International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6608
***Article Received**:18 February 2023 **Revised**: 29 March 2023 **Accepted**: 14 April 2023*

Security in 5G Networks: A Systematic Analysis of High-Speed Data Connections

V. Maruthi Prasad[1], Dr. B. Bharathi[2]
[1]Research Scholar, Department of CSE,
Sathyabama Institute of Science and Technology,
Deemed to be University, Jeppiaar Nagar, Chennai, Tamil Nadu 600119,
Email – maruthi.vv@gmail.com
[2]Research Supervisor, Department of CSE,
Sathyabama Institute of Science and Technology,
Deemed to be University, Jeppiaar Nagar, Chennai, Tamil Nadu 600119,
Email - bharathi.cse@sathyabama.ac.in

Abstract: Maximum user systems on 5G networks will now not be consumer phones or computers, but IoT device. Via 2021, there might be about 30 billion such devices. The quantity of attacks on the IoT is growing. Device protection is terrible and malware distribution is without problems scalable. Protection has ended up the primary challenge in many telecommunications industries these days as risks may have high outcomes. especially, because the center and enable technologies might be related to the 5G network, the confidential information will pass at all layers in destiny Wi-Fi structures. Even with modern-day 4G networks, now not each operator succeeds in securely configuring the center network and protecting it from all angles. As SDN and NFV are carried out for network cutting in 5G, the administration will become even extra difficult. Flexibility in 5G networks comes at the fee of multiplied complexity and high bandwidth communication settings to monitor. 5G will offer broadband access anywhere, entertain better person mobility, and permit connectivity of a large number of devices in an ultra- reliable and low-priced manner. Furthermore, we present protection solutions to those demanding situations and future instructions for secure 5G systems.

Keywords: 5G network, security, Software Defined Networking (SDN), Network Function Visualization (NFV) Telecommunication, Communication Channels.

I. INTRODUCTION

(Jinsong, M., & Yamin, M. 2020) Each new age of versatile guidelines since 2G has been intended for very much the same objective: to help data transmission on bundle organizations. Quicker Internet access is the situation. Different changes have been negligible. The 3G voice codec was only slightly revised. Many network managers have yet to deploy the IP Multimedia Subsystem (IMS), which is used by 4G networks to transmit voice traffic over bundle data. It's possible that the 4G organisation doesn't use voice communication at all, instead relying only on the 2G/3G networks to make decisions. In contrast to their forerunners, modern portable organisations have a few drawbacks. The energy efficiency requirements of the Internet of Things (IoT) make 3G and 4G networks less than optimal. That's why you have to keep your devices plugged up or constantly swap out their batteries. This is inadmissible for some IoT gadgets, which may require a battery life of as long as 10 years without trading or charging batteries.

(Olimid, R. F., & Nencioni, G. 2020) The advancement of versatile organizations offered to fulfill the new requests for improved execution, reliability, flexibility, and energy effectiveness of novel organization administrations. 5G portable organizations receive new systems administration ideas to additionally improve these highlights. The media transmission normalization bodies are chipping away at coordinating novel systems administration ideas like **(Liyanage, M., et al 2018)** implementation strategies for telecom companies using Software Defined Networking (SDN), Network Function Virtualization (NFV), distributed computing, Multi-access Edge Computing (MEC), and Network Slicing (NS). The objective of these efforts is to organise another another mobile product-based business. It will aid in the development of new business administrations to meet the need for scalable business development in the future. The SDN concept suggests disentangling the systems management tools' control and data planes. SDN-based networks have a single controller in which control and visibility are centralised. It may also provide a theoretical foundation for the underlying control mechanisms and business functionality. New approaches to developing, delivering, and managing infrastructure services are proposed by NFV. This concept intends to free the organization's capabilities from cumbersome machinery in favour of executing them as coding examples. On-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6608
***Article Received**:18 February 2023 **Revised**: 29 March 2023 **Accepted**: 14 April 2023*

demand network flexibility is a key benefit of distributed computing and MEC. In a 5G network, traffic of all types receives better support thanks to the reduction in red tape. Since the stakes are so high in these new media transmission networks, security and protection have risen to the top of the list of concerns.

(Ji, X., et al 2018) The purpose of 5G groups is to reflect these varying needs. They may provide lightning-fast connectivity with almost no downtime. They may arrange slower speeds with less device resources needed at the same time. Non-Standalone (NSA) is designated for the first wave of 5G companies and devices. The 4G networks we now have will support the 5G radios. Overall, IoT-enabled devices will rely on 4G and surprisingly 2G/3G organisations for voice calls and SMS informing, while connecting with 5G frequencies for information transmission due to the need for higher transfer speeds and lower inertia. In this way, in any event during the progress time frame, future 5G organizations will acquire every one of the weaknesses of past generations.

II. LITERATURE REVIEW

(Kursheed, B., & Budyal, V. R. 2020) explained with the expanding development in the remote correspondence frameworks, the data transmission necessity is additionally constantly expanding, and the expanding requests make the remote correspondence assets increasingly scant. Psychological radio innovation encourages a compelling answer for data transfer capacity shortage through a cycle of dynamic and deft range sharing over heterogeneous remote organizations. Be that as it may, the major objective of the 5G correspondence framework-based organization is to offer broadened inclusion, an extremely high information move rate, monstrous availability with the least inactivity as execution measurements of 5G correspondence framework. To accomplish these prerequisites, the 5G frameworks misuse the range from 30Ghz to 300GHz. This paper presents different parts of the hypothetical foundation that relate the examination experiences of psychological radio innovation, range sharing, and 5G correspondence framework. The construing of the examination advancement and patterns in the area of the community-oriented investigation of range detecting, psychological radio, and 5G gives future exploration bearings dependent on the research gap analysis.

(Gkonis, P. K., et al 2020) revealed about, an extensive report is given in regards to the most recent accomplishments in recreation procedures and stages for fifth-age (5G) remote cell organizations. In this case, it can be computationally demanding to estimate a wide range of performance metrics such as uplink and downlink throughput, mean Bit Error Rate, number of active clients, probability of blackout, handover rate, delay, inactivity, etc., due to the various boundaries that must be consolidated in the framework and connection-level reenactments. For instance, mmWave transmission, massive multiple inputs and multiple outputs (MIMO) models, and non-orthogonal multiple access (NOMA) are some of the potential solutions for 5G interfaces. This necessitates a more accurate and realistic depiction of channel coefficients and overall blockage in comparison to other cell interfaces. Increases in flag weight and handoffs are also inevitable as the number of directional pillars grows. Radio infrastructure planning will also face challenges related to the need for 5G networks to work in tandem with the 4G networks already in use. Finally, the potential misuse of 5G systems in future electrical keen matrices to support high data transfer capacity and zero idleness applications (such as semi or fully autonomous driving) directs the need for the development of reenactment conditions able to fuse the various components of 5G remote cell organisations.

(Gupta, A., 2018) All over the world, there is a colossal mix in the number of endorsers which offered meet people's high expectations, similar to obstruction the executives and limit upgrade. The empowering contender to manage this predicament is the empowering innovations of the 5G remote correspondence organizations. Despite the fact that the enhancements brought about by 5G suit the growing requirements, safety is nonetheless a key problem. With the game-hypothetical study of transfer speed satirising attack on the multistage 5G remote communication organisation, this research draws attention to the security challenges that are associated with 5G remote communication networks. The suggested Adaptive Intrusion Detection System is used to determine whether or not there was an intrusion on the transfer, the tiny cell passageway, and the base station, all of which are contributing to the formation of a multistage 5G distant communication organisation.

(Dahiya, M. 2017) As the client turns out to be more inspired by remote correspondence innovation, he/she will search for the ideal bundle that incorporates every one of the main highlights of remote correspondence innovation can have. Accordingly, the pursuit for cutting-edge innovation is everlastingly the excellent goal of the main remote correspondence innovation supplier to out-advance their opponents. Embellishment, the superb point of the 5G remote organizations is projected to engineering the incomparable remote world which is liberated from detriments and troubles of the former ages. 5G advancements will supplant the style max high data transmission clients associate their Mobile Radio Communication (MRC). Accordingly, this paper covers, prologue to 5G advancements, the requirement for 5G, their benefits,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6608
***Article Received**:18 February 2023 **Revised**: 29 March 2023 **Accepted**: 14 April 2023*

extraordinary applications, and the engineering of 5G networks.

(Munisankaraiah, S., & Arun Kumar, A. 2017) The fifth-generation (5G) organisation would be a critical facilitator to keeping up with the future remote application requirements, such as super high information rate, super broad radio inclusion, super low dormancy, countless devices connected, and so on. Keeping up with these requirements would be essential to keeping up with future remote application demands. Since distant communications by their very nature are susceptible to being broken into or hacked by malicious actors, security is a very important concern for the 5G organisation. In this study, the security problem that exists inside 5G networks, more specifically the real layer security, is broken down and examined. The real layer safeguards the confidentiality of the data by taking use of the inherent arbitrariness of the medium via which the communication takes place. There are several different advancements that are prevalent in 5G; however, the three most prominent ones—heterogeneous organisations, huge diverse information numerous yield, and millimeter-wave—have been considered and investigated. The potential problem areas and growth areas that are present in each of the technologies have been identified and broken down. This analysis will aid in the future when it comes to gaining a better understanding of real layer security.

III. OBJECTIVES OF THE STUDY

[1] To analyze and discusses in detail different security challenges related high bandwidth systems to key areas of 5G security.
[2] To Identify and converse the opportunities in security and privacy related to the 5G technologies.
[3] To examine the security issues and counteractions in 5G network monitoring and management.
[4] To review a few narrow objectives in retreat protections and security mechanisms in the 5G networks.

IV. KEY AREAS OF 5G SECURITY CHALLENGES

(Wu, Y., et al 2018) The coming 5G organizations can detonate vertical enterprises, empowering the formation of a wide exhibit of new administrations, all of which will request new, changing degrees of safety.

Independent Vehicles: The danger of auto digital assaults will ascend as self-governing vehicles become more inescapable. To battle this, the National Highway Traffic Safety Administration utilizes a complex way to deal with network protection as it endorses driver help advances.

Medical services: In the medical services field, 5G capacities will assist with the quicker exchange of huge patient documents, far off a medical procedure, and distant patient observing using IoT gadgets among different advances. In any case, those advances are tempered by the requirement for ever-more grounded security through high bandwidth systems in 5G security. Making chances that incorporate clinical deception, attack of wellbeing security, and clinical information the board. The above Wipro report expresses that the medical services industry was the objective of 48% of information penetrates in 2018. It adds that the development of IoT device use will make managing expanding network safety chances seriously testing.

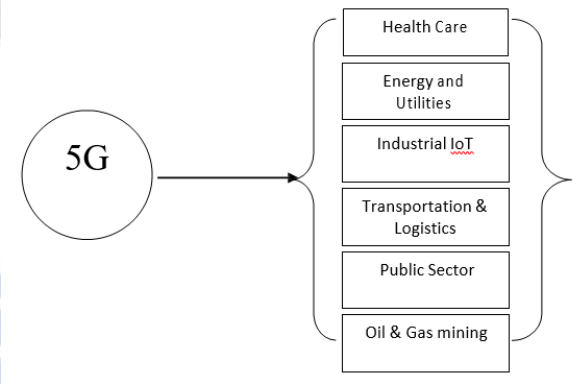

Fig 1 : 5G can transform various industries

Smart homes: Biometric recognisable proof, like that found in Sensory's programming that makes use of voice and face acknowledgment, or the assortment of finger impression access entryway locks available at home improvement stores, will be required for 5G-enabled smart homes. Multiple hacks of Amazon's Ring home video security product in December 2019 caused a stir, as hackers could potentially get access to customers' cameras in their homes and on their front porches and patios.

When all is said in done, IoT devices and sensors will request more mind-boggling confirmation to forestall unapproved access.

V. OPPORTUNITIES IN SECURITY AND PRIVACY RELATED TO THE 5G TECHNOLOGIES

(Panwar, N., & Sharma, S. 2020) 5G expands upon past 4G networks and is essential for the advancement in broadcast communications innovation. Almost certainly the innovation will take into account sensational new mechanical development, and yet, it represents some protection issues. The new organizations take into account information to be communicated from a more extensive number of web of-things gadgets to versatile transporters. The information they will get will be considerably more

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6608
***Article Received**:18 February 2023 **Revised**: 29 March 2023 **Accepted**: 14 April 2023*

explicit and created quicker than at any other time with lower inertness.

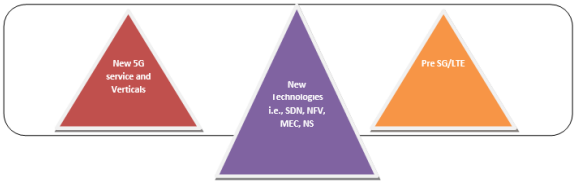

Fig 2 : 5G and Beyond 5G Security Requirements

5G additionally offers a higher transfer speed than past networks. The analyst compares it to interstate with a bigger number of paths than its archetypes, considering traffic to move quicker and more vehicles to be out and about. Protection experts may feel 5G addresses different boondocks brimming with difficulties. The GSMA, a versatile interchanges industry gathering, is amidst concluding a white paper on the potential protection chances encompassing 5G. With exceptionally precise information coming in at quicker rates, protection experts should zero in on guaranteeing associations are straightforward with how information is utilized and how to deal with social affairs assent for information preparing exercises occurring continuously. The whole of 5G may appear to be overpowering; in any case, the researcher trusts 5G can likewise be an extraordinary chance for protection experts, as long as they play it safe.

VI. 5G NETWORK MANAGEMENT AND MONITORING

(Celdrán, A. H., et al 2017) Answers for the Next Generation of 5G and IoT Network Deployments, centers on the enablement of continuous organization insight, observing, and investigation at the edge. This subject is opportune as broadcast communications transporters are preparing their fifth-age, or 5G, network organizations. The guarantee of higher velocities, lower inactivity, and more noteworthy throughput has shown up to convey improved advanced encounters and further empower the proceeded with development of the Internet of Things (IoT) network and connections. 5G and IoT encounters are anything from expanded or computer- generated reality (AR/VR) customer encounters, venture correspondences, streaming substance, associated urban areas, self-governing vehicles, intelligent computerized wellbeing, mechanical computerization, and associated homes - the requirement for solid 5G availability among the expanded thickness of gadgets utilizing those organizations is here. Thus, with more gadgets interfacing this makes new worries around execution and security for organization and security activities groups. What can endeavor networks do from a 5G networks identify, insight, and observing perspective to get ready to deal with the storm of information coming their way from extra end-focuses? (Mullins, et al 2017) In the first place, "the edge", or the edge of organizations accepting information is the key area to zero in on for streamlining traffic conveying 5G and IoT encounters. These cutting-edge organizations will progressively depend on half-breed SDN and progressed investigation explicitly working related to insightful work processes for business

measure rationale execution. Accordingly, we see a basic spotlight on carrying out checking and investigation to empower network knowledge at the edge.

(Irazabal, M., et al 2019) 5G adaptation and client experience depend on guaranteeing that 5G rollouts are done well since day zero. 5G presents another radio innovation and new recurrence groups, which makes smartphones much more intricate.

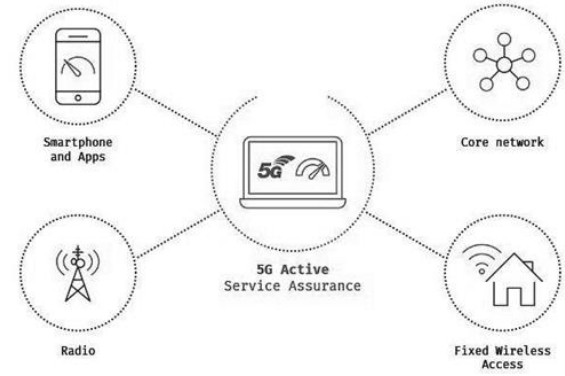

Fig 3 : 5G Active Service Management

The main 5G gadgets should uphold Dual Connectivity with both LTE and 5G. Besides, 5G organizations are planned from start considering virtualization, which will empower new highlights, for example, network cutting. Notwithstanding, this will bring expanded intricacy and make difficulties in disconnecting administration issues, particularly in multi-merchant conditions.

VII. PROTECTION AND MECHANISM IN THE 5G NETWORKS

(Zhan, W., & Tao, Z. 2020) To accomplish interoperability, and guarantee execution ensures as illustrated above, 5G versatile organizations should interconnect with heritage organizing arrangements and different access advancements. This calls for consistent versatility, network the executives, and execution affirmation, requiring specialized and business commitment between different innovation suppliers. Therefore, the security of 5G organizations, frameworks, and administrations is presently more testing than heritage

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6608
***Article Received**:18 February 2023 **Revised**: 29 March 2023 **Accepted**: 14 April 2023*

frameworks, thinking about the different kinds of subordinate organizations, gadgets, and administrations included. Security instruments for 5G frameworks should subsequently meet the accompanying in general prerequisites

Cross-layer security: (Gaber, C., 2020) whilst diverse security advances are successful in their areas, a brought together structure is important to organize these advances over various security layers. Inside this report, these layers are characterized as:

[1] Services, Applications, and Use Cases,
[2] Users and Things
[3] Inter-organizing
[4] 5G Mobile Network and Virtualization Systems
[5] Physical Infrastructure

This is to guarantee that a gap in one layer doesn't invalidate the advantages acquired in others. See this Section

End-to-end security: (Kumari, K. A., et al 2018) As in heritage frameworks, it is crucial to have security affirmation in the correspondence ways between client gadgets and the endpoint of the central organization, including radio access and transport network spine. New difficulties emerge because of the circulated and profoundly adaptable nature of 5G frameworks and organizations.

Cross-area security: (Kim, J. T., 2003) Problems with interoperability arise when different domains of authority, such as departments, agencies, and pieces of technology, collide. Because of the wide variety of use cases, each with unique performance requirements, and the recent addition of players like virtualization innovation sellers and suppliers to 5G frameworks, careful planning and coordination among stakeholders are needed to ensure that integrated arrangements are inherently secure and cross-layer security is also guaranteed across various domains. It's important to distinguish between cross-area security and cross-layer security; for example, cross-layer security is something that must be implemented in every space so that they may securely collaborate with other spaces.

Secure-by-plan: (Ricart-Sanchez, R., 2018) Security should be essential for the planning cycle and security arrangements should be sent right off the bat. Such a methodology limits potential gaps which may not be not difficult to address after the framework is completely sent and utilitarian.

VIII. OTHER RELATED/FUTURE INNOVATIONS TO IMPROVE SECURITY AND PROTECTION IN 5G

(Salva-Garcia, P., 2018) With the development of omnipresent figuring, it is normal that setting mindful correspondence and systems administration will overwhelm in past 5G time. A large number of things to come applications need solid admittance to different wellsprings of setting data. For example, exact area data on both inside and outside will be needed to offer media conveyance without fail and all over, quick record partaking as cell broadcasting and remote vehicle video administrations. Future versatile correspondence organizations (past 5G) are likewise as often as possible incorporated with IoT/IoE networks to give a wide scope of novel

administrations. In this manner, toward one side, these heterogeneous sorts of organizations will be viewed as urgent for improving setting mindfulness however on the opposite end, security and protection dangers will likewise arise. Enemies can target such organizations all the more effectively to dispatch different security assaults. Likewise, as clients are normally keen on securing their protection and subsequently just the necessary data will be gathered for the motivations behind setting mindful activity. Accordingly, setting mindfulness-based security system requires canny and controlled arrangements by the organization administrator and other included investors.

IX. FUTURE IMPLICATIONS AND RECOMMENDATIONS:

Bringing miniature division into 5G portable organizations has a few distinctive examination challenges. Our future work incorporates researching how the miniature division idea can be executed in versatile organization engineering. By and large, there should be a path to how to coordinate the various functionalities of versatile organizations with SDN and network virtualization developments.

This paper features a few provokes that should be tended to if the nation wishes to be an innovator in the turn of events and organization of 5G. Specifically, the requirement for additional venture and development identified with:

1) Cross-layer norms and structure empowering start to finish security for focused on basic or vertical section use cases,

2) another way to deal with foresee and pre-approve cross-layer user equipment (UE) associations, using Artificial Intelligence (AI) and setting mindful systems administration, to guarantee 5G execution isn't undermined,

3) An association that is entrusted to help screen and energize great security-by-plan practice, and set out and report a way to deal with planning secure 5G organizations, applications, and administrations,

4) Standardization and security tests and preliminaries

X. CONCLUSION

As the 5G network environment evolves, more and more security threats emerge across a wide range of layers and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6608
***Article Received**:18 February 2023 **Revised**: 29 March 2023 **Accepted**: 14 April 2023*

use cases. In order to provide a substantial understanding of the security difficulties, this study has examined 5G security challenges and high bandwidth networks via comprehensive studies and dialogues based on publicly available information. We've looked at the whole analysis of the 5G security model, the most recent risk scenario for 5G, the IoT risk scenario, and the reviews of threats in 5G networks. Validation, access control, correspondence security, and encryption are all vital components of 5G security, and we conducted comprehensive analyses of the corresponding problems. Software-defined networking (SDN), network function virtualization (NFV), distributed computing, multi-access edge computing (MEC), and network slicing (NS) are all examples of important 5G developments that were highlighted in the report, along with the unique security challenges they provide. 5G will uphold the vision of "everything associated". Rather than singular security components, the precise and logical. The approach is needed5G security can't be "replicated" from 4G (or more seasoned) security. While there are as yet substantial security approaches they should be returned to (trust models, gadgets, assurance). Attacker targets incorporate practically everything: client gadgets, access and center networks, home and outside networks. To execute miniature division, SDN and virtualization advancements are required. There should be a network virtualization stage that can make virtual networks that are detached from the actual network. Likewise, versatile network administrators and virtual portable network administrators would profit from the arrangement as they would have the option to give enough get sections of the versatile network for additional utilization.

REFERENCES

[1] Celdrán, A. H., Pérez, M. G., García Clemente, F. J., & Pérez, G. M. (2017). Automatic monitoring management for 5G mobile networks. In Procedia Computer Science (Vol. 110, pp. 328–335). https://doi.org/10.1016/j.procs.2017.06.102

[2] Dahiya, M. (2017). Need and Advantages of 5G wireless Communication Systems Network Security View project Need and Advantages of 5G wireless Communication Systems. International Journal of Advance Research in Computer Science and Management Studies, 5(6). Retrieved from https://www.researchgate.net/publication/321864810

[3] Gkonis, P. K., Trakadas, P. T., & Kaklamani, D. I. (2020). A comprehensive study on simulation techniques for 5G networks: State of the art results, analysis, and future challenges. Electronics (Switzerland). https://doi.org/10.3390/electronics9030468

[4] Gaber, C., Vilchez, J. S., Gur, G., Chopin, M., Perrot, N., Grimault, J. L., & Wary, J. P. (2020). Liability-Aware Security Management for 5G. In 2020 IEEE 3rd 5G World Forum, 5GWF 2020 - Conference Proceedings (pp. 133–138). https://doi.org/10.1109/5GWF49715.2020.9221407

[5] Gupta, A., Jha, R. K., Gandotra, P., & Jain, S. (2018). Bandwidth Spoofing and Intrusion Detection System for Multistage 5G Wireless Communication Network. IEEE Transactions on Vehicular Technology, 67(1),618–632. https://doi.org/10.1109/TVT.2017.2745110

[6] Irazabal, M., Lopez-Aguilera, E., & Demirkol, I. (2019). Active Queue Management as Quality of Service Enabler for 5G Networks. In 2019 European Conference on Networks and Communications, EuCNC 2019 (pp. 421–426). https://doi.org/10.1109/EuCNC.2019.8802027

[7] Jinsong, M., & Yamin, M. (2020). 5G network and security. In Proceedings of the 7th International Conference on Computing for Sustainable Global Development, INDIACom 2020 (pp. 249–254). https://doi.org/10.23919/INDIACom49435.2020.9083731

[8] Ji, X., Huang, K., Jin, L., Tang, H., Liu, C., Zhong, Z., … Yi, M. (2018). Overview of 5G security technology. Science China Information Sciences. https://doi.org/10.1007/s11432-017-9426-4

[9] Kumari, K. A., Akash, S. A., Sadasivam, G. S., Radhika, E. G., & Gowri, S. S. (2018). An Approach for End-to-End (E2E) Security of 5G Applications. In Proceedings - 4th IEEE International Conference on Big Data Security on Cloud, BigDataSecurity 2018, 4th IEEE International Conference on High Performance and Smart Computing, HPSC 2018 and 3rd IEEE

[10] International Conference on Intelligent Data and Security, IDS 2018 (pp. 133–138). https://doi.org/10.1109/BDS/HPSC/IDS18.2018.00038

[11] Kim, J. T., Koh, C., & Choi, J. T. (2003). A protection of mobile system in network systems. In Proceedings of the International Conference on Security and Management (Vol. 2, pp. 426–432).

[12] Kursheed, B., & Budyal, V. R. (2020). Survey: 5G wireless communication using cognitive radio. Indian Journal of Computer Science and Engineering, 11(5), 658–669. https://doi.org/10.21817/indjcse/2020/v11i5/201105231

[13] Liyanage, M., Porambage, P., & Ding, A. Y. (2018). Five driving forces of multi-access edge computing. arXiv.

[14] Mullins, Robert; Taynann, M. (2017). Cognitive Network Management for 5G. 5GPPP Working Group on Network Management and QoS, 1.02, 1–40. Retrieved from https://5g-ppp.eu/wp-content/uploads/2016/11/NetworkManagement_WhitePaper_1.0.pdf

[15] Munisankaraiah, S., & Arun Kumar, A. (2017). Physical layer security in 5G wireless networks for data protection. In Proceedings on 2016 2nd International Conference on Next Generation Computing Technologies, NGCT 2016 (pp. 883–887). https://doi.org/10.1109/NGCT.2016.7877535

[16] Olimid, R. F., & Nencioni, G. (2020). 5G Network Slicing: A Security Overview. IEEE Access. https://doi.org/10.1109/ACCESS.2020.2997702

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v11i5.6608
***Article Received**:18 February 2023 **Revised**: 29 March 2023 **Accepted**: 14 April 2023*

[17] Panwar, N., & Sharma, S. (2020). Security and Privacy Aspects in 5G Networks. In 2020 IEEE 19th International Symposium on Network Computing and Applications, NCA 2020. https://doi.org/10.1109/NCA51143.2020.9306740

[18] Ricart-Sanchez, R., Malagon, P., Alcaraz-Calero, J. M., & Wang, Q. (2018). Hardware- Accelerated Firewall for 5G Mobile Networks. In Proceedings - International Conference on Network Protocols, ICNP (Vol. 2018–September, pp. 446–447). https://doi.org/10.1109/ICNP.2018.00066

[19] Salva-Garcia, P., Alcaraz-Calero, J. M., Wang, Q., Bernabe, J. B., & Skarmeta, A. (2018).

[20] 5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks. Security and Communication Networks, 2018. https://doi.org/10.1155/2018/9291506

[21] Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K. K., & Gao, X. (2018). A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. IEEE Journal on Selected Areas in Communications, 36(4), 679–695. https://doi.org/10.1109/JSAC.2018.2825560

[22] Zhan, W., & Tao, Z. (2020). Research on 5G Mobile Communication Network Security Technology. In Journal of Physics: Conference Series (Vol. 1634). https://doi.org/10.1088/1742-6596/1634/1/012055

[23] Supriya, S., Bharathi, B. (2015). Efficient privacy preserving authentication for vehicular Ad-Hoc Networks. ARP Journal of Engineering and Applied Science 10(20), PP. 9233 – 9240