Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7778373

A SURVEY ON NEXT-GENERATION WIRELESS NETWORK SECURITY FOR DEVICE-TO-DEVICE COMMUNICATION

Chaithanya D J
Research Scholar, ACS College of Engineering,Bangalore, Visvesveraya Technological University, Belagavi – 590018, rcchaithudj@gmail.com

Dr.Anitha S
Research Supervisor, Department of Electronics and Communication Engineering
ACS College of Engineering,Bangalore, Visvesveraya Technological University, Belagavi-590018, dranithasammilan@gmail.com

Abstract— The new advanced characteristic of 5th Generation Wireless Network Systems (WNS) relent latest security challenges and requirements. In comparison to other typical cellular networks, this survey expands on a complete survey on security. The survey begins with a review on 5th Generation wireless network originality further on the advanced motivations and requirements of 5th Generation wireless security and the probable security attacks and services with its deliberation of its latest service specification in 5th Generation wireless networks will be summed up. Security services such as availability, authentication, data secrecy, privacy and key management are all used in current 5th Generation wireless security technologies and techniques. This survey provides an overview of the security risks that have arisen in recent technologies, as well as privacy concerns in the 5th Generation technology. This survey provides an in-depth examination of existing privacy- preserving systems and authentication methods for 4th and 5th generation cellular networks. We present an overview of existing surveys pertaining to 4th and 5th generation cellular networks. In addition, we use a table to explain categorization as well as a comparison of privacy-preserving techniques and authentication fourth and Fifth generation cellular networks.
Keywords—5G technology, Security, Privacy, Wireless network

I. INTRODUCTION

5th Generation wireless systems are the upcoming generation wireless telecommunication network beyond the current 4th Generation or International Mobile Telecommunications (IMT) Advanced Systems [1]. In comparison to recent 4th Generation Long Term Evolution networks, the vision of the upcoming 5th Generation wireless communication lies in big data rates of the order of Giga bits per second, Base stations provide low latency and considerable improvements in customers perceived quality of service (QoS) [2][3].

The convergency of computation and communication over the last two decades has given us the World Wide Web [46]. We trust that the upcoming phase of the information mechanization revolution will be the convergency of computation, communication, and control. This will give the potentiality for large numbers of statistical unit's

sensors and actuators interconnected over wires or wirelessly to interact with the physical environment. We argue that in the accumulation of this “convergency,” a commentative role will take part by the architecture. 5th Generation technology impart massive resolution for bi-directional large bandwidth shaping and cell phone user.

In Fifth Generation network send the envelope of execution to provide, where needed, example for this is higher throughput with its higher mobility range, low latency, high reliability with higher connectivity density. This upgrades the performance with the proficiency to control a large heterogeneous environment along with the capability to establish identity and privacy with security and trust [4]. Mobile applications and connected devices require wireless network access that is resilient and secure, capable of protecting individual privacy [5][6]. The 5th Generation system was designed with these requirements in mind, considering mobile applications and connected devices that require wireless network access that is resilient and secure.

The primary goal of 5th Generation networks is to combine multiple services into a single infrastructure, each with its own logical network [7]. The 5th Generation of mobile networks is the next step in the evolution of mobile networks and is regarded as the digital world's future.5th Generation refers to a collection of new wireless access technologies rather than a single piece of technology. The 5th Generation network is a fully integrated network that can support a variety of different network configurations [8].

In comparison to 4th Generation technology, 5th Generation provides better data rates and capacity, as well as lower latency, which is critical for the Internet of Things' billions of connected devices [9]. Security controls are defined as a level of flexibility granted to suppliers in terms of how to implement them, as well as to operators in terms of how to comprehend and apply them [10]. The modern billing interconnection of 5th Generation technology make it additional effective and attractive .5th Generation technology provides subscriber supervision tools for quick response. The elevated quality system of 5G technology construct a Policy to keep away from error [11].

For a wide range of devices, fifth-generation networks provide ubiquitous internet access, improved user mobility and ultrareliable connectivity. Only a few of the main technical enablers for 5G include cloud computing, SDN
[22] and NFV [1].

With future cellular communication technologies such as 5G, a unique multiple access approach known as Beam Division Multiple Access (BDMA) [45] was developed to overcome the inherent constraint and work on Quality of Service for low cost [11]. Because risks can have serious consequences, security has become a top priority in many broadcast communications sectors today. Private data will travel at all tiers in future wireless systems, as the core and enabling developments will be tied to 5G organization. Several events have indicated that the threat faced by an infected wireless organisation has an impact on the security of the network [5].

This paper also includes a section on 5G network security monitoring and management. This research also examines several standardisation organizations to assess the security measures and standards of key 5G technologies, as well as provide an overview of 5th Generation standardised security forces. Furthermore, large multinational projects that are under threat of security [12].

B. Structure and Organization of the Paper

This paper is organised as follows: Section II discusses the open and flexible 5th generation architecture. The security for 5G Mobile Wireless Networks is discussed in Section
III. In section IV, we go over a summary of key polls on 5G security. The Security Risk Assessment for 5G Networks is described in part V, and the Impact of Standards on 5G Architecture and Buildouts is presented in section VI. Finally, the section depicts the future influence of Wireless Evolution: 5G and beyond.

II. THE OPEN & FLEXIBLE 5G ARCHITECTURE

In wireless evolution focus on the radio frequencies, spectrum bands or RF design that includes indoor coverage design or antenna and tower. Radios and RF needs really to work (3G or 4G/LTE or 5G) at their capacity is devices and content or interaction between devices, cloud, backhaul transport and a dynamic and flexible core architecture to connect and make sense of things and finally, enterprises and consumers who have real problems to solve. There are many ways to slice and dice a 5G network architecture. Generally, the standards work in 3GPP divides the 5G network architecture into the following components as User Equipment (Terminals or Devices), Radio Access Networks, Access, or Transport Network (that connect the different RAN and Core components), Core Network [10].

III. 5G MOBILE WIRELESS NETWORK SECURITY [1]

A. 5G Mobile Wireless Network Security [1]

Requirements respect to 4G	Improve the network's resiliency and availability in the face of signalling-related difficulties like overload, which can be induced purposefully or unintentionally.
	Security solution was built for use circumstances that required exceptionally low latency.
	Meet the 4G 3GPP standards security requirements. It is very critical to apply to a virtualized network implementation.
	There is public safety and mission-critical communication.
Requirements in terms of radio access	Enhance the system's ability to withstand complex jamming techniques.
	5th Generation small cell node security needs to be upgraded.

B. Security is a major driver for 5G wireless.

- Supreme Built in Security

(i) Use cases, new technologies and networking paradigms are all being developed.

- Flexible security mechanisms

(i) New networking paradigms, technologies and use cases are all emerging.
(ii) New threats and new trust models [9].
(iii) Changing ecosystem and Growing need for dependability.

- Automation

Changing ecosystem and Growing need for dependability.

Built-in security of the highest order	New networking paradigms New use cases New technologies
Security Mechanisms thatare Adaptable	New dangers have emerged. New trust models are being developed.
Automation	Changing environments Increasing demand for resiliency

C. Analysis of Threats and Solutions for 5G Security [3][9]

Future networks will face significant challenges in terms of network security and user privacy. Since their beginnings, wireless communication technologies have been plagued by security challenges. Mobile phones and wireless channels were targeted for illicit cloning in the first generation (1G) of wireless networks. Because of IP-based communication, Internet security vulnerabilities and issues have been able to transfer into the wireless domains of third generation (3G) wireless networks [3].

D. 5G Security Design

5G Security Design [8]	a. E2E Security Protection	(i) Better Security with E2E Data Protection
		(ii) Differentiated Security Protection
		(iii) Avoid Repetitive Encryption and Decryption
	b. Unified Authentication	(i) Unified Authentication of Heterogeneous Access
		(ii) Support for Hybrid Authentication Protocols
	c. Security Capabilities Open Up	
	d. On-Demand Security Management	

E. For 4th Generation and 5th Generation cellular networks, research of available authentication and privacy- preserving approaches was conducted.

The 5th generation of cellular mobile communications is built to handle the significant increase in capacity and connectivity required for the future cloud of things, as well as the increased bandwidth required for new mobile data services. For security, both rely on the ability to identify people and entities that use network services. As soon as possible, businesses must evaluate the impact of 5G on their brand identity [9].

IV. OUR CONTRIBUTIONS

Literature survey is a critical stage in undertaking lifestyles cycle; therefore, its significance cannot be underestimated. The fact s accumulated through web sites is nicely analysed to honestly recognize the necessities. The cause of this literature survey is to power a new answer by understanding the failing and inadequacies of the existing gadget. The survey carries the look at of different technologies and drawbacks of the

preceding technology, contrast among preceding designs and proposed are also covered on this. For the sustentative and great look, at of the paper the following references had been made and for better implementation of the work few studies papers are referred.

According to a literature review [38], the great evolution from 1G (First Generation) to 4G yields 5G. This covers an introduction to 5G technologies, why 5G is needed, benefits of 5G network technology, outstanding applications, Quality of Service (QoS), and 5G network design. The 5G Master Core, as well as the hardware and software that goes with it. The important research topics for resource management in 5G networks are then highlighted [39].

TABLE II: SUMMARY OF IMPORTANT 5G SECURITY SURVEYS

Aspect	Ref.	Main contribution of the paper	Relevance to 5th Generation Security
5G General	[2]	An In-Depth Analysis of Next-Generation 5G Wireless Networks	There is no clear focus on security issues.
	[13]	A look at the future of 5G networks, including architectural possibilities, application implementation difficulties, and real-world demos and testbeds.	UE (User Equipment) issues and management, access networks, D2D communication, and C-RAN security and privacy are all discussed.

	[14]	An in-depth look at different 5G backhaul network technology and solutions.	There isn't a strong emphasis on security issues.
	[15]	A look at the most recent 5G research and development efforts.	There is no clear focus on security issues.
5G Security	[16],[17]	The privacy and security challenges that 5G networks confront, as well as potential security solutions, are discussed.	SDN, NFV, mobile clouds, and future 5G privacy issues will all be discussed.
	[9]	For 4th and 5th generation mobile networks, a survey of existing authentication and privacy-preserving technologies was conducted.	Threat models in 4G and 5G cellular networks are divided into four categories: attacks on privacy, integrity, availability, and authentication. It also divides countermeasures into three categories: cryptography, human factors, and intrusion detection systems.
	[18]	A survey on the topics of green communication and 5G network security.	The possibility of security attacks on users within 5G networks' Small Cell Access Point (SCA) has been investigated.
	[19]	For 5G networks, this survey is about security and the advancement of osmotic and catalytic computing.	To improve 5G security, emphasise the adoption of new computing paradigms as an alternative approach.

General Mobile network Security	[20]	A review of the available research on attacks and countermeasures in all three generations of pre-5G networks	Examine the security and privacy issues that exist in pre-5G mobile networks, as well as their implications for 5G networks. There is no mention of the impact of upcoming 5G technologies.
SDMN Security	[43]	A study of SDMN and the security issues it raises	In SDMNs, look at the data layer, control layer, application layer, and communication protocols to see what security concerns exist and what solutions are available.
	[21]	A study of concerns and obstacles in constructing wireless networks based on SDN.	Examine various 4G and 5G security solutions based on SDN.
	[22]	A look at how to improve security in SDN-based wireless networks.	Discuss how SDN may be utilised to make SDMNs more secure.
SDN Security	[23] - [26]	An examination of associated security concerns in SDN-based systems.	There is no clear focus on 5G and other 5G technologies' security considerations.
NFV Security	[27] - [29]	A look at the security challenges that surround NFV-based systems.	There is no clear focus on 5G and other 5G technologies' security considerations.

IoT Security	[30]	An examination of connected IoT security vulnerabilities.	There is no clear focus on 5G and its security implications.
Access control and Privacy	[31]	A overview of the Physical, Network, and Application layers for a host-centric network.	Concentrate on the existing mechanisms for access control, security, and privacy.
SDN security	[32]	The security of SDN and the programmability of the data plane are discussed. SDN to stateful SDN security implications.	Secure stateful SDN data planes and enlightened vulnerabilities with decreased exposure.

Suvarna Patil, Vipin Patil and Pallavi Bhat explained regarding 5th Generation architecture using nanocore which involves the technologies like All IP network, cloud computing and nanotechnology. Multiple Access technologies like TDMA, OFDMA, FDMA and CDMA technologies are defined. Beam Division Multiple Access (BDMA) [45] technique is proposed that allows several accesses to MS (mobile station) by enlarging the size of the system [33]. In 5th Generation Nanocore, nanodots are used to enhance the storage potentiality. Opto-electronics are used to enhance the speed in 5G nanotechnology [34].

Manjurul H. Khan focus discussion mainly on recognising future generations of wireless mobile transmission networks. They focused on the importance of light in the creation of several generations of networks and the advancement of mobile wireless technology, as well as the pros and disadvantages of each [35].

Sk. Saddam Hussain, Koushik Barman and Shaik Mohammed Yaseen talked about 5G and its advantages, as well as a hypothetical 5G design and probable 5G issues. Massive MIMO, millimetre wave communication, device-to-device communication, Beam Division Multiple Access, and other technologies may be employed in 5G. This study [36] investigated huge MIMO, channel estimation in massive MIMO, Beam Division Multiple Access in massive MIMO, antenna selection in massive MIMO, capacity, and energy efficiency in massive MIMO.

V. SECURITY RISK ASSESSMENT FOR 5G NETWORKS [42]

The development of 5G poses several security challenges for regulators. One of them is the implementation of a security architecture capable of addressing all user and by extension, government concerns. The European Commission published a plan in March 2019 to develop a coordinated response to security concerns about 5G networks across the European Union. This document describes one of the national solutions, which entails assessing the risk in accordance with EN-ISO or IEC 27005 and implementing appropriate risk mitigation measures. The purpose of this study is to introduce a logical approach to designing 5G security laws based on analysis of existing regulations.

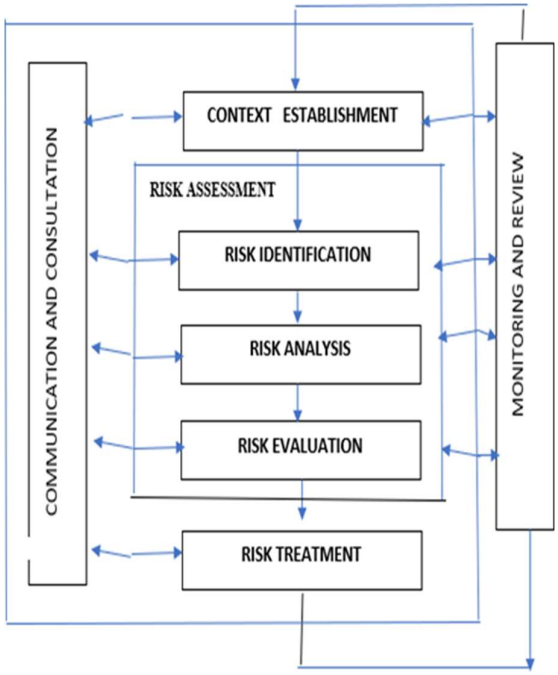
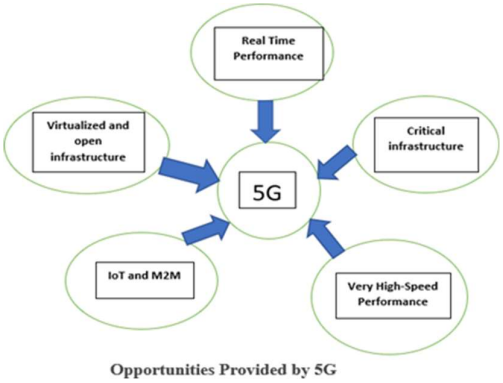


Figure: Relevant risk management activities [42]

VI. IMPACT OF STANDARDS ON 5G ARCHITECTURE AND BUILDOUTS

5G architecture using nanocore involve the technologies such as cloud computing, nanotechnology, and All IP network. Multiple Access technologies like CDMA, OFDMA, TDMA and FDMA are defined. By increasing the capacity of the system BDMA (Beam Division Multiple Access) [45] technique allows multiple access to Mobile Station (MS). Beam Division Multiple Access (BDMA) [11][45] transference or transmission provides concurrently numerous users completely over the discrete beams.

In terms of portals, performance, benefits, and downsides, a comparison of numerous existing forms of mobile wireless technology was attempted. The Worldwide Wireless Web (WWWW) [11], Real Wireless World and Dynamic Adhoc Wireless Networks (DAWN) [47] are all being studied for 5G. We propose a new network design for upcoming generation 5th Generation mobile networks in this paper [37].



Opportunities Provided by 5G

Open RAN, software-defined networks and network slicing are game changers for operators and vendors. This performance though is dependent on how the network is designed, what frequency band you are on, what the transport network can support and how many other users are congesting the network [41].

VII. Recommendations

Logistics, manufacturing, transportation, healthcare, the media, smart buildings, and local government are just a few of the businesses that will be affected by 5G. To maintain security and safety, it is vital to control who and which devices have access to which applications and services. Consider using robust authentication for sensitive devices (e.g., SIM / integrated SIM or certificates) [9]. Make sure IoT devices are secure and free of vulnerabilities, particularly default passwords, and integrate IoT device management with current IT asset management systems.

VIII. Future Impact of Wireless Evolution: 5G and Beyond

Some of the use cases that IEEE researchers are speculating will continue to transform as our networks evolve: virtual and physical experience sharing, remote control IoTs, pervasive connectivity everywhere. If you are just wrapping your head around 5G and wondering why we would need 6G, notice the difference in peak data rate and latency expected with 6G, and think about how that could impact the user experience.

References

[1]. Dongfeng Fang, Yi Qian, and Rose Qingyang Hu “Security for 5G Mobile Wireless Networks” IEEE, December 2017.

[2]. Mamta Agiwal, Abhishek Roy, and Navrati Saxena “Next Generation 5G Wireless Networks: A Comprehensive Survey” IEEE Communications, 2016.

[3]. Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila and Andrei Gurtov “5G Security: Analysis of Threats and Solutions” IEEE Conference on Standards for Communications and Networking (CSCN),September 2017.

[4]. N. Alliance, “NGMN 5G white paper,” Next Generation Mobile Networks, White paper, 2015.

[5]. “5G security - enabling a trustworthy5G system” Whitepaper – Ericsson,2021

[6]. “5G wireless access: an overview” Ericsson,2021.
[7]. Fadoua Debbabi, Rihab Jmal , Lamia Chaari Fourati and Adlene Ksentini “Algorithmics and Modeling Aspects of Network Slicing in 5G and Beyonds Network: Survey”IEEE,2016.
[8]. “5G Scenarios and Security Design” Huawei 2016.
[9]. Mohamed Amine Ferrag,, Leandros Maglaras, Antonios Argyriou , Dimitrios Kosmanos and Helge Janicke “Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes” Journal of Network and Computer Applications, November 2017.
[10]. Goran Milenkovic, Dr. Marnix Dekker “Security In 5G Specifications” European Union Agency for Cybersecurity (ENISA).
[11]. Pankaj Kumar Dalela, Pramod Bhave, Pushpender Yadav, Anshul Yadav, Vipin Tyagi. "Beam Division Multiple Access (BDMA) and modulation formats for 5G: Heir of OFDM?",2018 International Conference on Information Networking (ICOIN), 2018.
[12]. Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. “A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions” IEEE Communications Surveys & Tutorials, 2019.
[13]. N. Panwar, S. Sharma, and A. K. Singh, “A Survey on 5G: The Next Generation of Mobile Communication,” Physical Communication, vol. 18, pp. 64–84, 2016.
[14]. M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov, “5G Backhaul Challenges and Emerging Research Directions: A Survey,” IEEE access, vol. 4, pp. 1743–1766, 2016.
[15]. R. N. Mitra and D. P. Agrawal, “5G Mobile Technology: A Survey,” ICT Express, vol. 1, no. 3, pp. 132–137, 2015.
[16]. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, “5G Security: Analysis of Threats and Solutions,” in Standards for Communications and Networking (CSCN), 2017 IEEE Conference on. IEEE, 2017, pp. 193–199.
[17]. Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov “Overview of 5G Security Challenges and Solutions,” IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, 2018.
[18]. P. Gandotra and R. K. Jha, “A survey on green communication and security challenges in 5G wireless communication networks,” Journal of Network and Computer Applications, vol. 96, pp. 39–61, 2017.
[19]. G. Choudhary and V. Sharma, “A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Networks,” in 5G Enabled Secure Wireless Networks. Springer, 2019, pp. 69–102.
[20]. D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. P¨opper, “On Security Research towards Future Mobile Network Generations,” IEEE Communications Surveys & Tutorials, 2018.
[21]. A.K. Rangisetti and B. R. Tamma, “Software Defined Wireless Networks: A Survey of Issues and Solutions,” Wireless Personal Communications, vol. 97, no. 4, pp. 6019–6053, 2017.

[22]. A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, "Software Defined Networking for Security Enhancement in Wireless Mobile Networks,"Computer Networks, vol. 66, pp. 94–101, 2014.
[23]. W. Li, W. Meng, and L. F. Kwok, "A Survey On OpenFlow-Based Software Defined Networks: Security Challenges and Countermeasures," Journal of Network and Computer Applications, vol. 68, pp. 126–139, 2016.
[24]. I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security In Software Defined Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2317–2346, 2015.
[25]. I. Alsmadi and D. Xu, "Security of Software Defined Networks: A Survey," computers & security, vol. 53, pp. 79–108, 2015.
[26]. Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602–622, 2016.
[27]. W. Yang and C. Fung, "A Survey On Security In Network Functions Virtualization," in NetSoft Conference and Workshops (NetSoft), 2016 IEEE. IEEE, 2016, pp. 15–19.
[28]. H. Jang, J. Jeong, H. Kim, and J.-S. Park, "A Survey on Interfaces to Network Security Functions in Network Virtualization," in Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on. IEEE, 2015, pp. 160–163.
[29]. Farris, T. Taleb, Y. Khettab, and J. S. Song, "A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems," IEEE Communications Surveys & Tutorials, 2018.
[30]. F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A Survey," Journal of Network and Computer Applications, vol. 88, pp. 10–28, 2017.
[31]. R. Tourani, T. Mick, S. Misra, and G. Panwar, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," arXiv preprint arXiv:1603.03409, 2016.
[32]. T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti, "A Survey on the Security of Stateful SDN Data Planes," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1701–1725, 2017.
[33]. Suvarna Patil, Vipin Patil and Pallavi Bhat "A Review on 5G Technology" International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 1, January 2012.
[34]. "5G The Nanocore" Next Generation by Imthiyaz Ali.
[35]. Manjurul H. Khan and P.C. Barman "5G- Future Generation Technologies Of Wireless Communication "Revolution 2020", American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN : 2320- 0936 Volume-4, Issue-5, pp-206-215.
[36]. Sk. Saddam Hussain, Shaik Mohammed Yaseen and Koushik Barman "An Overview of Massive MIMO System in 5G" I J C T A, 9(11) 2016, pp. 4957-4968.
[37]. Meenal G. Kachhavay and Ajay P.Thakare "5G Technology-Evolution and Revolution" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March-2014, pg. 1080-1087.

[38]. Saddam Hossain "5G Wireless Communication Systems" American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-02, Issue-10, pp-344-353.
[39]. Ekram Hossain and Monowar Hasan "5G Cellular: Key Enabling Technologies and Research Challenges" IEEE Instrumentation & Measurement Magazine.
[40]. Chen Sun, Student Member, XiqiGao, Shi Jin, Michail Matthaiou, Zhi Ding, and Chengshan Xiao "Beam Division Multiple Access Transmission for Massive MIMO Communications", IEEE Transactions on Communications, Vol. 63, No. 6, June 2015
[41]. Mamta Agiwal, Abhishek Roy and Navrati Saxena "Next Generation 5G Wireless Networks: A Comprehensive Survey" IEEE Communications Surveys & Tutorials, Vol. 18, No. 3, Third Quarter 2016.
[42]. Batalla, J. M., Andrukiewicz, E., Gomez, G. P., Sapiecha, P., Mavromoustakis, C. X., Mastorakis, G., … Imran, M. (2020). Security Risk Assessment for 5G Networks: National Perspective. IEEE Wireless Communications, 27(4), 16–22. doi:10.1109/mwc.001.1900524 .
[43]. M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Software-defined mobile networks security", Mobile Networks and Applications, vol. 21, no. 5, pp. 729-743, 2016.
[44]. Sankareswaran M "5G NR White Paper"2018.
[45] Dalela, P. K., Bhave, P., Yadav, P., Yadav, A., & Tyagi, V "Beam Division Multiple Access (BDMA) and modulation formats for 5G: Heir of OFDM?" International Conference on Information Networking (ICOIN),2018.
[46]. T.J. Berners-Lee, R. Cailliau and J.F. Groff "The world-wide web" Computer Networks and ISDN Systems, Elsevier Science Publishers B.V,25 (1992) 454-459.
[47]. Johnson, D. B and Maltz, D. A. "Dynamic Source Routing in Ad Hoc Wireless Networks" Mobile Computing, 153–181,1999.