5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey

To cite this article: Mamoona Humayun *et al* 2021 *J. Phys.: Conf. Ser.* **1979** 012037

View the article online for updates and enhancements.

5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey

Mamoona Humayun[1], Bushra Hamid[2], NZ Jhanjhi[3], G.Suseendran[4], M N Talib[5]

[1]dept of Information systems,College of Computer and Information Sciences, Jouf University Al-Jouf KSA
[2]University Institute of Information Technology, PMAS, Arid Agriculture University, Rawalpindi,Pakistan
[3]School of Computer Science and Engineering (SCE), Taylor's University, Malaysia
[4]Department of Information Technology, Vels Institute of Science, Technologyand Advanced Studies,Chennai,India
[5]Papua New Guinea University of Technology, Lae, PNG,Papua New Guinea
Email : mahumayun@ju.edu.sa[1], noorzaman.jhanjhi@taylors.edu.my[2], muhammad.talib@pnguot.ac.pg[3],bushrakiani@uaar.edu.pk[4],suseendar_1234@yahoo.co.in[5]

Abstract—5G is expected to bring tremendous advancement in wireless cellular network by providing faster speed, high capacity and low latency. It has widely been adopted in various parts of the world and is expected to bring a noteworthy revolution in major industries and overall economies. Although 5G service providers are promising integrity, confidentiality and availability of data, still security is an important concern that needs to be addressed. This paper provides a detailed survey on 5G security by addressing 5G opportunities, common threats targeting 5G network along with their mitigation strategies, security services offered by 5G networks and 5G security challenges. We have also provided a case study to demonstrate the potentials of 5G. This survey will help 5G researchers, service providers and 5G users in getting quick awareness of 5G network.

Keywords—5G (fifth generation), Cellular network, Wireless Communication, Security, Latency

1. INTRODUCTION

The target of wireless communication (WC) is to deliver reliable, and high quality communication just like wired communication and each new generation is a step towards this direction. 5G is a leap forward in this direction by providing high coverage and very high frequency by deploying dense base station (BS) with enhanced quality, extremely low latency and increased capacity [1, 2]. According to 5G public-private partnership, it is expected to connect about 7 trillion things or devices, and average service delivery time will decrease from 90 hours to 90 minutes with advance privacy. 5G aims at a smart and digital society empowered with high quality service availability by using diverse technologies [3, 4]as shown in Figure.1

Figure.1. Interconnectivity of diverse devices using 5G

Almost all industries and enterprises will get benefits from 5G technologies. However, some key industries that will leverage the benefits of 5G include healthcare, transportation logistics, manufacturing, agriculture, financial service providers, public sector, communication & entertainment and retail [5]as shown in Figure.2. Healthcare is one of the key sectors that will be revolutionized by leveraging benefits of 5G, including the increase of telehealth using smart devices in unserved areas, real-time patient monitoring using wearable technologies and data analytics. Transportation and logistics will be revolutionized using 5G in terms of the vehicle to vehicle communication; real-time data collection, analysis and communication; improve transportation and shipping time and by making vehicle fuel-efficient and less polluting. Manufacturing is also expected to benefit the most from 5G, lower latency and higher bandwidth will enable manufacturers to improve production standards, stay in contact with remote employees and real-time analysis for machines [6, 7].

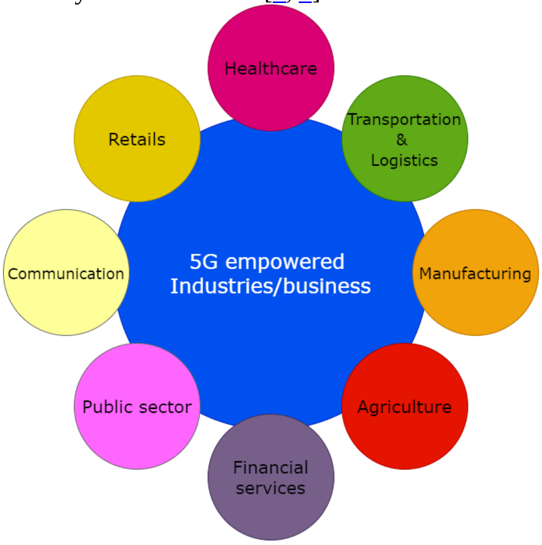

Figure.2. 5G empowered industries /business

5G will also improve the agriculture industry by providing smart farming, Figureht against climate change and increasing yields. The financial services industry is probable to get benefits from 5G in a big way by improving back-end processes, quick service delivery, mobile pay applications and more in-depth understanding of the customers. 5G is expected to revolutionize the public sector by making everything smart, 24/7 liaison with citizens and empowering government workforce with the latest technologies. Higher transfer speed and low latency of 5G is expected to bring significant improvement in communications. The high speed of 5G network will make communication a breeze. On the other hand, low latency will improve response time. Last but not least is retails that will be positively impacted by

5G. It will enable retailers to improve their services by transmitting a large amount of data to consumers [8, 9].

The above discussion shows that 5G is the need of the time and it will positively impact almost every field of life by connecting all aspects of life, however; it needs robust solutions and architecture to make it secure. Security and privacy of 5G network is a challenge for researchers and practitioners that need to be addressed to leverage its potential benefits. According to next-generation mobile networks (NGMN), some of the key challenges that are faced by 5G networks include; flash network traffic, user plane integrity, the security of radio interfaces, roaming security, signaling storms, Denial of service (DoS) attacks on the infrastructure and on end-user devices [10, 11]as shown in Figureure 3. Before providing any solution related to 5G network security and privacy, there is a need to synthesize key security issues, challenges and opportunities to provide detailed awareness to 5G researchers and practitioners. To do this, a detailed survey of 5G is provided in this paper.

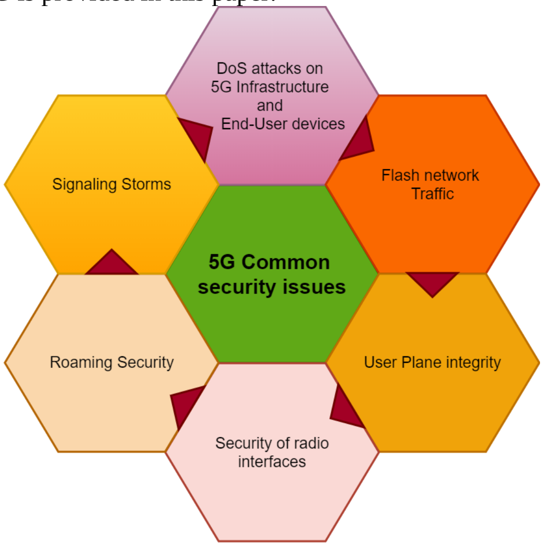

Figure.3. 5G common security issues

The remaining part of this paper is organized into 4 sections. Section 2 provides an overview of 5G literature that will include 5G Network,5G Network current and future research issues and challenges. Section 3 will provide a discussion on 5G. Paper will be concluded in section 4 by providing future research directions in section 5. The complete structure of the paper is shown in Figureure 4.

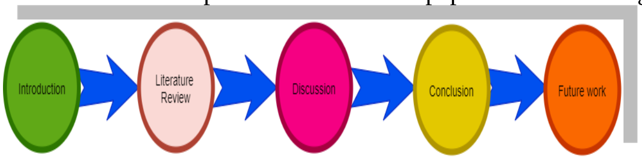

Figure. 4. Paper structure

2. Literature Review

This section of the paper will discuss 5G network opportunities, common security threats targeting 5G along with mitigation techniques, security services offered by 5G network providers and associated challenges.

2.1 5G Network opportunities

5G networks are expected to bring a great revolution in mobile broadband by providing enhanced opportunities to its users. Below we provide some important opportunities provided by 5G service providers to their clients[7, 12-15]

- Existing cellular networks are not sufficient to accommodate the tremendously increasing number of cellular phone users and data-intensive applications. 5G is expected to address this issue by providing high speed, more bandwidth and low latency.
- Various key sectors of economy, e.g. healthcare, manufacturing, education, energy, transportation and logistics will operate as anticipated without any failure.

- 5G will create a global digital economy by connecting everything everywhere.
- It will increase economic opportunities by providing easy access to social services, job hunting etc.
- It will provide affordable high speed internet access to people all around the world and thus will positively impact the communities of color.

2.2 Common Security Attacks on 5G Network and mitigation techniques

5G is a rapidly growing phenomenon with a lot of associated benefits; however; security is an issue that needs to be paid attention. Although 5G network providers are trying to provide secure and fast data transmission to its intended users, still there are chances of security attacks. In this section, we will provide some common security attacks along with mitigation techniques to help 5G practitioners

2.3 Eavesdropping and Traffic Analysis

It is a kind of passive attack in which an intruder tries to intercept a message from its intended receivers without affecting normal communication. This passive nature of the attack makes it difficult to detect; however, awareness, strong encryption, network access control, network segmentation and physical security are some measures that can mitigate the risk of eavesdropping. Another passive attack is traffic analysis in which intruders cannot access the data because it is encrypted; however, they try to intercept identity and location by analyzing traffic patterns. Recently, researchers are focusing on PLS analysis to tackle eavesdropping [14-17]. Figureure 5 shows the working of the eavesdropping attack

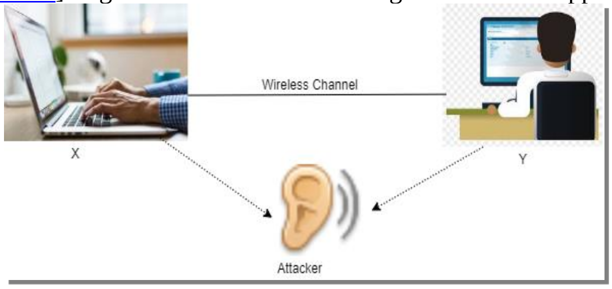

Figure. 5. Eavesdropping attack

According to Figureure 5, eavesdropper try to intercept a message to others by sensing traffic.

2.4 Jamming

Unlike traffic analysis and eavesdropping, jamming completely interrupt the communication between legitimate users. It prevents authorized users from accessing radio resources via intentional interference using malicious code. The jamming attack can be prevented using anti-jamming techniques e.g. spread spectrum technique(SST) and by using random key distribution method [16, 17]. Figureure 6 shows the working of the jamming attack

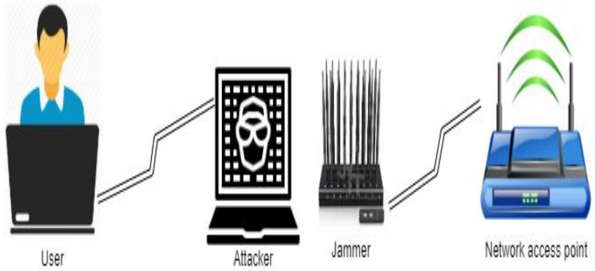

Figure.6. Jamming attack

2.5 DoS and DDoS

DoS and DDoS attacks are the key security issues for 5G operators due to massively interconnected devices. In this attack, attackers try to exhaust the network resources so that it may become unavailable for legitimate users. In DoS attack, attackers flood the server with TCP an UDP packets while in DDoS multiple systems target a system with DoS attack. DoS and DDoS attack can be seen in Figureure 7. DoS and DDoS attack can be prevented through more bandwidth, anti-DDoS hardware, DNS server protection, redundant infrastructure and proper network monitoring [15-17]

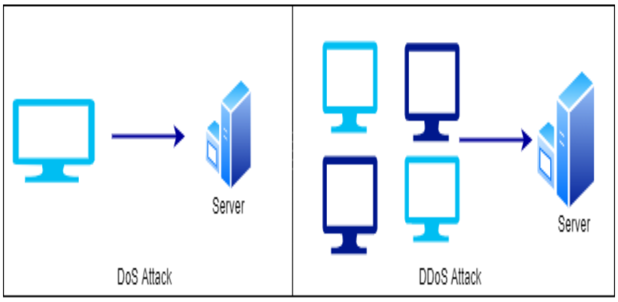

Figure.7. DoS and DDoS attack

2.6 Man-in-the-Middle attack (MITM)

MITM is a 4G vulnerability inherited by 5G; it is an attack in which intruder takes control of the communication channel between two legitimate users and intercept the message as per choice. It is a kind of active attack that compromise the availability, confidentiality and integrity of information. This attack can be prevented through mutual authentication, data encryption, using IDS solution, Security Services in 5G Network, awareness through employees training and base station [16, 18]. MITM is elaborated in Figureure 8

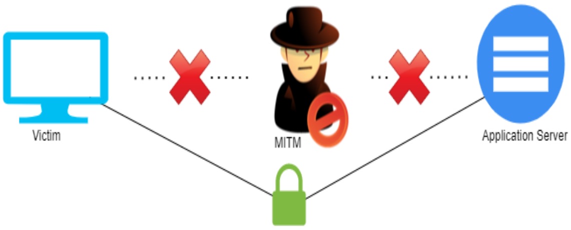

Figure.8. MITM attack

2.7 Security Services in 5G network

The latest technologies, new infrastructure, new architecture and 5G use cases provide new security requirements and services. This section will briefly elaborate some primary security services of 5G network

2.8 Authentication

Authentication in a 4G cellular network is mainly of two types: entity authentication and message authentication, entity authentication ensure that the communicating entity is the legitimate entity and is the same, which it claims to be. At the same time, message authentication ensures that the message to be communicated is from a legitimate user and is not been modified while transiting. The authentication between UE (user equipment) and MME (mobility management entity) in a 4G cellular network is symmetric-key based but this solution is not feasible in 5G. 5G not only need to ensure mutual authentication between UE and MME but also between service providers. Since 5G networks have varying trust models, new service delivery models, more privacy concerns than traditional cellular networks, therefore; flexible and hybrid mutual authentication of UE is required. This mutual authentication in EU is implemented in three ways, namely; authentication by service providers only, by the network only and by network and service providers only. Further, the multitier architecture of 5G demands quick handover and mutual authentication that need to be addressed using SDN enabled fast authentication and service-based architecture. To ensure authentication, 5G networks define three authentication methods namely; 5G-AKA (authentication and key agreement), EAP-TLS (extensible authentication protocol-transport layer security), and EAP-AKA.

2.9 Confidentiality

Confidentiality consist of two key concepts, namely; privacy and data confidentiality. Privacy refers to controlling and managing information of legitimate users. Privacy is mainly of three types, namely; data privacy, identity privacy and location privacy. All these privacy dimensions are equally important and need to be considered. On the other hand, data confidentiality ensures the protection of data from passive attacks during transmission. It needs limited access to intended users and preventing data disclosure to unauthorized users. Strong data encryption is used in 5G to preserve the confidentiality of data. Regarding privacy concerns; identity privacy can be preserved through anonymous authentication;

data privacy needs strong authentication and location privacy can be preserved through k-anonymity, location encryption and dummy location [17, 19].

2.10 Availability

Availability refers to the degree to which information or service is available to its intended users when and where required. This feature evaluates the robustness of a system and is one of the key performance metric used in 5G network. Attacks like DoS and Jamming make the service unavailable to users through interception. 5G network improves availability feature by providing more capacity and increased bandwidth. Still, massive interconnected IoT devices need more protection from these attacks. Pseudorandom time-hopping spread spectrum (PTHSS) and proper resource allocation can help in improving availability of information and services [19].

2.11 Integrity

Integrity is one of the key security requirements that prevent information from alteration and modification through active attacks by unauthorized entities. Malicious insiders compromise the integrity of data via insider malicious attacks e.g. code injection and data manipulation. Further, insiders are difficult to detect due to valid identities. 5G aims to provide massive interconnectivity of devices anytime and anywhere and is expected to support the applications that are closely related to human beings such as healthcare, transportation etc. In such cases, data integrity is a key challenge that needs to be addressed [4, 13].

2.12 5G Security Challenges

5G is expected to provide a lot of opportunities in every field of life; at the same time there are some challenges associated with it. Below we provide a brief overview of some key challenges faced by 5G network

2.13 New Trust Models

5G is expected to provide 10 times higher speed than 4G and will replace current Wi-Fi connections. However, building trust between network entities and stakeholders is a big challenge that needs to be addressed. Trust is an important factor for the adaptability; 5G operators need to make sure that every computing device has not been compromised. To do this, 5G service providers need to develop new trust models which need a new architectural approach. New trust models need to ensure the authenticity of hardware, operating system, network management and access management [12, 16].

2.14 More Privacy Concerns

The large volume of data transmission in 5G network poses the challenge of privacy. Massive interconnected devices, e.g. wearable IoT sensors, will transfer sensitive personal information that needs protection from cyber breaches. All three dimensions of privacy, namely; identity privacy, data privacy and location privacy need to be preserved. To do this, 5G service providers need to define new data granularity standards, strong encryption, awareness and proper identity management [7, 12, 13, 16].

2.15 New Security Attack Models

With the advancement in technology, attackers are coming with new ways to breach security. In such cases, end-to-end security is inevitable. Automated and sophisticated security features need to be built for monitoring and managing network devices. Some key security challenges expected to face 5G network providers include radio interface security, user plane integrity, flash network traffic, roaming security, DoS attack, signalling storms etc. [16].

2.16 New service delivery model

5G is not the replacement of previous network generation; rather, it is an enhancement with flexible new layers, high speed, low latency and more bandwidth. In such cases, new service delivery models are expected to emerge that will leverage the benefits from cloud computing, edge computing and SDN for delivering optimal network services [7, 15].

2.17 Threat Landscape

Massive interconnectivity and high-speed data transmission in a 5G network enhance threat landscape. In such cases, 5G service providers need to create comprehensive architecture, threat assessment, asset identification, exposure identification and proper network management and control for building client trust on 5G services. Key security attacks targeting each layer of 5G network need to be identified, and proper measures should be taken in advance to protect the network from internal and external cyber-attacks [12, 13, 16].

2.18 Case Study

Vodafone is a well-known Spain based cellular company that has launched 5G network cells phone. In this case, study a driving test of 5G was conducted in a metropolitan area of Madrid. The study was performed with Samsung Galaxy S10 (5G enabled devices) on two measurement days. The first day, the mobile setting was set to "5G preferred network" while on the second day it was set to "4G preferred network". The concentration was on measuring data connectivity; however, no voice measurement was done. The results of the two days were analyzed by comparing the performance of both networks. The results were positive, and as expected, the peak data rate using 5G preferred network rose up to 511.5 Mbps.

On the other hand, with 4G preferred network settings, 218.3 Mbps was maximum download data rate at the same location. Figureure 9 shows the area of Madrid where the test drive was performed. The spot marks in orange color show the areas where 5G Vodafone connection was provided.

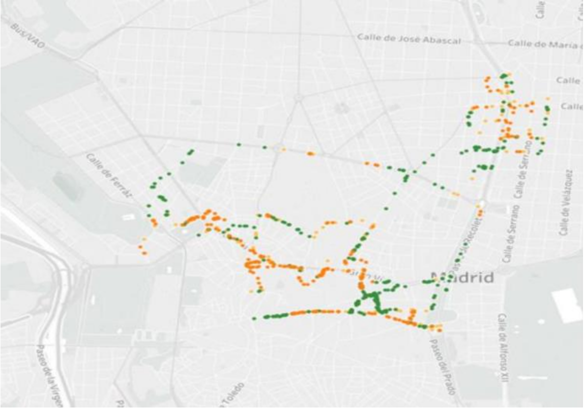

Figure.9. 5G test area of Madrid [20]

In the same way, the maximum upload speed for 5G network was 69.6 Mbps as compared to 4G preferred network that was 50.4 Mbps. Other than data rates, latency was also measured, during ping to various web services, an average latency in 4G/LTE preferred network was around 47 to 50 ms while the same ping reduced to 20 ms in case of 5G. Further, no security breach was reported. Although it was just a test drive for 5G network, still results were quite impressive as shown in Figureure 10

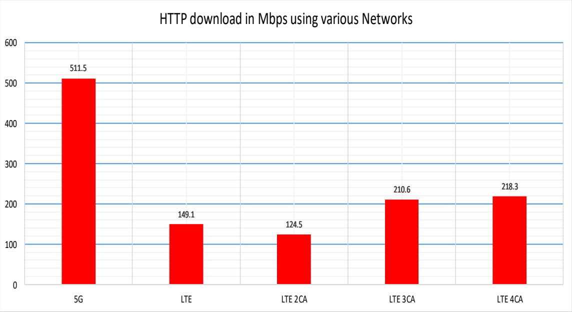

Figure.10. Comparison of 5G download speed with other networks [20]

Similarly, latency results can be seen in Figureure 11; there is a clear variation in the Latency of 5G Vodafone as compared to other networks

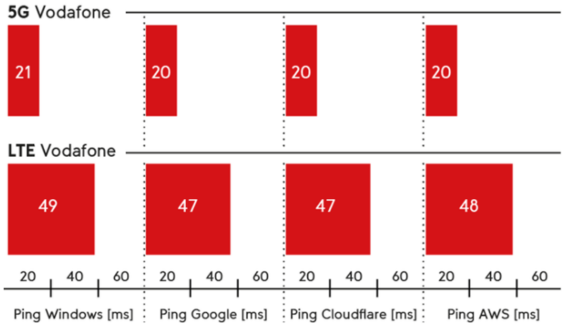

Figure.11. Comparison of 5G latency with other networks [20]

The above results show significant data speed and low latency in 5G cellular networks as compared to existing networks.

3. Discussion

The network operators all around the world are trying to shift on 5G. 5G is not only an advancement in existing 4G rather it's a big leap in terms of data rate, latency, capacity, bandwidth etc. However, in order to provide awareness to the common people as well as 5G researcher and practitioners, there is a need to synthesize 5G opportunities and challenges. To do so, we have conducted this survey, it provides an insight into 5G opportunities, challenges, 5G security services and common attack targeting 5G along with mitigation techniques.

We have also provided a case study of Spain-based cellular company to provide a comparison between 5G and existing networks. The results of the case study show that 5G is much better than 4G and other existing networks in terms of data rate and latency. However, still 5G is not implemented everywhere due to the scarcity of 5G enabled devices and cost. It is expected that in next few years, most of the cellular devices will support 5G and it will positively impact all the major sectors of life. Besides of that privacy issue is also highly considered in case of 5G [21-23]. In addition, smart IoT dependent applications where 5G can play an important role [24-25] such as E-health applications, body areas sensors applications, etc. will have higher boost using 5G. Security and privacy issues [26] will also increase with this growth.

4. Conclusion

This paper provides a survey on 5G network to provide state-of-the-art picture of 5G opportunities, security challenges, security services and its comparison with existing cellular networks. Some common attacks that are expected in the 5G network are discussed along with mitigation techniques. In the end, a comparison of 5G performance is evaluated using a case study and results are compared with existing studies. The case study results show a higher data rate and lower latency for the 5G over the existing networks.

5. Future Work

In the future, we are planning to extend our survey by providing more insights into 5G opportunities, challenges, issues and key security threats along with mitigation techniques with the help of more real-time case studies.

References

[1]. Duan, W., et al., Emerging technologies for 5G-IoV networks: Applications, trends and opportunities. IEEE Network, 2020.
[2]. Elayoubi, S.-E., et al. 5G innovations for new business opportunities. 2017.
[3]. Geller, M. and P. Nair, 5G security innovation with Cisco. Whitepaper Cisco Public, 2018: p. 1-29.
[4]. Khan, R., et al., A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. IEEE Communications Surveys & Tutorials, 2019. 22(1): p. 196-248.

[5]. Rao, S.K. and R. Prasad, Impact of 5G technologies on industry 4.0. Wireless personal communications, 2018. 100(1): p. 145-159.
[6]. Teece, D.J., 5G mobile: impact on the health care sector, in Working paper. 2017, Haas School of Business. p. 1-17.
[7]. Sharma, P.K., et al., Wearable Computing for Defence Automation: Opportunities and Challenges in 5G Network. IEEE Access, 2020. 8: p. 65993-66002.
[8]. Verma, L. and M. Lalwani, Digital Transformation: Impact of 5G Technology in Supply Chain Industry, in Technology Optimization and Change Management for Successful Digital Supply Chains. 2019, IGI Global. p. 256-274.
[9]. Campbell, K., et al., The 5G economy: How 5G technology will contribute to the global economy, in IHS Economics and IHS Technology. 2017, Qualcomm Technologies.
[10]. Alliance, N., Recommendations for NGMN KPIs and Requirements for 5G. techreport, June, 2016.
[11]. Javaid, N., et al., Intelligence in IoT-based 5G networks: Opportunities and challenges. IEEE Communications Magazine, 2018. 56(10): p. 94-100.
[12]. Zhang, P., et al., A survey of testing for 5G: Solutions, opportunities, and challenges. China Communications, 2019. 16(1): p. 69-85.
[13]. Li, G., et al., Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities. Entropy, 2019. 21(5): p. 497.
[14]. Wang, N., et al., Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. IEEE Internet of Things Journal, 2019. 6(5): p. 8169-8181.
[15]. Qiao, X., et al., Mobile web augmented reality in 5G and beyond: Challenges, opportunities, and future directions. China Communications, 2019. 16(9): p. 141-154.
[16]. Ahmad, I., et al. 5G security: Analysis of threats and solutions. in 2017 IEEE Conference on Standards for Communications and Networking (CSCN). 2017. IEEE.
[17]. Varga, P., et al., 5g support for industrial iot applications–challenges, solutions, and research gaps. Sensors, 2020. 20(3): p. 828.
[18]. Hussain, R., F. Hussain, and S. Zeadally, Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Computer Systems, 2019. 101: p. 843-864.
[19]. Hasnat, M.A., et al. Security Study of 5G Heterogeneous Network: Current Solutions, Limitations & Future Direction. in 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). 2019. IEEE.
[20]. https://www.connect-testlab.com/spain-2019-case-study-5g.
[21]. M. Humayun, N. Jhanjhi, M. Alruwailli, S. S. Amalathas, V. Balasubramaniam and B. Selvaraj, "Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things," in IEEE Access, doi: 10.1109/ACCESS.2020.3028764.
[22]. Alferidah, D. K., & Jhanjhi, N. Z. (2020). A Review on Security and Privacy Issues and Challenges in Internet of Things. International Journal of Computer Science and Network Security IJCSNS, 20(4), 263-286.
[23]. A. Almusaylim, Z., Jhanjhi, N. Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. Wireless Pers Commun 111, 541–564 (2020). https://doi.org/10.1007/s11277-019-06872-3
[24]. Alshammari, M. O., Almulhem, A. A., & Zaman, N. (2017). Internet of Things (IoT): Charity Automation. International Journal of Advanced Computer Science and Applications (IJACSA), 8(2).
[25]. Hussain, S. J., Irfan, M., Jhanjhi, N. Z., Hussain, K., & Humayun, M. (2020). Performance Enhancement in Wireless Body Area Networks with Secure Communication. Wireless Personal Communications, 1-22.
[26]. Natarajan, B., Obaidat, M.S., Sadoun, B., Manoharan, R., Ramachandran, S. and Velusamy, N., 2020. New Clustering-Based Semantic Service Selection and User Preferential Model. IEEE Systems Journal. DOI: 10.1109/JSYST.2020.3025407.
[27]. Nataraj, S.K., Al-Turjman, F., Adom, A.H., Sitharthan, R., Rajesh, M. and Kumar, R., 2020. Intelligent Robotic Chair with Thought Control and Communication Aid Using Higher

Order Spectra Band Features. IEEE Sensors Journal, DOI: 10.1109/JSEN.2020.3020971.

[28]. Babu, R.G., Obaidat, M.S., Amudha, V., Manoharan, R. and Sitharthan, R., 2020. Comparative analysis of distributive linear and non-linear optimised spectrum sensing clustering techniques in cognitive radio network systems. IET Networks, DOI: 10.1049/iet-net.2020.0122.

[29]. Sitharthan, R., Yuvaraj, S., Padmanabhan, S., Holm-Nielsen, J.B., Sujith, M., Rajesh, M., Prabaharan, N. and Vengatesan, K., 2021. Piezoelectric energy harvester converting wind aerodynamic energy into electrical energy for microelectronic application. IET Renewable Power Generation, DOI: 10.1049/rpg2.12119.

[30]. Sitharthan, R., Sujatha Krishnamoorthy, Padmanaban Sanjeevikumar, Jens Bo Holm-Nielsen, R. Raja Singh, and M. Rajesh. "Torque ripple minimization of PMSM using an adaptive Elman neural network-controlled feedback linearization-based direct torque control strategy." International Transactions on Electrical Energy Systems 31, no. 1 (2021): e12685. DOI: 10.1002/2050-7038.12685.

[31]. Fong, Teoh joo, Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). The Coin Passcode: A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices The Next Generation Swift and Secured Mobile Passcode Authenticator. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 10(1), 302-308.