IoT : Security & Challenges of 5G Network in Smart Cities

[1]Devasis Pradhan, [2]Hla Myo Tun , [3]Ajit Kumar Dash
[1]Assistant Professor, Department of Electronics & Communication Engineering,
Acharya Institute of Technology, Bangalore-560107
[2]Faculty of Computer and Electrical Engineering, Yangon Technical University
Yangon, Myanmar
[3]Global Research Consultant, Bijiu Pattnaik University of Technology
Bhubaneswar, India
devasispradhan@acharya.ac.in

Abstract : **The fifth era (5G) will overwhelm in the brilliant urban areas where 5G gives every one of the offices most extreme security and privacy. As to administrations, superfluous mishap rates are expanding with digital assaults also, dangers. All security issues for 5 G-based framework will confront many difficulties like secure transportation administrations which is one of the 2030 drives in quite a large number nations. Safeguarding the infrastructure is then extremely significant of 5G-empowered IoT sharing of information against these assaults. This requires the analysts working in this space to propose different sorts of safety conventions under various kinds of classes, as key administration, client validation/gadget confirmation, access control/client access control, and interruption discovery. As the interest for portable information develops, versatile administrators and makers are confronted with a problem. There is a limited measure of radio recurrence range accessible at any one second, yet to satisfy client interest, they should further develop limit and convey higher correspondence rates. This paper gives bits of knowledge into the basic issues and challenges connected with the security, protection, and trust issues of 5G network.**

Keywords: IoT, security,privacy,5G,smart cities,access control

I. INTRODUCTION

By 2023, fifth-age (5G) radio organizations had been carried out universally, with highlights like mass association, outrageous steadfastness, and dependable low inertness indicated [1-5]. 5G, then again, will miss the mark concerning meeting all future necessities past 2030. It works on the presentation and proficiency which capacitate the client experiences. The information move speed of 5G is roughly multiple times quicker than 4G which is focused on up to 35.46 Gbps. The advances that work behind the scenes are MIMO and mm-Wave Communication. Methods and advancements like "small cells", "massive MIMO", "millimeter wave" also "light fidelity (Li-Fi)" are used to give 10Gbps with exceptionally low idleness. It upholds associations around for 100 billion gadgets.

The security related with 5G advances has been viewed as one of the key prerequisites connected with both 5G and past frameworks. Besides, the majority of the security models in pre-5G (for example 2G, 3G, and 4G) organizations can not be straightforwardly used in 5G because of new engineering and new administrations [6-7]. Be that as it may, a portion of the security components can be utilized with some change. To begin with, practically all the above security threats and security necessities connected with pre-5G versatile ages are still pertinent in 5G and then some. Second, 5G will have a new arrangement of safety challenges because of the expanded number of clients, heterogeneity of associated gadgets, new organization administrations, high client security concerns, new partners and prerequisites to help IoT and strategic applications.[8-9]

II. 5G NETWORK IN SMART CITIES

As the up and coming age of versatile organizations, 5G is one of the exceptionally dynamic exploration spaces among media transmission specialists. Subsequently, a few overviews were at that point distributed on 5G organizations. Numerous future examination prospects like engineering, versatility the board, traffic the executives, security, protection, and techno-financial perspectives, talked about in these papers are mean quite a bit to be considered during the organizations of 5G organizations [10-12]. Security has been featured as one the very pinnacle of significant prerequisites in the 5G exploration area.

A. 5G Network Architecture

There are a couple of obstacles in the way for 5G organizers. One of the most basic hardships is the genuine shortage of radio recurrence spectra owed for cell correspondences. Likewise, these repeat spectra have been essentially used, and there isn't any more assistant in the current cell gatherings. A further test is the movement of state of the art far off developments goes with the tag of high energy usage. Current advances like OFDMA are represented to turn out basically for next 50 years. Additionally, there is no need of progress in development. The distant plan had worked out as expected from 1G to 4G.Then again, the development of an application or we can say improvement done at the simple association for fulfilling the client necessities is inducing the group providers to drift for a 5G association when 4G is economically set up. Figure1. depicts the basic architecture of 5G Network enabling in Smart cities.[13-15]

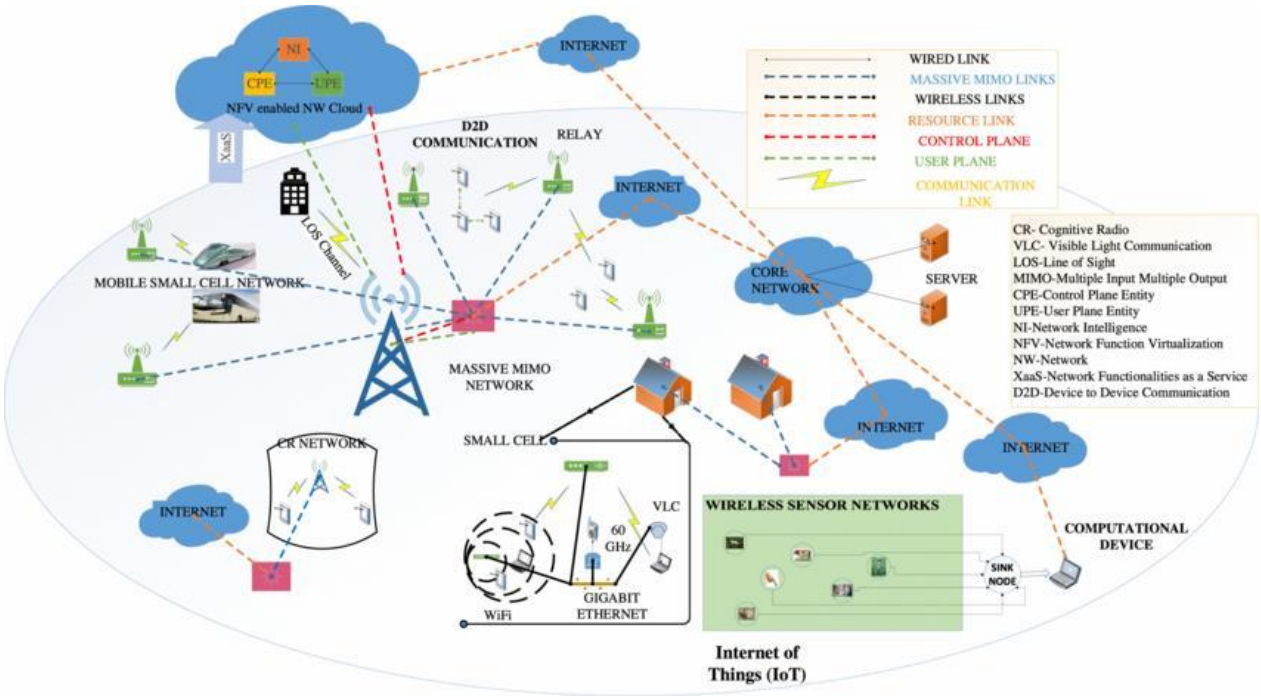

Fig. 1. Basic Architecture of 5G Network

B. Benefits of 5G Network

- Gives exceptionally high information move rate (1-20 Gbps) which works with the clients to download content rapidly.
- Conveys super low inactivity (1 ms) which permits clients to encounter less postponement while mentioning information from the network.
- Limit increments as the organization extends.
- Reasonable with the past ages of portable correspondence innovations.
- Viable and strong of heterogeneous administrations (i.e., confidential organization).
- Gives uniform, continuous, and predictable availability for the different applications (i.e., correspondence of shrewd vehicles) across the world.

C. Smart Living

Around here, IoT can be applied in regulator contraptions by which one can remotely turn machines on and off thusly preventing setbacks as well as saving energy [1, 3]. Other canny home contraptions consolidate ice chests fitted with LCD (Liquid Crystal Display) screens, engaging one to know about what is available inside, what has over remained and is almost slipping by as required to be restocked [16]. This information can moreover be associated with a cell application engaging one to get to it when outside the house and subsequently buy what is required. Furthermore, garments washers can allow one to screen clothing from a good ways. A couple of grills which have a self-cleaning component can be conveniently checked as well. As to in the home, IoT can be applied through ready structures and cameras can be acquainted with screen and distinguish window or doorway openings consequently preventing interlopers.

III. IoT

IoT, is a plan of interrelated handling devices, mechanical and high level machines, things, animals or people that are outfitted with exceptional identifiers and the ability to move data over an organization without anticipating that human should human or human-to-PC joint effort A thing in the trap of things can be a person with a heart screen implant, animals with a biochip transponder, an auto that has intrinsic sensors to alert the driver when tire pressure is low or whatever another normal or man-made object that can be distributed an IP address and can move data over an organization.

The Internet of Things (IoT) is an interconnected plan of especially address competent genuine things with various levels of taking care of, identifying, and in citation limits that share the capacity to interoperate and pass on through the Web as their joint stage [16-17]. In this way, the main target of the Internet of Things is to make it useful for objects to be related with various things, and individuals, at whatever point or wherever using any association, way, or organization. The Internet of Things (IoT) is gradually being seen as the subsequent work in Internet improvement. IoT will make it possible for typical devices to be associated with the web to achieve perpetual divergent goals. Right now, an expected number just 0.6% of gadgets that can be essential for IoT have been associated up until this point. The basic building blocks of IoT Paradigm is Devices, Gateway, Connectivity and Cloud based storage . Figure1. Depicts the building blocks.[18]

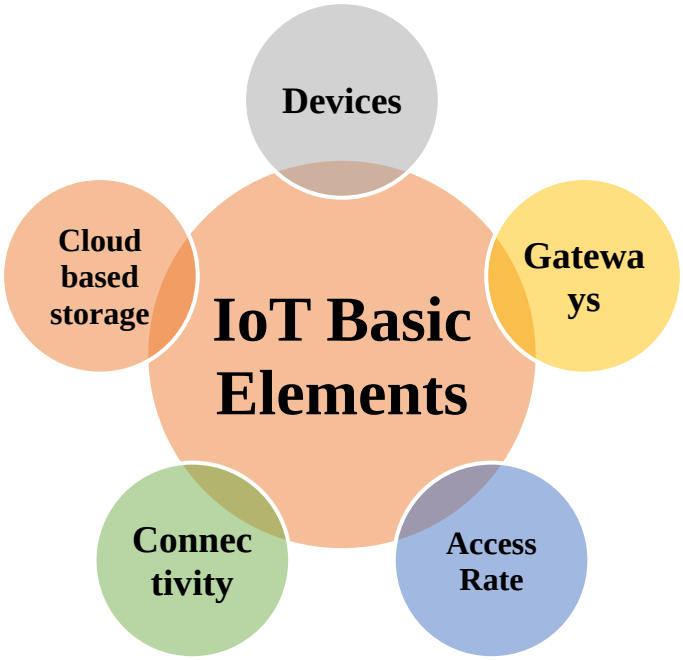

Fig. 2. Basic Elements of IoT

Connectivity : Since IoT is an organization based framework; 'network' plays a crucial job. The different specialist organizations have given numerous answers for the network of the end gadgets to the doors and afterward to the cloud. Likewise, it is a double/duplex framework. Thus, it works in the forward and backward correspondence framework among applications and equipment [16-19]. Consequently, the availability can work both in the remote or wired systems. For model: Bluetooth, Wi-fi, RFID, GSM and so forth.

A. Devices:

These are the most fundamental gadgets or key things in IoT. These are the dynamic detecting gadgets or actuators working in gathering the significant important data and playing out the ground level handling. For instance RFID at piece of clothing stores, temperature sensors at home, and cameras at the highways.[20]

B. Cloud based storage and Computing :

The IoT and Cloud Computing supplement each other, frequently being marked together while examining specialized administrations and cooperating to give a general better IoT administration. Nonetheless, there are pivotal contrasts between them, making every one of them a compelling specialized arrangement independently and together. Distributed computing in IoT fills in as a feature of a joint effort and is utilized to store IoT information. The Cloud is a concentrated server containing PC assets that can be gotten to at whatever point required. Distributed computing is a simple travel strategy for the huge information bundles created by the IoT through the Internet. Enormous Data can likewise help in this cycle [20-21]. Consolidated, IoT and Cloud Computing permit frameworks to be mechanized in a savvy way that upholds constant control and information observing.

C. Gateways:

It is the close by taking care of center point/device. It interfaces the end devices to the association or internet(cloud). It should not simply trade the material information assembled from the sensors or actuators yet furthermore process them to some degree and forward the particular information to the cloud. It in like manner gives information by sending back the data got from the cloud.[23-24]

D. Access rate:

The more data is accessible, the simpler it is to make an suitable choice. You approach continuous information and data that is far away from your area [22-23]. Knowing what you get from the grocery store by going out without checking yourself saves time as well as remains viable. This is just conceivable on the grounds that a gadget network gives an individual admittance to all data on the planet. This makes it extremely simple for individuals to go about their responsibilities in any event, when they are not actually present.

IV. AMALGAMATION OF 5G WITH IOT

5G is about another correspondence framework that incorporates a generally New Radio (5G NR) system and a completely new center organization that expects to further develop remote associations around the world. It additionally incorporates the idea of numerous entrance for network advances like satellites, Wi-Fi, fixed-line, and cell (as normalized by 3GPP). In view of IoT-empowered gadgets, 5G associates more gadgets at higher rates and makes things like slack almost non-existent. Accordingly, 5G makes a superb client experience regardless of what application, gadget, or administration you contact [24-26]. IoT advances are described as minimal expense, low-power utilization arrangements. They blossom with profound and expansive inclusion inside and outside. They convey secure availability and validation, are not difficult to send to any arrange

geography, and are intended for full degree adaptability and limit overhauls.

V. SECURITY ISSUES IN 5G NETWORK

As the 5G network approaches commercialization, we might expect sped up utilizing complex frameworks and high-security designs . 5G network' curiosity is their ability to associate the developing number of gadgets while conveying better caliber administrations to all arrange elements. The most direct way to deal with arranging security and protection issues in 5G network is to look at the network engineering. The 5G design incorporates access networks, backhaul networks, and central network. Numerous gadgets what's more, network access techniques present extra security issues.[23-24]

Two techniques for managing flagging over-burdens have been grown up until this point. Be that as it may, the new techniques for speeding up the 5G networks speed likewise make security weaknesses. For instance, enormous MIMOs are used to conceal dynamic and latent listening in. Furthermore, SDN execution through OpenFlow represents a danger introduced by rebel applications or exercises.

VI. THREATS IN 5G ENABLED IOT COMMUNICATION

A 5G-empowered IoT correspondence can have the accompanying potential assaults which might be performed by a uninvolved or an dynamic enemy [24]:

A. Listening in:

It is likewise called sniffing or sneaking around assault. It occurs for the situation when an assailant snoops the traded messages among the conveying parties. It is one of the possible assaults on 5G-empowered IoT correspondence as this will assist the aggressor with sending off further assaults.

B. Traffic examination:

It is one more type of latent assault in which aggressor do the capture and an assessment of the traded messages to sort out what's happening there.

C. Replay Strafe:

It happens when an assailant captures the traded messages and afterward underhandedly deferred or re-sends it to bewilder the getting substance.

D. Man-in-the-center Strafe :

In this censure movement, the primary aggressor seizes the communicated messages and afterward endeavors to refresh or erase the messages prior to sending them to the collector.

E. Pantomime Strafe:

In this censure movement, an aggressor effectively decides the personality of a certified imparting party and afterward makes a message and sends that to the beneficiary for the benefit of the "certifiable conveying party"

F. Malware Strafe:

Once in a while an enemy executes the noxious contents in a distant framework to perform various unapproved exercises, for instance, taking, erasure, refreshing, and encryption of significant data. Malware might be of various kinds, for instance, infections, worms, and keyloggers. They are likewise used to screen the exercises of the clients without his/her assent. For the spreading of malware in IoT climate foe can utilize botnets (related and worked together assailant frameworks). These assaults may likewise hurt the working of the 5G-empowered IoT climate.

VII. SECURITY MONITORING & MANAGEMENT

The basic elements of monitoring and management systems is : access control, device authentication, Intrusion detection and key management.

A. Access Control :

The section control procedures put limitations on the passage of the client or gadget to the assets of an affiliation or structure. The followed instrument awards access and regards to various clients or contraptions for the different accessible assets. To chip away at the general lifetime of the IoT correspondence domain, it is ordinary to add new contraptions i.e., smart IoT gadgets in the affiliation. That could happen on the off chance that a contraption stops working considering battery exhaustion or some genuine taking. There are similarly takes a risk with that an enemy tries to introduce their poisonous gadget in the objective district. Along these lines, segregating between hazardous gadgets and certifiable contraptions is major. Essentially, secure access control systems to confine the passage of unsafe substances in a 5G-empowered IoT domain ought to be organized.[24-26]

B. Device Authentication:

Client/gadget confirmation is a strategy of distinguishing proof what's more, confirmation of the characters of the imparting entities i.e., client or gadget. By and large, the imparting elements client, shrewd IoT gadgets confirm their characters among each other which is otherwise called common confirmation. After the effective fruition of "common validation", the disseminating elements lay out a meeting key to get their correspondence. Gadget validation likewise occurs in the same way. To improve on this, the subtleties of client authentication . The client validation plot for a 5G-empowered IoT interchanges the stages, for example,"framework arrangement and pre-sending stages". Figure 3. depicts the authentication of devices/gadget.[27-28].

C. Intrusion Detection:

The conventions are sent for the checking and investigation of malicious efforts inside a framework or an organization. A framework that accomplishes this work of interruption identification is named an "interruption recognition framework (IDS)". An IDS guards different gadgets i.e., brilliant IoT gadget against possible assaults. The pre-owned interruption identification method in a 5G-empowered IoT climate screens and confirms the various sorts of traffic (might be typical or malignant), and then, at that point, predicts the indication of interruptions. Assuming that an interruption is distinguished then the connected apparatus makes the expected move for instance, blocks the IP of a pernicious source or sends the data of interruption to the director.[22-23]

D. Key Management:

A key administration convention does the age, distribution, foundation and the executives of cryptographic keys among the imparting parties in an IoT domain. The characterized system contains different advances, for

example, "age of key", "trade of key", "utilization of key" and "disavowal of key" as indicated by the interest. Key administration convention uses a "cryptographic methodology" that keeps the subtleties of key servers (the confided in power), different kinds of clients (i.e., static or versatile) and gadgets required (for instance, shrewd IoT gadget)[23-28]

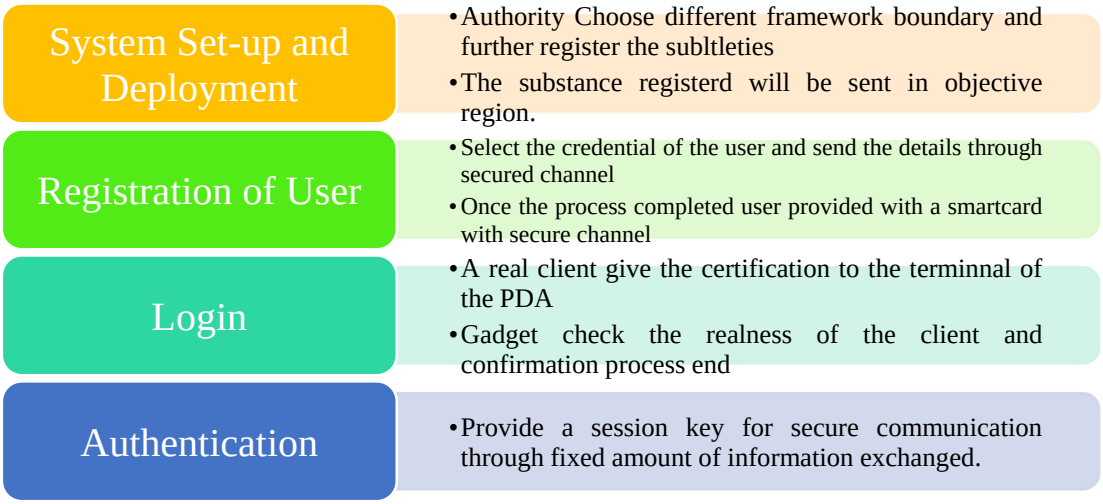

Fig. 3. User/Device Authentication

VIII. Research Challenges

5G-empowered IoT correspondences climate upholds different kinds of utilizations, like savvy home, shrewd transportation, shrewd medical care, brilliant lattice and savvy manufacturing. This climate requires lone necessities for instance, live handling and getting to of information (i.e., environmental checking of a modern plant continuously).

A. Protocols Security :

The majority of the dependability of the conventions proposed for IoT conditions shaky as it don't outfit total protection from potential assaults. Besides, a portion of the current conventions works for a specific assault and don't work for various goes after simultaneously.[29]

B. Storage of Large amount of Data :

The protection of information worries with the legitimate treatment of data over the different asset i.e., assent, notice, what's more, administrative commitments. 5G-empowered IoT is additionally used in "data touchy" tasks (like shrewd medical services).

C. Vast usage of devices :

Other than that, these gadgets work with different kinds of correspondence strategies. Gadgets are likewise differentiating according to their correspondence strength, calculation limit, capacity size, and sent framework programming (e.g., working framework). Subsequently security conventions ought to be planned in such a design that it gives security to various assortments of gadgets and related advances and systems.[30]

D. Scalability of Protocols:

Heterogeneous network of various correspondence component and applications. These applications have their own abilities and concerns. In such conditions arranging of a security show for this kind of correspondence environment will be many-sided task. For example, in a canny clinical benefits correspondence environment, patient's electronic prosperity records which should be taken care of over a cloud server for extra dealing with and course.

IX. Conclusion

5G-empowered IoT space experiences different kinds of wellbeing and protection issues as it is presented to various kinds of assaults. It becomes fundamental to protect the arrangement of the 5G-empowered IoT area against these assaults. In this way, various types of prosperity shows compelled came into picture. In this blueprint article, the subtleties of different framework models (for model, network model and danger model) are obliged 5G-connected with IoT space.

Reference

[1] M. B. M. Noor and W. H. Hassan, ‘‘Current research on Internet of Things (IoT) security: A survey,’’ *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.

[2] J. Sengupta, S. Ruj, and S. D. Bit, ‘‘A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT,’’ *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.

[3] Devices & Systems, IoT Tech Expo. (2019). *Unlocking IoT Data With 5G and AI*. Accessed: Oct. 2019. [Online]. Available: https://innovate.ieee.org/innovation-spotlight/5g-iot-ai/

[4] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, ‘‘AKM-IoV: Authenticated key management protocol in fog computingbased Internet of vehicles deployment,’’ *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[5] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H.-M. Aggoune, ‘‘Internet-of-Things (IoT)-based smart agriculture: Toward making the fifields talk,’’ *IEEE Access*, vol. 7, pp. 129551–129583, 2019.

[6] King’s Healthcare. (2019). *A Healing Hand-Giving the World Better Access to Medical Experts Through the Tactile Internet*. Accessed: Oct. 2019. [Online]. Available: https://www.ericsson.com/en/cases/2017/kings-college/kings-healthcare

[7] M. Wazid, A. K. Das, and J.-H. Lee, ‘‘User authentication in a tactile Internet based remote surgery environment: Security issues, challenges, and future research directions,’’ *Pervas. Mobile Comput.*, vol. 54, pp. 71–85, Mar. 2019.

[8] R. Hussain and S. Zeadally, ‘‘Autonomous cars: Research results, issues, and future challenges,’’ *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1275–1313, 2nd Quart., 2019.

[9] Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation and security challenges. *IEEE Commun. Surv. Tutor.* 2019, *21*, 3417–3442. [CrossRef]

[10] Shrestha, R.; Bajracharya, R.; Kim, S. 6G enabled Unmanned Aerial Vehicle Traffific Management: A perspective. *IEEE Access* 2021, *9*, 91119–91136. [CrossRef]

[11] Stoynov, V.; Ivanov, A.; Mihaylova, D. Conceptual Framework for Quality Assessment in human-centric 6G XR services. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Borovets, Bulgaria, 26–29 November 2021; Volume 1032, p. 012009.

[12] Soldani, D.; Guo, Y.J.; Barani, B.; Mogensen, P.; Chih-Lin, I.; Das, S.K. 5G for ultra-reliable low-latency communications. *IEEE Netw.* 2018, *32*, 6–7. [CrossRef]

[13] Chen, R.; Li, C.; Yan, S.; Malaney, R.; Yuan, J. Physical layer security for ultra-reliable and low-latency communications. *IEEE Wirel. Commun.* 2019, *26*, 6–11. [CrossRef]

[14] Hamamreh, J.M.; Basar, E.; Arslan, H. OFDM-subcarrier index selection for Enhancing Security and Reliability of 5G URLLC services. *IEEE Access* 2017, *5*, 25863–25875. [CrossRef]

[15] Pradhan, D., & K C, P. (2019). Effectiveness of Spectrum Sensing in Cognitive Radio toward 5G Technology. *Saudi Journal of Engineering and Technology (SJEAT)* , *4*(12), 473–485. https://doi.org/10.36348/sjeat.2019.v04i12.001

[16] Al-Eryani, Y.; Hossain, E. The D-OMA method for massive multiple access in 6G: Performance, security, and challenges. *IEEE Veh. Technol. Mag.* 2019, *14*, 92–99. [CrossRef]

[17] Pradhan, D., & K C, P (2020) 'RF-Energy Harvesting (RF-EH) for Sustainable Ultra Dense Green Network (SUDGN) in 5G Green Communication', *Saudi Journal of Engineering and Technology* ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online, 5(6), pp. 258-264 DOI: http://doi.org/10.36348/sjet.2020.v05i06.001

[18] Mahmood, N.H.; Böcker, S.; Munari, A.; Clazzer, F.; Moerman, I.; Mikhaylov, K.; Lopez, O.; Park, O.S.; Mercier, E.; Bartz, H.; et al. White paper on critical and massive machine type communication towards 6G. *arXiv* 2020, arXiv:2004.14146.

[19] Pradhan, D., & K C, P (2020) 'A Comprehensive Study of Renewable Energy Management for 5G Green Communications: Energy Saving Techniques and Its Optimization', *Journal of Seybold Report* ISSN NO: 1533-9211, 25(10), pp. 270-284.

[20] Pradhan, D., & Dash, A. (2020) 'An Overview of Beam Forming Techniques Toward the High Data Rate Accessible for 5G Networks', *International Journal of Electrical, Electronics and Data Communication*, ISSN(p): 2320-2084, ISSN(e): 2321-2950 , 8(12), pp. 1-5.

[21] Yamakami, T. A privacy threat model in xr applications. In *International Conference on Emerging Internetworking, Data & Web Technologies*; Springer: Cham, Switzerland, 2020; pp. 384–394.

[22] Pradhan, D., Kumar Sahu, P., R, R. and Tun, H., (2021). 'A Study of Localization in 5G Green Network (5G-GN) for Futuristic Cellular Communication', *3rd International Conference on Communication, Devices, and Computing - ICCDC-2021*. Department of ECE, Haldia Institute of Technology, West Bengal, India, 16th -18th August 2021. Singapore, Published: Springer, Singapore.

[23] Pradhan, D., & Rajeswari (2020) '5G-Green Wireless Network for Communication with Efficient Utilization of Power and Cognitiveness', in Jennifer S. Raj Professor, ECE, Gnanamani College of Engineering and Technology Namakkal India (ed.) *International Conference on Mobile Computing and Sustainable Informatics. Springer Nature Switzerland AG 2021*: Springer, Cham, pp. 325-335

[24] Pilz, J.; Holfeld, B.; Schmidt, A.; Septinus, K. Professional Live Audio Production: A highly synchronized use case for 5G Urllc Systems. *IEEE Netw.* 2018, *32*, 85–91. [CrossRef]

[25] Pradhan, D., Sahu, P., Dash, A. and Tun, H., (2021). 'Sustainability of 5G Green Network toward D2D Communication with RF- Energy Techniques', *IEEE International Conference on Intelligent Technologies (CONIT 2021)*. K.L.E.I.T, Hubbali, Karnataka, 25- 06-21. IEEE Bangalore Section: IEEE, pp.1-10.

[26] Pradhan, D., Kumar Sahu, P., R, R. and Tun, H., (2021). 'A Study of Localization in 5G Green Network (5G-GN) for Futuristic Cellular Communication', *3rd International Conference on Communication, Devices, and Computing - ICCDC-2021*. Department of ECE, Haldia Institute of Technology, West Bengal, India, 16th -18th August 2021. Singapore, Published: Springer, Singapore.

[27] H. M. Tun, Z. T. Thu Lin, D. Pradhan and P. K. Sahu,(2021) "Slotted Design of Rectangular Single / Dual Feed Planar Microstrip Patch Antenna for SISO and MIMO System," *IEEE 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2021*, Cape Town, South Africa pp. 1-6, doi: 10.1109/ICECET52533.2021.9698738

[28] Jamwal, A.; Agrawal, R.; Sharma, M.; Giallanza, A. Industry 4.0 technologies for manufacturing sustainability: A systematic review and Future Research Directions. *Appl. Sci.* 2021, *11*, 5725. [CrossRef]

[29] Pradhan, D., K.C, Priyanka., & Rajeswari (2021) 'GREEN- Cloud Computing (G-CC) Data Center and its Architecture toward Efficient Usage of Energy', in Mangesh Ghonge, Ramchandra Sharad Mangrulkar, Pradip M Jawandhiya, Nitin Goje (ed.) *Future Trends in 5G and 6G Challenges, Architecture, and Applications. : CRC Press - Taylor & Francis Group*, pp. ISBN 9781032006826.

[30] Pradhan, D., K.C, Priyanka., & Rajeswari. (2021) ‘SDR Network & Network Function Virtualization for 5G Green Communication (5G-GC)’ , in Mangesh Ghonge, Ramchandra Sharad Mangrulkar, Pradip M Jawandhiya, Nitin Goje (ed.) *Future Trends in 5G and 6G Challenges, Architecture, and Applications. : CRC Press - Taylor & Francis Group*, pp. ISBN 9781032006826

[31] Vikas Susmita, K. S., Kailas, & Pradhan, D **(2020)** 'A Comprehensive Study on Firewall for IOT Devices, Policies, and Security Issues.', *International Journal of Industrial Electronics and Electrical Engineering*, ISSN(p): 2347-6982, ISSN(e): 2349-204X, 8(12), pp. 1-5