanced to new technology known as 5G. [10]

1.2.7.3 Advantage

There are myriad of benefits of 4G technology such as: -

- Simple architecture and enhanced spectral efficiency
- Faster handover (Signaling and data transmission simultaneously)
- Higher user Data Throughput and cell edge bit rate
- Seamless mobility between various radio access technologies

1.2.7.4 Disadvantages

The disadvantages of 4G are: -

- High data prize for consumers and Need different handsets
- Latency issues are still there
- Handled limited voice calls and services at a time
- It requires a wide bandwidth as a concentrated data service
- Roaming and data or voice work together has not been implemented
- Require closer base station

1.2.8 FIFTH-GENERATION

In 2020, a tiny thing known as SarsCovid-19 shook and traveled the whole world. It restricted the movement of people. Big companies like European Space Agency and small businesses almost everything started operating remotely. Now, the internet has also become a basic utility like Water and Electricity. The world took a giant leap towards dependence on the internet. In the world of Telecommunication, spectral efficiency plays an important role.

- **Spectral efficiency = $\frac{\text{Bits / sec}}{\text{Hertz}}$**

The telecom operators get a spectrum from the government on lease and the operator provides the services over this spectrum. Spectrum efficiency reflects how efficiently the operator is utilizing the spectrum. In other words, the number of bits transmitted per second over a particular radio frequency reflects spectrum efficiency. In 4G the operation happens in different frequencies

ranges, starting from 450 MHz to up to 3.8GHz and in different modes (TDD/FDD). According to Moore's law, the number of transistors in a dense integrated circuit doubles about every two years and it leads to saturation at some point. Similarly, in mobile telecommunication, by the end of the 4th Generation, we are already at the peak of high data rates using the existing spectrum.

5G is the fifth mobile cellular communications generation, which provides a solution to **satisfy** the ever-increasing **customer demand** and to **increase spectral efficiency**. The emerging and latest buzzword 5G is shaping our digital future by satisfying customer needs or demands. 5G performance targets following features: -

- High data rate
- Lower latency
- Energy efficiency
- Lower cost
- Higher system capacity
- High device connectivity

1.2.8.1 Features & Requirements of New Radio

The radio of 5G operates in the following two frequency ranges: -

- Frequency Range 1 is below 6GHz and plans to reuse radio frequencies from other generations, including 4G. It will also help telecom operators to transition gradually.
- Frequency Range 2 is between 24GHz - 100GHz, which is popularly known as millimeter Wave (mmWave). This frequency range helps to accommodate high bandwidth requirements for various services like: -

    - The download of big files
    - High-quality streaming
    - Real-time gaming

- The effective utilization of both frequency ranges will help accommodate the massive tsunami of IoT devices.

To implement the above three operations, a new upgraded radio has been designed. The Radio part of 5g is called **NR- New Radio | Radio Access Technology beyond LTE**. International Telecommunication Union-Radio (ITU-R), the governing body, set the IMT 2020, which are the standards and requirements for the Fifth Generation networks, services, and devices. Some key requirements of the new radio are described in figure 12.

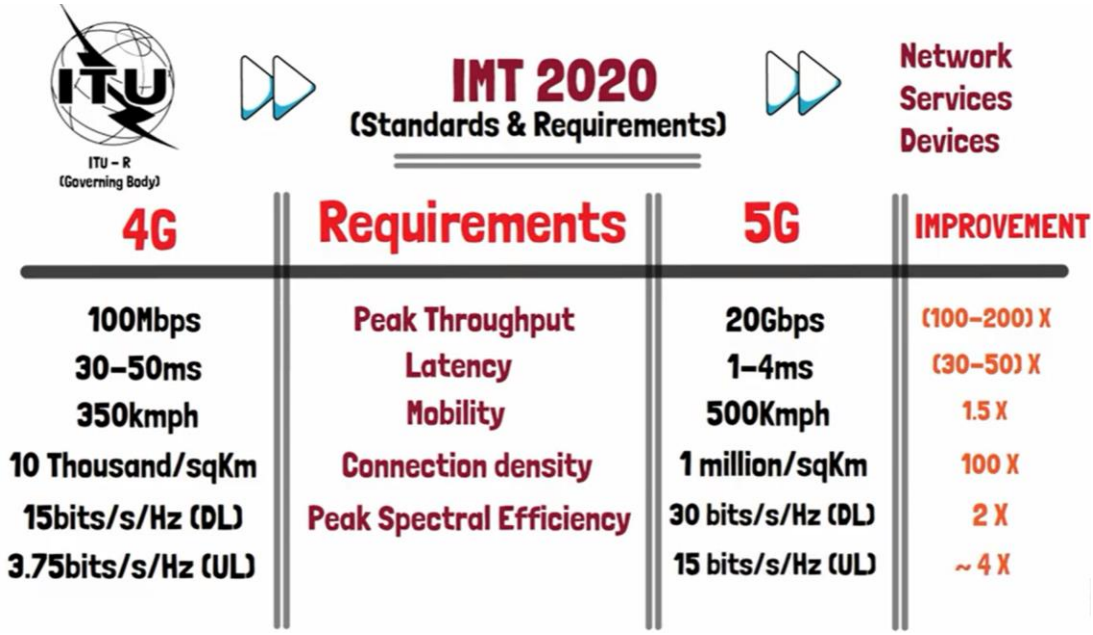

Figure 12: - 5G Radio Requirements [18]

To fulfill these requirements and realize the new features, various technologies have been upgraded and others are embedded as new.

1.2.8.2 Features & Requirements of New Core

In 5G's radio all technologies like OFDMA, MIMO, CA, CoMP, and HETNET are converged. To achieve more benefits, New Radio (NR) requires an upgraded core. Hence, IMT-2020 has other general requirements, mostly associated with the core network are: -

- Support diversity of services
- Dynamically scalable (with network functions, the core should be able to scale up or scale down based on demand)
- Access network agnostic (other than the NR people should be able to access services through WLAN, Fixed Broadband, or other modes as well)
- Distributed architecture (Till fourth generation the core is centralized. To reduce core network or backhaul traffic a distributed architecture should be adopted)
- Internetworking Automation (To mitigate the multi-vendor interworking and roaming problems, the core network should automate the processes as far as possible)
- Network Optimization (Dynamic data routing, reliability, security, privacy, and energy efficiency)

1.2.8.3 Major Enhancements

In the fifth generation, both the radio and core sides have been enhanced. Various technologies have been used for the following changes: -

- Increase the capacity

- Reduce the latency
- Increase support to the number of connections
- Improve the edge coverage

Hence, the network is made more flexible.

1.2.8.4 5G Use Cases

The advanced features of 5g open a world of opportunities for diverse end-users, including the range from individual users to large enterprises. The use cases are classified into three categories as shown in figure 13.

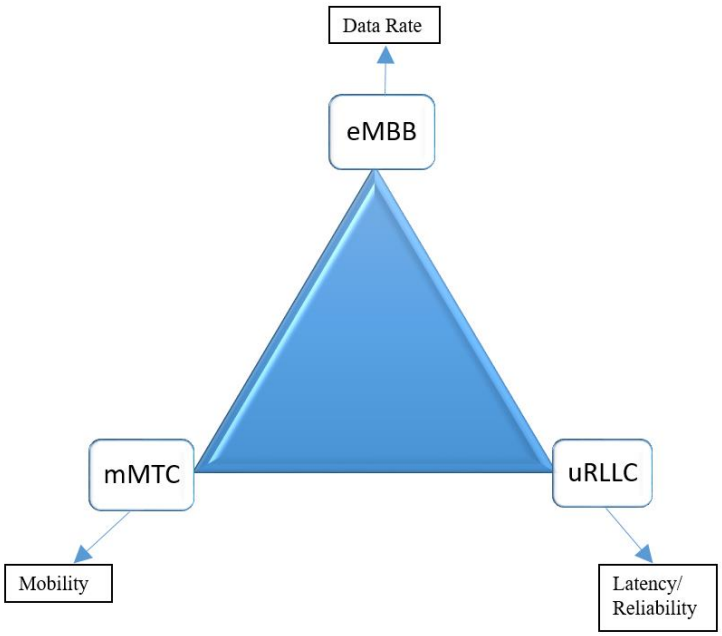

Figure 13: - 5G Use Cases

Enhanced Mobile Broadband (eMBB): - The network delivery capacity has been increasing to 100-1000 times as data traffic increases since 2020. Netflix videos and streaming of live events in high quality while traveling become a reality. 5G revolutionized the gaming industry.

Ultra-reliable and Low-latency Communications (uRLLC)/ Critical Communications: - Enhanced Mobile Broadband and Ultra-Reliable Low Latency Communication of 5g will be an important factor for massive mobile infotainment. Various automakers like Toyota, Ford, Tesla, BMW, and Lyft are working on autonomous driving, which requires a lot of information processing. 5g will make this processing on the go a reality. Optimizing the traffic and avoiding accidents will be the other benefit because of low latency. Following figure 14 shows the use scenarios of different use cases.

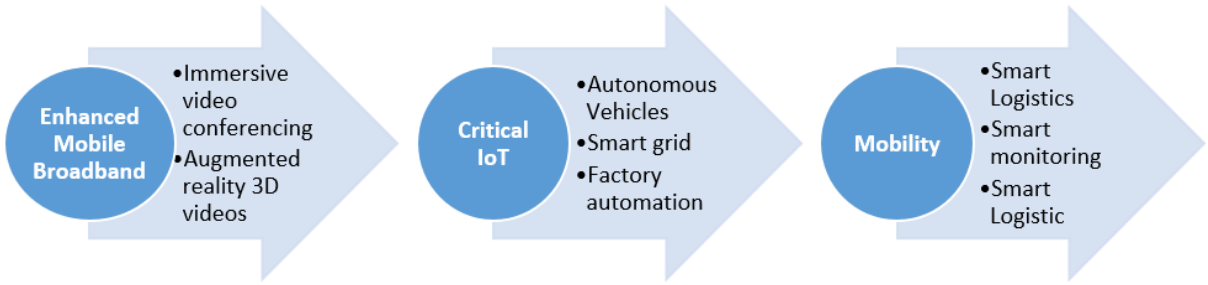

Figure 14: - 5G Usage Scenarios

Massive machine-type communications (mMTC): - Human interest in machine-to-machine communication and the Internet of Things (IoT) has been increased. Internet connects and manages thousands of objects. Machine-to-machine communication, thus taking us away from the internet of people to the internet of things. Remote operations can be processed in mMTC because of eMBB and uRLLC. Mine without man, monitoring of patient without the physical presence of the doctor is possible due to 5G. 5g will potentially revolutionize sensor-based IoT applications.

The high data rate, low latency, and mobility of 5G will make cloud platforms the new normal. There are various platforms like Google Colab - Kaggle which allows cloud computing and collaborative programming.

1.2.8.5 5G Key Performance Capabilities

There are the following figure 15 shows the key capabilities for IMT-2020 5G: -

Capability	Description	5G target	Usage scenario
Peak data rate	Maximum achievable data rate	20 Gbit/s	eMBB
User experienced data rate	Achievable data rate across coverage area	1 Gbit/s	eMBB
Latency	Radio network contribution to packet travel time	1 ms	URLLC
Mobility	Maximum speed for handoff and QoS requirements	500 km/h	eMBB/URLLC
Connection density	Total number of devices per unit area	10^6/km^2	MMTC
Energy efficiency	Data sent/received per unit energy consumption (by device or network)	Equal to 4G	eMBB
Spectrum efficiency	Throughput per unit wireless bandwidth and per network cell	3–4x 4G	eMBB
Area traffic capacity	Total traffic across coverage area	1000 (Mbit/s)/m^2	eMBB

Figure 15: - Key Capabilities of 5G (Ref: https://en.wikipedia.org/wiki/5G)

1.2.8.6 The transition from 4G to 5G (5G Deployment)

In 2021, the evolution from 4G to 5G had been started. A complete transformation from 4G to 5G will take time and it needs huge investment as well. As every operator cannot afford to adopt 5G immediately. To avoid the situation, the New Radio can operate in two modes, as shown in figure 16. In other words, there are two deployment options defined for 5G.

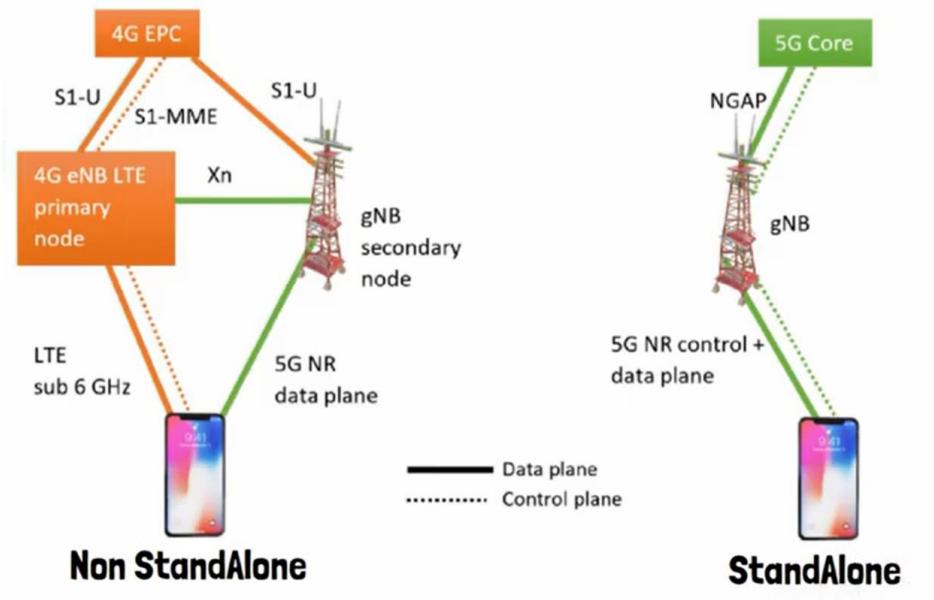

Figure 16: - Modes of 5G's New Radio [18]

Non-Stand Alone (NSA) Architecture: - In this mode, the existing Control Plane of 4G is used in 5G. Here 5G Radio Access Network (AN) and New Radio (NR) interface are used in aggregation with the existing LTE and EPC Core Network. As shown in figure 16, the node of 5G is connected to the master node corresponding to 4G. The control plane messages of 5G will reach the core through the master eNB but the user plane data will be sent directly to the core. This will enable easier and faster transition for the existing operator.

Stand Alone (SA) Architecture: - The standalone mode does not depend upon 4G, here the NR is connected to the 5G CN. It requires a complete up-gradation of the Core.

2 ENABLING TECHNOLOGIES, ARCHITECTURE & SECURITY OF 5G

5G is planned to support diverse services with dissimilar data traffic profiles (for instance, high throughput, low latency, and massive connections) and models (for example, IP data traffic, non-IP data traffic, short data bursts, and high throughput data transmissions) [19].

2.1 Technologies

Various technologies have been emerged in the 5G to achieve targeted requirements. Some of those technologies are elaborated as follows: -

- **Software-Defined Network (WSDN): -** To increase network performance flexibility, SDN has emerged primarily for data center networks. Its main goal for the coming up-gradation of the Internet is to separate the data plane from the control plane. SDN contains three layers named application, control, and infrastructure layer. These layers communicate using APIs. Applications communicate to the controller through its northbound APIs, while the controller and switches communicate via southbound APIs.

- **Network Function Virtualization (NFV): -** By using NFV, various virtual machines can work on different operating systems or different hardware. The concept of NFV offers the following benefits: -

    - Greater scalability and flexibility
    - Reduces the Capital Expenditure (CAPEX)
    - Saves Operating Expenditure (OPEX)

- **Millimeter-Wave (mmWave): -** 5G uses NR through millimeter-wave. Radiofrequency spectrum from 1GHz to 6GHz is very crowded because many technologies use this range, such as GPS, WiMAX, Wi-Fi, 4G, 3G, L-band satellite, S-band, C-band, etc. The spectrum range from 30 GHz to 300 GHz, known as millimeter-wave, and it is less utilized. It is new territory; thus, the range from 24GHz to 100GHz was proposed for 5G. Following figure 17 depicts the wave ranges. Table 2 shows the difference between Sub 6GHz and mmWave in terms of MIMO orders, main techniques, and channel characteristics.

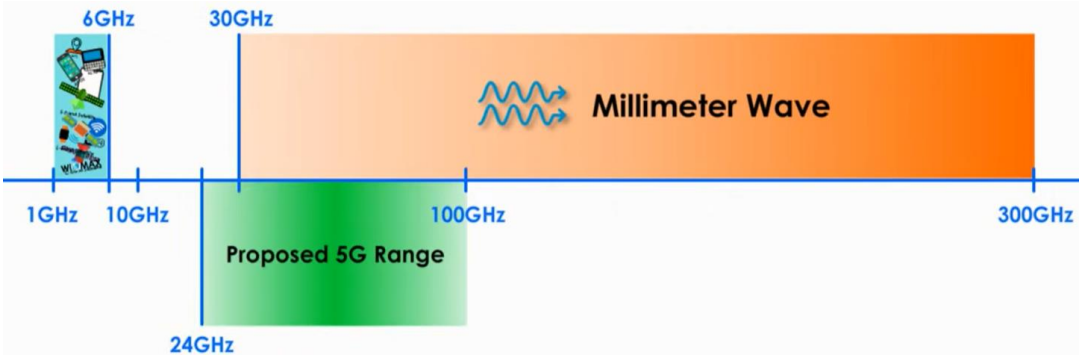

Figure 17: - Millimeter Wave's Range [20]

Table 2: - Sub 6GHz vs mmWave

	Sub 6GHz	mmWave
MIMO Order	Up to 8*8	Less MIMO (Usually 2*2)
Main Technique	Spatial Multiplexing	Beamforming to Single Device
Channel Characteristics	Rich Multipath ideal for Spatial Multiplexing	Fewer Multipath due to beamforming

The benefits of millimeter-wave are: -

- It is a new and less used band
- Higher frequency wave carries much more data
- It makes it possible to have a massive MIMO antenna

➢ **Spatial Multiplexing: -** In spatial multiplexing, different receiving wire components (antenna elements) are utilized to send variously separated and free encoded data streams. Every data stream goes through various propagation channels and collectors with various radio wires (antennas) can get and recreate the originally transmitted data with better spectral efficiency.

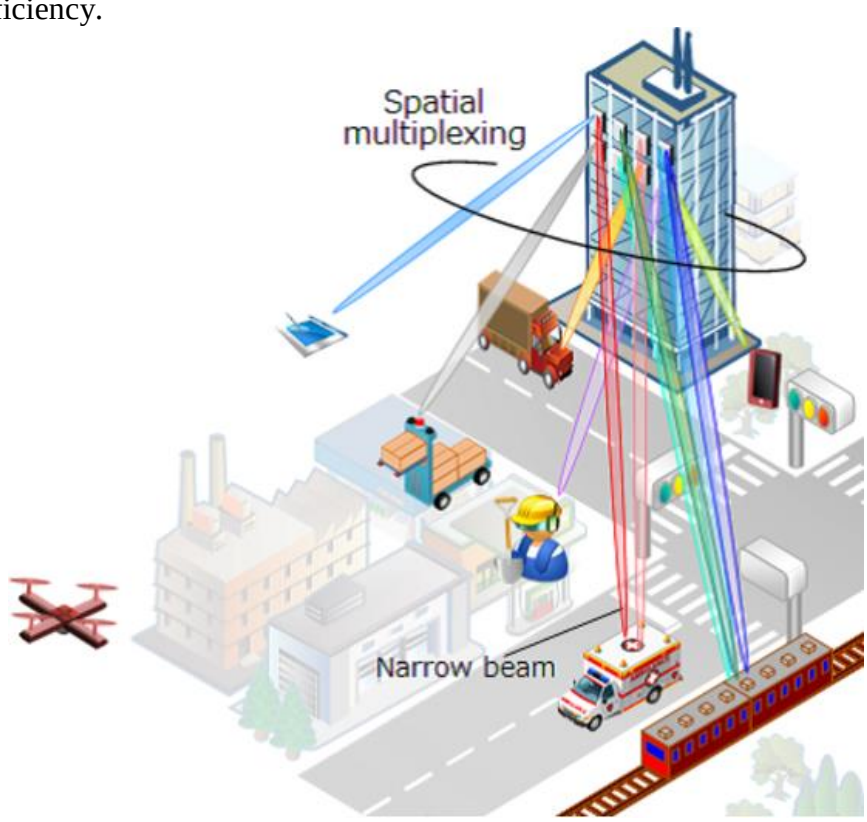

Figure 18: - Spatial Multiplexing [21]

Spatial multiplexing is best when numerous data streams can be supported by the propagation paths and when the channel has a high signal-to-noise ratio (SNR), which doesn't influence the signal strength when the first signal has to be isolated into several data streams. Figure 18 above shows the development of the 5G application, where spatial multiplexing plays an important role.

- **Beamforming: -** Beamforming consolidates antenna array elements adaptively at the base station and uses the increased beamforming loads on every component to control the directions to which data streams are sent. Explicit clients accordingly get the information, while others are not disrupted. Beamforming functions admirably if the channel has a low or limited SNR power. The following figure depicts the basics of beamforming where two transmit antennas have been used to generation closed beams.

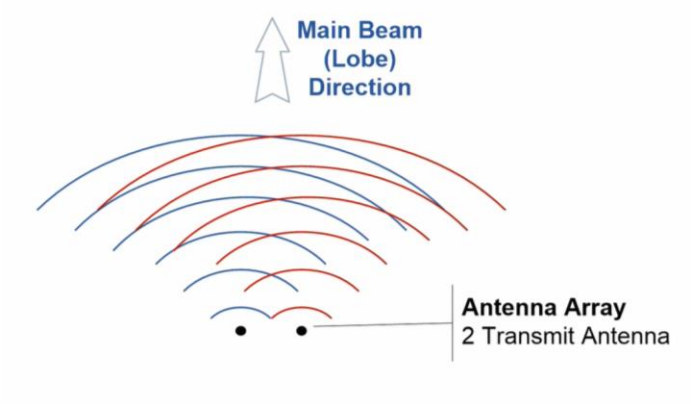

Figure 19: - Beamforming Basics [22]

Beamforming is done in two ways: -

- RF beamforming
- Digital beamforming

The following figure shows the hybrid beamforming, where additional antenna elements have been used to produce multiple beams.

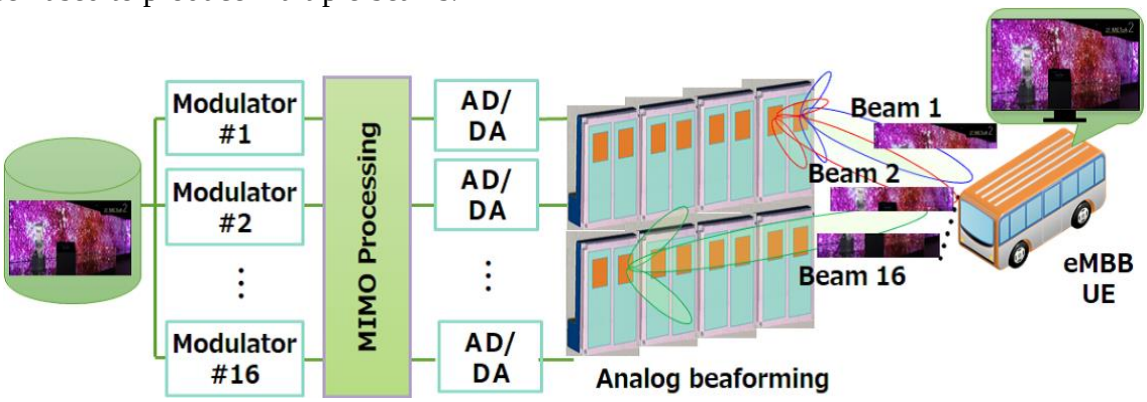

Figure 20: - Hybrid Beamforming [21]

- **Device-to-Device communication (D2D): -** Device-to-Device communication (D2D) permits two devices to communicate with one another without an intermediate base station (BS), which controls the communication. D2D utilizes a licensed spectrum than an

unlicensed spectrum, which is used by technologies like Wi-Fi and Bluetooth. This sort of correspondence gives a high data rate, improves QoS, and provides low latency because of the productive and direct communication between the two associated devices.

- **Massive MIMO: -** Massive MIMO is an extension of MIMO, which was used in earlier mobile communication generation. Massive MIMO expands the legacy systems by adding a much higher number of antennas on the base station. The huge number of antennas helps focus energy, and as a result, drastic improvements in throughput and efficiency have been achieved. In Massive MIML, both the network and mobile devices implement more complex designs to coordinate MIMO operations.

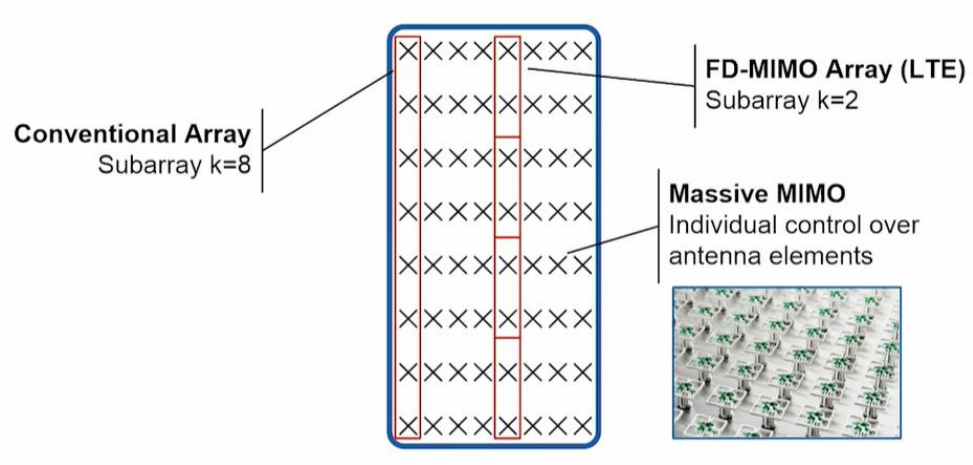

Figure 21: - Massive MIMO Antennas [22]

Even as depicted in figure 22, handsets of MIMO has been changed from multiple RF modules to NR supports antenna switching

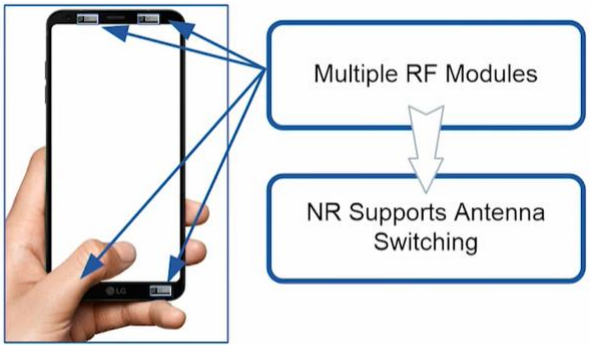

Figure 22: - MIMO in Handsets [22]

Different vendors have different solutions. Following figure 23 shows the Multi-Panel Antennas, where panels and elements of SU-MIMO and MU- MIMO has been elaborated.

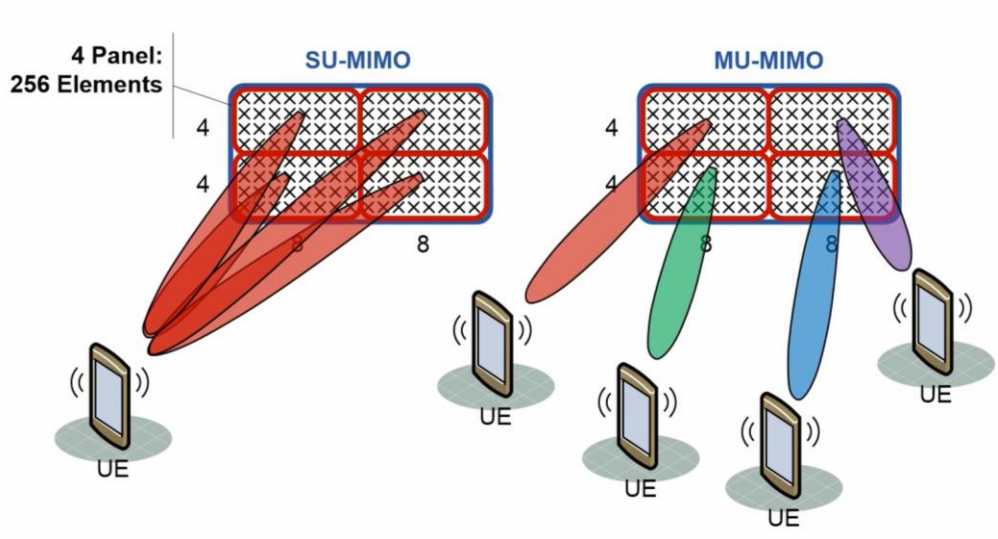

Figure 23: - Multi-Panel Antennas [22]

- **Internet of Things (IoT):** - 5G and IoT will be leading a paradigm shift in M2M communication management. New technologies like NB-IoT and LTE-M are being deployed to enhance the capabilities of IoT.

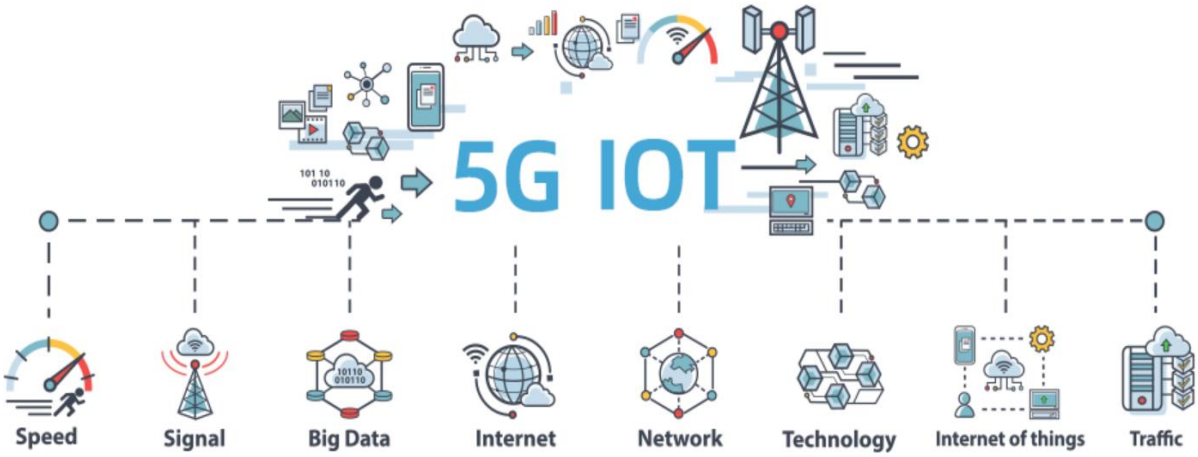

Figure 24: - Scenario of 5G IoT *(Ref:* - https://www.ursalink.com/en/wp-content/uploads/2019/10/5G-IoT.png*)*

The Internet of Things (IoT) is the key concept of 5G cellular networks. IoT can be defined as an everyday network of physical objects, equipment, devices, buildings, etc. Sensors used in these devices sensed some information and passed it on to a remote server via the Internet. The server can remotely issue device control commands. After that, the data collected on the server is processed to get information about the underlying process. This processed data is further used to build smarter systems like smart homes, smart cities, intelligent transport systems, healthcare systems, etc. [23]

2.2 5G Architecture

5G architecture is more flexible and scalable compared to 4G. It allows for a wider range of scenarios and services. To meet the challenges of 5G requirements, a new architecture with technical innovation and evolution has been designed to focus on the following major factors: -

- Support wider scenarios
- Increase the user data rate
- Reduce latency

For the core network, it is reconstructed based on a more convenient and flexible framework having the following characteristics:-

- Virtualization and NF modularization
- United service-based architecture and interface
- Partition of user and control plane
- Decoupling of mobility and session management functions
- For introducing the new services, new QoS architecture has been introduced
- Network slicing to support new business domains

The 5G system network architecture is designed to support data connectivity and services, enabling deployments to use Network function virtualization and software-defined networking. The 5G architecture is defined in two ways:

- **A service-based representation:** - Here, the network functions such as AMF within the control plane allow other network functions to access their services. If necessary, this representation also includes point-to-point representation. 5G Core follows the Service Based Architecture approach
- **A reference point representation:** - This shows the interaction between the NF services in the network functions described by the point-to-point reference point between any two network functions (e.g, AMF and SMF). [23]

Following figure 25 depicts that the basic architecture of the 5G system is mainly a combination of four parts that are: - UE, NG-RAN, 5G Core Network, Data Network.

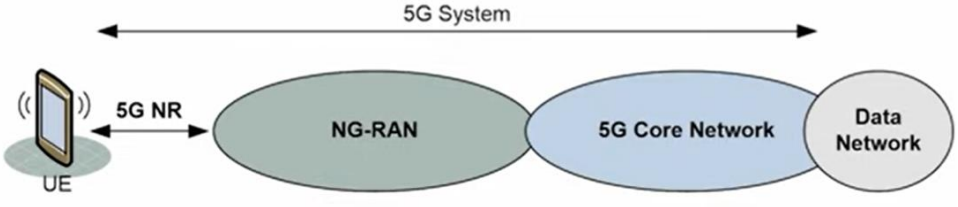

Figure 25: - 5G System (Ref: - https://www.youtube.com/watch?v=YVoCpqsPwmQ)

2.2.1 5G Core Network Architecture

5G Core network is a new architecture presented in the fifth generation of mobile communication. 5G Core Network Architecture involves three key focus areas: -

- PDU Sessions and Quality of Service (QoS) flows
- Actual architecture and key components
- Network functions virtualization
- Network slicing

Following figure 26 shows the reference point representation, where the various core network elements are connected up with different network reference points.

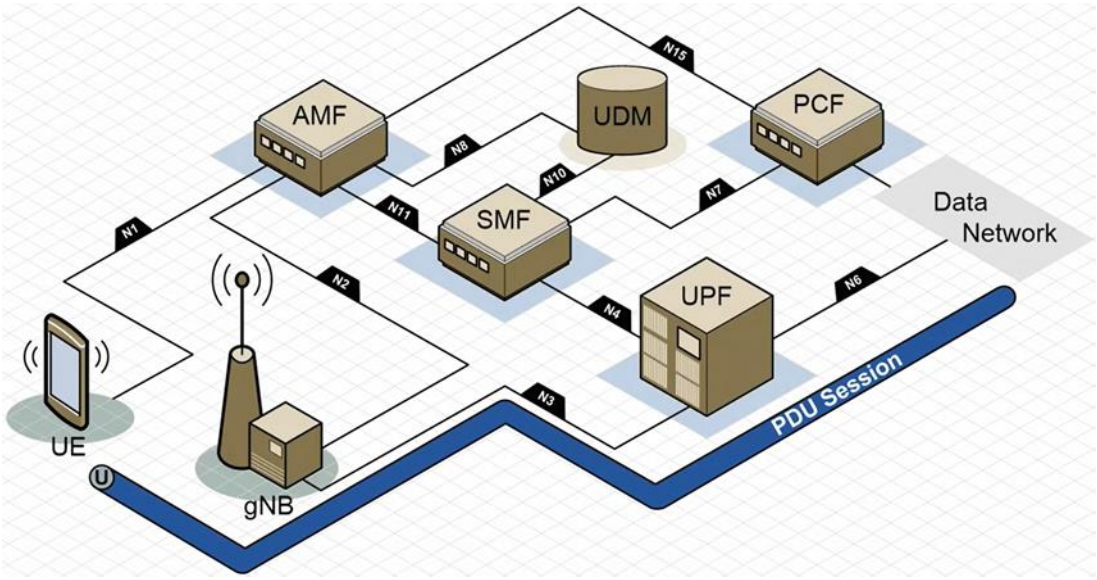

Figure 26: - 5G System detailed Architecture [24]

2.2.1.1 PDU Sessions and QoS Flows

Protocol Data Unit (PDU) session: - A user plane connectivity of earlier generation is known as PDU session in 5G. In figure 26, it has been depicted that, PDU runs from the mobile (UE) device, through the gNB to the UPF (User Plane Function), and then on to the Data Network (In LTE known as Packet Data Network). In the network, no other devices will be using the connectivity related to this particular PDU session. PDU sessions are unique to the device.

The multi-access PDU Connectivity Service is acknowledged by setting up a Multi-Access PDU (MA PDU) Session, for instance: - a PDU Session that might have user-plane resources on two access networks, as displayed on figure 27 beneath, extracted from TR 23.793 [25].

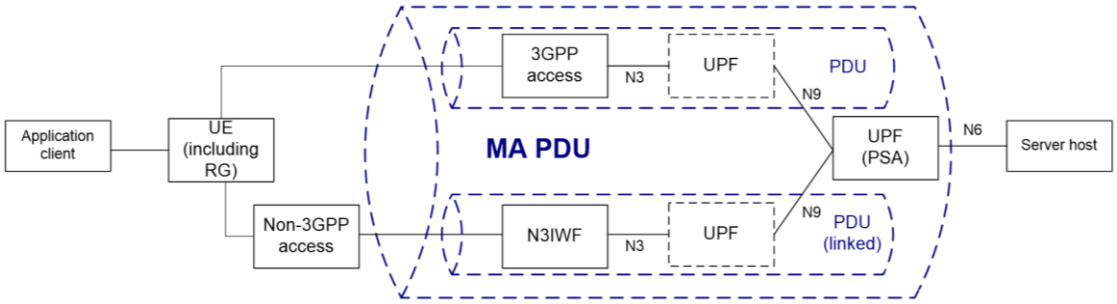

Figure 27: - MA PDU Session [25]

QoS Flows: - QoS flow is effectively a flow of user plane traffic that receives a particular level of Quality of Service. Default QoS flow has a particular level of Quality of Service.

Within a PDU session, Quality of Service is achieved by creating separated QoS flows. In the PDU session, there are several QoS flows actually in operation and these QoS flows are uniquely identified by QoS flow ID. One QoS flow is present with the default QoS profile and it can use all traffic related to the subscriber. QoS flows can be established and removed based on the QoS requirements of the User Plane traffic.

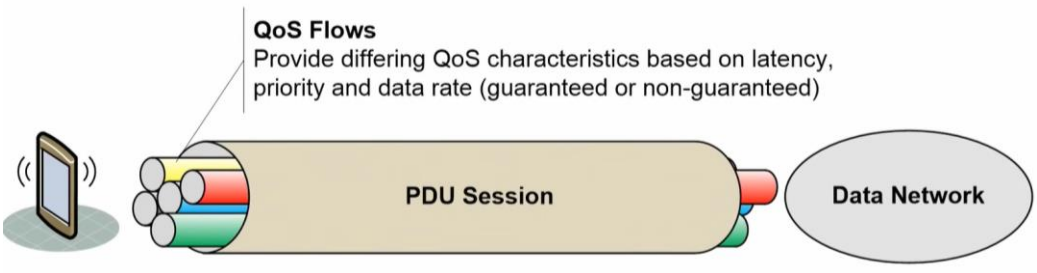

Figure 28: - PDU Sessions and QoS Flows [24]

When the additional QoS flows are added with different QoS requirements and different QoS levels, then filtering is necessary to select which traffic can go down these bearers.

Real-life Example: - If the data network was the internet, for example, then we typically only need one QoS flow. That would be the default flow and a best-effort QoS flow. If however, this is maybe 5G voice services and the data network is the IMS, then we could have a QoS flow that's carrying the signaling associated with voice, and then we would have a separate QoS flow that carries the actual voice packets themselves.

2.2.1.2 Actual architecture and key components

All components shown in figure 29 are fundamentally designed to keep the PDU session active for the subscriber and ensure that fundamentally, the PDU session follows them as the subscriber moves around the network. The detailed description of all components is as follows.

- **Access and Mobility Management Function (AMF): -** It is also known as the 'Core Access and Mobility Management Function'. This has got a similar role to the MME present in LTE whereby it looks after mobility management.

- In terms of subscriber mobility, it considers the fact that AMF always knows either the **tracking area that the subscriber is in**, or **the potential cell that they are in**, and it depends on whether the subscriber is idle or connected, respectively.

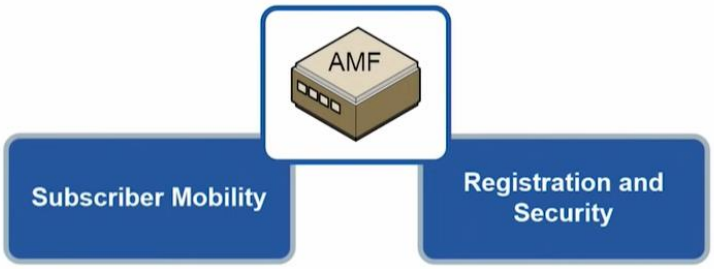

Figure 29: - Core Access and Mobility Management Function Flows [24]

- In terms of **security and registration**, the AMF liaise with various other subscriber databases to ensure that the subscriber is allowed on the network in the first instance.
- AMF plays a key role in **authenticating** that subscriber within the network.
- AMF provides the device with a **temporary identity** which you can use whenever it signals the network. Temporary ID is used in paging as well.

➢ **Session Management Function (SMF): -** So traditionally, in LTE, it would be the MME that does mobility management and session management. In 5G, that functionality has been split, so now the AMF does mobility management and the Session Management Function does session management. Major functions of SMF are as follows:

- The **establishment**, **modification,** and **teardown** of PDU sessions
- It routinely liaises with the **Policy Control Function** to determine whether or not a particular user data session is allowed to go ahead.

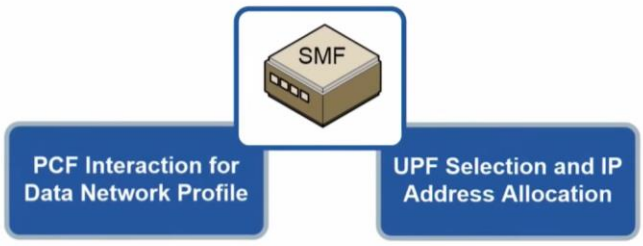

Figure 30: - Session Management Function [24]

- It is the job of the SMF to choose which **UPF** to be allocated and if the data session is IP-based, the SMF will also be allocating an **IPV4 or an IPV6** address.

PDU sessions can be based purely on **Ethernet or even unstructured data** in 5G. It's not everything around IP like it was in LTE.

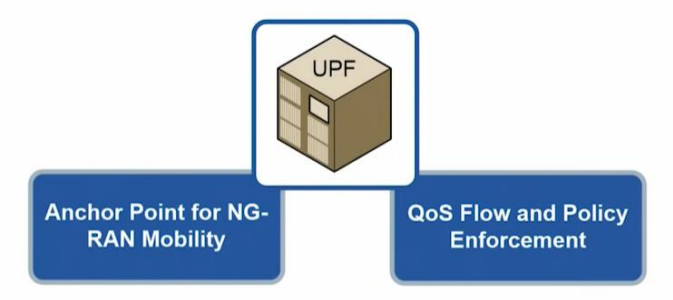

Figure 31: - User Plane Function [24]

- **Unified Data Management (UDM): -** UDM is a central repository of subscriber information. It is directly involved with **Access Authorization** because it holds security keys. UDM is also involved in **Registration and Mobility Management** because it tracks, where the subscriber is attached to and in terms of which AMF. After subscriber's allocation, it contains the **Data Network Profile or profiles**.

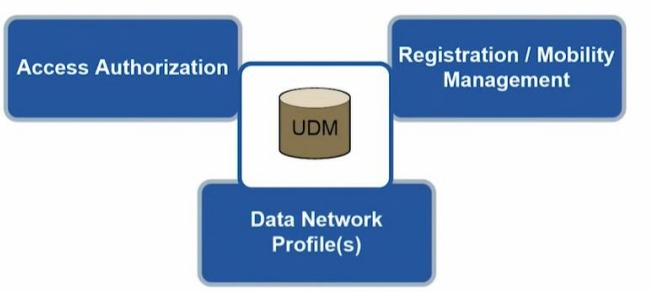

Figure 32: - Unified Data Management [24]

Data Network Profile effectively contains the subscriber profile and tells the AMF and the SMF about the subscriber's following access: -

- Exactly what the subscriber is and is not allowed to do.
- Which data networks they can connect to.
- What kind of QoS profile they can expect to be granted when they do connect to those data networks

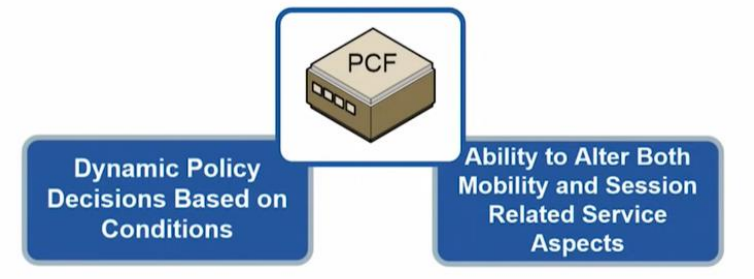

Figure 33: - Policy Control Function [24]

- **Policy Control Function (PCF): -** The function of PCF is to implement policy control and it is done on a dynamic basis. The decisions of dynamic policy are based on conditions that might be active in the network at that time. If there are subscribers in a particular geographical location and the PCF noticed that subscribers are not under the policy control.

In this case, PCF determines that the subscriber needs to be throttled at this time, or maybe isn't even allowed to get PDU session connectivity because the. As per the main diagram figure 33, the PCF does have connectivity into the data network as well, so the PCF can take session-related information such as if a subscriber is trying to make a phone call, PCF can take that information, send it into the 5G Core network to ensure that the correct resources are established. Hence, the PCF on a dynamic basis can **alter both mobility and session-related service aspects**. In the overall ecosystem, it does play a big part.

2.2.1.3 Network functions virtualization (NFV)

In 5G Core, much of these nodes are be virtualized as part of the NFV infrastructure. All devices of 5G Core architecture are not standalone devices but are software processes running on 'Commercial off the Shelf Server'. As figure 34 shows, virtualized devices like control plane, potentially user plane, subscriber management, billing, and policy control, all can run as software processes. There may be a small exclusion in the case of the UPF because there's an added complexity to the user plane, but certainly, from a control plan perspective, these elements can run as software processes.

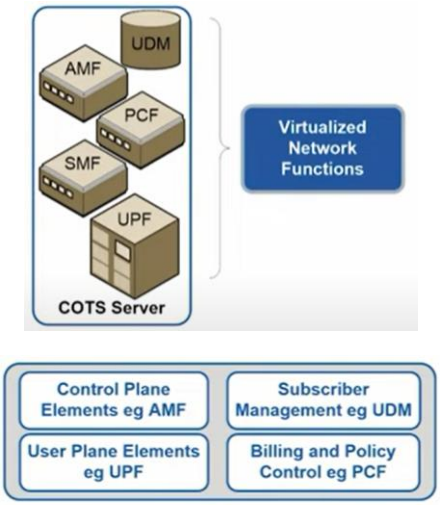

Figure 34: - Network Functions Virtualization [24]

The idea behind NFV is to have a Network Functions Virtualization infrastructure (depicted in figure 35). NFV infrastructure is fundamentally there to provide the software processes with the **compute**, the **storage**, and the **network** resources.

The key fact behind the NFV infrastructure is a shared infrastructure that all of these software processes will use and it's all built on Commercial Off The Shelf (COTS) hardware. Hence the **cost savings/potential cost savings,** to deploy the Core Network based on an NFV infrastructure is significant.

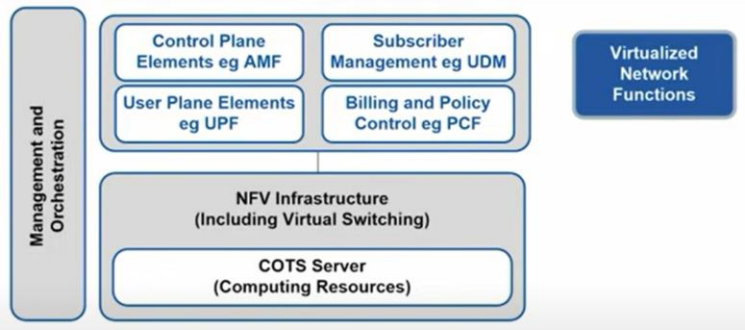

Figure 35: - NFV's main Components [24]

One key benefit of NFV infrastructure, other than financial, is **network flexibility.** As the processes are running as software processes, if we need to scale up or scale down capacity, it's much more straightforward in a virtualized environment. For instance, if there is a need for more AMF capacity if it's a traditional AMF deployed as a piece of hardware, then actually implementing a new AMF in the network can take weeks or even months, whereas if it's a virtualized AMF, so scaling up capacity could be a matter of minutes, but crucially, there is an of Management and Orchestration (MANO) to facilitate all of this. MANO is a piece of the infrastructure in and of itself.
Earlier in LTE, the protocols were exchanged between the core network elements but in 5G, Everything here is Application Programming Interfaces **(API) driven**. All virtualized devices or elements send API calls to one another to communicate.

2.2.1.4 Network slicing (NS)

Network Slicing allows the service provider to create multiple logical networks over the same physical infrastructure. As per section 1.2.8.4, 5G is not just about providing huge data rates to the subscriber, but 5G is about becoming an enabler network for various applications and third-party users of the network and the common example is the Internet of Things. So, there was a need to create a very adaptive, flexible network that would provide **different customers, different third parties with different features**. Network Slicing is a perfect solution to achieve the above requirements. Due to NS, the service provider has more flexibility in terms of how it provides specific services or service environments to customers.

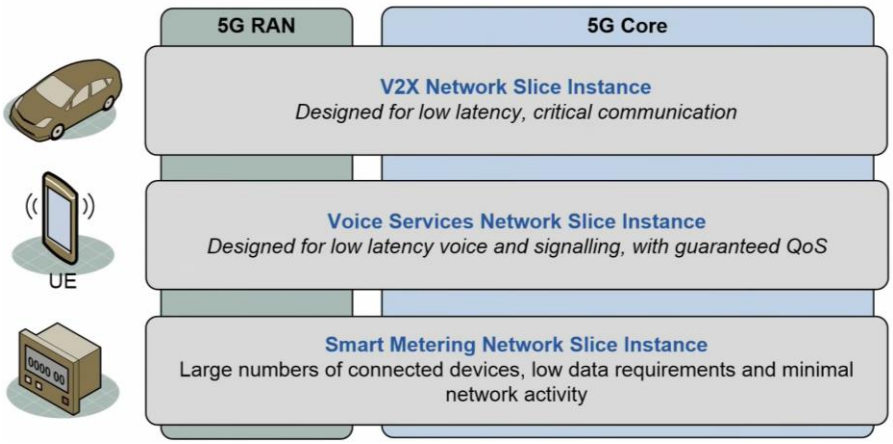

Figure 36: - Network Slicing [24]

Above figure 36 is illustrated that, on the same physical service, there are different network slices with different characteristics. In other words, lots of different environments can be accommodated by network slicing. In terms of standards, an individual device can connect to up **to 8 network slices** simultaneously.

In 3GPP Release 16 Network Slicing addresses two major following limitations of Release 15 in 5GC: -

- Enhancement of interworking between EPC and 5GC
- Support for NSSAA [25]

2.2.2 5G RAN Architecture

NR- New Radio | Radio Access Technology beyond LTE are the terms used for 5G Radio Access Network. The NG-RAN (NextGen RAN) consists of a set of gNBs connected to the 5GC through the NG interface. It is based on and very similar to the LTE's S1 interface. Figure 37 depicts the overall NG-RAN architecture.

2.2.2.1 gNB (5G Node B)

It can be connected to another gNB through the Xn interface. gNB may be further split into the following two types: -

- gNB-Central Unit (gNB-CU)
- gNB- Distributed Unit(s) (gNB-DU)

These gNBs are connected through the F1 interface and one gNB-DU is joined to only one gNB-CU. The gNB performs the following functions: -

- Radio transmission and reception
- Digital signal processing
- Access stratum signaling to UE
- Relay no-access stratum signaling between the UE and core network
- Radio resource management
- Interaction between the core network and nearby base stations
- Connection setup and release
- Paging messages' scheduling and transmission
- Measurement reporting configuration for mobility
- Measurement reporting configuration for scheduling
- Tight interworking between NR and E-UTRA

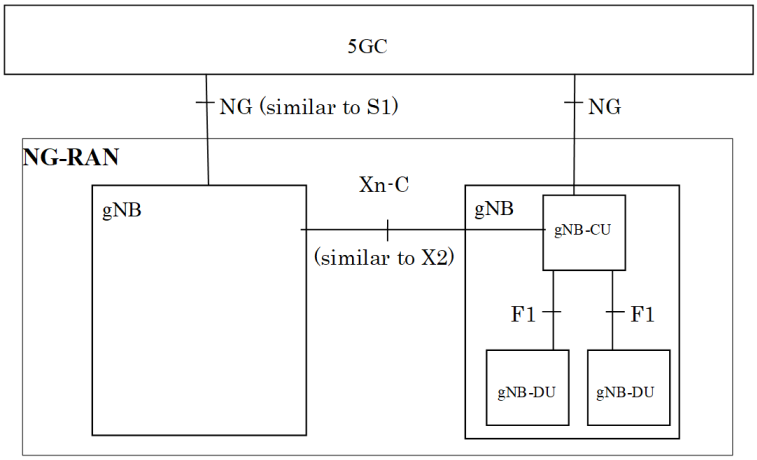

Figure 37: - Overall NG-RAN Architecture [19]

2.2.2.2 Xn Interface

Xn interface inherits the LTE's X2 interface's functionality. The functions of Xn are as follows: -

- Signaling and traffic forwarding during handover.
- Signaling and traffic forwarding for duel connectivity
- Self-optimizing network

2.2.2.3 NG Interface

NG is based on and very similar to the LTE's S1 interface. The functions of NG are as follows: -

- Control of base station by the core network
- Relay non-access stratum signaling
- Deliver user plan traffic

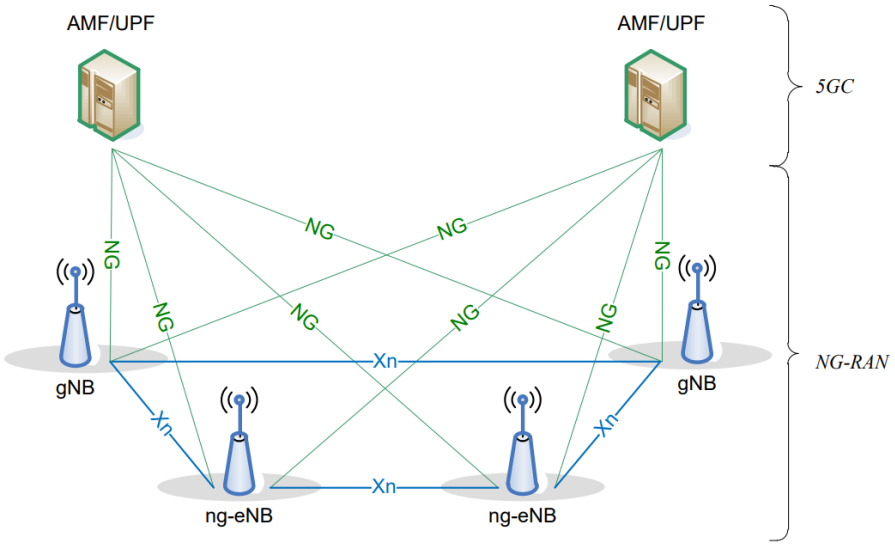

Figure 38: - NG-RAN in relation to the 5G system *(Ref:* 3GPP TS 38.300 V15.3.1 (2018-10)*)*

2.2.2.4 Enhancements in NR in Release 16

Above figure 38, illustrated the graphical representation of all elements of NG-RAN. Some new Radio features have been added and others have been enhanced in Release 16 of 3GPP. The applicable deployment scenarios [25] are described in release 16 as follows: -

- Scenario A: Carrier aggregation between NR in the licensed spectrum (PCell) and NR in the shared spectrum (SCell). It has further two scenarios: -
    - A.1: - Where SCell is not configured with UL, it uses DL only
    - A.2: -Where SCell is configured with UL (DL+UL)
- Scenario B: Double connectivity among LTE in licensed spectrum and NR in the shared spectrum (PSCell)
- Scenario C: NR in the shared spectrum (PCell)
- Scenario D: NR cell in shared spectrum. It uplinks in licensed spectrum
- Scenario E: Double connectivity among NR in the licensed spectrum (PCell) and NR in the shared spectrum (PSCell)

2.3 5G Security

Fifth-generation protects the data in transit and information by following various technologies and algorithms. In 5G following major security components have been emerged: -

- Enhanced Mutual authentication
- Protect NAS signaling
- protect RRC signaling
- protection of user plane traffic is also available
- Protection of IP connectivity using various technologies like IPSec

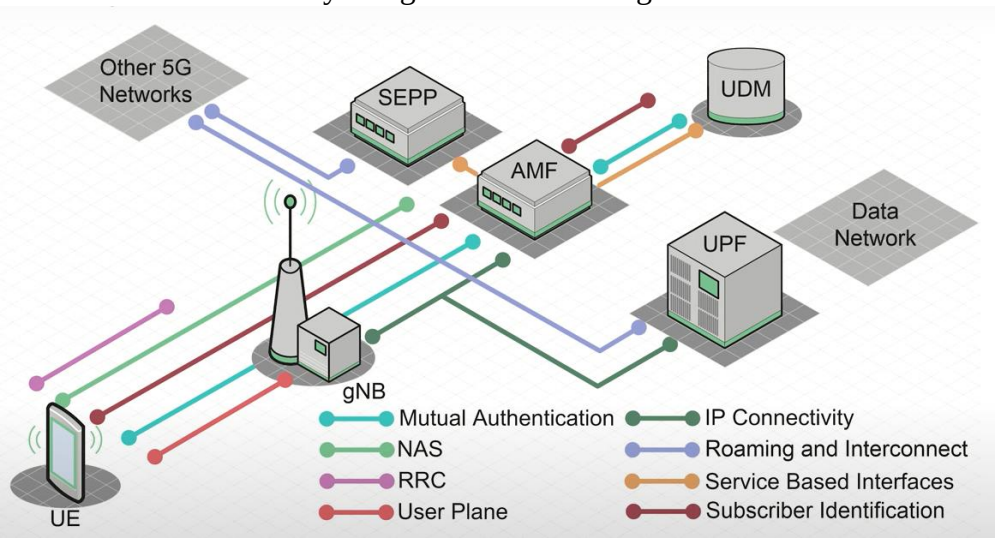

Figure 39: - 5G Security Overview [26]

- Roaming and Interconnect Security in both UP and CP perspective
- Protect service-based interface
- Protect subscriber identification

2.3.1 Mutual Authentication

Mutual Authentication is not a new technique. It was introduced in 3g. In the MU process, first of all, the device responds to any kind of security challenges that might come from the network The device UE verifies whether the network is legitimate or not. After verifying, the device responds to an authentication challenge to allow the core network to verify that the device is legitimate.

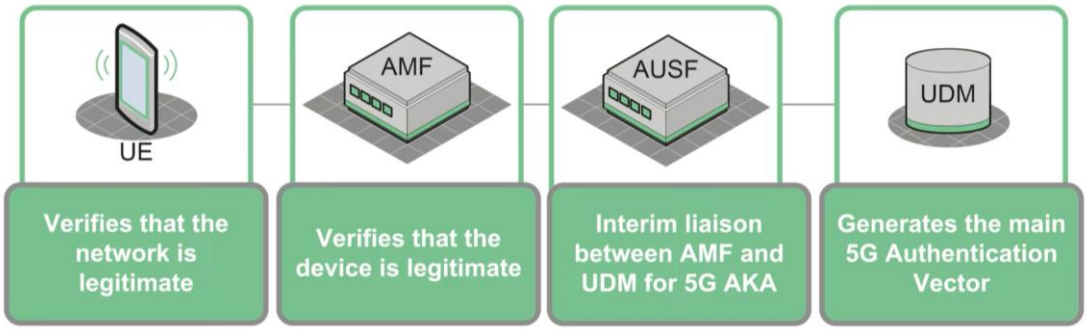

Figure 40: - Flow of Mutual Authentication [26]

So although mutual authentication is taking place between the device and the AMF, there is still a need for Authentication Server Function (AUSF) and Unified Data Management (UDM). AUSF uses AKA (Authentication and Key Agreement) process to check the authentication. UDM generates the authentication vector by using the secret key of the device. The device gets the secret key. The secret key is also stored at the UDM. Both are symmetrical keys. They are identical in each location.

2.3.2 Encryption and Integrity

Encryption means obscuring the data in transit, so if anybody is snooping on the radio link, no one can read the data because it is garbled data, it would not make any sense. **Integrity** checking is just ensuring that the data has not been changed or tampered with whilst it has been in transit. Because of two different techniques, different algorithms for encryption and integrity checking are used.

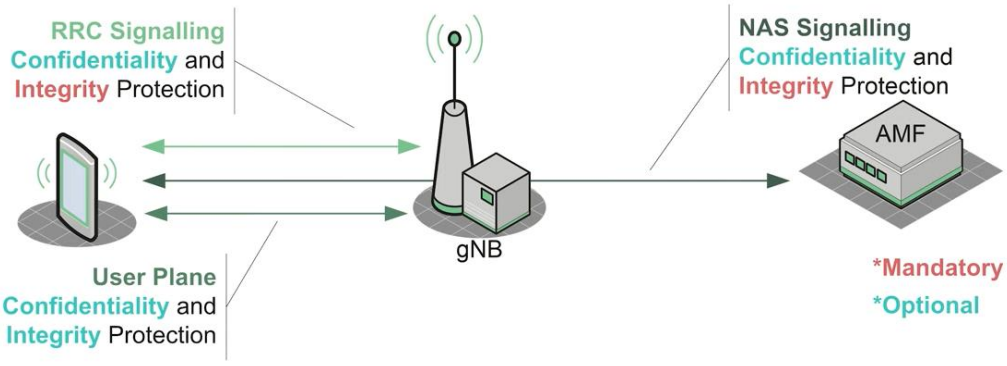

Figure 41: - Encryption and Integrity [26]

As depicted in above figure 41, between the AMF and the device (gNB), we are going to protect Non-Access Stratum (NAS) signaling. There is an option to encrypt and decrypt the NAS signaling. The integrity check is mandatory in the case of NAS signaling. There is no need to encrypt the traffic staying on the theme of signaling. In Radio Resource Control (RRC) signaling, encryption of the signaling is optional. Integrity checking is mandatory here as well.

In User Plane, **confidentiality, encryption, and integrity checking perspectives are optional**. It would depend on the scenario as to whether or not the user wants to use them. For a human subscriber using a smartphone, it would expect that confidentiality would be active and used. In the case of cellular IoT devices, whose data is not necessarily sensitive information, the user might not need to go to the complexity of actually encrypting it. All (UP, NSA, RRC) require separate keys so, during the 5g authentication and key agreement process, all of the keys agree upon and are distributed through the system where necessary.

2.3.3 Protecting Service based Interfaces

To protect **service-based architecture** and **service-based interfaces**, 5G provides two different options.

- Protocol Stack-based authentication
- Token-based authentication with OAuth 2.0

The **protocol stack** is used for service-based interfaces, and it is the same in each case. All interfaces adopt HTTP 2. Now there is a mechanism that is inherently supported, and that is the Transport Layer Security (TLS). If anyone wants to protect HTTP traffic, TLS can be used in the protocol stack, and figure 42 depicts that TLS sits between HTTP 2 and the Transmission Control Protocol (TCP). The 3gpp also specifies the different cipher suites that are allowed to be used. So this is the way to protect traffic using TLS. Integrity checking and encryption of all of service service-based interface messages are also present.

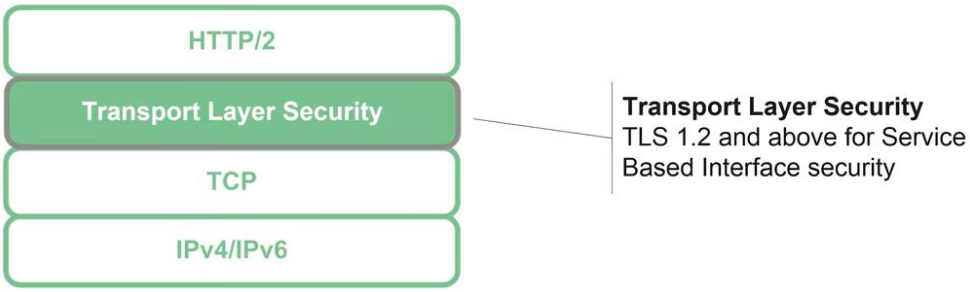

Figure 42: - Protecting HTTP message [26]

Token-based authentication with OAuth 2.0 is the second approach and it is not really about protecting the traffic in transit but this is more about protecting the service producer because no one wants malicious attempts to invoke services at a service producer by some kind of malicious service consumer. In a token-based authentication mechanism, Network Repository Function (NRF) serves as a token server. So on the bottom in figure 43, the consumer (Client) resides on the left and the producer (Server) on the right. Before a consumer asks for a service from the producer, it must, first of all, acquire an access token from NRF. The signed token is provided by NRF, and that token applies to maybe a specific type of network function.

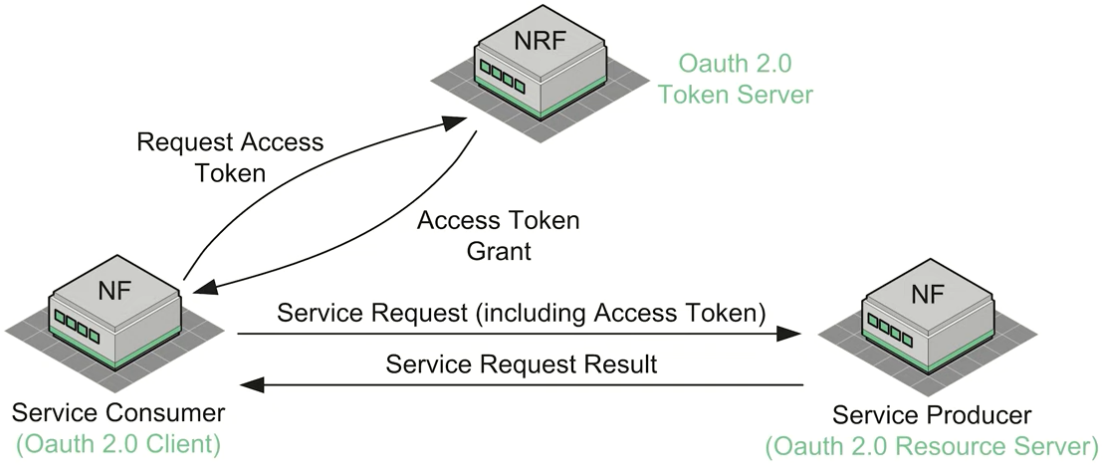

Figure 43: - Token-based authentication with OAuth 2.0 [26]

The signed token has a life span, and it can be used as part of the request that the consumer needs to send up to the producer. Token resides in the HTTP header. In other words, it resides within the authorization field of the HTTP 2 header itself. The service producer, before responding to a service request, verifies the authenticity of the token. It can use public key infrastructure methodologies to verify the access token. After assuming it does check out and assuming the permissions on it do cover the nature of the request well, SP delivers that service down. These two aspects of core network security are particularly important but are **optional to use**.

2.3.4 Roaming Protection – SEPP, PRINS & IPUPS

Roaming protection is very important because, in many cases, users do not have direct connectivity between a visited PLMN and a Home Public Land Mobile Network. There is an IPX (IP Packet Exchange) network that resides between our home and visits PLMNs. IPX is just a network of networks, but clearly and crucially, it is not owned by the Mobile Service Provider (MSP) but is owned by a third-party connection provider. So, it is necessary to secure traffic as it traverses the user's network to the network interface. In 5G, it is possible through SEPP, PRINS, and IPUPS.

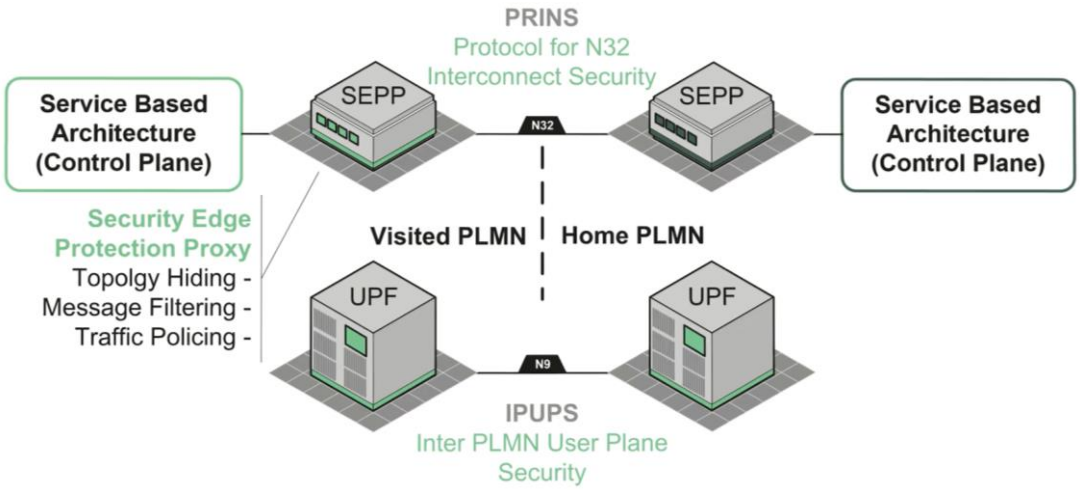

Figure 44: - Roaming Protection [26]

In **Control Plane traffic**, to protect the traffic, the Security Edge Protection Proxy (SEPP) is used. It includes several different security features like: -

- **Support topology hiding** (filter out any sensitive addressing information that might be found within signaling)
- **Message Filtering** (filter specific messages themselves)
- **Traffic Policing** (police traffic streams)

As depicted in figure 44, there is a protocol named PRINS that resides on N32 interconnect security. PRINS is known as Protocol for N32 Interconnect Security. PRINS has major two features: -

- It allows users to selectively protect just parts of the message and leave other parts of the message that are required for routing to be unsecured but to ensure that users do not have any malicious activity in terms of tampering with the message, users can still integrity protect the message.
- It allows IPX networks to be able to adjust the messages without actually breaking the overall integrity of the message.

In **User Plan** security, IPUPS (Inter-PLMN User Plane Security) is used on the N9 interface. The connectivity between N9 and IPUPS is fairly straightforward, where no traffic can pass across N9 unless it is associated with a pre-configured GTP-U (GPRS Tunneling Protocol) tunnel.

** GTP-U: - It transports user data within the core GPRS network, between RAN and the core network. GTP-U supports IPv4 and IPv6 user data. GTP-U transport is IPv4.
(Ref: - https://www.juniper.net/documentation/en_US/junos-mobility11.2/topics/concept/gtp-mobility-protocols-overview.html)

For instance: - If the UPF receives a piece of traffic saying the visited PLMN and wants to send it to the home PLMN and a GTP-U tunnel has not been set up or not available, N9 will not send that traffic or the traffic will be dropped. If a GTP-U tunnel has been set up N9 know that each end of the connection is aware of the traffic, there will be malicious or unexpected not be taking place.

2.3.5 Protecting the Subscriber Identity

The IMSI of a subscriber has long been considered to be sensitive information because IMSI does not change. So, there is a risk if a subscriber could be tied to a specific location and somebody is snooping the radio traffic.

**An IMSI is a 15-digit number for every user in a GSM.

Earlier generations (2G, 3G) used a temporary id when the user do not want the device to use the IMSI. In 4G and 5G, Globally Unique Temporary Identifier (GUTI) and 5G Globally Unique Temporary Identifier (5G-GUTI) are used, respectively. But there is some case when a user cannot use the temporary id only because the core network does not recognize it, particularly in case of no network connection. In this condition, in all generations, the device simply has to send its IMSI. The major problem occurs when a device sends IMSI and NAS signaling is not being encrypted.

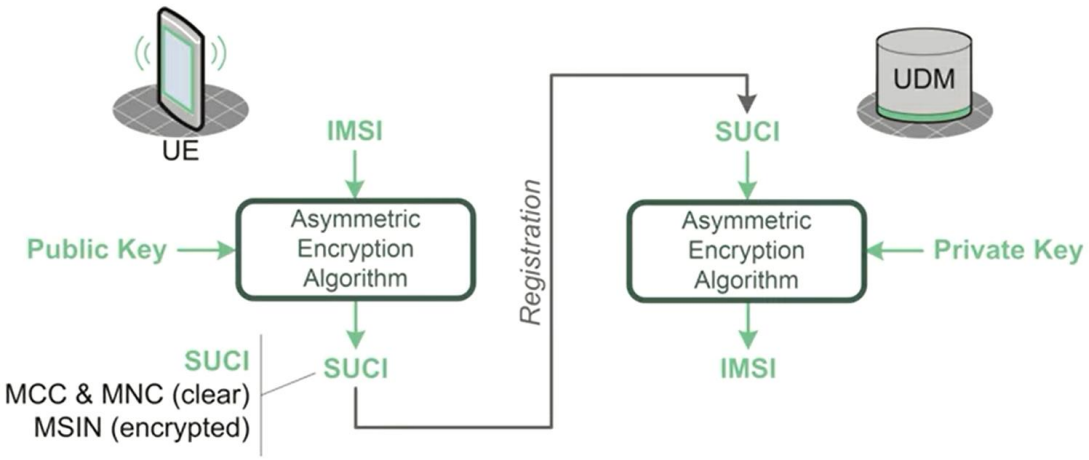

Figure 45: - Subscription Concealed Identifier [26]

To solve the problem, 5G introduced a new mechanism known as the **Subscription Concealed Identifier**. This essentially means that the device never needs to send up the IMSI in the clear now. In 5G IMSI is strictly known as **Subscription Permanent Identifier** (SUPI). In SUCI, an asymmetric algorithm is used. In 5G, the actual key derivation is quite complicated. As shown in above figure 45, it's only the Mobile Subscriber Identification Number (MSIN) portion of the SUPI

gets encrypted. Mobile Country Code (MCC) and Mobile Network Code (MNC) are clear because they use routing purposes.

2.3.6 Release 16 about Security

The following are some enhancements regarding security has been introduced in release 16 [25]: -

- Security aspects of 3GPP support for advanced V2X (Vehicle-to-Everything) services. These are specified in TS 33.536
- Add procedural texts as well. The Security Key IE may include KTNGF/KTWIF/KWAGF in TS 29.413
- Release 16 enlarges on the mission-critical security architecture, which is already defined in earlier releases accompanied by various mission-critical security clarifications and corrections.

2.4 5G VS 4G

Fourth-generation has its importance. It was known as a revolution in mobile communication. Now the world is planning to move from 4G to 5G. 5G is an enhancement of 4G. The following table describes major differences to be there in 5G as compared to 4G.

Table 3: - 5G VS 4G [23] [27]

Specifications	4G	5G
Peak Data Rate	1Gbps	10Gbps
Data Bandwidth	200Mbps to 1Gbps	1Gbps and higher as per need
Spectral Efficiency	30 b/s/Hz	120 b/s/Hz
TTI	1ms	Varying (100 µs (min.) to 4ms (max.)
Latency	10ms (radio)	<1ms (radio)
Frequency Band	2 to 8 GHz	3 to 300 GHz
Technologies	Unified IP, seamless integration of broadband LAN/WAN/PAN and WLAN	Unified IP, seamless integration of broadband LAN/WAN/PAN/WLAN and advanced technologies based on OFDM
Mobility	350Kmph	500Kmph
Core network	All IP network	Flatter IP network, 5G network interfacing(5G-NI)
Handoff	Horizontal and vertical	Horizontal and vertical
Multiple Access	CDMA	CDMA, BDMA, FBMC
Applications	High rate data Applications, Wearable Devices	Device-to-device, Machine-to-machine, IoT, 2-way gaming, Virtual reality glasses, Cloud-based computing, etc.

3 INTERNET OF THINGS (IoT)

“Internet of Things" is an extensive area in itself. The concept and term IoT first appeared in a speech by Peter T. Lewis in September 1985. Lewis described that the Internet of Things is an integration of people, processes, and technology with connectable devices and sensors. It assists in enabling the remote monitoring, status, manipulation, and evaluation of trends of such devices [28].

Internet of things is defined as *“The stage when two or more things or objects are connected to the Internet than people"* by Dave Evans. According to Cisco Systems, the IoT was "born" between 2008 and 2009. In this period, the things/people ratio has been intensified from 0.08 in 2003 to 1.84 in 2010 [29].

Figure 46: - IoT Perspective (Ref: - https://betterlifevisual.wordpress.com/)

The IoT can simply be defined as a collaboration of physical object/s, sensor/s, processing ability, software, and other technologies that communicate and interchange data with each other or with other devices and systems over the Internet/ other communications networks. Above figure 46, elaborates the idea behind IoT technology. The technical concept of the IoT is to enable different objects to sense information using sensors and send this information to a server. The server analyzes the information and translates that to certain behaviors or actions.

3.1 TYPES OF IoT

IoT has been divided into five fields as follows: -

3.1.1 Consumer Internet of Things (CIoT)

The Consumer Internet of Things knows as IoT for consumer applications and devices. Consumer IoT includes the following product: -

- Smartphones
- Wearables
- Smart assistants
- Smart home appliances

CIoT solutions use Wi-Fi, Bluetooth, and ZigBee to facilitate connectivity, which offers short-range communication. It is suitable for deployments in smaller venues, such as personal and home environments and offices.

3.1.2 Commercial Internet of Things

Commercial IoT is an enhancement to CIoT and it delivers the benefits of IoT to larger venues. It includes the following venues: -

- Commercial office buildings
- Supermarkets
- Stores
- Hotels
- Healthcare facilities
- Entertainment

There are major four use cases for commercial IoT: -

- Monitor environmental conditions
- Managing access to corporate facilities
- Economize of utilities and consumption in hotels
- Improvement in customer experiences and business conditions.

3.1.3 Industrial Internet of Things (IIoT)

It is the most dynamic wing of the IoT industry. Its focus is on adding existing industrial systems with IoT to make them more productive and efficient. IIoT deployments are typically found in the following streams: -

- Large-scale factories
- Manufacturing plants
- Industries (healthcare/agriculture/automotive/logistics)

The Industrial Internet is the most well-known example of the Industrial Internet of Things.

3.1.4 Infrastructure Internet of Things

Infrastructure IoT is a subset of the Industrial Internet of Things. It is concerned with the development of smart infrastructures. Smart infrastructure incorporates IoT technologies to boost

efficiency, cost savings, maintenance, etc. Infrastructure Internet of Things includes the ability to: -

- Monitor operations of urban and rural infrastructures.
- Control operations of urban and rural infrastructures

Urban and rural infrastructures are: - Bridges, railway tracks, and on-and offshore wind farms.

3.1.5 Internet of Military Things

Internet of Military Things (IoMT) is also recognized as Battlefield IoT. The IoBT includes the use of IoT in military settings and battlefield situations. Internet of Military Things mainly aimed at the following factors: -

- Increasing situational awareness
- Bolstering risk assessment
- Improving response times

Following are targeted to be interconnected in IoBT: -

- Connecting ships
- Planes
- Tanks
- Soldiers
- Drones
- Forward Operating Bases

In addition, the Internet of Battlefield applications has been developing to improve military practices, systems, equipment, and strategy.

3.2 CHALLENGES AND FEATURES OF IOT

3.2.1 Challenges in IoT

There are the following major challenges in IoT application development on a large scale: -

- **Security: -** Cyber hackers always try to develop methods to access back-end systems and hack into the network where they do not belong. As IoT is a combination of hardware and software technologies, there is a need to provide a security system that is compatible with both types of technology. In IoT, threats can occur from the following two aspects: -
    - among communication of devices
    - in the communication between different devices and remote servers
- **Awareness: -** The lack of awareness can occur from community or industry. In the case of community, the lack arises when people do not know about the importance of connecting

their devices to the internet. Secondly, in an industry sector, where not many enterprises know about IoT technology or even if they know, most enterprises still face problems which will be leading this initiative.

- **Interoperability: -** It becomes a major challenge because of the diverse range of devices to be connected to design or develop an IoT system. There is a need to coordinate these different devices has been increased. Different IoT devices are available, which are based on different hardware, different platforms, manufactured by different vendors. Even some IoT devices use their standards and interfaces to communicate with other devices or remote servers. This scenario may cause a conflict when different devices are used in the same domain. In other words, the incompatibility among devices, sensors, and even interfaces of remote servers is a reason behind the interoperability challenge in IoT.

Other challenges are related to the Business model, connectivity (Power consumption), and big data.

3.2.2 Challenges of IoT addressed by 5G

As 5G technology can address the major challenges of a cellular network more effectively rather than its predecessors, it is automatically addressed the challenges of IoT as well. Some of the challenges are appended as follows: -

- Large bandwidth and Higher data-rate
- Massive connectivity and Low end to end latency
- Cost-effective and Consistent Quality of Service
- Device computational capabilities
- Device intelligence services
- Security enhancements (Special updates related to security for advanced V2X services has been embedded in Release 16 of 3GPP [25])

3.2.3 Features of IoT

Following are the major features [30] of IoT: -

- **Dynamic &Self-Adapting: -** IoT devices and systems can dynamically adapt to the changing contexts and take actions based on the operating conditions, user's context, or sensed environment.

- **Self-Configuring: -** Due to the Self-Configuring feature, IoT allows several devices to work together to provide certain functionality like setup networking, fetch latest software upgrades.
- **Interoperable Communication Protocol (ICP): -** IoT devices may support several ICPs and can communicate with other devices and infrastructure as well.

- **Unique Identity: -** Each IoT device has a unique identity and a unique identifier like an IP address or a URI. IoT devices allow users to query the device, monitor the status, control them remotely.

- **Integrated into information network: -** This feature allows IoT devices to communicate and exchange data with other devices and systems. IoT devices can be dynamically discovered by other devices and can describe themselves to other devices or user applications.

3.3 IoT TECHNOLOGIES

Technologies behind IoT can be divided into three parts [31], entities, levels behind IoT, and major components of IoT system.

3.3.1 ENTITIES

There are the following entities used in IoT, which include various IoT technologies.

3.3.1.1 Hardware

- Arduino UNO
- Raspberry Pi
- Intel Galileo
- Intel Edison
- ARM embedded
- Boss XDK
- Beaglebone

3.3.1.2 IDE for developing device software

Each hardware has a separate IDE (Integrated Development Environment**)** environment like Arduino IDE, Python IDE, Arduino Software (IDE), Cloud9 IDE.

3.3.1.3 Protocols

- RPL (Routing Protocol)
- CoAP (Constrained Application Protocol)
- REST (Representational State Transfer)
- HTTP (HyperText Transfer Protocol)
- MQTT (Message Queuing Telemetry Protocol)
- XMPP (Extensible Messaging and Presence Protocol)

3.3.1.4 Communication

Ethernet, RFID, NFC, M2M, V2V, V2X, 6LowPAN (Low-Power Wireless Personal Area Networks), UWB (Ultra-Wide Band), ZigBee (Zonal Intercommunication Global-Standard), Bluetooth, Wi-Fi, WI-Max (Worldwide Interoperability for Microwave Access), 2G/3G/4G/5G are used to enable the IoT to communicate. Some of the approaches from these are described as follows: -

- **RFID (Radio Frequency Identifications): -** The RFID is a two-part wireless system: tags and readers.
    - Tags are attached to connected objects or devices. These tags use radio waves with different antenna frequencies to communicate between devices.
    - Tags contain stored information, which is normally read by **readers**. The tags can also be passive when powered by a reader or by batteries.

- **NFC (Near–Field Communication): -** NFC is the most important radio technology used for enabling wireless IoT communication. NFC is based on the RFID mechanism but it includes the same concept in smartphones. NFC depicts the concept of low-power wireless networks, in which all devices are connected to other mobile phones in the same domain and send small amounts of data. The range of typical NFC is 20 m.

- **Machine-to-Machine Communications (M2M):** - Diversity of connected objects is the key concept of M2M communications in IoT. M2M has five components as follows: -
    - M2M Device
    - M2M Gateways
    - M2M Communication Network
    - M2M Area Network
    - M2M Applications

- **Vehicle-to-Vehicle Communications (V2V): -** It requires a complex network infrastructure because it involves vehicle communication. Vehicles usually move from place to place, leading to a non-fixed topology. There are two types of interactions involved in describing V2V communication: -
    - Interaction between vehicle and vehicle
    - Interaction between vehicle and road infrastructure

3.3.1.5 Network Backup

- IPv4 (Internet Protocol Version 4)
- IPv6 (Internet Protocol Version 6)
- UDP (User Datagram Protocol)
- 6LowPAN (Low-Power Wireless Personal Area Networks)

3.3.1.6 Software

- RIOT OS
- Contiki OS
- Thing Square mist firmware
- Eclipse IoT

3.3.1.7 Internet Cloud Platforms / Data Centre

- Sense
- Thing Worx
- Nimbits
- Xively
- OpenHAB
- AWS IoT (Amazon Web Services)
- IBM BlueMix
- CISCO IoT
- Iox and Fog
- Azure
- TCS CUP

3.3.1.8 Machine Learning algorithms and software

- Knime
- Acccord.net
- Scikit-Learn
- TensorFlow
- Weka
- Pytorch
- RapidMiner
- Google Cloud AutoML

3.3.2 LEVELS BEHIND IOT

There are five levels behind an IoT system.

1. Hardware selection (Device Platform)
2. Connecting and internetworking
3. Servers & Web Services
4. Cloud platform to store data
5. Analysis (OLTP, OLAP, data analytics, Knowledge discovery)

3.3.3 MAJOR COMPONENTS OF IOT SYSTEM

- **Physical Objects** exist with embedded software into the hardware.
- **The hardware** consists of a microcontroller, firmware, sensors, control unit, actuators, and communication module. Figure 47 and figure 48 show different types of sensors and components of the control unit, respectively.
- **Communication Module** is the software consisting of device APIs and interfaces for communication over the network and communication circuit/port(s).

Figure 47: - Different Types of sensors [32]

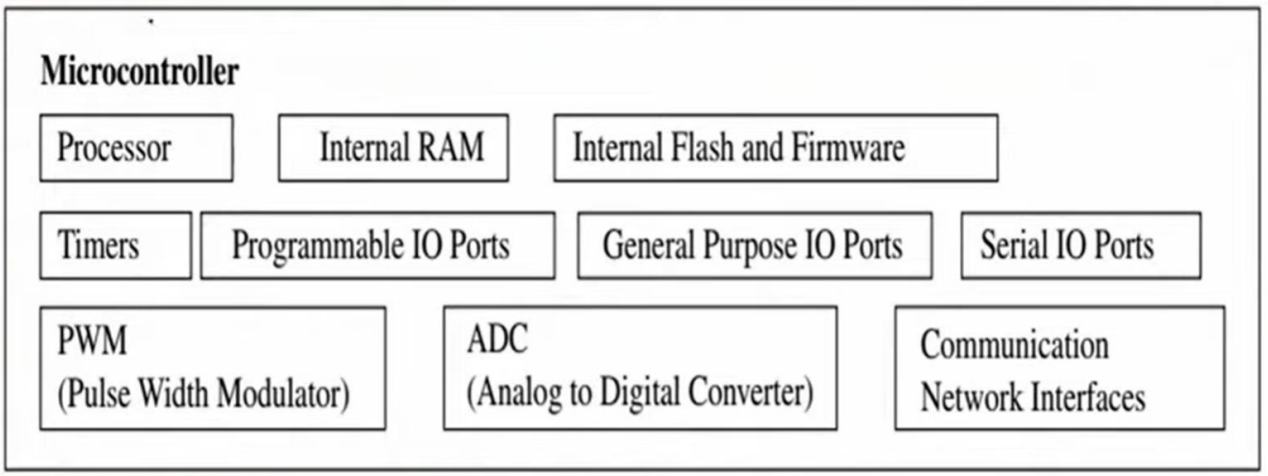

Figure 48: - Components of Control Unit [31]

- **Software** is used for performing actions on messages, information, and commands using glowing LEDs, robotic hand movement, etc. Following figure 49 depicts the layered architecture used in IoT devices.

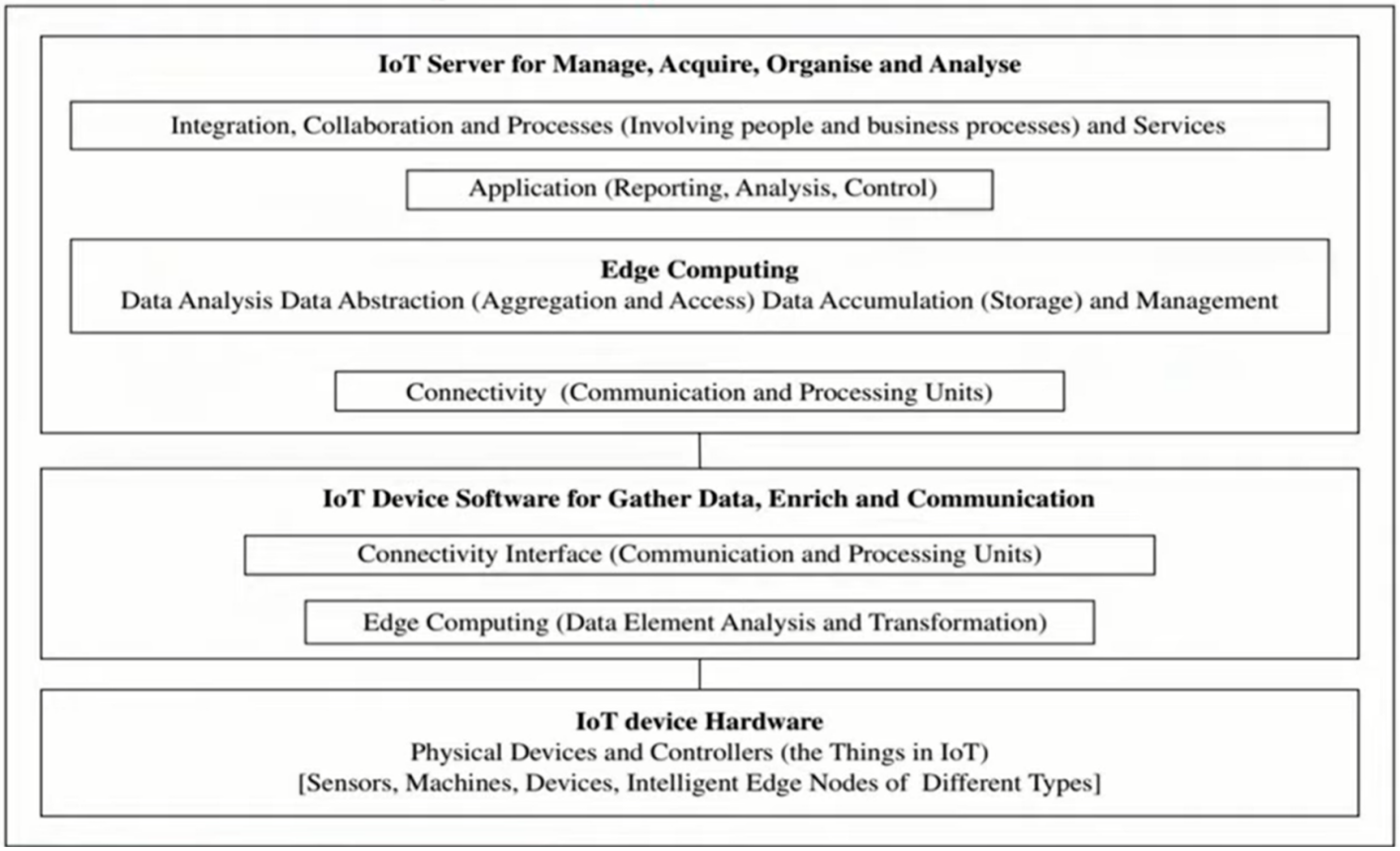

Figure 49: - Layered Architecture [31]

3.4 IoT ARCHITECTURE

There is no particular consensus on IoT architecture because different architectures have been proposed by various researchers based on the wide domain of internet objects. Most of the researchers designed IoT architecture based on three layers, but five-layer architecture is also famous.

3.4.1 Requirements for an end-to-end IoT architecture

For any kind of architecture (three, four, five-layered) there is some prerequisite [33], which must be completed by the used architecture.

- **Concurrent Data Collection: -** IoT architecture must support for collection, analysis, and control from a large number of sensors or actuators.
- **Efficient Data Handling: -** It must minimize raw data and maximize actionable information.
- **Connectivity and Communications**: - IoT architecture must provide network connectivity and flexible, robust protocol support between sensors/actuators and the cloud.
- **Scalable: -** It can scale individual elements in the system.
- **Availability and Quality of Service: -** It should have minimal latencies and fault-tolerant
- **Security: -** End to end encryption and monitoring is necessary.
- **Modular, Flexible, and Platform-independent: -** Each layer should allow for features, hardware or cloud infrastructure to be sourced from different suppliers.
- **Open Standards and Interoperable: -** Communication between the layers should be based on open standards so that interoperability must be ensured.
- **Device Management: -** It must enable automated/remote device management and updates.
- **Defined APIs: -** Each layer should have defined APIs. It must allow for easy integration with existing applications and other IoT solutions.

3.4.2 Three Layered IoT architecture

Three Layered architecture is the most used architecture till now. It is based on Perception, network, and application layer. Figure 50 depicts the 3 layered IoT architecture.

Three layers of 3-layered architecture are defined as follows [33] [34]: -

The perception layer is the physical layer. It includes environmental information sensors. In the surroundings, physical parameters are sensed and other intelligent objects are identified. In other words, Sensors, actuators, and edge devices that interact with the environment are the major components of this layer.

Network Layer usually connects to other intelligent devices. It also connects with network devices, and servers. The major function of this layer is to transmit and process sensor data. It also discovers, connects, and translates devices over a network and in coordination with the application layer.

The Application Layer provides specific application services to the user. It includes a myriad of applications for the IoT, such as smart homes, smart agriculture, and intelligent health. It provides data processing and storage with specialized services and functionality for users.

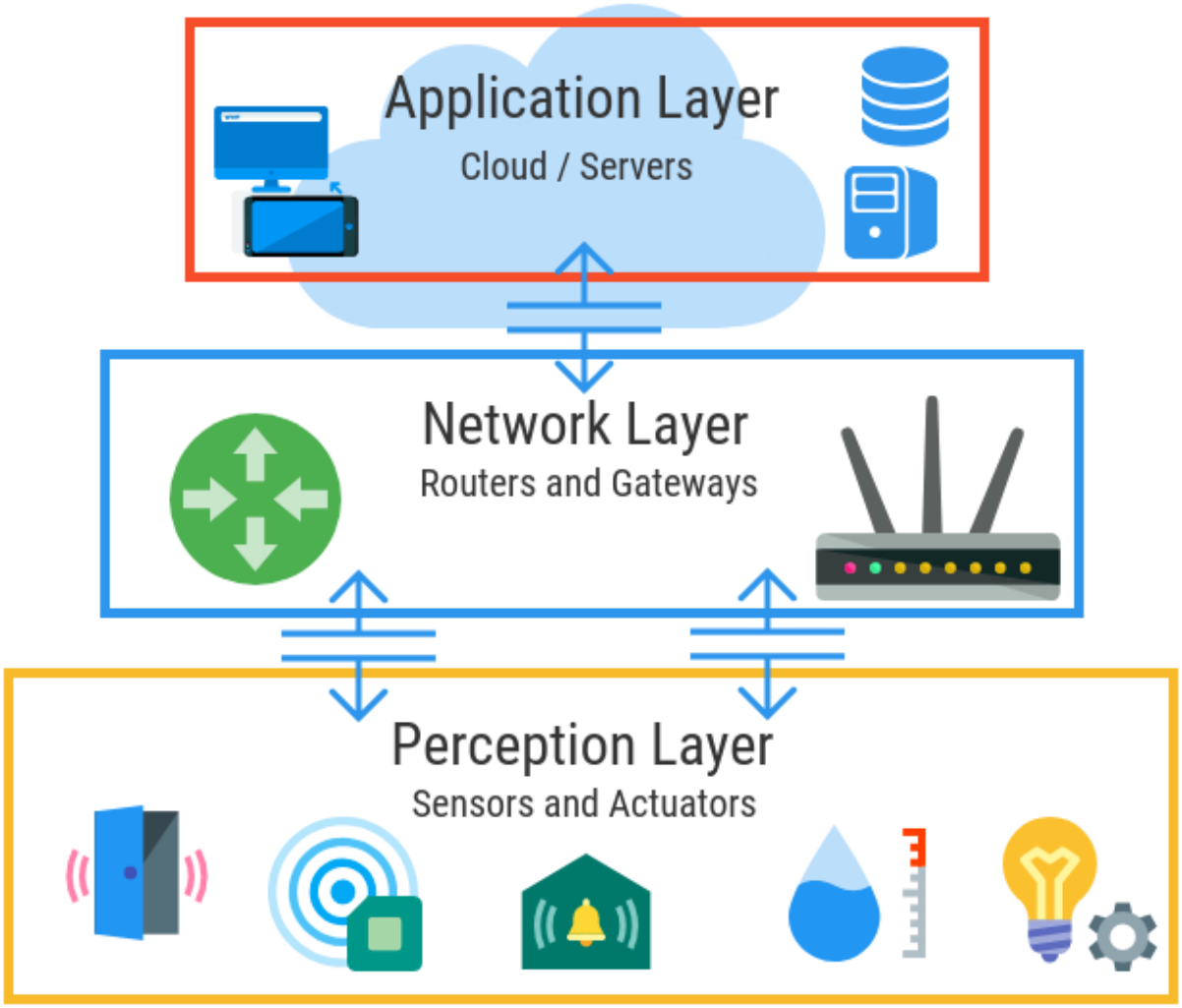

Figure 50: - Three-Layered Architecture [33]

3.4.3 Five Layered IoT Architecture

The three-layer architecture is the base of IoT. Researchers always focus on the deep aspect of IoT, so the five-layer architecture is defined.

The role of two layers (**Perception layer, Application layer)** is the same in 5-layered architecture as defined in 3-layered architecture. **The perception layer** is also renowned as **the Physical layer** here.

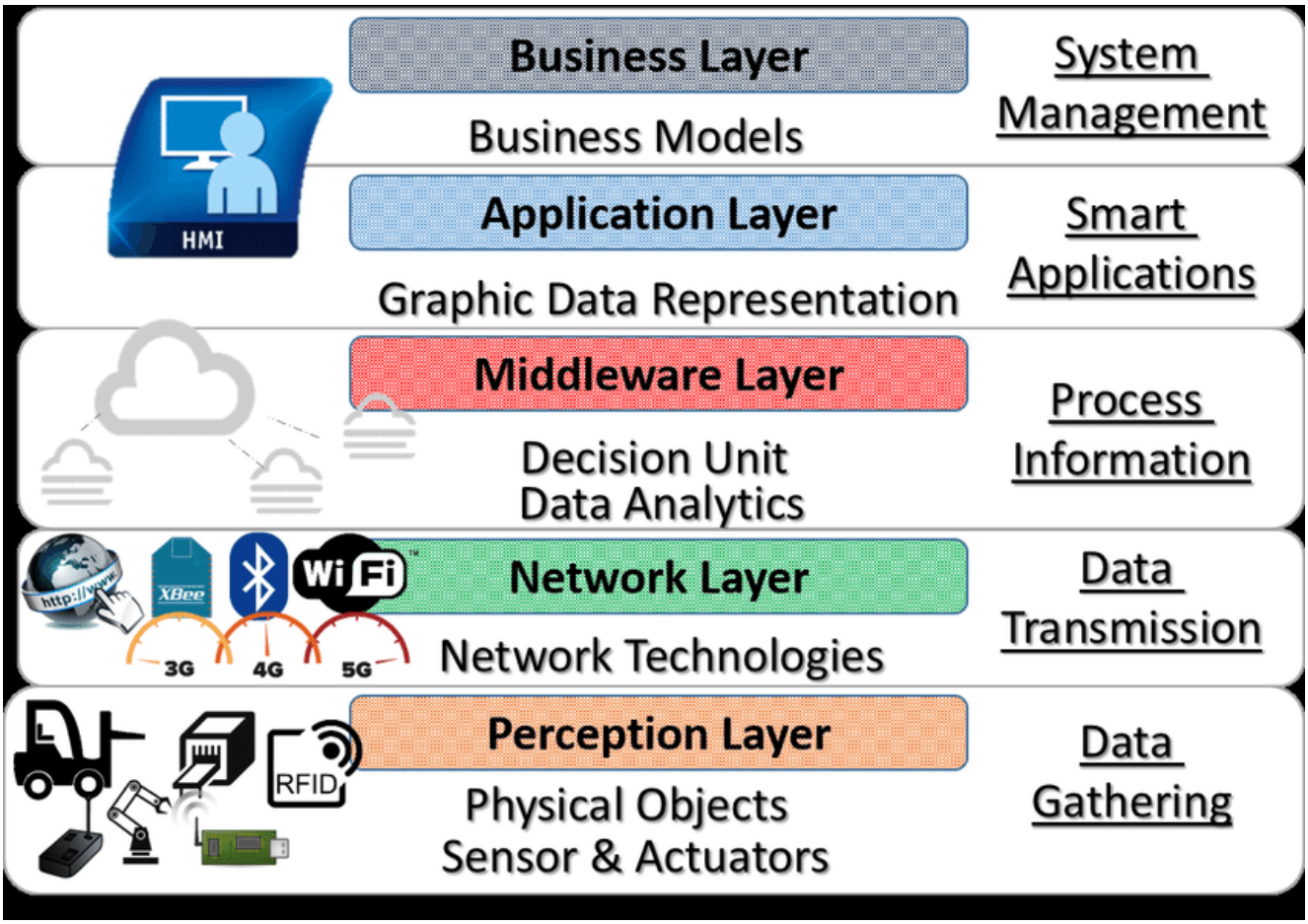

Figure 51: - Five-Layered Architecture [35]

The functions of the other three layers are defined as follows [34]: -

The network layer is also known as **the Transport layer** in this architecture and it transfers sensor data from the perception layer to the processing layer and vice versa via networks such as Bluetooth, wireless, 3G, LAN (Near Field Communications), NFC, and RFID.

The middleware layer is also recognized as **Processing Layer**. Large quantities of transportation data can be stored, analyzed, and processed by Middleware Layer. It manages and provides a variety of lower layers of services. It uses different technologies as processing modules like - databases, cloud computing, and big data.

Business Layer manages the entire IoT system. It manages applications, business, business models, and user privacy.

The following UML diagram in figure 52, shows the process of five-layered architecture.

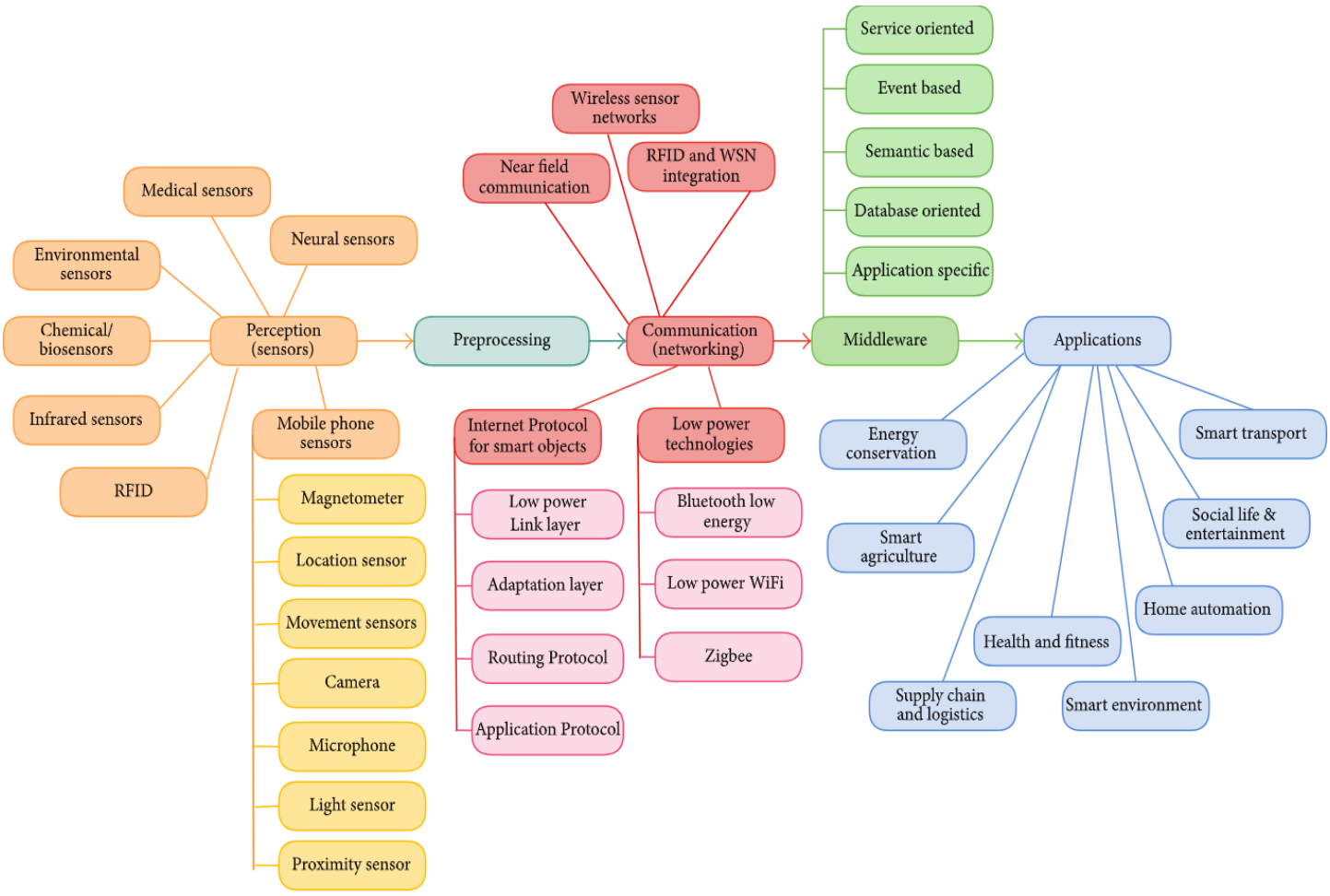

Figure 52: - Flow chart of 5-Layered Architecture *(Ref:* - https://static-01.hindawi.com/articles/jece/volume-2017/9324035/figures/9324035.fig.003.svgz*)*

3.4.4 NB-IoT

NB-IoT (Narrowband IoT) is an internationally acclaimed LPWAN based wireless communication standard. It is developed by 3GPP for devices that require low bandwidth and a small amount of data transfer. As a result, it includes features like: -

- Improved battery power
- Improved device density
- Enabling low complexity
- Enable low cost

Following figure 53 shows the enhancements in NB-IoT architecture in different releases of 3GPP.

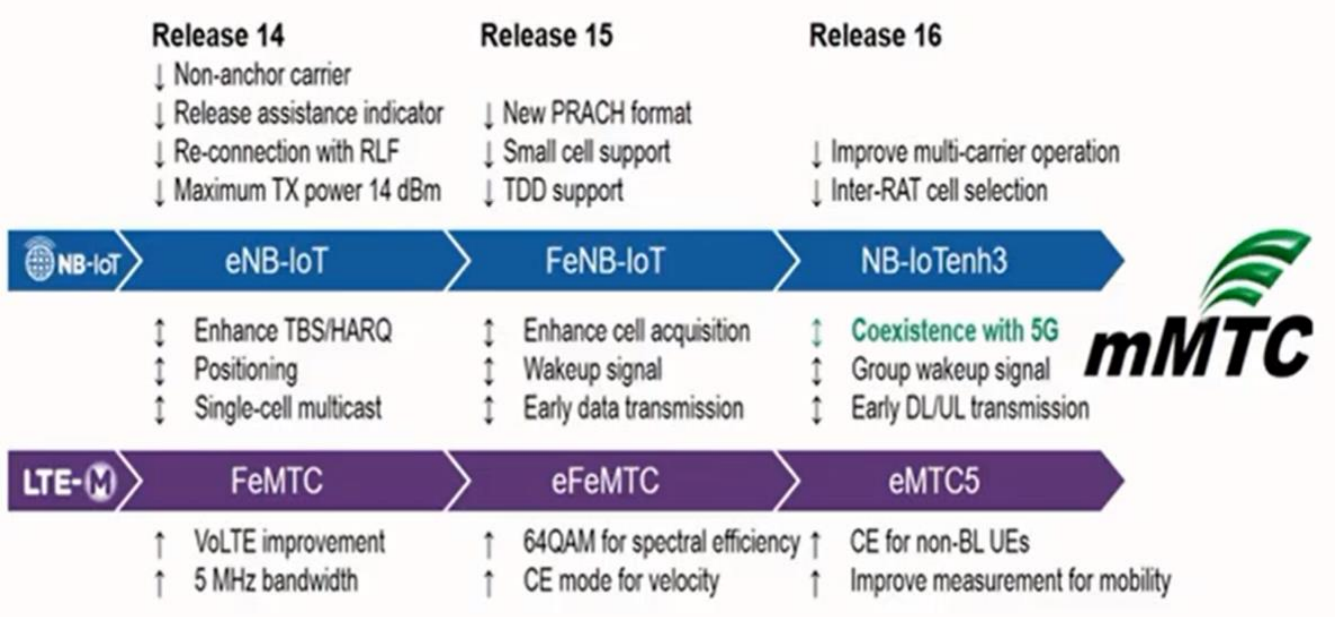

Figure 53: - Enhancements about NB-IoT & LTE-M in 3GPP [36]

3.5 SMART USE OF THE IOT

The following is the list [37] of major real-world use cases and applications of IoT.

3.5.1 Smart Home

Smart Home is an all-in-one solution that connects the activities of the home with IoT technology to develop a comprehensive, convenient, energy-efficient, comfortable and safe smart home system. It has become more user-friendly. As compared to a traditional system, smart home appliances may cheer up a little bit at first, but after some time, everyone loves to adopt the new system. Figure 54 and 55 shows the digital image of smartphone and the integration of smart home, IoT and cloud computing in advanced view of smart home respectively.

Internet and IoT technologies are used to attach various devices like: -

- Humidity and temperature regulation, light intensity, carbon dioxide monitoring
- Microclimate closed-loop control
- Elderly home care system (surveillance system)
- Visual management uses a touchscreen panel, able to remote access
- Professional aquarium system (temperature, flow rate, light intensity & timer, water change, etc.)
- Data collection for big data
- With multiple operating modes and parameter sets, the system runs fully automatic

Users can control devices like surveillance & security system, audio and video equipment, computer and communication equipment, kitchen appliances, alarm clock, and cleaning system remotely through mobile phones, tablets, and touchscreen panels. [39]

Figure 54: - Digital view of Smart Home [38]

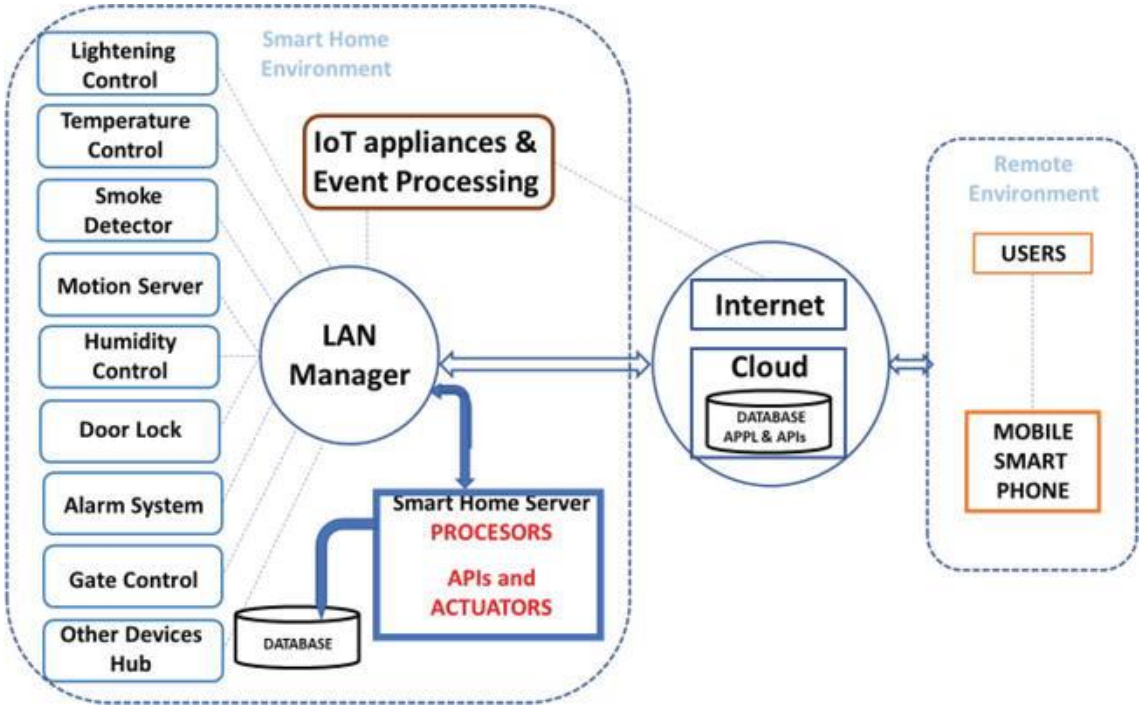

Figure 55: - Advanced Smart Home Architecture [40]

Smart home applications include smart power plug/light/gateway, weather/door/motion/vibration sensors, Intel switch, and smoke detector.

3.5.2 Wearables

In the IoT field, wearables first appeared in terms of **Bluetooth headsets** and more that can communicate with phones and computers of users. Today, the IoT wearables ecosystem is almost incomprehensible. IoT wearable technology at the workplace includes smart glasses, trackers, watch, phones, and shoes. Figure 56, depicts different wearable devices.

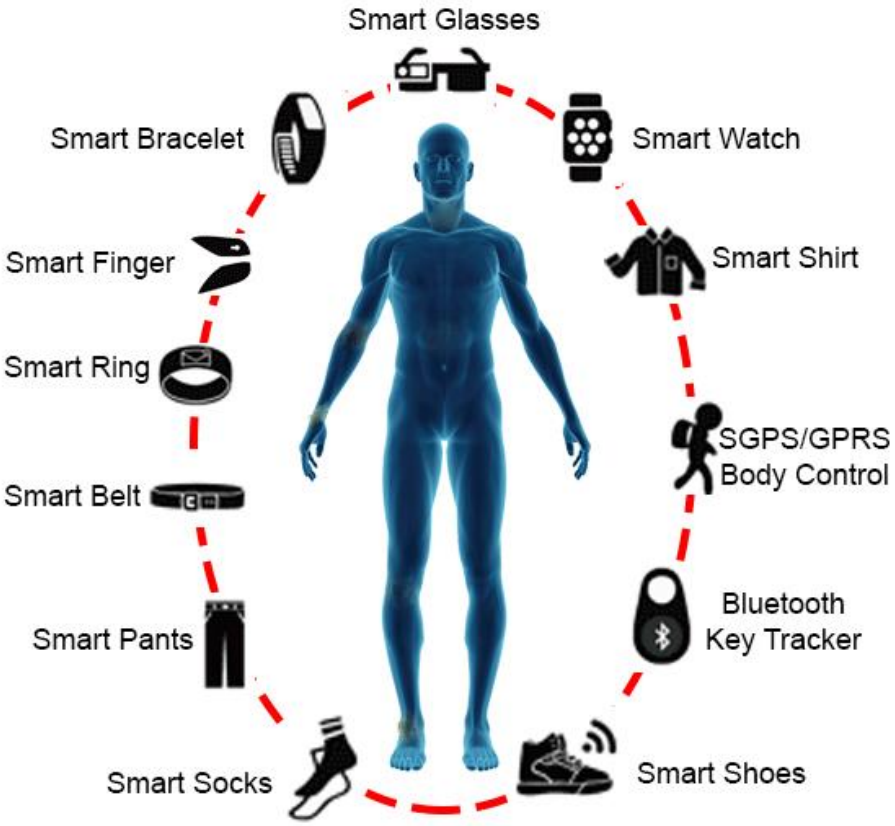

Figure 56: - Different Types of Wearable Technology [41]

The list of most popular wearable devices [42] includes Mojo Lens, Ōura Ring, Norm Glasses, Omron HeartGuide Watch, Welt Smart Belt Pro, Withings Move ECG Smartwatch, and Aō's Atōms Air Mask. Following Figure 57 illustrates the block diagram of the wearable system.

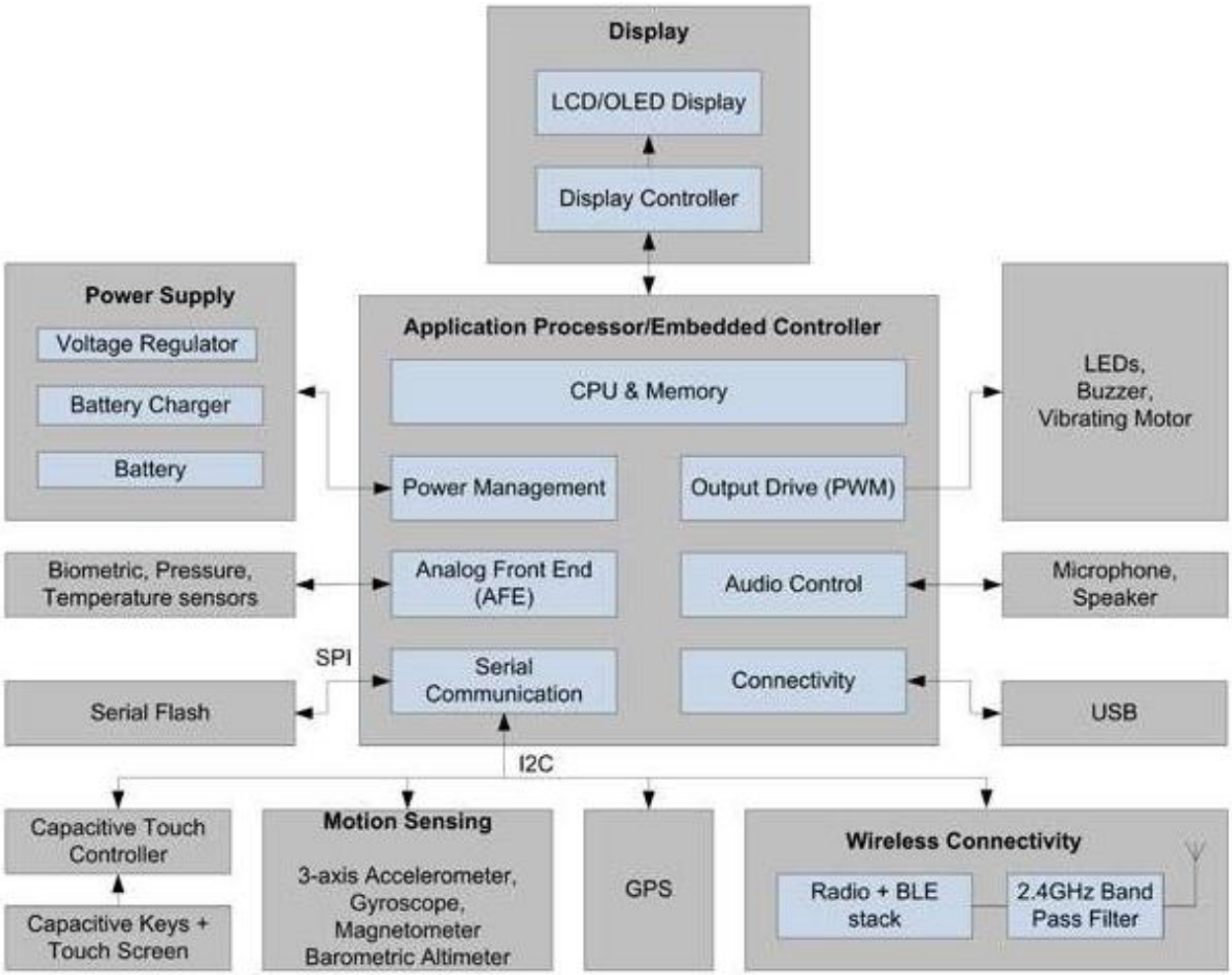

Figure 57: - Wearable electronic system's Block Diagram [43]

3.5.3 Connected Cars

A connected car is any motor vehicle, which is capable of connecting to the internet. The functionality of sharing internet access and data with other devices inside or outside of the car is possible using IoT in these types of vehicles [44]. Figure 58 shows the general working principle behind connected cars and the IoT.

There are the following features of connected cars: -

- Self-Driving Cars and Autonomous Vehicles
- Vehicle-to-Vehicle (V2V) Communications
- Vehicle-to-X (V2X) Communications
- Onboard Communications and Integrations
- Logistics and Fleet Management
- Edge Computing and Autonomous Vehicles
- Smart Public Transportation, Traffic, and Parking Management

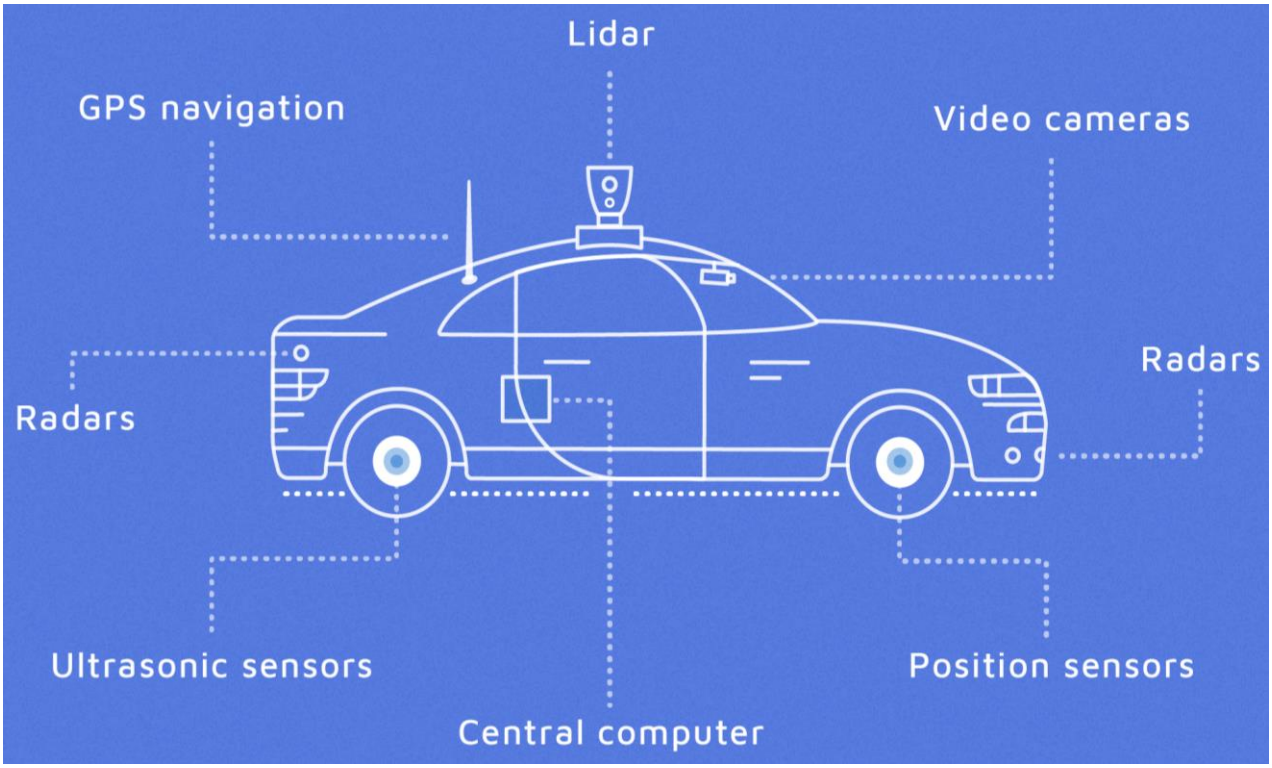

Figure 58: - Connected Car and IoT [45]

A real-time example: - An ambulance is connected to a hospital computer to send data on the exact physical condition (through IoT-enabled sensors and applications), not to mention the medical history of an emergency patient. The patient information can be transferred to the hospital before the ambulance arrives. It allows doctors and nurses to prepare all they need for personalized care in advance.
Major Functions/Advantages of Connected Car are: -

- Automatic roadside assistance
- Information calls to Telematics Service Providers (TSP)
- Stolen Vehicle Tracking (SVT)
- Remote Service (Vehicle on/off, vehicle lock/unlock)
- Vehicle Updates
- Video streaming / Web browsing

3.5.4 Industrial IoT

The Industrial Internet of Things (IIoT) is a rapidly growing field. It accounts for the majority of IoT expenses on the world market. In almost every sector, industrialists and producers have a tremendous opportunity not exclusively to monitor yet additionally to automate many complex manufacturing processes. Earlier industries and plants had sensors and systems to monitor progress, but now IoT is providing a solution to even minor problems. Following figure 59 describes the future of IIoT.

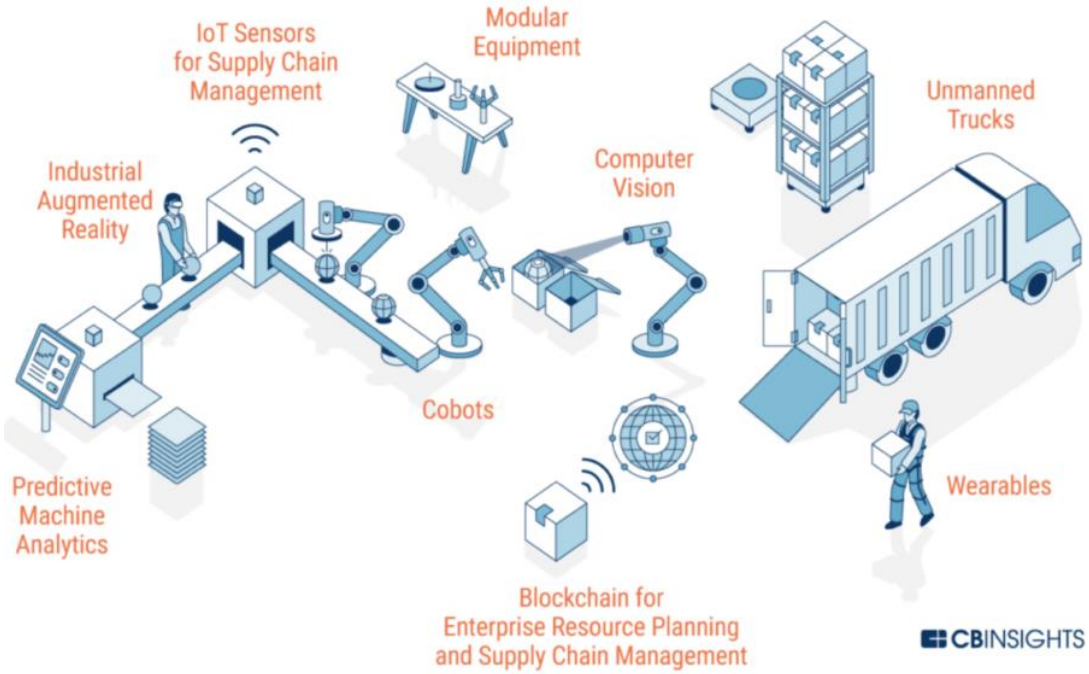

Figure 59: - Future of IIoT [46]

There are the following renowned feature of Industrial IoT applications: -

- Digital/Connected Factory
- Facility Management
- Production Flow Monitoring
- Inventory Management
- Plant Safety and Security
- Quality Control
- Packaging Optimization, and Logistics and Supply Chain Optimization

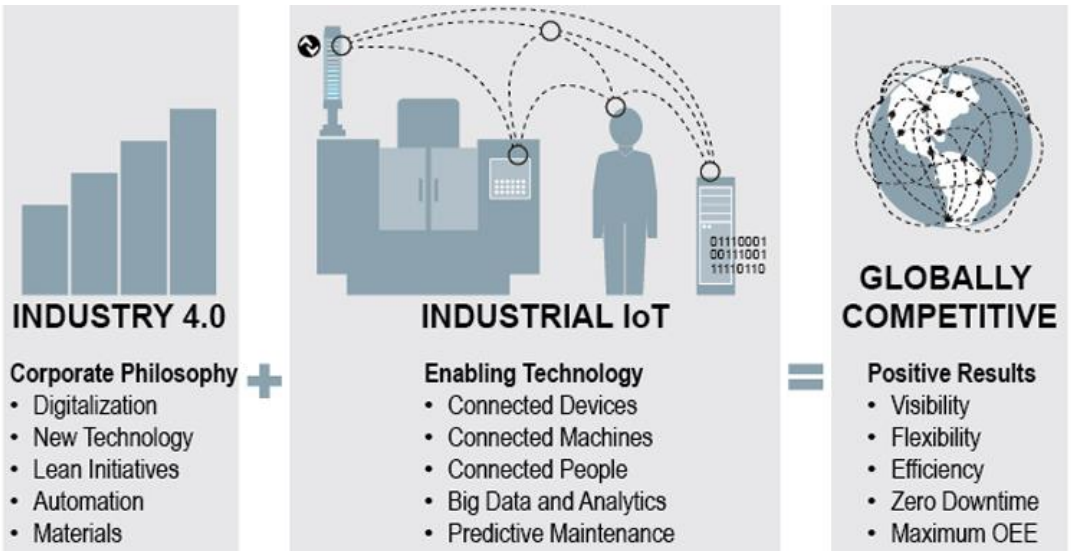

Figure 60: - Results of IoT in Industry [47]

Above figure 60, depicts the possible benefits of integrating industry 4.0 with industrial IoT, which will lead to a globally competitive industry area.

3.5.5 Smart Cities

IoT has the potential to solve the problem of urbanization pressures, create new experiences for urban residents, and make everybody's life more comfortable and safe. Figures 61 and 62 illustrate the smart city view and layered architecture of smart city respectively. Fully smart cities using IoT will include the following features: -

- Includes Road Traffic Control to determine the vehicle number, location, speed, and to a central traffic management platform in real-time.
- Smart parking to check parking spaces are occupied or available.
- Public Transport Control to improve the travel experience and to achieve a higher level of safety and timeliness.

Figure 61: - Smart City View [48]

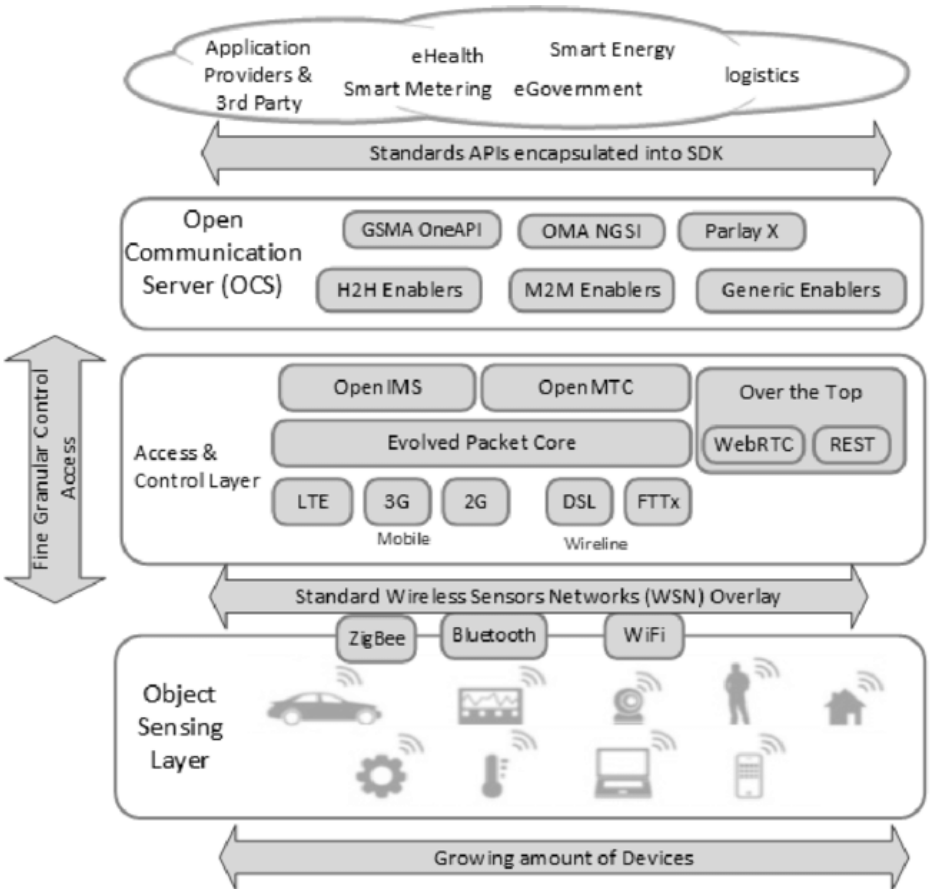

Figure 62: - Layer Architecture of Smart City [49]

- Control over their home utility, including approaches like Smart Meters and Billing and Remote Monitoring.
- Includes street lighting control to make it an easier and more cost-effective system.
- Waste Management to optimize waste collection by tracking waste levels, optimizing the route, and providing operational analytics.
- Environment control to optimum tracking of critical parameters for a healthy environment.
- Provide Public Safety using tools for monitoring, analysis, and decision-making in real-time to improve public security.

3.5.6 IoT in Agriculture

Smart farming using IoT-based applications helps farmers to reduce waste and increase productivity. A set of moveable systems to check the climate of agricultural areas using Android mobile applications and IoT has also been developed. Different mobile applications have also been developed for different purposes [50].

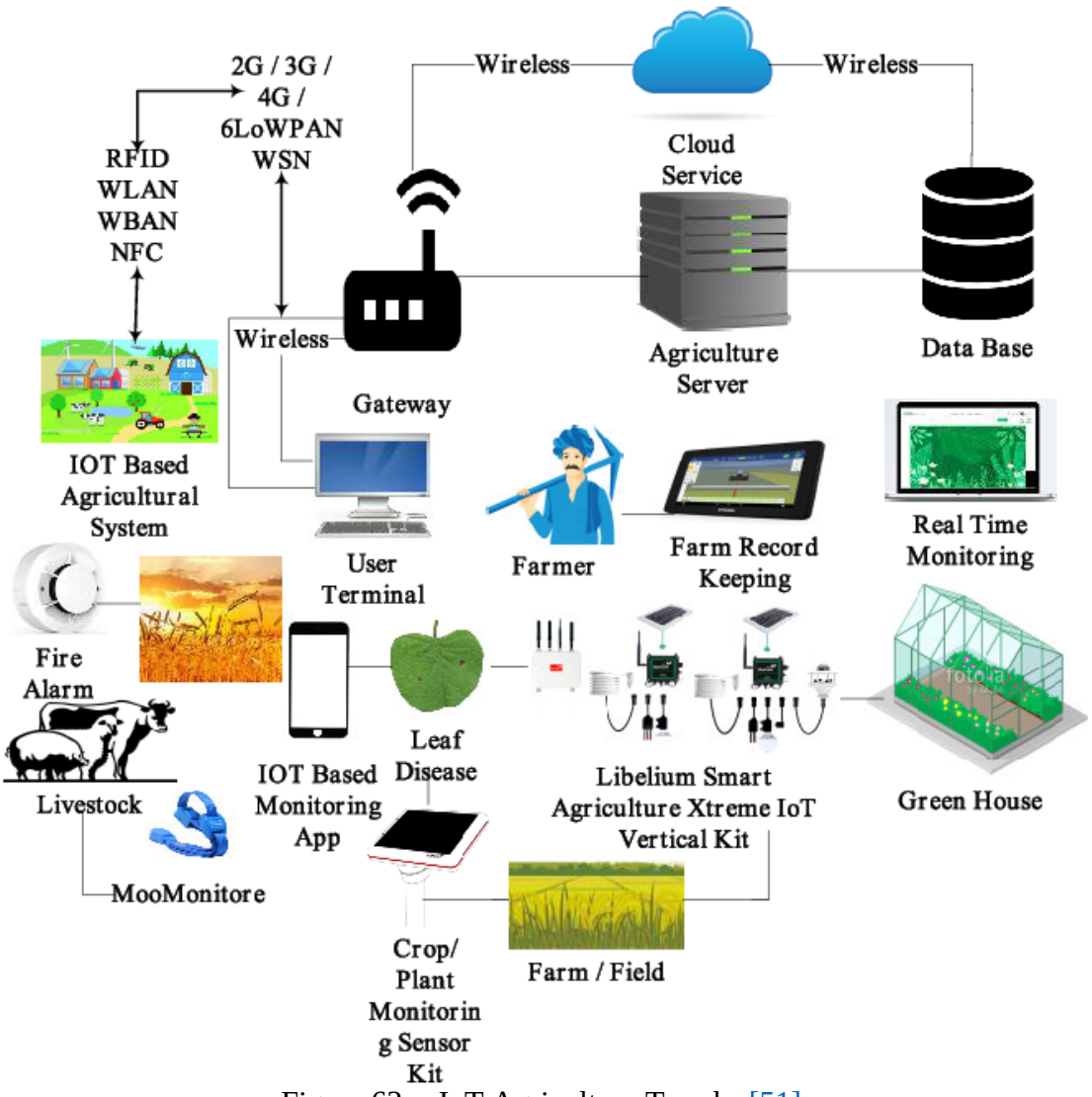

Figure 63: - IoT Agriculture Trends [51]

There are different categories of agriculture M-Apps listed as follows: -

- Agriculture Information Resource Apps
- Agriculture Calculator Apps
- Agriculture NEWS Apps and Weather Apps
- M-Government Apps

The major benefits of IoT in farming are listed below: -

- Livestock monitoring and Greenhouses automation
- Monitoring climate conditions and Crop monitoring
- Farm management systems and Monitoring through drones

3.5.7 IoT in Retail

IoT can transform the business relationship to essential utility use in a variety of ways. The main features of IoT in retail are as follows: -

- Day-to-day energetic engagement
- Intelligent analysis and planning
- Proactive and preventive maintenance
- Employee engagement and satisfaction

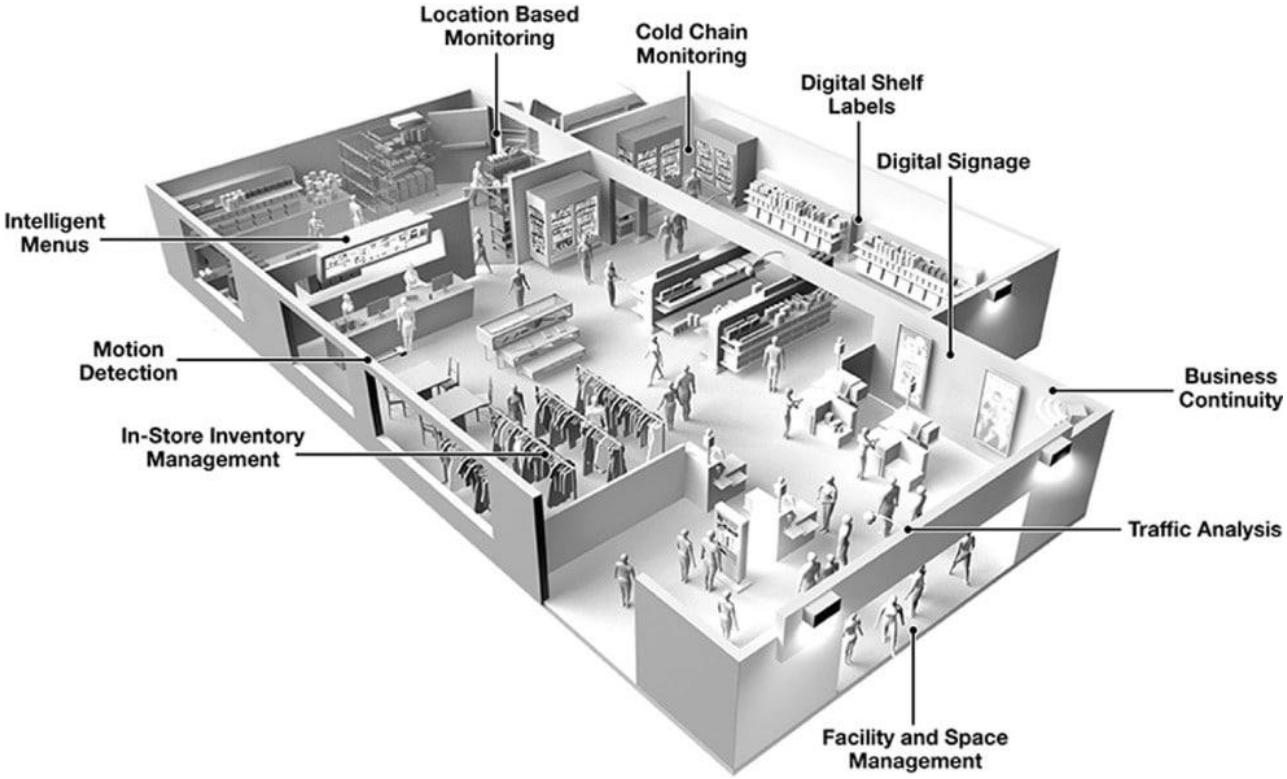

Figure 64: - Model of IoT in Retail [52]

Different IoT based applications for Retailing are being designed which will help follow factors: -

- **Automated Checkout**
- **Personalized Discounts**
- **Beacons** (small Bluetooth devices that send smartphones warnings based on location proximity)
- **Smart Shelves** (Intelligent shelves have weight sensors and use RFID tags and readers to scan both display and stock shelves for products)
- **In-store Layout Optimization** (the layout of a shop can be improved with IoT technology by using an infrared sensor)
- **Robot Employees**: - OSHbot, is the newest robot employee in Lowe. It helps customers in finding specific products and provides promotional and inventory information. It is a bilingual system and can answer questions in English or Spanish.

- **Optimizing Supply Chain Management** (Place temperature at which an item is stored or the length of time it spent in transit, this data used to improve the quality of transport)
- **Energy Engagement** (It assists businessmen to make up-to-date decisions about everything from energy procurement to everyday decisions)

3.5.8 Energy Engagement

IoT will greatly assist in saving energy. Smart grid based on IoT framework can increase usages of IoT smart devices like smart meters, sensors, and many actuators for different purposes like: -

- It includes the automation of devices, controlling, monitoring, and overall connectivity in the power grid.
- IoT-based smart grid systems upgrade many network-based activities at the main levels of power generation and transmitting side unanimously.
- The integration of IoT with energy will lead to embellishing functionality, energy, and cost-effectiveness.

Following table 4, describes the benefits of the smart grid in the IoT of an energy field.

Table 4: - Benefits of IoT enabled smart grid

Benefit	The technique works behind the benefit
Condition Monitoring Control	Asset Optimization
Demand response monitoring	VPP (Virtual Power Plant)
Monitoring of feeder	Fault management
Monitoring of voltage	Optimization of voltage
Substation monitoring	Balancing of load
Security and connectivity	

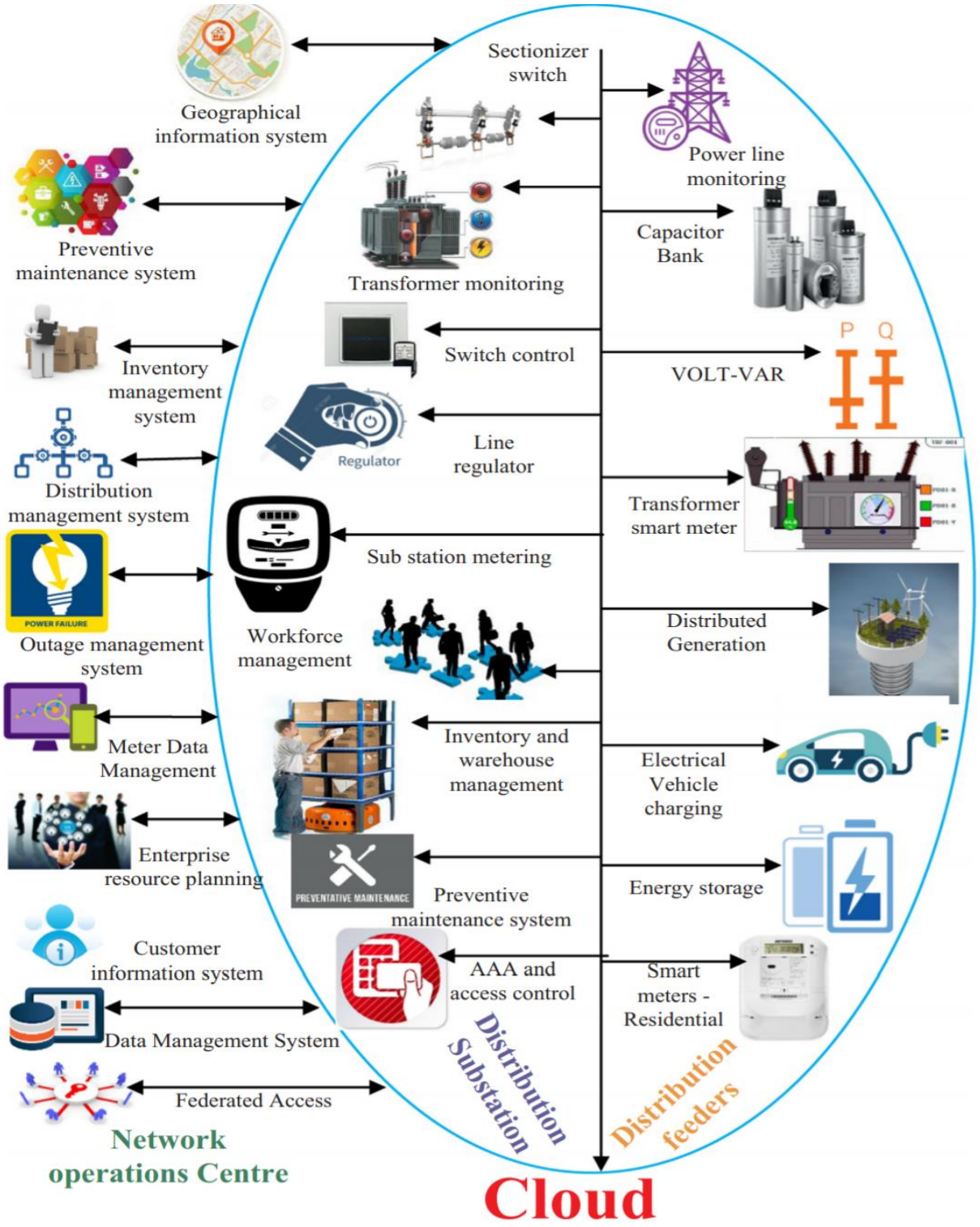

Figure 65: - Components of IoT enabled smart grid [53]

Above figure 65, depicts the components of IoT in energy which will lead to different IoT-based application areas like Smart meters, Smart charge devices, Agent switchers, Home controllers, Smart plugs.

3.5.9 IoT in Healthcare

IoT in health care is a popular field, where multiple applications have been developing for the last 2 years. Most applications are used for keeping fitness-related records and a growing number of records are available. IoT healthcare devices are mainly focused on the following factors: -

- Make healthcare faster, more personal-centered, and more affordable,
- Focused on the fitness of the affected person
- Assist health experts during their duty

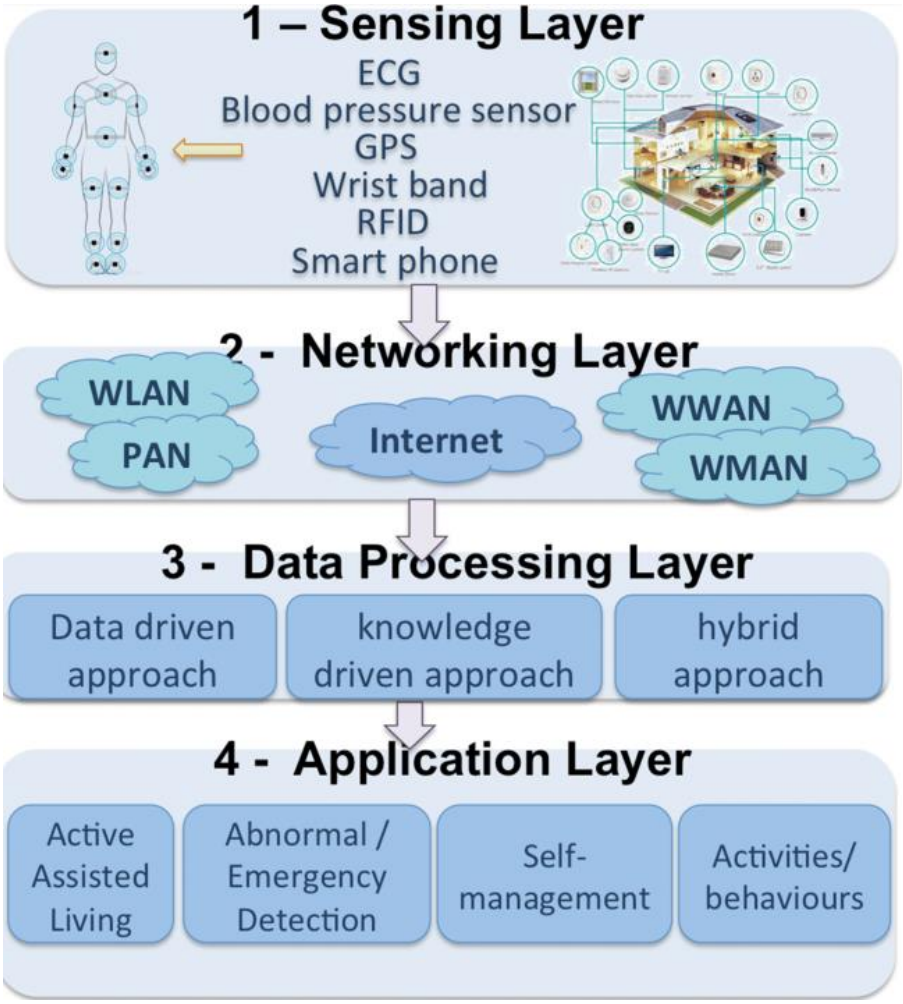

Figure 66: - IoT linked framework for Healthcare [54]

Internet of Medical Things in the field, where the healthcare system is integrated with IoT. Nowadays, healthcare using IoT is not limited to wearable devices, which are used to monitor the fitness of health, but it has been enhanced to find the solution to the physical presence of doctors while surgery as well. Above figure 66, depicted a framework for embedding IOT technologies to personalize healthcare. Recent applications of IoT healthcare are listed as follows: -

- Tracking Real-Time Location
- Monitoring Hand Hygiene
- Remote Health Monitoring
- Ambient and Specially abled people Assisted Living
- Assistance to Specially Abled People
- Remote/Robotic Surgery
- Smart labeling on drugs
- Screen hand sterility (RFID-labeled blood containers)

Figure 67: - IoMT Applications

A large number of projects developed by companies and the work of researchers clearly show the demand for IoT solutions in the field of health and fitness. Following table 5, elaborates the latest applications designed and developed by researchers in the field of healthcare.

Table 5: - Applications of IoT in Healthcare by Researchers

S. No.	Research Topic	Applications	Year	Ref.
1	Emergency Management	To monitor the transportation of preterm born babies including heart rate, saturation, breath rate, oxygen, temperature, diastolic pressure, systolic pressure	2016	[55]
2	Robot-Assisted Surgery based on Internet of Things (IoT)	Presents a controllable robotic arm	2017	[56]
3	Wearable IoT	Heartbeat, temperature, blood pressure can be checked using Sensors	2018	[54]
4	Telesurgery System for Healthcare	A Telesurgery System for Healthcare	2019	[57]
5	Tele Robotic Spinal Surgery	Robot-assisted spinal surgery	2020	[58]
6	Mobile Application for Specially Abled People	To assist specially-abled people through call, message, and facility to access other functions like date, time, and alarm in case of emergency	2020	[59]
7	Remote Healthcare Monitoring to Detect Cardiac Diseases	Cardiac disease remote healthcare monitoring	2021	[60]
8	Enabling Time-Critical Communications	Remote surgery setup scenario	2021	[61]
9	COVID-19 Pandemic	Treatment of COVID-19 patient, Smart Hospitals, Smart bed, Detection of an asthma attack, etc.	2021	[62]
10	IoT Based Healthcare	Different applications described including IoT Based Diabetes Management, IoT Devices for Asthma Management, IoT for Mental Health, IoT Role in Pandemic Situation, and IoT for Sleep Disorder	2021	[63]
11	Pregnancy Women- Smart Care	Measurement of heartbeat, temperature, and fetal movement by using blood pressure, temperature, heartbeat, and accelerometer sensors	2022	[64]
12	Advanced Applications in Healthcare	Electronically Controlled Nursing Bed, which is safely operated by the patient, auto sanitary management, auto sideways turning, room lighting control,	2022	[65]

		room curtain control, calling an attendant		
13	Wearable Technology and Visual Reality Application	EMG signals collect so that, the users can check their muscle conditions. Fig. In addition to EMG signals, the app could collect biomedical data including ECG, EEG, and blood oxygen	2022	[66]

Following table 6, elaborates the latest applications designed and developed by leading companies in the field of healthcare [67].

Table 6: - Applications of IoT in Healthcare by Renowned Companies

S. No.	Product Name	Benefit	Website's Link
1	QardioCore	ECG monitor	https://www.qardio.com/qardiocore-wearable-ecg-ekg-monitor-iphone/
2	Zanthion	Measure the health and welfare, If a patient falls out of bed, or remains motionless for too long, an alert is sent to the family.	https://zanthion.com/
3	ScreenCloud	With applications that are thinking far outside the box of traditional digital signage to improve patient welfare in hospitals	https://screencloud.com/
4	Up by Jawbone	Counting calories and steps, weight and sleep patterns to activity and diet	https://www.jawbone.com/
5	Sensor Metrix	Wireless sensors are used in hospital refrigerators, freezers, and laboratories to ensure that blood samples, medications, and other materials are kept at the proper temperature	https://www.siretta.com/products/
6	NHS testbeds	Connected beds being used in the UK's NHS system	https://www.england.nhs.uk/aac/what-we-do/how-can-the-aac-help-me/test-beds/
7	Swallowable sensors	Use to avoid colonoscopies by swallowing a sensor, the sensor can diagnose problems surrounding conditions like irritable bowel syndrome and	https://www.smh.com.au/national/gut-feeling-the-swallowable-gut-sensor-that-could-replace-a-colonoscopy-20170118-gttout.html

		colon cancer in place of more invasive surgeries	
8	Propeller's Breezhaler device	The management of asthma or COPD easier	https://propellerhealth.com/how-it-works/
9	Apple Watch	Major depressive disorder, allow tracking of moods outside of healthcare appointments	https://www.cambridgecognition.com/news/entry/takeda-cognition-kit-partner-pilot-wearables-patients-major-depression
10	Smart thermometer	Detect patient illness, provide analysis for better care, and map human illness through the collection of data	https://kinsahealth.com/shop

The top 10 Companies in the IoT Medical Devices Market by Revenue are listed below [68]: -

- Siemens AG
- Abbott Laboratories
- Honeywell Life Care Solutions
- Medtronic Plc
- Boston Scientific Corporation
- GE Healthcare
- Omron Corporation
- Biotronik
- Johnson & Johnson
- Philips Healthcare

4 EVOLVED SECURITY THREATS FOR HEALTHCARE IOT (IOMT)

Security can be defined as a method for protecting something from potential harm or any other unwanted coercive change. Harms can be caused by others through different means. Referents of security threats may include objects and institutions, ecosystems, persons and social groups, or anything else vulnerable to unwanted change [69].

Computer Security is also renowned as cybersecurity or IT security. It refers to the security of computing devices like laptops, computers, smartphones, computer networks, internet. It includes the protection of hardware, software, data, people, and also the procedures by which systems are accessed. Physical security and security of information are two concerns, which are solved by Cyber Security specialists with the help of physical and virtual security. [69]

IoT security includes the security of **computers** and **Electronics** on one platform. It refers to various methods of protection, which are used to secure internet-connected or network-based devices.

Network Security works on three core parameters known as CIA (Confidentiality, Integrity, and Availability)

- **Confidentiality:** - Only access by people who are authorized
- **Integrity:** - Information is true to what it should be
- **Availability: -** Information can be accessible when it needs to be

Security is based on triple-A: -

- **Authentication: -** It is used to check the validation of identity. It has three factors known what users know (user name/password), what users have (phone code, any token), and who are users (biometric/thumbprint/face recognition).
- **Authorization: -** It describes what users able to do after authentication are
- **Accounting: -** It defines what happened and what a user did after authentication and authorization.

**CIA and AAA mainly apply to data in transit.

There is another way to respond to security as follows: -

- **Step 1: -** Detect
- **Step 2: -** Prevent
- **Step 3: -** Analyze
- **Step 4: -** Respond

4.1 IoMT SECURITY OVERVIEW

Internet of Medical Things is a renowned field where the integration of healthcare and electronics, and computer industries is involved. Security is a crucial factor in IoMT because IoMT is directly connected to people, hospital staff, and life of patients. The information and data here are very sensitive. A single vulnerability can cause more danger. Hence, securing the connectivity of IoMT systems at all layers of its architecture must be on high priority because the modification, disclosure, or unavailability of any relevant information may be life-threatening. Following figure 68 depicts the characteristics and profiles of attackers and their corresponding impact.

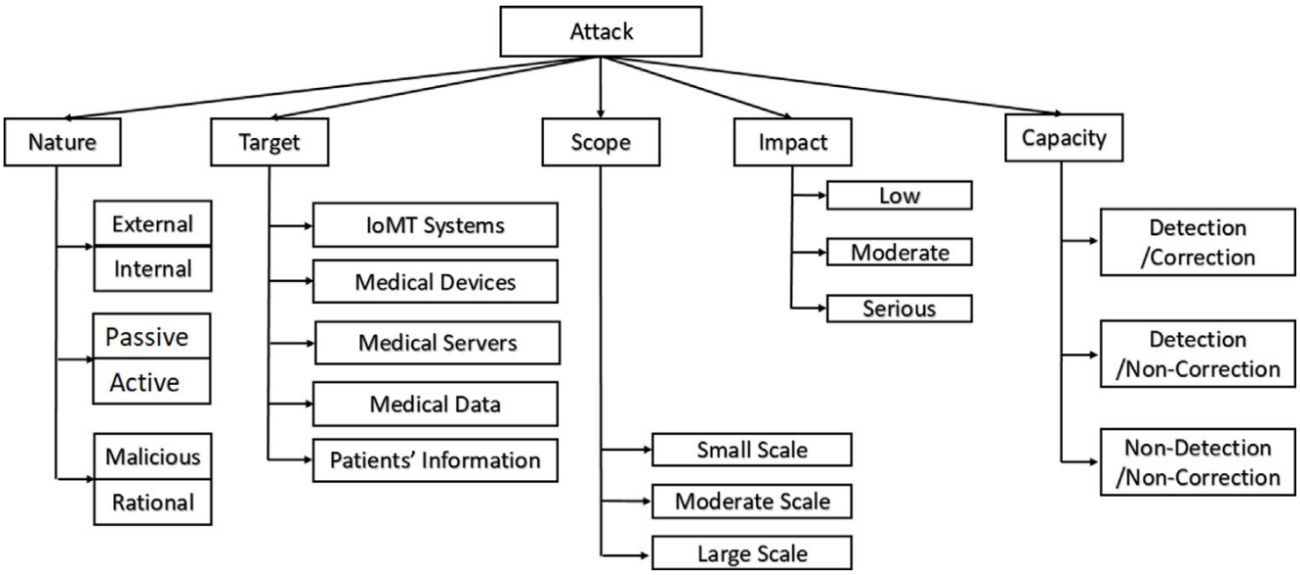

Figure 68: - IoMT attacks flow chart [70]

4.2 PROTOCOL/TECNOLOGY/STANDRADS BASED STUDY [71]

There are different protocols, standards, and technologies being used in different layers of IoT architecture. This section includes the IoT protocols, standards, and technologies used in medical devices.

4.2.1 IoT protocols/technologies/standards used in Context of IoMT

IoMT devices are a subsection of the IoT network. So, the communications of IoMT devices rely on IoT-specific protocols, standards, and technologies, but IoMT devices do not use all of them. The list of protocols, standards, and technologies are decided to describe as based on three-layered architecture, which is explained in section 3.4.2.

4.2.1.1 Perception Layer

Most protocols of the perception layer are based on or implement the **IEEE 802.15.4 standard**. IEEE 802.15.4 standard is used for providing different features like: -

- It provides ultra-low complexity.
- Provide cost and power consumption efficiency
- Focuses on cheap and low spectrum IoT devices
- Describes the specifications for various types of devices (fixed, portable, or moving devices), which reside on the physical (PHY) and the MAC (data-link) layers. Some devices have very limited battery consumption requirements and others even have no battery at all
- It supports physical layer operations in the following frequency bands: -

    - 868 MHz band (available in Europe)
    - 915 MHz band (available in the US)
    - 2.4 GHz ISM band (available globally)

- The physical layer has the following features: -

    - Data transfer and receipt
    - Energy detection of the current channel
    - Link quality
    - Clear channel assessment

- The MAC layer has the following features: -

    - Joining PAN
    - Leaving PAN
    - Use CSMA-CA for channel access
    - Guaranteed Time Slot (GTS) transmissions
    - Link establishment between peer MAC entities is reliable
    - Controlling beacon transmissions for a coordinator
    - Ensuring synchronization to the beacons

- Various network layer's IoMT related protocols are also compatible with IEEE 802.15.4, such as ZigBee, LowPan, and ISA 100.11a.

The list of perception layer protocols (used by healthcare systems to gather clinical information from the sensors) is described as below: -

4.2.1.1.1 Infrared

Infrared technology was proposed by the Infrared Data Association (IrDA). Some features of Infrared technology are: -

- It uses infrared light for short-range communication.
- The IrDA protocol stack is comprised of the following three layers: -

    - **Physical Protocol**
    - **Infrared Link access protocol (IrLAP): -** (Provides basic link-layer connection between pairs of devices, Device discovery processes)
      It is based on the **HDLC standard for connection establishment and data transfer
    - **Infrared Link management protocol (IrLMP): -** (Tell multiple entities within pairs of IrDA devices how to use the single IrLAP connection simultaneously and independently. Allows service discovery by pairing entities)

Uses of infrared in the **healthcare system** are as follows: -

- Ir is used in **temperature sensors, thermometers, and cameras**.
- **Thermal imaging technology** is also based on infrared and it is used to take images of a body and find its local temperature as well.

4.2.1.1.2 RFID

RFID is a wireless **object identification technology**. It uses radio frequency signals for very short-range communications. There are two main entities in RFID communications: -

- A reading device (**RFID reader**): - It stores data and has remote distance reading features.
- Radio transponder device (**RF tag**): - It first receives a message from the reading device and after that, respond by sending some identification information back to the reader, Where unique serial number = identification information and additional information may be product-related, such as stock or batch number, production date, etc.

Two main technologies in RFID tags are used:

- **Active reading tags: -** These tags are power-driven, high-frequency bands, and relatively high-priced.
- **Passive reading tags: -** It operates on lower frequencies and does not have an internal power source.

The following frequency ranges are usually operated in RF communications: -

- Low Frequency (LF, 125 kHz)
- High Frequency (HF, 13.56 MHz)
- Ultra-High Frequency (UHF, 433 MHz, 860–960 MHz)
- Microwave (2.45 GHz, 5.8 GHz)

The uses of RFID in the **healthcare system** is as follows: -

- **Autonomous RFID tags** are placed inside or close to a patient's body. These tags are used **to develop body area healthcare systems**. This technology is fully transparent to the patient.
- **Passive RFID tags** are used for the ambient monitoring of patients' environments. Modification in physical or chemical parameters is also detected by using passive RFID tags.
- It is used for physical access control.
- A combination of RFID tags and sensors is used to provide: -
  - Temperature monitoring for drug storage
  - Regulation for a suitable temperature for each type of drug accordingly [72].

4.2.1.1.3 NFC

NFC protocol supports very short-range communication among devices. It is standardized in **ECMA-340 and ISO/IEC 18092**. Major features of NFC are as follow: -

- Its **short-range** (few centimeters at most) and **high frequency** (13.56 MHz) technology allow data transfer rates up to 424 Kbps.
- It operates in: -
  - **Passive mode: -** where one device is active and generates an RF field
  - **Active mode: -** The passive target device is woken up by using the energy generated by the active one.
- NFC is used for easy and low-cost connections among IoT devices.

The uses of NFC in the **healthcare system** is as follows: -

- Mostly, NFC is used for **authentication purposes**. For instance, it checks whether an IoT device is registered in an authentication server and whether the user is registered in the server. It helps hospital staff to differentiate between authenticated and unauthenticated devices.
- NFC signals use for **medical devices (ingestible or implantable sensors**) inside a human body as well.
- NFC-enabled medical objects **do not necessarily require a battery.** In other words, it does not require external electrical connections for its custom operation. So these are known as energy-efficient devices.

4.2.1.1.4 Bluetooth/ BLE

Bluetooth is widespread wireless communication technology. BLE is based on the **IEEE 802.15.1 standard**. Renowned features of Bluetooth are: -

- Suitable for low-power, low-cost devices and used for data transmission between mobile devices over a short-range
- Operates at the 2.4 GHz band
- Support star topology-based PAN with lower power consumption, low setup time, an unlimited number of nodes.
- Bluetooth's version 2.1 supports a maximum indoor range of up to 100 m, while version 5 (BLE), supports a range up to 400 m. Its ultra-low power version is known as Bluetooth Low Energy (BLE) or Bluetooth Smart.
- Bluetooth's data rate in various versions is ranged up to 2 Mbps.

Uses of BLE in the **healthcare system** is as follows: -

- It is used for IoMT applications that necessitate short distance communication for instance: -
    - low latency and low bandwidth targeting applications
    - Human Interface Devices (HID)
    - Sports monitors
    - Fitness monitors
    - portable medical devices

4.2.1.1.5 Z-Wave

Z-wave is developed by Zensys and it is known as a **low-power wireless MAC protocol**. Some features of Z-Wave are: -

- Mesh topology networks can be set up through Z-Wave
- Supports controlling and slave devices
- It may host up to 232 nodes and cover distances up to 32 m using P2P communications
- Operates at 900 MHz
- Supports a data transmission rate of 40 kbps
- It is suitable to support short messaging among IoT devices and not suitable (due to low bandwidth & half-duplex protocol) for transferring a larger amount of data

Uses of Z-Wave in the **healthcare system** is as follows: -

- Support short messaging among IoT devices utilized for light, energy, and healthcare control.
- Used in wireless healthcare areas to connect 30–50 nodes.
- For IoT communications, it is used in hospitals' smart locks, smart wearables, and smart sensor control.

4.2.1.1.6 UWB

UWB developed over the **IEEE 802.15.3 standard**. It supports high-speed and short-range indoor wireless communications. Major features of UWB are as follow: -

- UWB's data rate vary from 110 up to 480 Mbps.
- Suitable for different applications of higher demand, like audio or video home networking applications.
- Because of high bandwidth, UWB act as a wireless cable replacement as well, particularly for the high-speed serial buses such as USB 2.0 and IEEE 1394.
- It transmits information by creating radio energy at specific time intervals and occupying a large bandwidth, thus enabling time or pulse-position modulation.
- It consumes low power and has high precision
- Used to transmit signals from sensors to a microcontroller

The uses of UWB in the **healthcare system** is as follows: -

- UWB is suitable for real-time applications in RF-sensitive environments, like hospitals.
- When communicating with an implanted sensor in hospitals, requires a protocol that transcends channel limitations. In this case, UWB works very well.

4.2.1.2 Network Layer

The network layer of IoT architecture includes various hardware devices like gateways, routers, and access points. It deals with Internet Protocol (IP) addressing (Subnetting) and other network capabilities. Most of the protocols of the network layer are based on the **IEEE 802.15 standard**. The list of protocols used in medical systems is as below: -

4.2.1.2.1 Wi-Fi

Wi-Fi is a well-known protocol. It follows the **IEEE 802.11** family of standards but nowadays, the most common Wi-Fi standard used is **802.11n**, which may support a throughput rate of hundreds of Mbps. It makes it suitable for file transfer. Renowned features of Wi-Fi are: -

- It is a middle range (up to 100 m) protocol
- It is widely used for handheld devices
- Used for local area networks to support Internet access for multiple devices
- Due to high power consumption and significant frame overhead, it is not always suitable for IoT applications, but IEEE 802.11 working group initiated the **802.11ah** task group, for developing a standard that is friendlier to devices with low-power consumption and low frame overhead needs, such as sensors and motes.
- For IoT compatibility, the Wi-Fi alliance (www.WiFi.org) proposed **Wi-Fi HaLow**. Major characteristics of Wi-Fi HaLow are: -

    - Operates in the spectrum below the one GHz

- Based on IEEE 802.11ah standard
- The range of WiFi HaLow is longer than many other IoT-compatible technology options.
- Delivers a more vigorous connection in indoor environments, especially in cases of penetrating walls and another barrier.
- Enables low power connectivity.

The uses of Wi-Fi in the **healthcare system** is as follows: -

- Wi-Fi can be used for the communication of the monitoring devices in an IoMT system
- If there is a network of various critical medical care devices, including infusion pumps, defibrillators, lung ventilators, and anesthesia machines, Wi-Fi will effectively and securely apply for the communication of these devices.

4.2.1.2.2 ZigBee

ZigBee is known as Zonal Intercommunication Global-Standard. It is based on **IEEE 802.15.4** standard. It has the following features: -

- ZigBee is a low-cost, low-speed, and low-power, wireless communication protocol
- Its transmission range is up to 100 m
- Supports data rate between 40 and 250 Kbps.
- It is specially crafted for PAN at the 915/2.4 MHz frequencies
- Supports different network topologies like star, tree, and mesh
- It can accept up to 65,000 nodes in a network.

The uses of ZigBee in the **healthcare system** is as follows: -

- It is extensively used in healthcare areas to connect sensors with the coordinator
- Used for the connection among the coordinators themselves as well
- In 2009, **ZigBee Health Care's** public application profile was introduced by ZigBee Alliance. It was designed for use by assistive devices operating in non-invasive health care.

4.2.1.2.3 WIA-PA

WIA-PA is based on the **Chinese industrial wireless communication standard** for process automation. Some of the features of WIA-PA are: -

- It is designed for measuring, monitoring, and open-loop controlling of production processes
- It is used in industrial-based systems

Uses of WIA-PA in the **healthcare system** is as follows: -

- In the medical field, WIA-PA is used in a remote monitoring system as a transmission protocol in the wireless sensor network.

4.2.1.2.4 6LoWPAN

6LoWPAN is developed by the **Internet Engineering Task Force** (IETF). Major characteristics of this protocol are: -

- It is a wireless protocol with low bandwidth
- It has limited packet size and varying address length
- It is mainly used for allowing IoT devices to join IP networks
- Supports the transmission of typical IPv6 packets

Uses of 6LoWPAN in the **healthcare system** are as follows: -

- 6LoWPAN helps in connecting IoMT sensors and local devices to IP networks
- It allows the interconnection among a group of sensors
- It also allows the interconnection of sensors with middleware devices or Internet-connected routers

4.2.1.2.5 LoRaWAN

LoRaWAN works with LoRa, which is a physical layer protocol, it is originally developed by Semtech. Features of LoRa are: -

- It supports low-power and wide area networks
- Uses license-free frequencies that vary in different geographic areas like: -
    - 868 MHz in Europe
    - 915 MHz in North America and Australia
    - 923 MHz in Asia
- It may support long-range and low-power transmissions (may exceed 10 km)
- Lora defines the physical layer, so to support it, a MAC layer protocol (LoRaWAN) is used

Features of LoRaWAN are as follows: -

- LoRaWAN mainly acts as a network layer protocol
- Manages the routing between gateways and end devices
- Manages the communication between gateways and end devices
- LoRaWAN focuses on WAN applications
- Supports low-cost and bidirectional communication
- Data rates of LoRaWAN range from 0.3 kbps up to 50 kbps

- Supports secure communication

The uses of LoRaWAN in the **healthcare system** is as follows: -

- LoRaWAN infrastructure can be used in a loT-based health monitoring system in which medical data is collected by sensors.
- It is used to transmit the collected data to a remote analysis module in a secure way.
- LoRaWAN based system mainly focuses on monitoring glucose, blood pressure, and temperature of patients residing in rural areas.
- An IoMT biofluid analyzer has been proposed by Phillip et al. [73]. It uses LoRa and Bluetooth to support long-range data transmission. It is a smartphone application to create a community-based healthcare examination platform for urinary tract infections.

4.2.1.3 Application Layer

The Application Layer is an interface between medical-specific software applications and end devices. Previous layers send information to medical-specific software applications. The application layer transfers this information into a processed form that can be understandable by the end devices and medical servers. The list of general-purpose application layer protocols, which are used in healthcare systems are listed as below: -

4.2.1.3.1 HL7

HL7 is a set of standards known as **medical data encoding protocol**. It is recognized as the most commonly used medical-specific application layer protocol. Features of HL7 are listed as below: -

- It allows the exchange, integration, sharing, and retrieval of electronic health information between different health entities.
- Helps in the establishment of flexible and effective processes
- Ensures the information exchanged between health systems is transparent.
- It defines the packaging and transmission details of the information swapped amongst various systems.
- HL7 supports clinical practice
- It manages the delivery and evaluation of health services.
- HL7 supports medical data standardization
- It enhances the collection of measured data from standard and nonstandard medical devices.

4.2.1.3.2 COAP

COAP is a web transfer protocol and standardization by the IETF. It is suited to IoT-constrained nodes with limited memory and processing power. Renowned features of COAP are as follows: -

- Used in power-constrained and lossy networks.
- COAP is designed to enable IoT systems to use RESTful services

- It is built over the UDP
- It uses the REST architectural style using its protocol which is much lighter than the typical HTTP protocol.
- It supports unicast and multicast both
- COAP can be used as an application layer protocol for a remote monitoring system in combination with ZigBee, 6LowPAN, and WiFi, at the other three layers.

4.2.1.3.3 MQTT

MQTT is an asynchronous publish/subscribe messaging protocol developed by IBM. Its main goal is to support lightweight M2M communications. Features of MQTT are listed as follows: -

- It operates at the application on top of the TCP stack.
- It allows applications/users to exchange data through networks.
- Provides bandwidth and power consumption efficiency
- Blockchain-based medical applications may use MQTT to connect various devices to an IoMT platform.
- In the IoMT scenario, MQTT may be used as the application layer protocol for the communication between the cloud and an end-user

4.2.1.3.4 HTTP

Mostly HTTP is used at the application layer of IoMT. Many researchers described in paper [71] used HTTP for IoMT scenarios. The list of different scenarios is as follows: -

- HTTP is used for the transmission between the cloud and the doctor in a simple IoMT scenario.
- HTTP is used in a system with a wearable thermometer and a thermopile infrared sensor where a microcontroller board processes signals. After that, data is sent through a Wi-Fi module to the cloud for storage via HTTP
- HTTP has been used in a system that includes a wearable medical module, which is equipped with a pulse oximeter and accelerometer.

** Wireless communication technologies (such as GPRS or 3/4/5 G) can be used for remote data transfer and communication. HTTP can be protected by applying HTTPS using the TLS protocol.

4.2.2 Possible vulnerabilities & Attacks

There is a need to consider some prominent security controls during the design and development phase of the most common protocols used in IoMT. Security issues and attacks in all IoMT protocols (described in section 4.2.1) are explained in this section as per the 3-layered architecture of IoT.

4.2.2.1 Perception Layer Security Issues &Attacks

The possible security issues and attacks in different protocols of the perception layer are described as below: -

Infrared

Security Issue/s: -

- There are no embedded security controls available in IR
- IR technologies are directed beams. It works in very close proximity only.

Possible Attack/s: -

- Attackers can intercept the IR beam to read data sent between the transmitter and the receiver.
- If an attacker is very close to the IR device and is equipped with the appropriate material, the threat can occur. For instance: - snoop on data transmitted by intercepting the reflected infrared light and filtering out the surrounding ambient noise.

RFID

Security Issue/s: -

- Embedded data are unprotected and read-only. RFID implements no protection or authentication controls by default against tag scanning.
- There are some security mechanisms available in RFID for symmetric key encryption, but active (continuously transmitting) and passive (electromagnetic field) RFID systems have several weaknesses.

Possible Attack/s: -

- Insecure embedded data open a door for attackers to attack the tag data, confidentiality attacks against devices/equipment/medical data, unauthorized cloning of tags, unauthorized tag tracking, replay attacks, and DoS attacks.
- Studies have shown that intended interference may cause RFID systems to fail and directly impact the physical safety of a patient. For instance, by switching equipment off or by inducing service disruptions.

NFC

Shared Channel (SCH) and Shared Secret (SSE) security services are present in NFC through its security protocol, which is standardized in ECMA-385. SSE uses key exchange, key derivation, and confirmation, whereas SCH uses data encryption and data integrity checks. SCH and SSE both use the Advanced Encryption Standard (AES) algorithm with a 128-bit key. ECMA-386 defines the cryptographic mechanisms in SSE and SCH services.

Security Issue/s: -

- NFC utilizes three modes of operation: -

    - Read/Write
    - Peer-to-Peer
    - Card Emulation Mode

  Each mode utilizes different protocols and thus is prone to different security vulnerabilities.

- NFC regulates RF to allow for data exchange between two devices nearby and standards of NFC provide no stringent security measures against proximity attacks.

Possible Attack/s: -

- Man-In-the-Middle attacks using simple antennas can cause breaches of data confidentiality or corrupt signals, resulting in integrity or Denial-of-Service attacks. Bit manipulation in particular types of NFC card modulation is also possible.
- NFC MITM attack variations involving the PICC was read or written by a proximity reader
- It is based on the ISO14443 standard that can be happened using PICC.

Bluetooth/BLE

BLE can operate under four diverse security modes. Mode 4 is known as the strongest mode. It uses SSP for service-level security. Authentication of the BLE device is performed before connection establishment and utilizes stream cipher encryption.

Security Issue/s: -

- Bluetooth encryption only encrypts the payload (by default), but not the entire packet. Many medical devices implement BLE without changing default settings. These use specific channels for similar services (like device model verification and service listing).
- Every BLE device chip is assigned a unique identifier. Still, methods to bypass this restriction and alter multiple device information exists.
- Matching the Bluetooth connection's frequency hops is possible.

Possible Attack/s: -

- Implementation of the same interface type and specific channels for similar services can be exploited by attackers.
- Device addresses are possible to change on certain chips by using firmware modification, for instance, by using the Bdaddr app. Moreover, the device name and class can also be modified through software injection with the use of the Hciconfig software.
- Matching the Bluetooth connection's frequency hops leads to capturing data in that frequency range. In this case, sniffing and capturing of Bluetooth packets is possible for MITM confidentiality attacks.
- Other known Bluetooth attacks can: -

    - Misuse the ability to brute-force Bluetooth PINs from pairing process packets
    - Jam signals and create DoS on services
    - Send unwanted messages to enabled devices (BlueJacking attacks)

Z-Wave

AES encryption with three shared keys is present in Z-Wave.

Security Issue/s: -

- It does not apply a standard key exchange protocol
- Z-Wave devices indirectly trust the source and the destination fields of the MPDU aggregation frame

Possible Attack/s: -

- **Key Reset** is possible, and protocol can be exploited by attackers.
- Implicitly trust leads to **impersonation attacks** where fake device sources by spoofing the frames originating from the controller or another device (**node spoofing**).
- If malicious nodes are assigned by the hacker to be part of a path between two devices, **Black Hole** (involve intermediary nodes that silently drop application frames when it is expected to forward them) attacks can take place.

UWB

LRP/HRP secure-ranging schemes used in UWB for security purposes. To mitigate some positioning attacks size of the UWB symbol has been embedded.

Security Issue/s: -

- UWB is a distance-based protocol, and there is a long symbol length present.
- Numerous events like power failure or wrong access control configuration may result in vulnerability to the Access control list.

Possible Attack/s: -

- The distance-based protocol is vulnerable to physical layer attacks, like the early detection and late commit (ED/LC) attack.
- The related attack is known as Same-Nonce, where clearing of the Access Control List occurs. An attacker can share the same nonce and the same security key for two consecutive messages.

  **A spy can recover partial information by using XOR on these two consecutive ciphertexts.

4.2.2.2 Network Layer Security Issues &Attacks

Wi-Fi

WPA2 standard (encrypts data sent over wireless networks with a 256-bit key), MAC filtering, and static IP address used as security measures in Wi-Fi. SSID hiding is used for covering the service identifier and partially protecting against scanning

Security Issue/s: -

- WPA2 is not enforced by default in all networks
- Lack of granular device authentication
- In the same network, connected devices are vulnerable to other connected devices
- Wi-Fi can be exploited through MAC spoofing

Possible Attack/s: -

- Data can be decrypted easily in the absence of WPA2
- Denial of service attacks can occur. Different DoS attacks due to insecure Wi-Fi on different layers are: -
  - Physical Layer: - Rogue stations, node tampering, proximity attacks, and Wi-Fi Channel Collision
  - Software Layer: - Race conditions, packet replay attacks, or battery exhaustion
  - Network Layer: - Network flooding, wormhole attacks
- Common attacks on medical Wi-Fi networks due to connected devices vulnerability are peer-to-peer and eavesdropping attacks.
- A malicious device can spoof the MAC address of an existing medical device and, it can launch integrity and confidentiality attacks against all data traveling to the spoofed device.

ZigBee

128-bit AES with pre-share keys, global link key, frame-protection mechanisms, essential key (encryption in network layer), and unique link key (App layer) are used in ZigBee as security measures.

Security Issue/s: -

- Implementation vulnerabilities: - It focuses on encryption configurations like utilizing insecure key transportation for pre-shared keys, reusing Initialization Vectors (IVs) during encryption, installing default link keys for all the devices, transferring security headers in clear text on auxiliary frames.
- Protocol vulnerabilities (Acknowledgement packets have no integrity checks, only sequence numbers that can easily be intercepted).
- Insufficient registration of network keys
- lack of verification in PAN IDs

Possible Attack/s: -

- Where code-based errors exist, attackers can easily hack the devices to fetch information.
- Attackers can build ACKs at the MAC layer with numerous adverse effects. For instance, disassociate services and access control from legitimate devices.
- Insufficient registration allows reuses of Initiation Vectors, which may lead to key compromise.
- Lack of verification allows attackers to reset to Factory defaults all device network connections.

** Other types of ZigBee attacks include exploitation in energy-consuming services to deplete power, especially on portable devices.

WIA-PA

A join key is communal between a security manager and a device to authorize access is used as security measures in WIA-PA.

Security Issue/s: -

- Lack of public-key encryption algorithm
- No intrusion prevention
- No broadcast key
- The first request is not encrypted

Possible Attack/s: -

Sybil, DoS, wormhole, Jamming, and traffic analysis attacks can be made due to the above security issues in WIP-PA

6LoWPAN

6LoWPAN uses AES cipher suite, ESP, IKEv2 (protocol associated with IPSec), and DTLS as security measures.

Security Issue/s: -

- Attacks focus on the IP network or the radio signal

Possible Attack/s: -

- Due to this security issue, attackers use **malicious intermediary network nodes** that attack a 6LowPAN network from the inside. Attacks involve **signal jamming** (in radio signals), where attackers replay attacks to cause address depletion. Moreover, **flooding attacks** can be imposed to do DoS against legitimate devices.

LoRaWAN

Security features of LoRaWAN include a 128-bit application session key (AppSKey), AES-CMAC, and MIC.

Security Issue/s: -

- Resetting frame counters without re-keying
- Caching and replay of ACK packets
- Transmit fake gateway signals to wake up sensors repeatedly
- Utilize a dictionary of past message

Possible Attack/s: -

- Recovery of passwords
- Replay attacks
- Battery exhaustion and DoS
- Malicious message modification

4.2.2.3 Application Layer Security Issues &Attacks

HL7

No built-in security is present in HL7. It depends on security features delivered by the underlying communication protocols.

Security Issue/s: -

- Message sources are frequently not validated by default
- Frequently, the size of HL7 messages is not validated

Possible Attack/s: -

- Spoofing or integrity attacks
- Flooding attacks

COAP

COAP has four modes where NoSec mode implements no security controls, SharedKey mode uses a pre-shared key for all communicating parties, MultiKey mode utilizes unique keys for each device participating in the network, and Certificate mode provides end-to-end security through the use of certificates together with the aforementioned shared or multi-key mechanisms. It has no embedded authorization mechanisms and it works in conjunction with **DTLS,** which have issues of large messages and handshake compression and does not suit COAP proxy mode.

Security Issue/s: -

- Security issues arise from proxies having to decide if the DTLS implementation will be a multicast or unicast message.

Possible Attack/s: -

- Parsing attacks (node could execute malicious code), Cache attacks (proxy server can gain control of a part of the network), Amplification attacks (convert a small packet into a larger packet and launch DoS attacks), Cross-Protocol attacks (packet translation from TCP to UDP is liable to attacks) and Spoofing attacks.

MQTT

It does not support any security mechanisms by default because it is designed to operate in already secure networks but it imposes a four-way handshake mechanism to ensure message delivery.

Security Issue/s: -

- No embedded data encryption mechanism
- IP broker (sometimes is insecure)

Possible Attack/s: -

- If it is not operating an insecure network, Attackers can hack it easily because there is no embedded mechanism.
- Attacks due to IP brokers are Traffic analysis, Port Obscurity, and Botnet Over MQTT.

HTTP

HTTP protocol comprises two types of authentication mechanisms, Basic and Digest (both are not considered as secure methods).

Security Issue/s: -

- Data transfer is not encrypted
- Get request

Possible Attack/s: -

- Eavesdropping- theft- breach and manipulation
- Flooding attacks include: -
  - Waste Flood
  - GET Flood
  - HTTP methods flood

4.3 OBJECTIVE-BASED STUDY

4.3.1 Security Objectives In IoMT Edge Network

There are six major security objectives (defined in section 4) that have been identified in the context of the IoMT edge network.

- Confidentially
- Integrity
- Non-repudiation
- Authentication
- Authorization
- Availability

4.3.2 Attack types In IoMT Network

The list of potential attacks against IoMT edge networks is as follows: -

4.3.2.1 Eavesdropping attacks

Eavesdropping attack takes advantage of unsecured network communications to access data as it is being sent or received by its user through a computer, smartphone, or another connected device. This attack is difficult to detect because it does not cause abnormalities to the network transmission operations.

4.3.2.2 Spoofing attacks

The thoughtful encouragement of an entity or resource to act incorrectly. In other words, it is a situation in which a person or program successfully identifies as another by faking data to gain an illegitimate advantage. For example, the attacker uses a fake sending address in transmission data to illegally enter into a secure system. Two types of spoofing are: -

- Piggybacking
- Mimicking

4.3.2.3 Traffic analysis attacks

It is known as a passive form of attack in which an intruder gains knowledge of the transmitted information. The information may not be directly available in case of data encrypted, but identities, locations, data flow, and flow's presence, absence, amount, direction, frequency, and duration of occurrence may be fetched.

4.3.2.4 Masquerading attacks

During this type of attack, unauthorized entities illegitimately pose as authorized entities to gain the greater privilege to a system than what they are authorized for. This is known as an active attack. An attacker may perform malicious actions as well.

4.3.2.5 Physical attacks

Attacks on the physical layer or on the devices itself known as physical attacks. Physical attacks include: -

- Device capture
- Tampering
- Invasive hardware attacks
- Side-channel attacks
- Reverse engineering attacks

4.3.2.6 Malware attacks

Malware is malicious software or firmware which is designed and operated by an attacker to violate the security of a system. It is mostly inserted into another program to destroy data run destructive or intrusive programs. It can infect an application or full-fledged operating system. Well-known types of malware are: -

- Worms
- Virus programs
- Malicious mobile code
- Trojan horses
- Rootkits

4.3.2.7 Man-in-the-middle attacks

MITM attack can be possible in both active and passive ways. In this attack, an attacker interferes in the communication between two authenticated entities.

4.3.2.8 Denial-of-service attacks

DoS aims at the obstruction of provisioning time-critical functions. It can also restrict access to authorized assets and facilities. This process of achieving it is flooding the resource-constrained IoMT edge network with a huge number of requests.

4.3.2.9 Battery drainage attacks

A battery drainage attack occurs when an attacker utilizes resources for a long period to drain its battery or make it unavailable for the legitimate user. For instance, a malicious user overruns the IoMT device with a large number of no authorized requests.

4.3.2.10 Impersonation attacks

Here, an attacker playacts as a legitimate entity (Claimant or Verifier) in an authentication protocol to gain access to resources to which he/she is not authorized.

4.3.2.11 Message fabrication/modification/replay attacks

In message fabrication/modification, a malicious actor replays with a transmitted message to produce an unauthorized effect or gain unauthorized access.

4.3.3 Security Threats In IoMT Network

Following figure 69 shows the possible security threats in the IoMT network based on various objectives of security in IoMT.

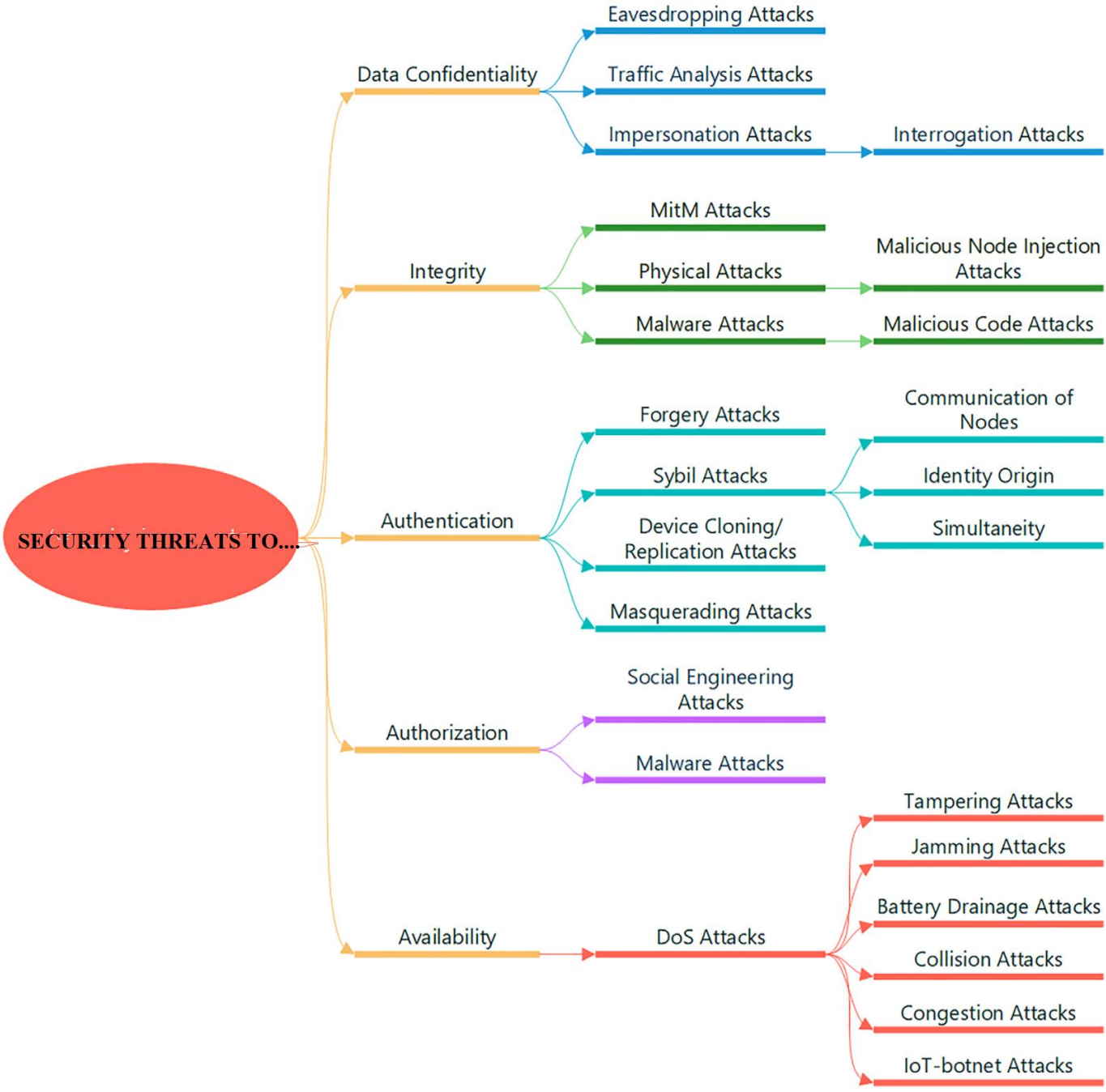

Figure 69: - Security threats in IoMT network [74]

4.4 SECURITY THREATS & ROBOTIC/REMOTE SURGERY

Robotic/ remote surgery is the most crucial field of medicine and in the case of IoMT in robotic/remote surgery, it needs to be strictly secure. A single vulnerability can cause a high risk including a threat to a human's life.
Attacks on Surgical Robotics can occur in two ways: -

- Realistic attacks involve direct attacks against connected surgical robots
- Indirect attacks against ambient devices. For instance: - Gyroscope sensors, that may affect a surgical operation

The micrometer's accuracy is highly important during surgery. The major vulnerabilities are listed as follows: -

- A direct attack on the surgical robot or an indirect attack against the sensors is possible
- Attacks elaborated in the perception layer are the main threat for gyroscope sensors
- **Indirect Attack: -** Malicious actor can make replay attacks, by producing signals to confuse the original gyroscope signals. It creates problems in the mapping of the human body and may change the coordinates or produce error signals. This type of attack requires proximity with the sensor. As the doctor has to operate from outside the surgery room and the surgery room has a lack of monitoring and identification systems, the attackers get a chance to breach the security.
- **Direct attack: -** Following attacks can exist in case of a direct attack on a surgical robot

    - **Modification of robot's intent: -** Attacker may modify the packets during the transportation of packets. It may cause minor malfunctions in the device like unusual robot movements or delays.
    - **Manipulation of the robot's intent: -** In this case, the intruder cannot handle the medical device but may **affect the feedback** of the device like the images and coordinates.
    - **Hijacking: -** Surgical robots can be hijacked by an intruder to takes over the working of robots.

In the above-mentioned methods, the attackers may act in several ways like: -

- As network **eavesdroppers** who collect information
- As active attackers who can **inject small packets** as well
- Act as **network mediators** (MITM attack). In this case, the in-hospital device stops communicating straight with the IoMT network.
- The **ARP poisoning attack** could be a method to improve direct attacks against surgical robotics, where an attacker sends distorted ARP messages over a LAN.

In the case of remote monitoring and treatment, a node may be connected with an external end device. As result, the aim is to design a **secure channel** for data transmission, need a **high data rate**, focus on **constant availability, and data integrity**.

5 SOLUTION TO EVOLVED SECURITY THREATS FOR IoMT

Firstly, to secure Data in Transit, it is necessary to know answers to the following questions: -

- Why do we secure data in transit?
- What are we securing?
- Where do we secure it?
- When do we secure it?
- Who secures it?
- How do we secure it?

There are different methods are present to secure data in transit like: -

- Virtual Private Networks
- Remote Access
- Site-to-Site
- IPSec
- Transport Layer Security (TLS)
- The Onion Router (ToR)

To secure data in transit, the TLS cipher suite is available with different components. The most secure combination of TLS cipher suite components to date is: -

"**TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**"

This combination includes the following components: -

- Cipher suite: - TLS1.2
- Key Exchange: - ECDHE
- Digital Signature (Authentication): - RSA
- Data Encryption: - AES_128_GCM
- Message Integrity: - SHA256

5.1 PROTOCOL/TECNOLOGY/STANDRADS BASED STUDY

There are different protocols, standards, and technologies [71] being used in different layers of IoT architecture. Section 4.2.1, described the list of protocols, standards, and technologies, which are further used in IoMT.

5.1.1 Measures to Control Weaknesses

Section 4.2.2 elaborated on possible vulnerabilities & Attacks that can occur in IoMT related protocol/technologies and standards. This section includes the measure to control present weaknesses in IoMT related protocols, standards, and technologies.

5.1.1.1 Perception Layer Mitigations

Infrared

As attacks against infrared communications involve a line-on-sight interaction with the target, **physical security controls** can be applied to protect eavesdropping (Snooping/Spying) or jamming (Congestion/Blocking) attacks.

RFID

Common protection mechanisms are difficult to implement in RFID because it is used in devices with very low-power features. Some custom authentication mechanisms can be used like **authentication-hash based protocols and encryption functions**

- An authentication protocol has been designed by two researchers for RFID tags to assure tag location privacy, replay attack, and DoS attack protection, as well as backward and forward traceability protection. [75]
- Sun et al. [76] proposed a hash-based RFID security protocol. It provides forward privacy and the goal of this protocol is to protect the RF tag from tracking attacks. It is based on observing previous unsuccessful sessions of the tag.

NFC

As NFC architecture is complex so real-wold execution of MITM attacks in NFC is very difficult to deploy. To tackle the attacks in NFC **a secure channel with a standard key agreement protocol** can be introduced.

- SSL and VPN technology and encryption can mitigate most of the attacks (e.g., Sniffing, DoS, Eavesdropping, and Data corruption)
- Standard key agreement protocol based on Diffie-Helman (DH), RSA, and elliptic curves.
- For addressing data corruption, checking of the RF field of NFC readers during data transmission can be introduced
- DH has been replaced with DHE and after some time with ECDHE
- To secure ECDHE **Forward Secrecy** is a new concept that can be upgraded.

Bluetooth/BLE

Different researchers argue that devices connected through BLE may be vulnerable to numerous threats on all communication layers but there are many solutions to secure the BLE devices that have been introduced as well like: -

- **AES-CCM** encryption has been proposed to achieve confidentiality and integrity. The data channel PDUs can also be authenticated with a **4-byte MIC module**
- Lanzetta et al. [77] proposed solutions to protect BLE against attacks which include practical, technical, and application-based solutions. They proposed the following recommendations: -

- Regular updations in device settings and BLE version
- Authentication credentials must be updated frequently
- Avoid auto-pairing and pair only with authenticated devices
- In case of the idle state, turn off Bluetooth modules
- Set the BLE device to undiscoverable mode
- Utilize strict pairing policies

- Technical solutions: -

  - To prevent MITM attacks combination keys can be used instead of link/unit keys
  - Use link encryption to prevent eavesdropping
  - Do not use multihop communication when encryption is not supported
  - Use of encrypting broadcast interceptions
  - At the link layer with a 128-bit encryption key, the use of security mode three can be implemented.

The best choice nowadays is to use **AES with 128 bits GCM** than AES-CCM.

Z-Wave

Z-Wave already offers confidentiality, source integrity, and data integrity services through AES (mostly 128) encryption. However, some techniques which can help to further protect IoT devices using Z-wave are listed as below: -

- AES_128 can be used with GCM rather than CCM
- Hide the WLAN SSID
- WPA2 should be used instead of WEP
- Use a Reverse Proxy Server
- Inspect log files

UWB

UWB is threatened by attacks that differentiate the distances between the nodes. **Localization and distancing protocols** can secure the range between nodes. Moreover, a simple and practical countermeasure is to **store the nonce states in NVM** and recover them after each power failure. To prevent ED/LC attacks, **UWB-PR** was used as the first modulation method.

5.1.1.2 Network Layer Mitigations

Wi-Fi

WEP authentication, WAP, WAP-PSK, technologies used to protect Wi-Fi previously. **WAP2** is the new version that is used to protect Wi-Fi where a key hierarchy is used. A single key must be placed at the uppermost level and all subsequent keys are generated from this key. Further in this

technique, Robust Security Network Information Elements (**RSN IE**) field has been expanded with the two bits SA Query (Association Query) mechanism.

A step forward to secure the Wi-Fi, **Forward secrecy** (FS) can be used.

ZigBee

To secure implementation vulnerabilities, AES for symmetric key cryptography is used in several security modes (AES-CTR, AES-CBC-MAC, and AES-CCM). **GCM form of AES** is more secure and can solve the existing problems. **Wake-on-radio** is a feature that prevents an attacker from guessing the activity period of the network but it is not available from all chip vendors. **Cluster key** could be used to prevent non-repudiation security issues.

Another measure is to use the **NVM** of a node to store the nonce states to recover nodes in case of power failure.

WIA-PA

Certain hopping mechanisms for the extenuation of the interference attacks are available like: -

- **AFS** (Adaptive frequency switch)
- **AFH** (Adaptive Frequency Hopping)
- **TH** (Timeslot hopping)

For the tampering, the WIA-PA application layer and the Datalink sublayer use **MIC** to achieve data integrity.

6LoWPAN

It has already a strong mechanism for security but to handle the attacks defined in section 4.2.2.2, **DTLS** (Encryption technique), **HIP** (host identification technology), and **IKE** can be used to compound a secure transportation channel, cryptographic techniques can be used. An **IDS** is a tool that can be used to enable the detection of abnormal activities carried out by an intruder.

LoRaWAN

AES-CMAC, AAES-CTR, MIC are already used in this approach. Other measures which can be used to enhance the security of LoRaWAN are: -

- Include **HTTPS**
- Include **VPNs**

5.1.1.3 Application Layer Mitigations

HL7

To create a secure connection and protect data from public connections **SSL VPNs** should be used. **DE identification/anonymization** (like deleting directly identifying data, replacing identifying data with artificial identifiers or pseudonyms, and suppressing/generalizing quasi-identifiers) helps to protect patient data as well.

COAP

Blocking/Slicing modes can be used to mitigate amplification attacks. An **intrusion system** can detect any suspicious activity in the system. **Strong authentication techniques** must be included with DTLS.

MQTT

MQTT brokers require **username/password authentication**, which is handled by TLS/SSL (Secure Sockets Layer). TLS 1.2 includes the latest **cipher suites** to protect data in transit.

HTTP

Basic and Digest methods are not considered secure without the use of **SSL/TLS** encryption. To achieve the desired security level HTTPS should be used rather than HTTP. **TLS 1.2** is the stable version that can be used to secure connections effectively.

5.2 OBJECTIVE-BASED STUDY

Section 4.3 elaborated the Security Objectives in IoMT Edge Network and security threats as well. This section describes the security countermeasure in the IoMT edge network.

5.2.1 Security Countermeasures in IoMT Edge Network

Securing countermeasures are also based on the six security objectives of the IoMT network

5.2.1.1 Ensuring confidentiality

To ensure confidentiality, the security team must emphases on the management of data of IoMT devices that are considered confidential. Data can be managed during the following stages: -

- Data generation
- Data storage
- Data transition
- Data Processing

5.2.1.2 Ensuring integrity

A combination of **symmetric cryptography** and **attribute-based encryption** (ABE) can be used to ensure the integrity of the transmitted data in the IoMT edge network environment. Message integrity algorithms are used to ensure data integrity. **SHA256** is the latest algorithm used for checking message integrity.

5.2.1.3 Ensuring non-repudiation

If disputes come from an entity denying previous commitments/actions, a solution to the problem must find out. In IoMT devices, to handle these situations logs are accessed. In logs, all the performed operations are stored securely. To prevent it from occurring, advanced encryption methods and access control lists should be used.

5.2.1.4 Ensuring authentication

Authentication is an important parameter for security in IoMT. A great number of authentication protocols and techniques exist, but there is a need for lightweight authentication mechanisms because the IoMT combination of heavyweight authentication techniques with their limited battery and computing power creates a problem. **The digital signature** is one aspect of **TLS**, which can be used to validate the identity. Different digital signature algorithms are available for validating the identity like - **RSA, DSA, ECDSA**

5.2.1.5 Ensuring authorization

The level of access for each authorized requester should be controlled to reduce the risk of intrusion attacks. **ACLs** can be used to control the authorization process.

5.2.1.6 Ensuring availability

In a hospital, the availability of interconnected medical devices should be ensured. IoMT devices face limitations majorly regarding resource and computational power. The use of a **centralized system** is imperative to meet the computational cost. **Strength of Crowd** (SOC) protocol is a solution to resource-constrained IoMT devices.

5.3 SECURITY MEASURES & ROBOTIC/REMOTE SURGERY

Security measures elaborated in a study of IoMT based protocol/technologies/standards/objectives can help in securing the robotic/remote surgery. In addition, there are some other measures which can be followed.

- The patient should not use personal data such as special IDs for medical purpose
- Encrypt the whole information not selectively
- Assign access rights for all users
- Users with admin rights like doctors must follow a strong password policy
- Avoid excessive protection to keep fast the process of network
- Avoid complicated third-party solutions that slow down the network

Horizontal rule during encrypting data in the IoMT is mandatory but there is a need to address it at a legal level, where possible extensions or an explanatory circular on the GDPR can purposely be used to tackle encryption schemes for modern IoMT networks.

Because of inherent complexity and diversity, IoMT networks cannot adopt a single network protocol for all possible implementations. Hence, there is **no unified approach** available to mitigate security concerns for **WSN and ad-hoc networks** to the extent required by medical services. Currently, it is tough to balance **secure authentication mechanisms with power consumption**. It is very important in remote surgery because computation and communication overhead can result in power depletion. There is a need to **establish a secure channel for data transmission**, need **high data rate**, focus on **constant availability** and **data integrity**. "**5G"** may become the solution to these problems of remote/robotic surgery.

5.4 5G AS A SOLUTION TO EVOLVED SECURITY THREATS

All around the world, various initiatives are taken for adopting and standardizing the 5G enabled IoT. There are many features involved in 5G, which can become a solution to the existing problems of IoMT. There is a quotation from WHO (World Health Organization) about 5G in healthcare, depicts in figure 70.

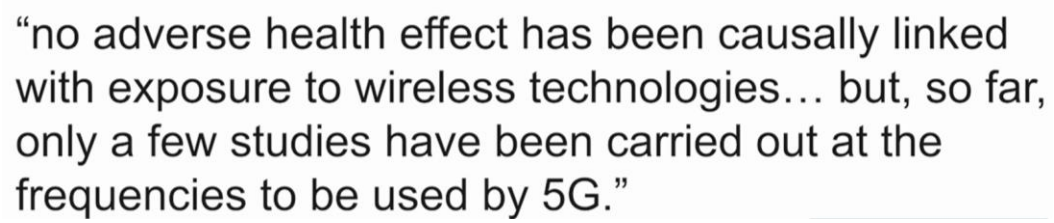

Figure 70: - WHO about 5G

Security features of 5G have been elaborated in section 2.3, and different features of 5G included in IoT are elaborated in section 2.1. Features employed in 5G’s Physical Layer to support 5G-IoT are: -

- Carrier Aggregation
- Coordinated Multipoint Processing
- Massive-MIMO (M-MIMO)
- Heterogeneous Networks (HetNets)
- D2D Communications
- Centralized Radio Access Network (CRAN)

Features employed in 5g networking layer to support 5G-IoT: -

- Software-Defined Wireless Sensor Networking (SD-WSN)
- Network Function Virtualization (NFV)
- Cognitive Radios (CRs)

Other renowned features for IoT that have been enabled in 5G are enhanced **QoS** and **Standardization**.

5G-IoT involves mainly two types of standards: -

- **Technology standards: -** Deal with network technology, protocols, and wireless communication and data aggregation standards
- **Regulatory standard: -** Comprises of security and privacy of data

Bandwidth and latency are big issues in remote surgery that can counter using 5G easily. Moreover, the combination of IoT using 5G and AI in the field of healthcare can improve the lives of millions of people by upgrading the existing system.

The overall trend in Rel-16 is to make the 3GPP 5G System (5GS) a communication-enabling platform suitable for healthcare and other industries.

5.5 LATEST RESEARCH ABOUT SECURITY MEASURES IN IoMT

The following table includes the latest research about security for IoMT devices.

Table 7: - Latest research about security for IoMT devices

S. No.	Research Topic	Defined problems	Outcomes	Year	Ref.
1	Deep Q-Learning-Based Neural Network	Security and Privacy	Proposed deep Q-learning-based neural network with privacy preservation method	2022	[78]
2	Blockchain Technology	Client's, Consensus Mechanism's, Mining Pool, Network and smart contract vulnerabilities	Vehicular Network including IPFS and marginal transport nodes	2022	[79]
3	Telesurgery and Robotics	Global Network Development, Legal Issues, Billing Issues, Equipment Acquisition, Cost, Cyber Security Threats, Latency	The proposed approach to use includes high speed 5G network, haptic feedback, tactile robotics, one-to-many remote surgery, IoT	2021	[80]
4	5G mobile communication applications for surgery	Reliability, end-to-end delay, low data error rate, bandwidth, and latency	Benefits and applications of 5G in surgery, Current status of research about 5G in surgery	2021	[81]
5	Fog-to-Cloud Networks	Cloud Challenges including security, high latency, service level agreement, real-time response, high bandwidth demand, Interoperability	Proposed Fog Computing Paradigm to overcome the limitations of cloud computing	2021	[82]
6	Security Vulnerabilities and Solutions	Security and privacy challenges	Security measures proposed for Ontology, Biometric, and Blockchain-based security models	2021	[83]

6 CONCLUSIONS

The IoMT systems are likely to play an important role in providing affordable, easy, and secure healthcare for future generations. In other words, IoMT systems can provide intrusive and dynamic support for remote and robotic surgery. However, there is a need to develop new security mechanisms to make the system robust and secure. The report presents research on evolved security threats and solutions for Healthcare IoT (IoMT).

The importance of 5G in the future as a context in IoMT has been evaluated through the study of history, system standard, key features, and technical overview of previous network technologies and 5G. Further, the research includes IoT types, challenges, technologies, levels, components, architecture, and smart use case of IoT. After the study of 5G and IoT, a deep study on evolved security threats for healthcare IoT has been conducted. It includes: -

- IoMT security overview
- Protocol, technologies, and standards of IoT used in IoMT
- Possible vulnerabilities & attacks on IoMT related protocol, technologies, and standards
- Security objectives in IoMT edge network
- Attack types and security threats in IoMT Network
- Security threats & robotic/remote surgery

The solution to security threats is based on the above study. The report presents countermeasures in security through different aspects. The solution to evolved security threats for IOMT includes: -

- Measures to control weaknesses of IoMT related protocol, technologies, and standards
- Security countermeasures in IoMT Edge Network
- Security measures & robotic/remote surgery
- 5G as a solution to evolved security threats
- Latest research about security measures in IoMT

Remote/robotic surgery is a promising surgical advancement, however, faces many challenges. Zero-latency time and improvement in haptic feedback technology, secure protocols, and models are required for precise and well-done surgeries. Technologies like 5G network, with upgrade models and standardization for IoT-based surgery devices, can overcome these barriers.

7 REFERENCES

[1] G. S. T. D. P. K. G. C. D. Dimitris Koutras, "Security in IoMT Communications: A Survey," *Sensors*, vol. 20, no. 4828, pp. 1-49, 2020. https://www.mdpi.com/1424-8220/20/17/4828

[2] N. G. N. A. M. C. N. P. M. M. C. Hanif Ullah, "5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases," *IEEE Access*, vol. 7, pp. 37251 - 37268, 2019. https://ieeexplore.ieee.org/document/8668495

[3] J. Q. S. F. M. A. I. Siddique Latif, "How 5G (and concomitant technologies) will revolutionize healthcare," *Future Internet*, vol. 9, no. 93, pp. 1-24, 2017. https://arxiv.org/abs/1708.08746

[4] R. R. D. B. B. D. T. M. C. J. B. H. F. F. Leandra Börner Valdez, "5G mobile communication applications for surgery: An overview of the latest literature," *Artificial Intelligence in Gastrointestinal Endoscopy*, vol. 2, no. 1, pp. 1-11, 2021. https://www.wjgnet.com/2689-7164/abstract/v2/i1/1.htm

[5] D. T. David Denyer, "Producing a systematic review," in *The SAGE Handbook of Organizational Research Methods*, Thousand Oaks, CA, USA, Sage Publications Ltd, 2009, pp. 671-689. https://www.cebma.org/wp-content/uploads/Denyer-Tranfield-Producing-a-Systematic-Review.pdf

[6] C. Thapa, "Evolution of Wireless Communication," Lewis Williamson, 2015. https://slidetodoc.com/evolution-of-wireless-communication-by-chandra-thapa-evolution/

[7] D. Bliss, "The First Mobile Phone Call Was Made 75 Years Ago," Smithsonian Magazine, June 16, 2021. https://www.smithsonianmag.com/innovation/first-mobile-phone-call-was-made-75-years-ago-180978003/

[8] J. Kulubi, "ADVANCED MOBILE PHONE SERVICE (AMPS)," MULTIMEDIA UNIVERSITY OF KENYA, May 2016. http://ece2526.elimu.net/Notes/AMPS/Amps_Home.html

[9] S. R. F. R. I. A. Z. K. Shahriar Shahabuddin, "Evolution of Cellular Systems," in *A Comprehensive Guide to 5G Security*, John Wiley & Sons Ltd, March 2018, pp. 1-28. https://cris.vtt.fi/en/publications/evolution-of-cellular-systems

[10] Group of engineers, "EVOLUTION OF COMMUNICATION -1G TO 4G & Towards 5G," LTE, India, March 2018, https://www.youtube.com/watch?v=NUovkXWe15s.

[11] Telecom learning, "GSM Architecture," Jan 2019. [Online]. Available: https://www.youtube.com/watch?v=6qR102lcXoY.

[12] Mpirical, "3G UMTS Architecture," Jul 2017. [Online]. Available: https://www.youtube.com/watch?v=qNddSi0wugw. [Accessed 03 12 2021].

[13] S. R. M. Z. A. S. A. R. R. Z. M. A. M. O. M. A. Azar Abid Salih, "Evolution of Mobile Wireless Communication to 5G Revolution," *Technology Reports of Kansai University*, vol. 62, no. 05, pp. 2139-2151, June 2020. https://www.academia.edu/43475437/Evolution_of_Mobile_Wireless_Communication_to_5G_Revolution

[14] Group of Engineers, "TDD VS FDD IN LTE 4G Updated," Youtube, India, March 2018, https://www.youtube.com/watch?v=MJFsDBzUr5U&list=PLE6yE0jB6BTOY6Z1DKEkQ8yZ8fFPUiCD8&index=1.

[15] Group of engineers, "MIMO TECHNIQUES - CAPACITY & COVERAGE ENHANCEMENT IN 4G LTE," Youtube, India, Feb 2017, https://www.youtube.com/watch?v=hIl4ZQb-A70.

[16] Group of engineers, "LTE 4G RAN ARCHITECTURE - eUMTS - INTRODUCTION," Youtube, India, March 2018, https://www.youtube.com/watch?v=1_x9axf0jlk.

[17] M. V. Sonia Forconi, "4G LTE architectural and functional models of Video Streaming and VoLTE services," *2015 Seventh International Conference on Ubiquitous and Future Networks, IEEE Xplore*, pp. 787-792, August 2015. https://ieeexplore.ieee.org/abstract/document/7182650

[18] Group of engineers, "5G - A Step Towards Smart Ecosystem," LTE, YouTube, India, Mar 2021, https://www.youtube.com/watch?v=dsIwmmpo1H4.

[19] 3GPP, "Release 15, V15.0.0, 3GPP TR 21.915," 3rd Generation Partnership Project, Sep, 2019. https://www.etsi.org/deliver/etsi_tr/121900_121999/121915/15.00.00_60/tr_121915v150000p.pdf

[20] S. Sun, "5G cellular networks: 6 new technologies," Sunny Classes, YouTube, United States, Dec 2018, https://www.youtube.com/watch?v=hQvHNVRv_ms&t=47s.

[21] K. N. H. I. N. I. A. O. N. N. S. S. J. M. A. O. Y. O. Manabu Sakai, "Indoor Experimental Trial on Hybrid 16-Beam Spatial-Multiplexing for High SHF Wide-Band Massive MIMO in 5G," in *IEEE 88th Vehicular Technology Conference (VTC-Fall) 2018*, 2018. https://ieeexplore.ieee.org/document/8690841

[22] Mpirical, "What is Beamforming (Massive MIMO)?," Mpirical, Youtube, United Kingdom, June 2019, https://www.youtube.com/watch?v=pE_FsnHtTxc&t=4s.

[23] S. Kaur, "Study and Design of 5G Network for Smart Water Meter IoT Applications," "Capstone Project MINT 709", University of Alberta, Canada. https://era.library.ualberta.ca/items/b1778ecb-a8d9-4679-ada3-736dfa96dbb1

[24] Mpirical, "What is 5G Core Network Architecture," Youtube, United Kingdom, Jan 2019, https://www.youtube.com/watch?v=YVoCpqsPwmQ.

[25] 3GPP, "Release 16, V16.1.0 , 3GPP TR 21.916," 3rd Generation Partnership Project, Jan, 2022. https://www.etsi.org/deliver/etsi_tr/121900_121999/121916/16.00.01_60/tr_121916v160001p.pdf

[26] Mpirical, "5G Security Overview," YouTube, United Kingdom, Dec 2021. https://www.youtube.com/watch?v=AJ8xuN2zT7U.

[27] M. M. M. A. I. H. K. H. R. Ibrahim Salah, "Comparative Study of Efficiency Enhancement Technologies in 5G Networks - A survey," *Procedia Computer Science*, vol. 182, pp. 150-158, 2021. https://www.sciencedirect.com/science/article/pii/S1877050921004841

[28] C. SHARMA, "CORRECTING THE IOT HISTORY," March 2016, http://www.chetansharma.com/correcting-the-iot-history/.

[29] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," CISCO White Paper, April 2011. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[30] Ekeeda, "Definition and Characteristics of IoT - Introduction to IoT - Internet of Things," YouTube, India, Feb 2021, https://www.youtube.com/watch?v=sXuTiaH9l_w.

[31] F. Minds, "Internet of Things | JNTUK | Unit- I | Lecture 2 | Technology behind IoT | Fab Minds |," YouTube, India, May 2021, https://www.youtube.com/watch?v=5NfKeofbac4.

[32] Electrical Technology, "What is a Sensor? Different Types of Sensors with Applications," Nov 2018, https://www.electricaltechnology.org/2018/11/types-sensors-applications.html.

[33] A. Calihman, "Architectures in the IoT Civilization," San Diego, USA, Jan 2019, https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/.

[34] B. B. A. H. P. A. F. N. Mohammad Ali Jabraeil Jamali, "IoT Architecture," in *Towards the Internet Architectures, Security, and Applications*, EAI/Springer Innovations in Communication and Computing, 2020, pp. 9-29. https://link.springer.com/book/10.1007/978-3-030-18468-1

[35] R. P. J. ˜. a. R. G. G. Liliana Antao, "Requirements for Testing and Validating the Industrial Internet of Things," in *2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, Sweden, July 2018. https://ieeexplore.ieee.org/document/8411739

[36] S. Electronics, "What is Narrowband Internet of things? NB-IoT basics Tutorial," YouTube, United States, Sep 2020, https://www.youtube.com/watch?v=kIxTUcVpP0k.

[37] B. B. A. H. A. F. N. Mohammad Ali Jabraeil Jamali, "Some Cases of Smart Use of the IoT," in *Towards the Internet of Things Architectures, Security, and Applications*, EAI/Springer Innovations in Communication and Computing, 2020, pp. 85-127. https://www.springerprofessional.de/en/some-cases-of-smart-use-of-the-iot/16802468

[38] "https://sm.pcmag.com/pcmag_in/how-to/h/how-to-pro/how-to-protect-your-smart-home-from-hackers_c3hj.jpg".

[39] Visioforce, "Smart Home," Visioforce Automation Systems, Hong Kong, http://visioforce.com/smarthome.html.

[40] M. Domb, "Smart Home Systems Based on Internet of Things," in the *Internet of Things (IoT) for Automated and Smart Applications*, Feb 2019, pp. 1-13. https://cdn.intechopen.com/pdfs/65877.pdf

[41] J. &. S. D. &. A. J. H. &. S. M. &. P. R. &. A.-M. J. &. A. V. Rodrigues, "Enabling Technologies for the Internet of Health Things," *IEEE Access*, pp. 1-9, 2018. https://ieeexplore.ieee.org/document/8246498

[42] C. M. Gonzalez, "7 Wearable Devices for 2020," The American Society of Mechanical Engineers, Jul 2020, https://www.asme.org/topics-resources/content/7-wearable-devices-for-2020.

[43] E. Staff, "The basics of designing wearable electronics with microcontrollers," June 2014, https://www.embedded.com/the-basics-of-designing-wearable-electronics-with-microcontrollers/.

[44] Pareteum, "Connected Cars 2021: Top Benefits and Features," Nov 2021, https://www.pareteum.com/connected-cars-2021-top-benefits-and-features/.

[45] N. SAKOVICH, "IoT in Automotive Industry: the Creation of Self-Driving Cars," Sam Solutions, https://www.sam-solutions.com/blog/iot-in-automotive-manufacturing/.

[46] N. Pappageorge, "Industrial IoT & The Future of Factories," Cbinsights, May 2018, https://www.cbinsights.com/research/briefing/factory-of-the-future-manufacturing/.

[47] W. H. III, "Connecting Fluid Power to the Industrial IoT and Industry 4.0," AUTOMATION INSIGHTS, 2018, https://automation-insights.blog/2018/11/14/connecting-fluid-power-to-the-industrial-iot-and-industry-4-0/.

[48] "Global smart city platform market to reach $755m by 2027," https://internetofbusiness.com/global-smart-city-platform-market/.

[49] T. M. A. A.-H. Asma Elmangoush, "Towards Standard M2M APIs for Cloud-based Telco Service Platforms," in *11th International Conference on Advances in Mobile Computing & Multimedia*, Vienna, Austria, 2013. https://dl.acm.org/doi/abs/10.1145/2536853.2536892

[50] K. S. D. Sukhpreet Kaur, "Comparative Study of Android-Based M-Apps for Farmers," in *International Conference on Intelligent Computing and Applications*, Springer Singapore, 2018. https://www.springerprofessional.de/en/comparative-study-of-android-based-m-apps-for-farmers/15333268

[51] M. S. S. R. A. A. K. A. a. M. A. N. Farooq, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," *IEEE Access*, vol. 7, pp. 156237-156271, 2019. https://ieeexplore.ieee.org/document/8883163

[52] A. Electronics, "IoT Retail Solutions Overview," https://www.arrow.com/en/iot/iot-retail-solutions/overview.

[53] T. D. S. Sofana Reka, "Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid," *Renewable and Sustainable Energy Reviews*, vol. 91, pp. 90-108, March 2018. https://www.sciencedirect.com/science/article/abs/pii/S1364032118301837

[54] M. A. A. H. A.-a. M. L. M. O. X. G. J. W. N. C. Jie Wan, "Wearable IoT enabled real-time health monitoring system," *EURASIP Journal on Wireless Communications and Networking*, vol. 298, pp. 1-10, 2018. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-018-1308-x

[55] S. M. M. S. Massimo Canonico, "TEEM: a Mobile App for Technology-Enhanced Emergency Management," in *The 3rd EAI International Conference on IoT Technologies for HealthCare*, VÄSTERÅS, SWEDEN, 2016. https://www.igi-global.com/article/teem/193259

[56] N. M. K. Mohamad Khairi Ishak, "Design and Implementation of Robot-Assisted Surgery based on Internet of Things (IoT)," in *2017 International Conference on Advanced Computing and Applications*, 2017. https://ieeexplore.ieee.org/document/8392580

[57] S. T. S. T. N. K. Rajesh Gupta, "Tactile-Internet-Based Telesurgery System for Healthcare 4.0: An Architecture, Research Challenges, and Future Directions," *ENABLING NETWORKED SERVICES AND TECHNOLOGIES FOR CONNECTED HEALTHCARE, IEEE Network,* pp. 23-29, 2019. https://ieeexplore.ieee.org/document/8933555

[58] M. F. C. Z. Y. L. D. H. Q. Z. Wei Tian, "Telerobotic Spinal Surgery Based on 5G Network: The First 12 Cases," *Neurospine*, pp. 114-120, 2020. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7136105/

[59] K. S. D. Sukhpreet Kaur, "Design and Development of Android Based Mobile Application for Specially Abled People," *Wireless Personal Communications,* vol. 111, pp. 2353-2367, 2020. https://www.springerprofessional.de/en/design-and-development-of-android-based-mobile-application-for-s/17479752

[60] R. S. G. V. M. R. a. A. K. Ashok Kumar Munnangi, "Wearable Smart Devices for Remote Healthcare Monitoring to Detect Cardiac Diseases," on *Internet of Medical Things Remote Healthcare Systems and Applications*, Springer, 2021, pp. 75-94. https://link.springer.com/chapter/10.1007/978-3-030-63937-2_5

[61] H. F. S. P. D. S. Dino Mustafa, "ENABLING TIME-CRITICAL COMMUNICATIONS IN MEDICAL IoT APPLICATIONS," in *International Conferences ICT, Society, and Human Beings 2021*, 2021. http://www.es.mdh.se/pdf_publications/6177.pdf

[62] I. H. K. Mohd Javaid, "Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic," *Journal of Oral Biology and Craniofacial Research,* vol. 11, pp. 209-214, 2021. https://www.sciencedirect.com/science/article/pii/S2212426821000154

[63] G. Munjal, "IoT Based Healthcare: A Review," in *Evolving Role of AI and IoMT in the Healthcare Market*, Springer Nature Switzerland AG 2021, 2021, pp. 61-77. https://www.springerprofessional.de/en/iot-based-healthcare-a-review/20008188

[64] P. M. B. R. R. T. A. K. S. A. S. S. Usharani, "Pregnancy Women—Smart Care Intelligent Systems: Patient Condition Screening, Visualization and Monitoring with Multimedia Technology," *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, pp. 147-169, 2022. https://link.springer.com/book/10.1007/978-981-16-6542-4

[65] V. G. a. J. Singh, "The Internet of Things and Advanced Applications in Healthcare," in *Artificial Intelligence in Industrial Applications, Learning and Analytics in Intelligent Systems*, Springer Nature Switzerland AG 2022, 2022, pp. 91-110. https://link.springer.com/book/10.1007/978-3-030-85383-9

[66] B.-X. P. Kuang-Hao Lin, "Wearable Technology and Visual Reality Application for Healthcare Systems," *Electronics,* vol. 11, no. 178, pp. 2-17, 2022. https://www.mdpi.com/2079-9292/11/2/178

[67] ScreenCloud, "15 IoT Applications in the Connected Healthcare Space," https://screencloud.com/blog/iot-applications-healthcare-space.

[68] Emergen Research, "Top 10 IoT Medical Device Companies Leading the Digital Revolution in Healthcare," https://www.emergenresearch.com/amp/blog/top-10-iot-medical-device-companies-leading-the-digital-revolution-in-healthcare, 2021.

[69] Wikipedia, "Security," https://en.wikipedia.org/wiki/Security, 2022.

[70] M. N. E. Y. H. N. R. C. O. S. A. C. Jean-Paul A. Yaacoub, "Securing the Internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems, Elsevier*, pp. 581-606, 2020. https://www.sciencedirect.com/science/article/am/pii/S0167739X19305680

[71] G. S. T. D. P. K. D. G. C. D. Dimitris Koutras, "Security in IoMT Communications: A Survey," *Sensors*, vol. 20, no. 4828, pp. 1-49, Aug 2020. https://www.mdpi.com/1424-8220/20/17/4828

[72] R. L. S. M. C. O. G. M. Sara Amendola, "RFID Technology for IoT-Based Personal Healthcare in Smart Spaces," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 144-152, 2014. https://ieeexplore.ieee.org/document/6780609

[73] D. S. M. L. S. M. J. M. Philip A. Catherwood, "A Community-Based IoT Personalized Wireless Healthcare Solution Trial," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 6, May 2918. https://ieeexplore.ieee.org/document/8355907

[74] M. K. M. S. E. R. L. Maria Papaioannou, "A Survey on Security Threats and Countermeasures on Internet of Medical Things (IoMT)," *Transactions on Emerging Telecommunication Technologies*, pp. 1-15, July 2020. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4049

[75] C. J. M. Boyeon Song, "RFID authentication protocol for low-cost tags," in *In Proceedings of the First ACM Conference on Wireless Network Security*, Alexandria, VA, USA, April 2008. https://dl.acm.org/doi/abs/10.1145/1352533.1352556

[76] J.-D. Z. Da-Zhi Sun, "A hash-based RFID security protocol for strong privacy protection," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 4, pp. 1246 - 1252, November 2012. https://ieeexplore.ieee.org/abstract/document/6414992

[77] P. C. J. C. B. J. M. Angela M. Lanzetta, "Security Vulnerabilities in Bluetooth Technology as Used in IoT," *Journal of Sensors and Actuator Networks*, vol. 7, no. 28, pp. 1-26, 2018. https://www.mdpi.com/2224-2708/7/3/28

[78] A. C. N. I. M. R. A. H. G. Nirmala Devi Kathamuthu, "Deep Q-Learning-Based Neural Network with Privacy Preservation Method for Secure Data Transmission in the Internet of Things (IoT) Healthcare Application," *Electronics*, vol. 11, no. 1, pp. 1-14, 2022. https://www.mdpi.com/2079-9292/11/1/157

[79] B. G. B. J. Bheemeswara Sastry, "Imposing Security and Privacy in the Healthcare Industry Using Blockchain Technology," in *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, Springer, 2022, pp. 237-264. https://link.springer.com/chapter/10.1007/978-981-16-6542-4_13

[80] U. U. W. M. T. A. S. R. M. R. Z. A. Z. Anmol Mohan, "Telesurgery and Robotics: An Improved and Efficient Era," *Cureus*, vol. 13, no. 3, pp. 1-5, March 2021. https://www.cureus.com/articles/54068-telesurgery-and-robotics-an-improved-and-efficient-era

[81] D. R. B. B. M. D. B. C. F. H. Börner Valdez L, "5G mobile communication applications for surgery: An overview of the latest literature," *Artificial Intelligence in Gastrointestinal Endoscopy*, vol. 2, no. 1, pp. 1-11, March 2021. https://www.wjgnet.com/2689-7164/full/v2/i1/1.htm

[82] K. A. S. F. T. A. Ayeni, "Toward Healthcare Data Availability and Security Using Fog-to-Cloud Networks," in *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, Springer, 2021, pp. 81-103. https://link.springer.com/chapter/10.1007/978-981-16-6542-4_6

[83] T. P. J. M. M. a. U. H. J. Jeyavel, "Security Vulnerabilities and Intelligent Solutions for IoMT Systems," on *Internet of Medical Things*, Springer, April 2021, pp. 175-194. https://link.springer.com/chapter/10.1007/978-3-030-63937-2_10

8 ABOUT AUTHOR and SUPERVISOR

SUKHPREET KAUR KHALSA is doing a Master of Science in Internetworking at the University of Alberta, Canada. She earned her Master in Computer Applications with a merit certificate from Punjab Agricultural University (Ludhiana, Punjab) in the year 2013. After that, she has spent time as a Research Scholar in the Dept. of Computer Applications at I.K. Gujral Punjab Technical University, Jalandhar, Punjab, India. She has authored three publications in esteemed International refereed journals (including SCI, SCOPUS, SCIe) and reputed International Conferences (IEEE, ACM) proceedings. She also served as a computer programmer at Akal Technologies Ltd. Her research areas include IoT, Mobile Application Development, Mobile Computing, Database & Advanced Network Security, and Web Designing.

SANDEEP KAUR is a 5G/IoT/Cloud/Cybersecurity specialist with 12 years of experience in Cybersecurity, Solution Consulting (presales), Network Designing, Network infrastructure Support, and Technical writing roles. She earned her Master of Science in Internetworking from the University of Alberta (Alberta, Canada) in the year 2019. Having held positions at Ericsson, Nokia, Bell Canada, and Ciena Corporation, Sandeep has led numerous 5G, and IoT projects focused on implementing, testing, and assessing security integrity and information security controls in 5G and IoT deployment. Sandeep contributed to various security research capstone projects as a Project Mentor focusing on 5G/IoT physical layer security, Anomaly detection using AI/ML, and security threats on 5G key technologies (SDN, SDMN, NFV, MEC, and network slicing). Sandeep is currently working as a Senior Developer at Ciena Corporation Canada.

9 GLOSSARY

Term	Explanation
3GPP	3rd Generation Partnership Project
6LowPAN	6 Low-Power Wireless Personal Area Networks
A	
AAA	Authentication Authorization & Accounting
ABE	Attribute Based Encryption
ACK	Acknowledgement
ACL	Access Control Lists
AES	Advanced Encryption Standard
AES-CMAC	AES- Cipher-based Message Authentication Code
AFH	Adaptive Frequency Hopping
AFS	Adaptive Frequency Switch
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
AMPS	Analogue Mobile Phone System
API	Application Programming Interfaces
AppSKey	Application Session Key
AUC	Authentication center
AUSF	Authentication Server Function
B	
BS	Base Station
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Stations
BW	Bandwidth
C	
CA	Carrier Aggregation
CAPEX	Capital Expenditure
CDMA	Code Division Multiple Access
CIA	Confidentiality Integrity and Availability
CIoT	Consumer Internet of Things, Commercial IoT
CoAP	Constrained Application Protocol
CoMP	Coordinate Multi Point
COTS	Commercial Off The Shelf
CN	Core Network
CR	Cognitive Radios
CRAN	Centralized Radio Access Network
CSCN	Circuit Switched Core Network
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
D	
DH	Diffie-Hellman

DHE	Diffie-Hellman Ephemeral
DL	Downlink
DTLS	Datagram TLS
DoS	Denial-of-Service
E	
ECDHE	Elliptic-Curve Diffie-Hellman Ephemeral
EDGE	Enhanced Data Rates for GSM Evolution
ED/LC	Early Detection and Late Commit
EDN	External Data Networks
EIR	Equipment Identity Register
Embb	Enhanced Mobile Broadband
eNB	Evolved Node B
EPC	Evolved Packet Core
ESP	Encapsulated Security Payloads
ETSI	European Telecommunications Standards Institute
eUTRAN	Evolved UMTS Terrestrial Radio Access Network
F	
FDD	Frequency-division duplexing
FDMA	Frequency Division Multiple Access
FM	Frequency Modulation
G	
GDPR	General Data Protection Regulation
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
gNB-CU	gNB-Central Unit
gNB-DU	gNB- Distributed Unit
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communication
GTP	GPRS Tunneling Protocol
GTS	Guaranteed Time Slot
GUTI	Globally Unique Temporary Identifier
H	
HDLC	High-level Data Link Control
HetNets	Heterogeneous Networks
HF	High Frequency
HID	Human Interface Devices
HIP	Host Identity Protocol
HL7	Health Level 7
HLR	Home Location Register
HPR	High Pulse Repetition
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSS	Home Subscriber Server

HSUPA	High Speed Uplink Packet Access
HTTP	Hyper Text Transfer Protocol
I	
ICP	Interoperable Communication Protocol
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things, Infrastructure IoT
IKE	Internet Key Exchange
IoBT	Internet of Battlefield
IoT	Internet of Things
IoMT	Internet of Medical Things
IoMT	Internet of Military Things
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IMTS	Improved Mobile Telephone System
IP	Internet Protocol
IPFS	Interplanetary File System
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	IP Packet Exchange
Ir	Infrared
IrDA	Infrared Data Association
IrLAP	Infrared Link access protocol
IrLMP	Infrared Link management protocol
ISIM	IP Multimedia Services Identity Module
ITU	International Telecommunication Union
ITU-R	International Telecommunication Union-Radio
Iu	Interface UMTS
IuCS	Interface UMTS Circuit Switched
IuPS	Interface UMTS Packet Switched
IV	Initialization Vectors
J	
J-TACS	Japanese- Total Access Communication System
K	
KHz	Kilohertz (a measure of frequency equivalent to 1,000 cycles per second)
L	
LF	Low Frequency
LoRa	Long Range
LPR	Low Pulse Repetition
LTE	Long-Term Evolution
M	

M2M	Machine-to-Machine
MANO	Management and Orchestration
MCC	Mobile Country Code
ME	Mobile Equipment
MIC	Message Integrity
MITM	Man-In-the-Middle
MME	Mobility Management Entity
M-MIMO	Massive-MIMO
mMTC	Massive machine-type communications
mmWave	Millimeter-Wave
MNC	Mobile Network Code
MPDC	MAC protocol data unit
MTS	Mobile Telephone System
MTSO	Mobile Telecommunication Switching Office
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Subscriber Identification Number
MSP	Mobile Service Provider
Multi RAT	Multi Radio Access Technology
MQTT	Message Queuing Telemetry Protocol
N	
NAS	Non-Access Stratum
NB-IoT	Narrowband IoT
NFC	Near Field Communication
NFV	Network Function Virtualization
NG-RAN	NextGen RAN
NMT	Nordic Mobile Telephone
NOMA	Non-Orthogonal Multiple Access
NR	New Radio
NRF	Network Repository Function
NSP	Network Service Provider
NSS	Network Subsystem
NSSAA	Network Slice Specific Authentication and Authorization
NVM	Non-Volatile Memory
O	
OFDMA	Orthogonal Frequency Division Multiple Access
OMS	Operation & Maintenance Subsystem
OPEX	Operating Expenditure
OTP	One Time Password
P	
P2P	Point to Point
PAN	Personal Area Network
PCEF	Policy Control Enforcement Function
PCRF	Policy and Charging Rule Function

PDN	Packet Data Network
PDU	Protocol Data Unit
P-GW	Packet data network Gateway
PICC	Proximity Inductive Coupling Card
PLMN	Public Land Mobile Network
PRINS	Protocol for N32 Interconnect Security
PSCN	Packet Switched Core Network
PSK	Pre-Shared Key
PSTN	Public Switch Telephone Network
Q	
QoS	Quality of Services
R	
RAN	Radio Access Network
REST	Representational State Transfer
RF	Radio Frequency
RFID	Radio Frequency Identifications
RNC	Radio Network Controller
RPL	Routing Protocol
RRC	Radio Resource Control
RSN IE	Robust Security Network Information Elements
S	
SC-FDMA	Single-Carrier Frequency Division Multiple Access
SD-WSN	Software-Defined Wireless Sensor Networking
SEPP	Security Edge Protection Proxy
S-GW	Serving Gateway
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMS	Short Message Service
SOC	Strength of Crowd
SSP	Secure Simple Pairing
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SVT	Stolen Vehicle Tracking
T	
TACS	Total Access Communication System
TC	Transcoder
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TH	Timeslot hopping
TLS	Transport Layer Security
ToR	The Onion Router
TRX	Transceiver
TSP	Telematics Service Providers

TTI	Transmission Time Interval
U	
UDM	Unified Data Management
UDP	User Datagram Protocol
UE	User Equipment
UHF	Ultra High Frequency
UTRAN	Universal Terrestrial Radio Access Network
UL	Uplink
UMTS	Universal Mobile Telecommunications Systems
UPF	User Plane Function
uRLLC	Ultra-reliable and low-latency communications
USIM	Universal Subscriber Identity Module
Uu	User UMTS
UWB	Ultra-Wide Band
UWB-PR	UWB with Pulse Reordering
V	
V2V	Vehicle-to-Vehicle
V2X	Vehicle to Anything
VLR	Visitor Location Register
VMS	Voice Mail System
VoIP	Voice over IP
VoLTE	Voice over LTE
W	
WAN	Wide Area Network
W-CDMA	Wideband Code Division Multiple Access
WHO	World Health Organization
Wi-Fi	Wireless Fidelity
Wi-Max	Worldwide Interoperability for Microwave Access
WPA2	WiFi Protected Access 2
WSN	Wireless Sensor Network
X	
XMPP	Extensible Messaging and Presence Protocol
Z	
ZigBee	Zonal Intercommunication Global-Standard