Implications of IoT with 5G

Ahmed Albakr, Mohammed Alqubaisi, Falah Alroaished, Abudulaziz Alsaif, Ahmed Alqaroos, Atta-ur-Rahman*
College of Computer Science and Information Technology,
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia.

Abstract
This research is mainly concerned with the identification of the Internet of Things (IoT) in contrast to the fifth generation (5G) telecommunication mechanism in daily life and how to face this technological revolution in its various aspects of control, use and risks. This research illuminates the path towards the ambiguity of digital communication speed in the 5G technology and how to penetrate the finer details of daily movement and enhanced data rates and support to billions of devices connected over the network with adequate quality of service (QoS). We also specified the possible challenges during integration of IoT with 5G and their possible projected solutions. That would greatly help the researchers and scholars in this field to find the research gap and possible research directions.

Keywords:
5G, Internet of Things, Communication, Protocols, Challenges, ICT

1. INTRODUCTION

The Internet of Things (IoT) is the concept of connecting any device to the internet that includes an extraordinary number of the object of all shape and size. Fifth generation (5G) of mobile phone telecommunication standard has a super-fast mobile network to link all the objects together, whether they are smart phones or any other object having the identity. Its high Gbps data transfer rates, low latency, and high capacity. IoT will make life much easier with making each object connected with us remotely. 5G will help the IoT technology to grow and send the data accurately and that is very important in some fields, and it may save much life if its id used in the right way for example in healthcare or emergency time, also it will be useful for personal use [1]. Rest of the paper is organized as follows: section 2 and 3 highlight the applications of IoT and 5G in daily lives individually. Section 3 talks about the integration of IoT and 5G technologies and the possible outbreaks in this regard. Section 4 highlights the plenty of advantages of integrating IoT with 5G as communication technology compared to the previous 4G and long-term evolution (LTE) integrations. Section 5 shows the possible disadvantages of this integration. Section 6 narrates the solution to the major problem associated with 5G, that is security risks and related issues while section 7 concludes the paper.

2. IOT USES IN REAL LIFE

.3

Many of us have dreamed of smart homes where the tools and machines are able to execute our orders automatically, the alarm bell and the coffee machine activate the moment you want to start your day, illuminate the lighting as you walk through the house, some hidden computing devices respond to your voice commands to read your schedule and messages when they are ready, and play the news on TV. Your car can lead you to work on the less crowded road and give you a chance to read or prepare for a morning interview while you are on the move. These are few of many possible implications of the information and communication Technologies (ICT) [13]. These connected devices produce large crowding in the Internet, including large amounts of data that make the device useful, and are also used for other purposes. All of this new data and the nature of these devices that allow access via the Internet requires an increase in privacy and security standards, as this technology allows access to a level of access to information in real time that we could not get before, where we can monitor our homes and families remotely And make sure they are safe. In business you can improve the process by increasing productivity, reducing material loss and sudden breakdowns. Sensors in the city's infrastructure help reduce road congestion and alert us if the infrastructure is in danger of collapse. Some devices in nature can monitor changes in environmental conditions and alert us to imminent disasters, so we see these devices everywhere and use their capabilities to enhance almost any physical object [14].

Manuscript received December 5, 2025
Manuscript revised December 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.12.6

Although most of us don't have a smart home full of interactive gadgets yet, IoT applications are already very popular. The statistics are very different, and researchers probably use different criteria to surround them, but according to some calculations they number between 15 and 25 billion connected devices and the number is expected to increase to 50 to 212 billion by 2020, and even some analyzes predicted that there will be a trillion A connected device by 2025 [15]

Even though this number is huge, you can believe it when you realize that you can include or attach sensors and microcomputer equipment for almost anything you want. Many of us have a smartphone, a device that serves as a point of contact for many connected machines, so it can be considered an IoT. Wearable sports trackers are also commonly used. Built-in processing equipment, sensors and connectivity have been added to almost any appliance that comes to mind, from a small home scale to a fridge, to shoes. Smart thermostats, smoke detectors, and security cameras can monitor your behavior's, help you save energy, and enable you to remotely visualize your home or send an alarm when something is abnormal, making it easier to connect to emergency services. Car keys or pets and even children. Many other connected devices are already on the market and will be announced soon [16] .

Currently, most of us probably have a few smart devices that can be dealt with individually (often using their own smartphone apps), but they can't be connected in general, but some companies and industry groups are working to create standards and platforms. Work to make it easy to program these devices to work together continuously and improve security. Outside the home, many industries and cities are adopting (or have already) adopted IoT technology as well [17].

Once several devices can work together, even with devices from different manufacturers, we can automate many everyday tasks. Essentially for common physical purposes, we have provided high computing power and sensitivity. For example, these tools can take readings from our environment (including our bodies) and use this data to change their own settings or give signals to other devices to do so and combine them so we can study them and analyze the results. Many do their work with complex algorithms, not just if-then, if-then, simple conditional directives, which were previously used with embedded computing, either in their own processors or using cloud servers [18].

The web has grown considerably, with high-speed Internet access into homes and wireless networking becoming very popular. During that time, microchips and other computer hardware are getting smaller and smaller so we can finally put them into mobile devices. Nowadays, our smart devices can access the Internet via cellular or Wi-Fi wireless signals, as well as communicate with other devices using Bluetooth technology or another local communication method. Thanks to some of these technologies, we were able to create many electronic tools. Data processing occurs on web-connected servers in large data centers, which we call the cloud and have a significant contribution to enabling ordinary devices to become IoT devices. These devices may connect to the Internet by sending data to your phone or to specialized equipment in your home that acts as a distributor through a local communication methodology [19].

IoT communication tools include computer hardware including processors with built-in programming that guides their work, sensors that combine different types of readings (temperature, humidity, light, movement, chemical level, heart rate, body movement), as well as communication devices that send and receive Signals. Some connected systems may be able to use nearby data collection devices such as city road systems that send signals to smartphones to help monitor traffic. Smart devices can work with tag technologies such as RFID tags, QR codes, barcodes, etc. to obtain material data. They also need a power source that can be obtained by connecting to a power outlet, solar panels or even rechargeable batteries (if the included equipment requires low amounts of energy), and companies are now working on wireless power as a possible future source. For energy. These devices often work with their own built-in software or firmware and can load and process many processes via cloud-based online software that can process a large amount of data. Some use advanced algorithms that enable them to learn and adapt to different types of stimuli and models (making them program themselves to a certain extent). Processes and transmissions from the data detector often occur in real-time, thanks to the high speed of the Internet connection, allowing these devices to respond in real time [20].

These devices, which contribute to the Internet of Things (IoT), have expanded from personal to family and public use as well as in business and industry, and any field that does not include IoT now will be used in the future. The most important smart equipment that many of

us use and interact with every day are smart phones connected to the Internet where they include many sensors such as accelerometers, gyroscopes gyroscopes balance, GPS, and sometimes a heart rate monitor, but all this is only A very small part of the Internet of Things [21].
For personal use, there are wearable devices such as a fitness monitor or cardio where our phones are used to send and receive data. For example, smart watches like Apple and Pebble do these and more by pairing with the phone. Positioning sensors and processors in the clothes are not too far away (they can now be done using printed boards and sensors from Arduino or other companies), and even pets can be placed on the list where we can put sensors that track targets on them [22].

We already have a range of devices such as cameras that send images to the Internet, weight scales that share our weight on social networks, a toothbrush that monitors how teeth are cleaned, and a gaming system that performs voice commands. One of the most important applications used in homes (thermostats, water heaters, security cameras, lights) where they collect data and connect them remotely to their destination and connect to the Internet when there is a problem, some of which are able to learn a set of models over time and then can change Settings or alert you when something sudden happens. Connected garage doors or digital door locks can bring you home using data from your phone. Instead of traditional keys, we can monitor stoves and ovens with Wi-Fi signals as well as turn them on or off remotely. One of the theoretical applications that people often discuss is a refrigerator that recognizes the ingredients inside, informs you of the lack of food or tells you dinner that can be prepared from the available ingredients [23].

We are very close to building smart cities where the entire metro is covered by sensors and other technologies. Devices that take sensor readings and then send them are suitable for use in things like monitoring or monitoring. In some areas, this still requires workers to take measurements from Each house separately. Some smart devices can monitor many important events (serious road accidents, pollution levels, consumption of energy and water resources), roads will have detectors to predict possible events such as traffic and street conditions, so nearby cars or smartphones can warn you of traffic delays. Other detectors adjust traffic lights to suit real-time conditions, monitor trash cans to see when they can be emptied, and provide information on available parking spaces [24].

Scientists are working to make a detector or sensor that is too small to be placed in cement or other materials, so that the properties of the physical material and its infrastructure can be verified before the structural work of disasters such as the collapse of bridges. Cars also become smart. For example, GPS has been in the car for years. We had attached payment cards that automatically run when passing through charging stations, and now we are starting to add new functional computer detectors for automatic cars. Smart cars can act as mobile infotainment distributors, supplying Wi-Fi signals to other devices and tracking the driving process including speed and fuel consumption. Someday, the car will be able to drive, and you don't need hands or eyes to drive. It monitors the road and nearby vehicles to avoid accidents. We have built cars and services that allow you to operate or locate your car and open doors remotely [25].

There are already many devices in the healthcare field, many of which are currently under construction. For example, a doctor or health supervisor will be able to monitor a patient's vital signs to see how well he or she is active, detect important factors remotely and thus save their lives or possibly allow older people to live independently longer. The reagents embedded in hospital beds or patient clothes collect important data on the condition of the patients. Researchers are now working on things like a fall-sensing carpet and small computer equipment that can be injected into the human body [26].
There are many more smart devices used in other industries and businesses where monitoring (without the need for workers) can save a lot of time and money as GE tested several sensors to be used in the process of ceramic mixing for the manufacture of batteries. The researchers also analyzed the data to determine what to watch to see when the ceramic mixture was ready, allowing them to obtain a proportional density and significantly reduce error rates. Thus, the condition and conditions of products from their raw materials can be monitored until the end of the production process, and the same control is used for any other work. In retail, stockpiles are tracked, and a reserve alert is sent out when items need to be refilled. In agriculture, it is possible to monitor land and crops that need watering and to monitor livestock and locate them. In office buildings and companies, the controlled environment is automatically controlled, and energy and cost losses are reduced. The possibilities of the Internet of Things are endless [27].

Such data is used to detect and stop fraudsters who use credit cards or bank accounts. Data analysts may activate hard-to-detect purposes in cards, businesses, homes, and other needs. Surveillance takes place with a system that can recognize faces or verify our identity through phones, cars and other smart technology [1].

3. How does this affect you, me, and everyone around us?

The new rule for the future will be, "Anything that can be connected, will be connected to the Internet. But why do we want to connect so many devices connected to each other on our planet? There are many examples of what it might look like or what the potential value might be. For example, if you are on your way to a meeting and want to arrive as quickly as possible. Your car can be informed of your appointment history and choose before the meeting the shortcut to your meeting. For example, if traffic is crowded your car can send text to the other party telling them that you will be delayed. Also, what if your alarm alerts you to swap at a certain hour in the morning and can tell your coffee maker to make your own coffee at the time you take it without even thinking about it. What if the work suit can tell you when and where you are more active and productive and provide you with all the information about other devices that you used during the work and provide you with all reports reporting on your work. Examples of what the Internet of Things or Value Internet, Internet of things or IoT will create. Anything connected to serve people, every machine works for you without pressing any button. Without tiring yourself to repeat things the machine can do for you and understand when, where and how long you do business for us.

More broadly, IoT can be applied to transport networks, smart cities that can help us reduce waste and improve efficiency for things like energy use, and this helps us understand and improve our way of life and how we work. Figure 1 shows a similar scenario [2].

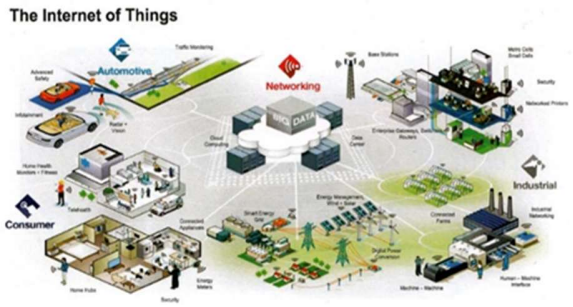

Figure 1: IoT in daily life

4. 5G and the IoT: What Do They Really Mean for Us?

5G and the internet of things, or IoT, are two buzzwords that are constantly thrown around. Despite this prevalence, there is an overwhelming lack of knowledge among the general population on what 5G and the IoT are and how they impact their lives.

Syniverse has been right in the thick of these technologies, with the release of a major 5G study and a 5G signaling service this year, and extensive work with the IoT through our private, isolated network, Syniverse Secure Global Access, and this has provided us with some perspectives that I would like to share here.

Take this statistic, from a survey by Decluttr of 2000 U.S. smartphone owners, which found that one-third of respondents "believed they had a device capable of 5G wireless connections." While to the uninformed eye this would make sense, this statistic causes concern because 5G just recently went on the market in large cities, and the "coverage is pretty spotty and inconsistent for now."

Our other fateful buzzword, the IoT, has not fared much better, with "36% of consumers [saying] they still don't know what IoT is, but 70% of consumers indicate, they owned a connected device." [28]

So, where does this disconnect come from? What are these buzzwords? Why are they buzzwords in the first place? And what makes them likely to stick around? 5G, or fifth generation-cellular wireless, is a wireless technology that is essentially the next iteration of the well-known 4G. The idea is that, as we've been sharing through many Syniverse blog posts, 5G will soon be the standard of wireless tech, with lightning-fast speeds and quicker connections. 5G employs "a system of cell sites that divide their territory into sectors and send encoded data through radio waves." However, this system has just recently been deployed by the major companies, with Verizon focusing

on the internet service and AT&T, Sprint, and T-Mobile all hopping on this mobile phone trend as well.

So why is 5G a buzzword, besides its novelty? Well, the advantages of 5G are remarkable, as once described as having "blazing speeds, a responsive network, and extensive coverage" making up "5G's Holy Grail." Speed in and of itself may sound nice for those of us tapping our toes in the line to pick up our morning coffee while trying to read the news, but perhaps not as life-changing as the hype makes it out to be. The incredible potential of 5G is its ability to empower other up-and-coming technologies, such as self-driving cars and virtual reality systems.

While people talk about 5G as if its widely available, many companies do not even sell 5G phones, so this is still a concept in the abstract. We need better education so that people understand what 5G is when they see it and to myth-bust some of the perceived risks of 5G, such as the millimeter wavelengths that are thought to cause adverse health effects. The U.S. Food and Drug Administration and Federal Communications Commission have both said "there's nothing to be worried about" health-wise in terms of 5G. People need to know that for us to really take advantage of this technology. [29] The internet of things, or the IoT, is 5G's partner in creating a more interconnected world. The IoT is essentially billions of physical devices around the world that are now connected to the internet, collecting and sharing data. If this seems a little abstract, some examples will turn a lightbulb on. In fact, many light systems are now part of the IoT. As with any new development, though, these are not reasons to dismiss the IoT, but guideposts in how we shape the development, implementation, and regulation of these technologies. Essential to this process is readily accessible, easily digestible education about the IoT and 5G. Part of this falls on advertisers and brands. These companies need to get better at answering "how will the device improve the life of the consumer?" [30]

5G and the IoT are just going to keep getting bigger and better. As mobile traffic continues to explode and new technologies continue to connect more and more devices online, 5G and the IoT will play an essential role in our future, where all facets of the world will be integrated with and powered by mobile. Syniverse is looking forward to playing a central role in this exciting future. But all of us in the tech industry must make sure that everyone is ready to connect in this future together.

Experts from Nokia, iboss and Sectigo talk 5G mobile security for internet of things (IoT) devices in this webinar YouTube video (transcript included). When it comes to the next generation of mobile networks, 5G promises a more Internet of Things-friendly ecosystem with vast improvements over the current capabilities of 4G – however, its intersection with IoT will also raise the stakes on cybersecurity. The benefits of 5G are myriad: Not only will it allow extremely fast data feeds of 1Gbps and better (equivalent to top-tier home broadband speeds), but 5G also offers ultra-low latency (less than one millisecond according to the standard). It also supports greater density (up to 100 times more connected devices per unit area, all of them getting the same speed and latency) and better network energy usage. To that latter point, the 5G standard calls for a 90 percent reduction in energy consumption, which translates into low-power IoT devices in industrial environments boasting 10 years' worth of battery life. [31] Taken together, this opens new use cases. Ultra-low latency for example makes it possible to support self-driving cars; IoT sensors on autonomous vehicles will be able to measure temperature, traffic conditions, weather, GPS location, distance to other objects, and so on in real-time. Similarly, in the medical field, applications like remote-controlled surgery for rural areas can potentially change the face of medicine. And, in industrial IoT, tracking sensors throughout the supply chain can support real-time water delivery, streamlined waste management, live traffic monitoring and light changes, and even on-demand electrical grids. The downside is that the risks involved from a cyber perspective tend to grow exponentially in these scenarios; when controlling your car on the freeway, performing remote surgery or providing power to cities, cyberattacks can literally become a matter of life or death [32]. Figure 2 shows a 5G in a snapshot.

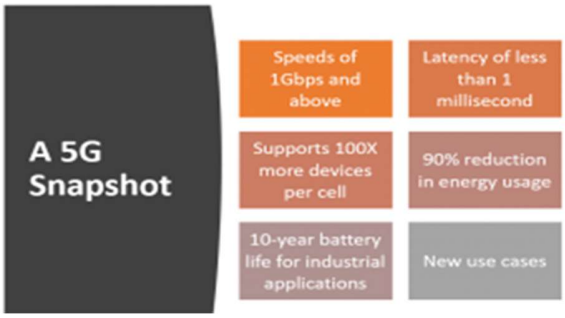

Figure 2: A 5G snapshot

So how do we tie this in with 5G? Bear in mind, there are not many 5G networks currently out there, so most of the information you've seen so far comes from existing 4G mobile networks. Going to 5G, 5G does introduce some new security features of great value. I mean first, on the pro side, the control plane in 5G is strongly authenticated and encrypted. This means that the actual core of the 5G network is going to be less vulnerable to attack, and that's a good thing. The other thing is that 5G introduces the slicing capability, which enables you to create network segments that are separate from each other, and one segment can't be attacked from another. That is a good thing too. This means that if you've got a segment that's dedicated to electronic banking, then the segment that's dedicated to mobile phones can't attack that segment. They're not visible to each other. They're physically separate. And from a security perspective of course that's good. Another aspect is that, and this is the visibility aspect, within a lot of the mobile networks today the use carries a great net and so the actual mobile devices are not visible from the internet. They can't attack them from the outside. But with 5G and the move to IPv6 addressing, it could create the situation where the IoT devices out there, unprotected, no firewalls in front of them may be much more visible and therefore much more vulnerable to attack. Remember, I've said if the device is vulnerable and is visible, it is going to be attacked [3].

5. ADVANTAGES OF IOT IN 5G

The main advantage of 5G is to increase the speed of transmission and decreasing the latency where the speed of transmission up to 20 Gbps, that will let the people able to access the files faster. With 5G the number of connected devices together will be increased greatly. All connected devices will be instant of internet connection this will favor the IoT [4]. Away from smartphones, 5G can also improve connectivity worldwide and connect billion of objects together, in turn, it is boosting the connectivity in our home, office, and cities too. Imagine cites reacting with each other around the world by taking information from people and sensors data and vehicles, buildings and much more and more to improve our life quality and make our life easier [5]. Through mobile technology 5G, we expect to provide more connectivity across our cities. It will support many types of communication for transportation, and the most important types are:

- Vehicle to vehicle (V2V): the vehicles are directly connected to each other's [38].
- Vehicle to infrastructure (V2I): the vehicles communicate with sensors in roads and bridge and traffic light [6].
- Leaps in transportation [39]
- We have all seen a future vision for smart cities that shows in sci-fi movies and TV shows and video games, where flying the cars through the air. Also, it helps the driver to avoid congestion by sending alerts to the driver and give him the easiest way to go to his destination. Were IoT will also help the cars to connected to avoid the accident and that will decrease the number of accidents around the world, also it helps the driver to found parking and improve the global positioning system (GPS) into the car for searching into the maps based on driver needs. IoT could start the auto-driving cars where the computer will be smart and fast enough to decide a very fast amount of time and with accurate results. Emergency also becomes improve with IoT where the ambulance car relates to 5G bridge and that will help the ambulance to choose the fastest way and avoid traffic to go to the hospital as fast as possible [5]. Traffic light also can adept with traffic around to minimize unnecessary delay by getting all information of a number of vehicles in each road and apply the traffic light timer based on number vehicles [6].

5.1 IoT in healthcare

In some cases, the doctor or patient needs to travel from country to other countries to treat and it needs attention because it is very sensitive, where the people are travel from other areas with a lot challenging and time-consuming. And because the use of IoT technologies continues to grow, the amount of data transmit into network expected to increase, and 5G has the potential to help resolve these challenge, and here there are the five ways 5G can help healthcare organization meet the growing demands of digital transmutation [7] [40].

5.2 Transmitting a large imaging file quickly.

Other image machines are typically very large files, and it must be sent to a specialist to analysis and review.

When the network has low bandwidth, the transmission will take a long time, or it might be not sent successfully. This means the patient waits a long time during the treatment. The 5G network speed can help quickly and reliably transport [7].

5.3 Expanding telemedicine

Study by Market Research Future, the market of telemedicine expected to grow at a compound annual with a growth rate of 16.5% from 2017 to 2023. Where the study mentions the reason for the increase is the need in a rural area for healthcare requires a high-speed network that can support real-time and high-quality video, with 5G healthcare system can enable mobile network that helps healthcare care system to work in deferent place and handle telemedicine appointments, which can greatly increase the reach of the program [7] [33].

5.4 Improving AR, VR and spatial computing

Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) are the most fashionable topics in today's technology world. They have gained great interest from the media and major technology companies that have become heavily invested in in these technologies. These three techniques will affect many aspects of our lives. They are now used in education, entertainment, communication, medicine and many other industries. While AR, VR and spatial computing are already being used in healthcare on a limited basis, 5G may eventually further enhance a doctor's ability to deliver innovative, less invasive treatments. Among 5G's many ultimate potential applications, some of the most exciting involve its role in simulating complex medical scenarios and enabling alternative treatments for the critically ill. AT&T is working at the forefront of this exciting field, exploring opportunities to apply 5G to medical challenges. AT&T is collaborating with VITAS Healthcare to study the effects of eventual 5G-enabled AR and VR on patient engagement. The goal is to reduce pain and anxiety for terminally ill patients in hospice by providing calming, distracting content via 5G-enabled AR and VR [7].

Example

Surgery to remove cancerous tissue from the intestines of a patient for the first time using a 360-degree VR camera took place at the Royal Hospital in London. The process was viewed through the VR app in AR using a VR headset paired with a smartphone A live webcast was made. This approach is a shift in the course of medical education; instead of a small number of students wrapping around the surgeon to watch a surgery. Many medical trainees can now experience this experience anytime, anywhere. It is known that augmented reality works with smartphones. It is expected to have a stronger future. AR technology can enter the health care industry at different levels. Augmented reality is different from virtual reality in that users don't lose contact with the reality around them. It provides them with interactive information by displaying the camera live on smart phone screens and these powers are particularly relevant to health care. One example is the ability of augmented reality to assist patients in eye conditions. There is an Eye Decision application that doctors can show the simulation of the disease in certain cases. This enables patients and service providers to better understand the problem. It improves how management manipulates them. There are charities that use virtual reality technology such as the National Autism Society in the UK, which provided a VR film to convey the life of autistic patients [7].

5.5 Reliable, real time remote monitoring

With IoT devices, healthcare providers can monitor patients and gather all needed information that can used to improve personalized and preventive care. Despite the benefits, remote monitoring technology usage is limited by the capacity of the network that make the data difficult to handle. Slow network speeds and unreliable connections could mean doctors are unable to get the real time data they need to make quick healthcare decisions. But with 5G which has lower latency and higher capacity. Healthcare systems can offer remote monitoring for more patients. Providers will be confident that they will receive the data they need in real time and can provide the care their patients need and expect [7].

5.6 Artificial intelligence

Artificial intelligence is the cornerstone of the use of the fifth-generation technology, perhaps the most important uses of this technology are the medical use in conjunction with the Internet of Things. Recently the surgery was performed using this technique where the surgeon in one country and the patient in another country and because the speed of data transfer is crucial and determines the life of a person came to the fifth generation technology to meet this desire, which led to the success of the operation with less time and less cost and without the need to transfer the patient that the presence of Doctor [34].

6. DISADVANTAGES OF USING THE 5G TECHNOLOGY IN IOT

Every development or progress of mankind in any field must have some negatives that directly or incidentally affect this green planet. Since communication technology and the digital world is the greatest scientific revolution brought by human beings, there must be negatives that would cause a problem in the long run 5G technology is probably one of these problems that has been used in the Internet of Things. Since the use of this technique is under trial and the possibility of its involvement in the computerization and control of things is inevitable, so it is difficult to predict the negative effects early. But from similar experiences, it is possible to predict the dangers of this communicative mutation, which will enter and control every detail of life. Figure 3 shows a public reaction to 5G.

Figure 3: Public reaction to 5G in a developed country

The mediator to the congestion of networks and the frightening spread of the devices that communicate between them through these networks notes that the carrier medium of these electromagnetic oscillations does not hinder anything in order to reach the recipient. It is worrying about the impact of these vibrations on the brain, which is based on weak electrical nerve signals (Figure 4).

Figure 4: Electromagnetic field impact on human brain

In a scientific paper published by Dr. Annette Deyhle on the dangers of being exposed to such data-transferable electromagnetic fields such as 5G technology, he says " The electromagnetic fields generated by power supply systems, telecommunications, appliances, computers and other technology produced by humans are extremely powerful and in some cases have been associated with increased incidence of cancer, heart disease, depression and other diseases. Exposure to strong electromagnetic fields in residential areas and in certain occupations has been documented as significantly increasing the incidence or risk of the listed diseases. Certain groups of people such as the elderly, children, women who are pregnant and the weak have been found to be more sensitive or susceptible to adverse effects from these fields than the rest of the population [8] .

However, awareness of these dangers of the disease is spreading among the general public. Perhaps one of the best examples of what the Swedes did last month. Where they held demonstrations against the fifth generation and used in the country where published: "Opponents of the introduction of fifth generation cellular network technology (5G) in Switzerland gathered in Bern on Saturday to protest against “forced radiation”. Several speakers at the parliament square warned of considerable risks to health, the environment, democracy and safety associated with mobile communications in general and the introduction of 5G in particular. They called for a national moratorium on 5G and the creation of radiation-free zones. The demonstration - scheduled between 4:30 and 6:30 in the afternoon - was coordinated by the organization

Frequencies that was formed after the first significant anti-5G demonstration this May in Bern. “We are for low-radiation living spaces and for freedom of choice with regard to the means of communication,” the organization stated in a communiqué. Frequencies claims that only 20% of all mobile connections are made outdoors and therefore want a low-radiation solution based on the fiber-optic network for indoor use. They also want mobile masts to only serve mobile connections outdoors and radiate much weaker signals [9].

6.1 Supply Chain

Though equipment designed and manufactured by trusted suppliers is not immune to manipulation, equipment produced or otherwise handled by untrusted partners presents more risk of malicious or inadvertent introduction of vulnerabilities. Counterfeit components and the insertion of malicious software and hardware are a few examples of such vulnerabilities. Even if ICT components are purchased from trusted companies, the company may maintain production facilities overseas which may be vulnerable to supply chain risk. Compromised components could affect network performance and compromise the confidentiality, integrity, and availability of network assets. Furthermore, compromised devices may provide malicious actors with persistent access to 5G networks and the capability to intercept data that routes through the devices as shown in Figure 5. [10]

Figure 5: Electromagnetic field impact on human brain

Compromised devices may infect connected computers, phones, and other devices with malware and may have data rerouted, changed, or deleted. Untrusted companies that have significant international market share within telecommunication networks may introduce risks even if they do not have a large presence within the U.S networks. Therefore, even if the U.S. network were completely secure, data traveling overseas may pass through untrusted telecommunication networks and potentially be vulnerable to interception, manipulation, disruption, or destruction [10].

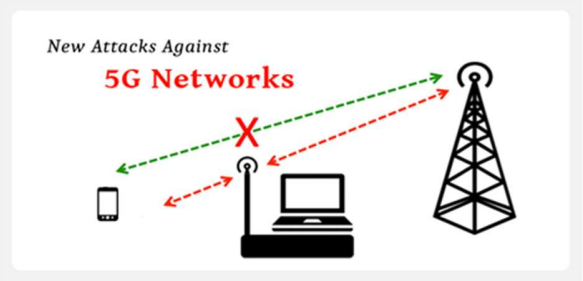

Figure 6: 5G vulnerability

6.2 Network Security

Component manufacturers and service providers are developing technologies and security specifications to mitigate vulnerabilities in wireless networks. 5G will push ICT components and data management to the edge of the network, which will enhance security through network slicing, edge computing power, device management, authentication functions, and automated threat detection and response. Network slicing, if implemented properly, should limit an attacker’s ability to access critical areas within a network.

The migration of functions to the edge of the network will increase computing and network management power, which will secure traffic and prevent intrusions to core network systems. Despite 5G’s security improvements, as with all new technologies it is likely that 5G equipment and protocols will inadvertently contain vulnerabilities that could expose components and data to exploitation. Even as security updates are released, some entities may be slow to implement them for a variety of reasons, such as the potential impact to operations from taking systems offline. Therefore, any vulnerabilities inherent in 5G technologies may be exploitable even after fixes are developed.

5G network technologies are being designed to be more secure than previous mobile network generations, and organizations and standard bodies continue to enhance security in previous wireless networks, including protecting core networking systems from malicious edge networking devices. 5G technologies will, however, initially be overlaid on the existing 4G Long-Term

Evolution (LTE) network that contains legacy vulnerabilities.

These could be inadvertent, technical vulnerabilities inherent to the network, or due to 5G technologies' integration into untrusted 4G and 4G LTE networks [35-37]. The inheritance of security settings, permissions, and technical specifications from an untrusted core network may negate built-in 5G device security [10].

6.3 Loss of Competition and Trusted Options

Section 889 of the 2019 National Defense Authorization Act (NDAA) prohibits federal agencies from procuring certain equipment and services from Huawei and ZTE, two of the world's largest manufacturers of telecom equipment although limited in their share of the U.S. telecommunications market, these companies have significant market share internationally and may be less likely to participate in interoperability efforts. This is evidenced by the lack of involvement in the O-RAN Alliance, a collection of telecommunication organizations that work towards open and interoperable architectures.70 Communication network operators that previously purchased 4G equipment from a company like Huawei that uses proprietary interfaces in their technologies cannot easily use another vendors' equipment for 5G. The proprietary interfaces lock customers into a single vendor procurement cycle, which could negatively affect competitive balance within the 5G market. Loss of market share could limit trusted companies' ability to invest in research and development and could eventually drive them out of the market. Loss of trusted suppliers could potentially lead to a situation where untrusted entities are the only options. Custom 5G equipment, that does not meet interoperability standards, may be more difficult to update and repair. Poorly developed code makes vulnerability management significantly more difficult and can lead to unsupportable software. If a critical outage occurs, systems, programs, and data with custom code are more difficult to recover and may lead to extended outage times. Slowing or blocking interoperability between networks could also substantially delay or increase the cost of deploying 5G. A customer currently using Huawei equipment who wants to use a new vendor for 5G may have to first remove and replace all their equipment from the network [10].

The emergence of the 5th generation wireless standard for telecommunications (5G) will enable the Internet of Things (IoT), a huge network of interconnected devices that can be utilized in almost every aspect of our daily lives, either that is in healthcare, transportation, environmental monitoring, and so on. As good as it sounds though, individuals with malicious intent will always be around to try and compromise what has been built for their gain. Therefore, nothing can be accomplished unless the system and communication between devices are secured [11]. As 5G begins to be widely available, several things will happen: 5G also will also have an influence beyond connecting endpoint devices. when we will come to the IoT devices will be included to track devices and other users, monitor inventory and collect user and device information [12].

7. SECURITY IMPLICATIONS FOR 5G AND IOT

With threats and attacks, it will be a major challenge the rapid and improved expansion of Internet-based devices and edge-based computing. They will not necessarily be connected to a central network. With so many devices connected through a networked edge environment, any one of them can become the weakest link between them in the security path. To keep communicating and the devices are as secure as possible [12].

- To do this, everything connected to the enterprise ecosystem needs to be identified, criticality rated, and their state confirmed. Then, all requests for access to network resources will need to be verified, validated and authenticated [12].
- Security should conjointly support elastic, edge-to-edge hybrid systems combining well-tried ancient ways with new approaches.

  While network segmentation may be a well-tried technique for holding cybersecurity risks and protect sensitive resources, recent ways might not be best suited to a 5G world.

  New segmentation ways can navigate native and remote resources that blend segments that organizations might or might not have management.

  IT groups can value a way to manage the complexness of multiple co-managed systems as they implement 5G networks and public cloud services [12].

- Sharing threat intelligence, correlating event information and supporting automatic incident response would require security technologies to be deeply integrated.
  This will need the event and adoption of a comprehensive, fabric-based security design.
  Machine learning, computing and automation are going to be key to fast decision-making, thereby closing the gap between detection and mitigation [12].

These are just a few of the security implications resulting from the adoption and deployment of 5G networks. But that's simply the beginning of the impact of this new era of networking and computing. Security will also need to address the following scenarios [12]:

- Automated network application lifecycle management would require security tools to not solely be high activity however additionally extremely adjustive to confirm that constant innovation includes consistent protection.
  It will additionally need organizations to transition from a DevOps model to a DevSecOps model to confirm that security is integrated directly into the event strategy [12].
- Support for cloud-optimized distributed network applications would force security to maneuver seamlessly between and across absolutely fully completely different network ecosystems whereas not losing track of workflows or dropping security utility [12].
- Digital transformation can generate Brobdingnagian amounts of latest knowledge, most of which can be encrypted. Encrypted data currently constitutes more than 70% of network traffic. That share can solely grow as cryptography is employed to shield knowledge moving through open network environments. This will need superior security tools in IoT and different edge devices that may examine encrypted traffic at each speed and scale
- New methods, like network slicing, can change organizations to a lot of with efficiency consume resources moving through large information environments.
  This will additionally need segmentation and edge-based micro-segmentation to safeguard crucial resources whereas uninflected them from open and fewer secure environment.

6. CONCLUSION

This research focuses on the issue that how important the fifth generation (5G) is in the Internet of Things in various details of our daily lives, regardless of the advantages and disadvantages that may exist in the future. This speed of information transfer and use will undoubtedly make human life better and will bring quality in various areas of life. On the other hand, the dangerous aspect of the proliferation of this computer revolution should not be overlooked, because even a simple error will cost a lot, especially since these technologies will be secondary life or in other words the mastermind of all the tasks of the individual and society. The work is a beacon for those who are aiming to research in this field.

REFERENCES

[1] J. Brockman, "HOW IS THE INTERNET CHANGING THE WAY YOU THINK?," Raqs Media Collective,Edge, Mon Oct 2019. [Online]. Available: https://www.edge.org/responses/how-is-the-internet-changing-the-way-you-think. [Accessed Mon Dec 09 2019].

[2] S. F. III, "What is 5G? The business guide to next-generation wireless technology," ZDNet, September 19 2019. [Online]. Available: https://www.zdnet.com/article/what-is-5g-the-business-guide-to-next-generation-wireless-technology/. [Accessed Mon Dec 2019].

[3] T. Seals, "How to Approach the Security Implications," threat post, September 26 2019. [Online]. Available: https://threatpost.com/5g-and-iot-how-to-approach-the-security-implications/148681/. [Accessed Mon Dec 2019].

[4] IOTSWC, "ADVANTAGES OF 5G AND HOW WILL BENEFIT IOT," IOT SOLUTIONS WORLD CONGRESS, 2019. [Online]. Available: https://www.iotsworldcongress.com/advantatges-of-5g-and-how-will-benefit-iot/. [Accessed Mon Dec 9 2019].

[5] M. Moore, "5G and smart cities: everything you need to know," techradar, June 12 2019. [Online]. Available: https://www.techradar.com/news/5g-and-smart-cities-everything-you-need-to-know. [Accessed Mon Dec 9 2019].

[6] A. B. E. Team, "How 5G will impact the transportation industry," AT&T Business, [Online]. Available: https://www.business.att.com/learn/tech-advice/how-5g-will-impact-the-transportation-industry.html. [Accessed Mon Dec 9 2019].

[7] A. B. E. Team, "5 ways 5G will transform healthcare," AT&T Business, [Online]. Available: https://www.business.att.com/learn/updates/how-5g-will-transform-the-healthcare-industry.html. [Accessed Mon Dec 9 2019].

[8] P. a. G. R. T. Annette Deyhle, "Influence of Geomagnetism and Schumann Resonances on Human Health and Behavior,"

HeartMath Institute, [Online] available: https://www.heartmath.org/gci-commentaries/influence-of-geomagnetism-and-schumann-resonances-on-human-health-and-behavior/. [Accessed Mon Dec 9 2019].

[9] K. /. A. Anex, "Several thousand protest against 5G in Swiss capital," swissinfo.ch/, SEP 21 2019. [Online]. Available: https://www.swissinfo.ch/eng/radiation-fears_several-thousand-protest-against-5g-in-swiss-capital/45246224. [Accessed Mon Dec 9 2019].

[10] I. S. D. CISA Cybersecurity Division (CSD), "OVERVIEW OF RISKS INTRODUCED BY 5G ADOPTION IN THE UNITED," CISA Cybersecurity Division, July 31 2019. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf. [Accessed Mon Dec 9 2019].

[11] V. Hadjioannou, "Security in IoT with 5G," *Internet of Things (IoT) in 5G mobile technologies,* pp. 371 ,375 , 378, 2016.

[12] J. Nguyen-Duy, "What Are the Security Implications for 5G and IoT?," fortinet, January 16 2019. [Online]. Available: https://www.fortinet.com/blog/industry-trends/the-security-implications-for-5g-and-iot.html. [Accessed Dec 4 2019].

[13] S. Dash, S. Biswas, D. Banerjee, A. Rahman, "Edge and Fog Computing in Healthcare – A Review", Scalable Computing 20(2):191-206, May 2019.

[14] A. Rahman, K. Sultan, S. Das, M.A. Khan, "Management of Resource Usage in Mobile Cloud Computing", International Journal of Pure and Applied Mathematics, Vol. 119 No.16, pp. 255-261, 2018.

[15] A. Rahman et al (2018) A Comprehensive Study of Mobile Computing in Telemedicine, Advanced Informatics for Computing Research, pp. Proc: Second International Conference, ICAICR 2018, Shimla, India, July 14–15, 2018.

[16] F.A. Alhaidari, A. Rahman, M.A.A. Khan, S. Das, "Motion Detection in Digital Video Recording Format with Static Background", SEAHF'19, 2019.

[17] N. Ahmed, A. Rahman, S. Dash, M. Mahmud, "Flood Prediction Techniques Based on Geographical Information System using Wireless Sensor Networks", Springer LNNS: International Conference on Data and Information Systems, 2017.

[18] A. Rahman, "Memetic Computing based Numerical Solution to Troesch Problem", Journal of Intelligent and Fuzzy Systems, 37(1):1545-1554, 2019.

[19] F.A. Alhaidari, A. Rahman, "Telecommunication Networks in Disaster Management: A Review", Journal of Communications, Vol. 14, No 6, pp. 432-447, June 2019.

[20] M.H. Salam, S. Memon, L. Das, A. Rahman, Z. Hussain, R.H. Shah, N.A. Memon, "Sensor based Survival Detection System in Earthquake Disaster Zones", International Journal of Computer Science and Network Security, vol. 18, no. 5, pp. 46-52, 2018.

[21] D. Jin, C. Hannon, Z. Li, P. Cortes, S. Ramaraju, P. Burgess, N. Buch, and M. Shahidehpour, "Smart street lighting system: A platform for innovative smart city applications and a new frontier for cyber-security", The Electricity Journal, vol. 29, no. 10, pp. 28-35, 2016.

[22] J. Cubo, A. Nieto and E. Pimentel, "A Cloud-Based Internet of Things Platform for Ambient Assisted Living", *Sensors*, vol. 14, no. 8, pp. 14070-14105, 2014.

[23] L. Bittencourt, R. Immich, R. Sakellariou, N. Fonseca, E. Madeira, M. Curado, L. Villas, L. DaSilva, C. Lee and O. Rana, "The Internet of Things, Fog and Cloud continuum: Integration and challenges." In Internet of Things, vol. 3, no. 4, pp. 134-155, 2018.

[24] S. Abdelwahab, B. Hamdaoui, M. Guizani and T. Znati, "Cloud of Things for Sensing-as-a-Service: Architecture, Algorithms, and Use Case," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1099-1112, Dec. 2016.

[25] Carr, Jillian and Doleac, Jennifer L., The Geography, Incidence, and Underreporting of Gun Violence: New Evidence Using Shotspotter Data (April 26, 2016).

[26] Dang, L. M.; Piran, Md. J.; Han, Dongil; Min, Kyungbok; Moon, Hyeonjoon. 2019. "A Survey on Internet of Things and Cloud Computing for Healthcare." Electronics 8, no. 7: 768.

[27] A. Rahman, Dash, S., Luhach, A.K. et al. A Neuro-fuzzy approach for user behaviour classification and prediction. J Cloud Comp 8, 17 (2019) doi:10.1186/s13677-019-0144-9.

[28] https://www.decluttr.com/mobile-device-secondhand-market-analysis/ (visited 14 December 2019).

[29] Razvi, S. M., Abdullah Al-Dhelaan, Mznah Al-Rodhaan and Riman A. Bin Sulaiman. "IoT Cloud-Sensor Secure Architecture for Smart Home." Proceedings of Int'l Conf. Security and Management (SAM'15), 2015.

[30] Sherif Abdelwahab et al. "Cloud of Things for Sensing-as-a-Service: Architecture, Algorithms, and Use Case" IEEE Internet of Things Journal, Volume: 3 , Issue: 6 , Dec. 2016.

[31] Thomas Renner, Andreas Kliem, Odej Kao, "The Device Cloud -Applying Cloud Computing Concepts to the Internet of Things" 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence & Computing and 2014.

[32] Y.S. Patel and T. Parmar, "Cloud of Things: A State-of-the-art Review on Integration of Internet of Things with Cloud Computing", Proc. of National Conference on Contemporary Computing (NC3-2016), International Journal of Computer Applications, pp. 37-41, 2016.

[33] A. Rahman, M.I.B. Ahmed, "Virtual Clinic: A CDSS Assisted Telemedicine Framework", Chapter 15, Telemedicine Technologies, 1st Edition. Elsevier, 2019.

[34] A. Farahzadi, P. Shams, J. Rezazadeh and R. Farahbakhsh, "Middleware technologies for cloud of things: a survey", Digital Communications and Networks Volume 4, Issue 3, pp. 176-188, 2018.

[35] A. Rahman, Qureshi I.M., Malik A.N., Naseem M.T., "QoS and Rate Enhancement in DVB-S2 using Fuzzy Rule Base System", Journal of Intelligent & Fuzzy Systems (JIFS), vol. 30 (1), pp. 801-810, 2016.

[36] A. Rahman, Qureshi I.M., Malik A.N., Naseem M.T., "Dynamic Resource allocation for OFDM Systems using DE and Fuzzy Rule Base System", Journal of Intelligent & Fuzzy Systems (JIFS), vol. 26 (4), pp. 2035-2046, 2014.

[37] A. Rahman, Qureshi I.M., Malik A.N., Naseem M.T., "A Real Time Adaptive Resource Allocation Scheme for OFDM Systems using GRBF-Neural Networks and Fuzzy Rule Base System", International Arab Journal of Information Technology (IAJIT), Vol. 11, no. 6, pp. 593-601, 2014.

[38] A. Rahman, "Efficient Decision Based Spectrum Mobility Scheme for Cognitive Radio Based V2V Communication System," Journal of Communications, vol. 13, no. 9, pp. 498-504, 2018. Doi: 10.12720/jcm.13.9.498-504.

[39] P. Charoenporn, Smart logistic system by IOT technology. In Proceedings of the 6th International Conference on Information and Education Technology (ICIET '18). ACM, New York, NY, USA, 149-153, 2018.

[40] A. Rahman and J. Alhiyafi, "Health Level Seven Generic Web Interface", J. Comput. Theor. Nanosci. 15, 1261–1274, 2018.