International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 3, May-Jun-2022, ISSN (Online): 2395-566X

A Cyber Security of IOT in 6G Era

Mr. R Vignesh, Asst. Prof. Ms. Sumaiya M
Department of Information Technology,
Rathinam College of arts and science,
CoimbatoreTN,India
Vigneshr.mit21@rathinam.in, sumaiya.cs@rathinam.in

Abstract- With the deployment of more 5g networks, the limitations of 5g networks have been found, which undoubtedly promotes the exploratory research of 6G networks as the next generation solutions. These investigations include the fundamental security and privacy problems associated with 6G technologies. Therefore, to combine and solidify this foundational research as a basis for future investigations, we have prepared a survey on the status quo of 6G security and privacy.

Keywords- 6G, IoT Cybersecurity,5G & IoT,5G pros & cons, evolution of networks, working of 6G .

I. INTRODUCTION

6G (6th era remote) is the replacement to 5G cell innovation. 6G organizations will want to use higher frequencies than 5G organizations and give significantly higher limit and much lower dormancy. One of the goals of the 6G web is to help one microsecond dormancy interchanges. This is multiple times quicker or 1/1000th the inactivity than one millisecond throughput.

The 6G innovation market is supposed to work with huge upgrades in the space of imaging, presence innovation and area mindfulness. Working related to manufactured reasoning (AI), the 6G computational foundation will want to recognize the best spot for figuring to happen; this incorporates choices about information ability, handling and sharing.

Similarly, as the leap from 4G to 5G addresses an extension of ranges used and presentation of new frequencies, so will the advancement somewhere in the range of 5G and 6G interchanges. While 5G use mm Wave in the microwave recurrence range, 6G will exploit much more modest frequencies at the Terahertz (THz) band, which is normally alluded to as 100 GHz to 3 THz.

II. WHEN WILL 6G BE AVAILABLE?

6G web is supposed to send off economically in 2030. The innovation uses the circulated radio access organization (RAN) and the terahertz (THz) range to increment limit, lower idleness and further develop range sharing. While a few early conversations have occurred to characterize the innovation, 6G innovative work (R&D) exercises began vigorously in 2020.

6G will require improvement of innovative portable correspondences innovations, for example, mental and exceptionally secure information organizations. It will likewise require the extension of phantom transmission capacity that is significant degrees quicker than 5G.

China has sent off a 6G test satellite offered with a terahertz framework. Innovation goliaths Huawei Technologies and China Global allegedly plan comparative 6G satellite send-offs in 2021. A considerable lot of the issues related with conveying milli meter wave radio for 5G should be settled in time for network originators to address the difficulties of 6G.

III. DO WE EVEN AND NEED 6G?

There are several reasons we really want 6G innovation. They incorporate the accompanying:

1. Technology Convergence:
The 6th era of cell organizations will coordinate beforehand dissimilar advancements, for example, profound learning and huge information examination. The presentation of 5G has made ready for a lot of this assembly.

2. Edge figuring:
The need to convey edge figuring to guarantee throughput and low inertness for ultrareliable, low-inactivity correspondences arrangements is a significant driver of 6G.

3. Internet of things (IoT):
Another main thrust is the need to help machine-to machine correspondence in IoT.

4. Elite execution registering (HPC):
A solid relationship has been recognized among 6G and HPC. While edge registering assets will deal with a part of the IoT and versatile innovation information, a lot of it will require more incorporated HPC assets to do the handling.

IV. DEFINE IOT CYBERSECURITY?

IoT (the Internet of Things) is the idea of interfacing articles and gadgets of distinct kinds over the web. Progressively more items and frameworks in our lives are becoming installed with network availability and figuring power to speak with comparatively associated gadgets or machines. Makers, service organizations and production network associations, (for example, auto producers, power organizations and transportation organizations) likewise love their IoT. This type of IoT, however, is alluded to as functional innovation (OT).

A term related with OT is modern control framework (ICS). Modern control frameworks incorporate gadgets and systems administration ability that allows robots, wind turbines and compartment boats to proficiently work. On the off chance that an IoT gadget is used to control an actual framework, for example, a part in the power network or a gadget on the production line floor, being an OT device is said.

The issue is, cybercriminals love IoT and OT gadgets, as well. More than we do. The significant issue with IoT and ICS gadgets is that they make it workable for an individual or organization to direct new and different cyberattacks. Programmers will track down pernicious ways of impeding the tasks of an organization, city or even country.

Network protection experts often allude to this reality by saying that IoT expands the assault surface that programmers can take advantage of. Security experts know this and are the ones who aid with dealing with the later security chances. Network safety experts often allude to this reality by saying that IoT builds the assault surface that programmers can take advantage of. Security experts know this and are the ones who aid with dealing with the later security gambles.

V. INTERNET OF THREATS

The main flood of IoT security assaults hit in 2016 when the Mirai Botnet compromised the security on various IoT gadgets, including IP cameras and switches and transformed the gadgets into midway controlled botnets. These botnets made a troublesome bottleneck that upset admittance the Internet for a great many clients around the world.

Organizations across an expansive scope of ventures are conveying IoT answers for make a more significant level of perceivability and further developed efficiencies. Aggressors are watching out for better approaches to think twice about and get close enough to information stores and frameworks. From route frameworks on associated vehicles to savvy clinical gadgets, any IoT framework could turn into an ideal aim for programmers.

Fig 1. IoT framework

VI. WHAT ARE IOT ACCESS POINTS TO HACKERS?

Since IoT is a perplexing organization holding various parts, it gives programmers more than one mark of passage:

1. Edge:
The edge incorporates sensors and actuators that cooperate with the actual world and our environmental factors.Since, talking, there is strain on makers to continue to carry out new gadgets and administrations, less consideration goes into making them secure. Harvard Business Report's investigation into the matter cases that 80% of associations do not regularly test their IoT applications for security weaknesses. This implies the actual gadgets are the most defenceless, not least on the grounds that the greater part of the simple gadgets does not uphold programming refreshes. This leaves gadgets like cameras and DVR players, helpless against malware.

2. Communication Networks:
Communication networks are the entryways that interface gadgets together. Hacking Bluetooth networks is a typical procedure of seizing the honesty of the gadget. In Belgium, for research purposes, a gathering had the choice to hack a Tesla Model X's Bluetooth interact with a gadget costing an aggregate of $195. The specialists guaranteed they had the possibility to think twice about framework 5 meters away, accessing the vehicle's locking framework.

3. The cloud:
The cloud is an information extra room where IoT gadgets' information is gathered and handled on outsider premises. By gaining admittance to the cloud, even though you will not have the possibility to control the gadgets, as such, you will approach valuable data that they gather. In 2021, Russian programmers had the possibility to get close enough to classified data and traded email strings of more than 100 U.S organizations and a few government offices, like the Treasury, Energy, Justice, and Homeland Security divisions.

VII. WHY IOT SECURITY IS IMPORTANT?

IoT networks are expanding in number. They are not simply bound to our homes — several savvy indoor regulators here, a few shrewd lights there. They are filling in height in medical services, savvy urban areas arrangements, the retail area, and assembling, among different areas.

As the productivity and adequacy of IoT gadgets and organizations builds, so will their effort into added areas, and thus, so will society's reliance on their usefulness. Also, since more organizations could move on the web (with internet business supplanting physical stores, for instance) keeping their uprightness will be foremost in staying away from shutdowns.

VIII. 5G AND IOT

It addresses an essential change in the versatile biological system, releasing a strong blend of phenomenal speed, extended data transmission, low idleness, and expanded power effectiveness that is driving billions of added associations in the following five years and changing our reality.

Fig 2. GSMA.

As wrote down by the GSMA, 5G associations are supposed to develop from 10 million toward the finish of 2019 to 1.8 billion by 2025 - and we are well coming! In June 2020, the Global Mobile Suppliers Association (GSA) distinguished 81 Mobile Network Operators (MNOs) in 42 nations who had sent off 5G business administrations, and more than 385 MNOs in 125 nations were putting resources into 5G turn of events.

1. **How did 5G come about?**

The main emphasis of remote innovation, 1G, cut the line for voice calls introducing another time of versatility.

- Whenever 2G arose supporting voice and information, machine-to-machine interchanges (M2M) empowered basic arrangements, for example, telematics, remote seeing and control and that is just the beginning.
- When 3G advanced, web-perusing incredibly extended opportunities for the IoT, and development took off.
- Along came higher-speed information and video real time of 4G alongside the approach of distributed computing. This released a tsunami of creative mind and advancement that requested higher transfer speed, more noteworthy limit, more grounded security, and consistent availability with lower dormancy. Enter 5G.

2. Pros of 5G:

2.1 High speeds: 5G works quicker on cell phones and different gadgets when contrasted with 4G and 4G LTE. It allows clients to download motion pictures, recordings, and music in seconds instead of minutes. The organization has 20 Gbps speed empowering associations to involve something similar for administrations, for example, robotization, high level web conferencing, and so on.

2.2 Low latency: 5G has low inactivity when contrasted with 4G that will uphold new applications like AI, IoT, and augmented reality productively. Not just that, it empowers cell phone clients to open a website page and peruse things with next to no issues.

2.3 Increased ability: 5G can convey up to multiple times more limit than 4G. It allows organizations to switch among cell and Wi-Fi remote procedures that will aid a ton with encountering better execution.

2.4 More bandwidth: One of the principal benefits of 5G is that it increments more transmission capacity that will aid with moving the information quickly. Besides, cell phone clients can guarantee a quicker association with more data transmission after picking a 5G organization

2.5 Powering innovation: 5G innovation is the ideal decision for associating with an entire scope of various gadgets including robots and sensors. It gives ways of fueling the reception of IoT permitting businesses to improve their efficiency and different things.

2.6 Less tower congestion: 4G cell networks often get blocked which will bring about different issues while getting to significant information. Then again, 5G organizations allow clients to stay away from them because of better speed and more data transmission.

3. Cons of 5G:

3.1 Limited global coverage: The fundamental weakness of 5G is that it has restricted worldwide inclusion and is accessible just in unambiguous areas. Only urban communities can help a ton from 5G organization and far off regions may not get the inclusion it for certain years. Besides, the costs for setting tower stations are high when contrasted with different organizations.

3.2 Decreased broadcast distance: Although 5G works quickly at rapid, it will not go as far when contrasted with 4G. In addition, tall structures and trees might impede the recurrence of the 5G organization that will bring about different issues.

3.3 Upload speeds: 5G advances permit cell phone clients to guarantee high download speeds. Then again, the transfer speeds are not north of 100 Mbps when contrasted with 4G. Moreover, cell phones need better battery innovation while using a 5G association. Many telephone clients say that they experience more intensity on their gadgets while running 5G.

3.4 Cybersecurity: Cybersecurityis one of the disadvantages of 5G on the grounds that it will bring about hacking. The extension in the transmission capacity empowers hoodlums to take the information base easily. In addition, it uses programming that prompts weak assaults. As 5G associates with added gadgets, the possibilities of assaults are exceptionally high. Consequently, organizations and organizations ought to safeguard their framework with a security activities focus that will bring about extra costs.

IX. IOT'S MULTIFACETED SECURITY RISKS

2020 Cybersecurity Insiders overview uncovered that 72% of associations met an expansion in endpoint and IoT security occurrences recently, with the main three issues being malware (78%), unreliable organization and remote access (61%), and compromised accreditations (58%).

An IoT organization can incorporate enormous number of shrewd gadgets — and every one is a door to (or focus of) digital assaults. When one gadget is hacked, it is conceivable an assailant might abuse that gadget and move along the side through the organization, getting to delicate records, licensed innovation, and other associated gadgets.

Whenever you ponder IoT applications in medical care, brilliant urban communities, and other strategic administrations, the online protection gambles become significantly clearer. Simply envision an aggressor assuming command over an associated vehicle or dealing with somebody's pacemaker!

As IoT speeds up in a 5G-or 6G empowered worlds, organizations should put resources into security drives to safeguard all passage focuses. Also, since networks give the establishment to IoT, it is basic to guarantee their unwavering quality and security. At last, while digital availability obligation should not fall exclusively on the end-client, organizations that influence IoT ought to teach representatives on digital cleanliness.

X. OPEN SOURCE CREATES NEW SECURITY THREATS

5G and future 6G organizations will be worked with open-source programming and norms, considering quicker and more incessant executions and, thusly, a more extensive assault surface.

Open source's expanded straight forwardness implies that anybody, including cybercriminals, will want to investigate the code to recognize and take advantage of weaknesses. Incidentally, as a new 5G Americas report (PDF) calls attention to, the very straightforwardness that expands hazard can likewise make open source advances safer.

Expanded code perceivability empowers a lot bigger local area of engineers to distinguish, fix, and update weaknesses. To get ready for 5G, organizations need to operationalize how they will oversee and follow up on weaknesses and patches hailed by the open source local area.

XI. SECURING 5G AND 6G IS A TOP BUSINESS PRIORITY

These forthright security ventures and digital constancy drives are savvy business procedures for all gatherings taking part in 5G and in the end 6G. Staying more than one stride in front of digital foes will guarantee that organizations, clients, representatives, and customers, will want to receive the rewards of the following ages of organizations.

XII. IMAGINE A 6G WORLD

In the business world, the force of 6G will change the way we work and meet. Consider having high-loyalty portable 3D images at the dash of a button. You can have a discussion with an associate as though you were both finding a spot at a similar table in the corner coffeehouse. Gatherings can go genuinely virtual, decreasing the requirement for long stretch flights and huge in-person meetings.

Medication can utilize 6G to give quicker crisis reaction to more extensive inclusion regions, diagnosing and endorsing treatment across landmasses. Specialists can prepare and administer colleagues in nearby networks the nation over, giving quicker and better clinical treatment. What is more, we should not do not remember web-based gamers, who have often stretched the boundaries of augmented reality. With the speed of 6G, internet games and rivalries can be changed into genuinely vivid Extended Reality (XR), complete with brilliant wearables, headsets, and even embeds.

XIII. EVOLUTION OF SECURITY AND PRIVACY ISSUES IN WIRELESS SYSTEMS

1. 1G:
The 1G organization was presented during the 1980s and intended for voice administrations. It depends on simple transmissions to communicate data and has no settled remote norm. This prompts many inconveniences, including hard handovers, an absence of safety and protection certifications, and low transmission productivity. Telephone administrations are not scrambled, implying that information transmissions and telephone discussions neither can nor be secure nor private. Subsequently, the whole organization and its clients face critical security and protection challenges, including cloning, listening in, and unlawful access.

2. 2G:
The 2G organization depends on advanced regulation strategies, like Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA), which can uphold both voice and short message administrations. The most significant and broadly involved versatile correspondence standard in 2G is GSM (Global System for Mobile Communications). The motivation behind the GSM is to make the framework as secure as a Public Switched Telephone Network (PSTN).

Its security and security administrations include: 1) namelessness, 2) verification, 3) flagging assurance, and 4) client information insurance. Obscurity is done using transitory identifiers, which make it challenging to follow the client's genuine personality. Nonetheless, the genuine character should be used when the gadget is first turned on, after which a brief identifier is given. Validation is used by network administrators to recognize clients.

The confirmation part is an encryption-based approach alluded to as "challenge and reaction". Flagging and client information security are likewise carried out using encryption, and the Subscriber Identity Module (SIM) assumes a significant part in the encryption keys. There are two principal techniques for protecting security for clients: the first is radio way encryption, and the second is Temporary Mobile Subscriber Identity (TMSI).

3. 3G:
The 3G organization arose in 2000 to give "high velocity" information transmission and admittance to the web, and that implies no less than 2 Mbps. Nonetheless, this speed could uphold progressed administrations that are unrealistic in the 1G and 2G organizations, including web perusing, TV web based, and video administrations. The security of the 3G framework depends on the 2G advances. In other words, GSM and different components joined in 2G ended up being important, while extra vigorous security components likewise should have been embraced. The 3G additionally lessens a part of the security shortcomings of the 2G and presents the Authentication and Key Agreement (AKA) as well as two-way verification.

In addition, the third Generation Partnership Project (3GPP) gives a total security framework overseeing access that has two sections: air interface security, which is used to safeguard clients and the flagging data communicated by remote connections; and the arrangement of client network confirmation to guarantee the actual unwavering quality of clients and the two sides of the organization. Concerning security, 3GPP combines some endorser protection necessities for 3G clients, like secrecy of client character, area, and detectability.

Nonetheless, the 3G organizations are yet defenceless against dangers related with the Internet Protocol (IP) traffic and encryption keys. Further, the radio connection point between the terminal gear and the help network likewise gives open doors to a bunch of assaults. Dangers connected with remote point of interaction assaults fall into the accompanying classifications: 1) unapproved admittance to information; 2) dangers to respectability; 3) Denial of Service (DOS); 4) unapproved admittance to administrations. Protection issues relate to sorts of assaults, for example, AKA blunder messages, intended to annihilate client characters and private or delicate data.

4. **4G:**
The 4G of Long-Term Evolution (LTE) networks were presented in 2009, giving the information pace of up to 1 Gbit/s on the downlink and up to 500 Mbits/s on the uplink. These organizations give better range productivity and diminished inactivity, and that implies they can meet the prerequisites of innovative applications, for example, Digital Video Broadcasting (DVB), High-Definition Television (HD TV) content and video talk. The LTE incorporates a blend of existing and new innovations, for example, Coordinated Multi-Point Transmission and Reception (CoMR), Multiple Input Multiple Output (MIMO) and Orthogonal Frequency Division Multiplexing (OFDM).

5. 5G:
As we stand near the very edge of the 5G organization, we can expect quicker speeds, more complete frameworks, and safer designs. The fundamental progression of 5G organizations is to work with the association of a rising number of gadgets and offer excellent types of aid for all gadgets all the while. In addition, the upheld gadgets will not be restricted to cell phones; different gadgets like IoT hardware can likewise interface with the organization. The security and protection issues in 5G organizations can best be separated by network design and, more explicitly, into three levels of the engineering: the entrance organizations, the backhaul networks, and the centre organization. In access organizations, the variety of hubs and access

instruments bring about some new security challenges as handovers between various access advances increment the gamble of assault.

Taking everything into account, backhaul correspondence happens between the base station and the centre organization, which can be acknowledged through remote stations, microwaves and occasionally satellite connections, as well as wired lines. Without any associations between gadgets, these organizations experience less security and protection dangers than access organizations.

The weaknesses they truly do have come from changed components of the entrance organization, like EUTRAN Node B (EnBW) or the Mobility Management Entity (MME) in the centre organization, albeit the GPRS Tunnel Protocol (GTP) can give some extra security ensures. In addition, the backhaul network is moved into the information plane using Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) procedures, so security dangers are likewise sent to the centre organization.

XIV. KEY AREAS IN 6G NETWORKS

A few parts of the 5G organization have proactively been thought of, and a few parts have previously conveyed AI as their spine, e.g., divert coding and assessment in the actual layer, many entrance in the MAC layer, and different applications in the organization layer [26]. Nonetheless, AI applications are not normal, and the, the help for AI-driven advancements in 5G organizations is restricted by the requirements of the customary design that was accessible in the beginning phases of its origination.

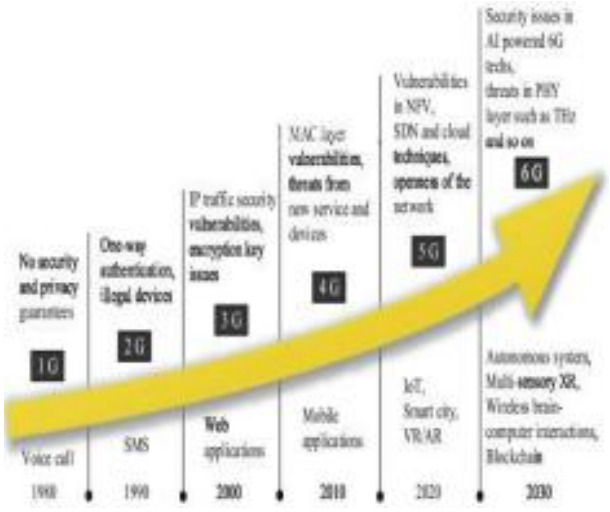

Fig 3. 5G organizations is restricted by the requirements

As needs be, there is no help for the circulated AI or the savvy radio, as these two regions are completely AI-based. Besides, albeit the constant clever edge, for example, vehicle organizations, have previously been carried out for 5G organizations, crisis conditions cannot be dealt with in that frame of mind because of idleness issues.

Notwithstanding, 6G organizations can. For instance, the radio dormancy of 6G organizations is 0.1 Ms, which is one-10th of that of 5G organizations. Additionally, 5G inclusion is still just at the ground level; space and submerged correspondences at certain degrees of 3D radios are impractical. Likewise, in the accompanying, we will depict how these four regions could progress in 6G organizations. Obviously, we additionally talk about the reasonable security and protection issues we hope to look around there.

1. Will 6G Address 5G's Shortcomings for the IoT?
With all the astounding innovation imagined, siphoned up by genuine advances in things like broadened the truth, it is hard not to become amped up for fantastical things like computerized clairvoyance. It is conceivable these things may one day be in our future, yet they will not show up with 5G. All things being equal, it will take until 6G before we have figured out the issues with the subtleties - including a part of the weaknesses that 5G right now displays.

2. What are a few things we need to figure out (and how should 6G location them)? We have a couple:

2.1 Security: It is notable that the IoT has significant security issues because no norms exist, we are yet not used to the possibility that a thing that does not seem as though a PC can be associated with the web, and can get hacked. 6G specialists are trying to resolve this issue.

2.2 Privacy. On the off chance that everyone is wearing an installed association with the web, what kind of protection exists? (We have not had the choice to track down a response from 6G scientists, for the same reason.)

2.3 Complexity. 5G as of now faces monstrous intricacy issues because of the need to work out framework. 6G may have a response with network reconfigurations, yet no strong response exists.

2.4 Sovereginty. An undiscussed worry around 5G includes whether worldwide norms ought to exist, or state-run administrations ought to declare command over network in their individual nations. That might bring about the IoT being limited from its maximum ability except if this contention can be settled.

3. What Lies Ahead in the 2030s? That is What We are Exploring:
The 2022s will see an expansion of the Internet of Things as our reality tilts towards a mixing of the computerized and actual real factors. Through advancements like expanded reality and savvy gadgets, we can expect that

the web should take on a more three-layered presence that infiltrates our lives through more than screens.
The Internet of Senses is the greatest mark of this future, offering the likelihood that one day we might have the choice to see, hear, and experience surfaces, yet in addition smell and taste on the web, as well. Will that occur with 5G? Not - however only another thing makes 6G innovative work so invigorating.

XV. DIFFERENCES BETWEEN 5G AND 6G NETWORK

1. **Use of different spectrum:**
5G and 6G utilize remote range of higher reach for information transmission quicker than 4G, 3G, and 2G organizations. In any case, while contrasting 5G versus 6G, the earlier one is apportioned for low band and high band frequencies - sub-6 GHz (Gigahertz) or more 24.25 GHz separately. The last one will be usable at the recurrence range 95 GHz to 3 THz (Terahertz). Since, various range is used, 5G versus 6G innovation can have many use cases for an assortment of modern areas to upgrade their ability.

2. Faster than 5G technology:
Taking into the presentation factor, 6G will add to better execution which is far superior than recently sent 5G remote organizations. Working at terahertz recurrence groups, 6G will convey a pinnacle information pace of 1,000 gigabits/s having air inactivity under 100 microseconds. At the point when we discuss 5G versus 6G organization speed, 6G speed is supposed to be multiple times quicker than 5G with upgraded dependability and more extensive organization inclusion.

3. 6G wireless accelerates IoT after 5G:
Web of Things (IoT) is turning into a reality today with the execution of 5G based arrangements following broad 5G organization testing which was impractical with past organizations like 4G LTE because of lack of common sense of frequencies applied.

Frequencies used were excessively restricted and swarmed for sending information expected by shrewd gadgets to give wanted results. This is where 5G filled in the whole and pushing forward with 6G we hope to associate multiple times more gadgets per square kilometre with expansion in number of associated gadgets in the forthcoming years.

4. Low dormancy in both G's:
The time taken by a bundle of data sent over a recurrence is known as inertness. 4G organizations had a dormancy of around 50 milliseconds (Ms) while 5G organizations had multiple times lower inertness than 4G i.e., 5ms. With 6G web, inactivity will descend to go 1millisecond to 1microsecond, bringing dormancy down to multiple times than that of fifth-age network making gigantic information transmissions conceivable in under a moment.

XVI. WHO ARE WORKING ON 6G?

- Numerous associations and colleges are showing interest and including themselves in investigating the innovation as given underneath:
- College of Aveiro delivered a whitepaper on 2019 'Why 6G?' which examines the main thrusts behind the improvement of new organization like 6G, what are the most recent elements and key advancements that can be expected.
- Samsung is additionally sharp in taking part in the exploration race as it started 6G examination in 2019 in the long stretch of June.
- SK Telecom, a South Korean telecom association has consented to arrangements with Ericsson, Samsung and Nokia to together direct innovative work in 6G versatile organization innovation.
- Tera View, terahertz test gear fabricating association was as of late upheld with £191 million assets from the Sustainable Innovation Fund with Innovate UK, a development office situated in United Kingdom. This is viewed as an urgent advance forward in making 6G a reality. With an emphasis on using its aptitude and licensed innovation, Tera View will help in building the squares for future 6G organization and speed up its turn of events.
- Google and Apple have communicated their advantage in 6G explorations and joined the Next G Alliance that was implicit October 2020 to make a 6G guide and spur North American organizations to plan themselves and be at the very front of embracing 6G across the globe.
- Korean MNC, LG Electronics has moved forward to foster 6G innovation with the foundation of exploration focus. Organization's CTO Park II-Pyeong referenced to help R&D for innovative 6G organization and lead the job with worldwide normalization and formation of new business valuable open doors.

XVII. CONCLUSION

With the 5G organization research stage reaching a conclusion and destined to be sent, 6G organizations have turned into the plan of many analysts. The 6G organization will without a doubt carry network administration to a more elevated level than those of past ages. In this paper, we led an itemized examination concerning the security and protection issues connected with 6G organizations.

To start with, we introduced an outline of the achievements from 1G to 5G, proving a groundwork for the advancement of the 6G organization. We then, at that point, analyzed four vital region of the 6G organization to reveal the security issues connected with the upcoming

innovations. The examination closes with a conversation of the potential applications that the 6G organization will uphold. We trust that this conversation will animate individuals' advantage and further exploration on 6G organization security and protection issues.

REFERENCE

[1] Christos L. Stergiou Kostas E. Psannis IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network
[2] Dr. Melike Erol-Kantarci from the University of Ottawa will present AI Enabled Wireless Networks: A Bridge from 5G to 6G
[3] https://www.techtarget.com/searchnetwo rking/d efini tion/6G
[4] https://whatis6g.com/6g-and-the internet-of-things/
[5] https://timesofindia.indiatimes.com/blog s/digital-mehta/pros-and-cons-of-5g technology/
[6] https://www.sciencedirect.com/science/a rticle/pii/S2352864820302431