ISSN 2320 - 2602
Volume 13 No. 1, January 2024
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst031312024.pdf
https://doi.org/10.30534/ijacst/2024/031312024

The Impact of 5G Networks on the Development of Connected and Autonomous Cars

Tejashwini G Jampannanavar[1],Tharun Kumar R[2],T.M.Bharath Kumar[3],Y.V.Karthikeya[4], Prashanth Kumar [5]
Students, Department of Computer Science and Engineering[1,2,3,4]
Assistant Professor, Department of Computer Science and Engineering[5]
[1]Alva's Institute of Engineering and Technology,India,tejashwini82g@gmail.com
[2]Alva's Institute of Engineering and Technology,India,tharungowda0046@gmail.com
[3]Alva's Institute of Engineering and Technology,India,tmbharathk@gmail.com
[4]Alva's Institute of Engineering and Technology,India,4al20cs172karthikeya@gmail.com
[5]Alva's Institute of Engineering and Technology,India,prashanthjune18@gmail.com

Received Date : November 29 , 2023 Accepted Date : December 29, 2023 Published Date : January 07, 2024

ABSTRACT
Smart The development of connected and autonomous cars (CACs) is set to revolutionize transportation, offering increased safety, efficiency, and convenience. However, the widespread adoption of CACs relies heavily on the availability of reliable and high-speed wireless networks. This paper explores the impact of 5G networks on CACs, focusing on their ability to provide higher speeds, lower latency, and greater capacity. Additionally, it examines the benefits of 5G for CACs, including improved safety, increased efficiency, and the emergence of new transportation services. The paper concludes that 5G networks play an important role in advancing CAC technology and driving its adoption. 5G networks pave the way for the emergence of new transportation services that can revolutionize the mobility landscape. With the high-speed and low-latency capabilities of 5G, CACs can seamlessly connect to other smart devices and infrastructure, enabling innovative services such as ride-sharing, on-demand transportation, and mobility-as-a-service (MaaS) platforms. These services can transform the way people access transportation, offering flexible and convenient options that cater to individual needs

Key words: 5G networks, connected cars, autonomous cars, vehicle-to-vehicle communication, vehicle-to-infrastructure communication, real-time data processing, cybersecurity, driver assistance systems.

1. INTRODUCTION

The advent of the fifth generation (5G) of wireless communication has ushered in a new era of connectivity, promising unprecedented speed, reliability, and low latency. This technological leap not only transforms the way we communicate but also holds profound implications for various industries, including the automotive sector. In recent years, the automotive industry has been undergoing a paradigm shift towards connected and autonomous vehicles, leveraging the capabilities of 5G networks to redefine the driving experience.

The integration of 5G networks with connected and autonomous cars represents a pivotal moment in the evolution of transportation technology. As we move towards a future where vehicles are not merely modes of transportation but intelligent entities capable of communication, coordination, and decision-making, the role of 5G becomes increasingly crucial. This review explores the multifaceted impact of 5G on the development and deployment of connected and autonomous cars, delving into the technological advancements, challenges, and broader implications for society. To appreciate the significance of 5G in the automotive landscape, it is imperative to trace the evolution of connectivity in vehicles. From basic telematics systems to the integration of 4G LTE, each phase has laid the groundwork for the comprehensive connectivity solutions that 5G promises. The transition from disconnected, standalone vehicles to a seamlessly connected network of cars marks a transformative period in the automotive industry. The unique capabilities of 5G, including ultra-low latency, high data transfer rates, and massive device connectivity, open up new possibilities for connected and autonomous vehicles. The paper explores how these features enable real-time communication between vehicles, infrastructure, and cloud-based systems, fostering an environment where cars can make split-second decisions, enhance safety, and optimize traffic flow. As we embark on this exploration of the symbiotic relationship between 5G and the automotive industry, it is evident that the intersection of these technologies holds immense promise for the future of transportation. The subsequent sections of this paper will delve into specific aspects, shedding light on the intricate dynamics and unveiling the transformative potential that 5G brings to the realm of connected and autonomous cars These visual aids serve as integral components of the narrative, providing readers with a comprehensive and accessible understanding of the intricate interplay of the 5G networks and the development of connected or autonomous cars.

2. ARCHITECTURE

The 5G networks offer exceptional reliability, ensuring that the communication between connected and autonomous cars remains steadfast and uninterrupted. The reliability of 5G is achieved through various means, such as redundant infrastructure, advanced error correction techniques, and dynamic network management. This reliability is crucial for the safe and efficient operation of connected and autonomous cars, as any communication failures or disruptions could have severe consequences on the overall functioning of the vehicles.

Greater capacity: 5G can handle a much larger volume of data traffic than 4G. This is important for supporting the large amount of data generated by CACs, which includes sensor data, video footage, and maps.[4]

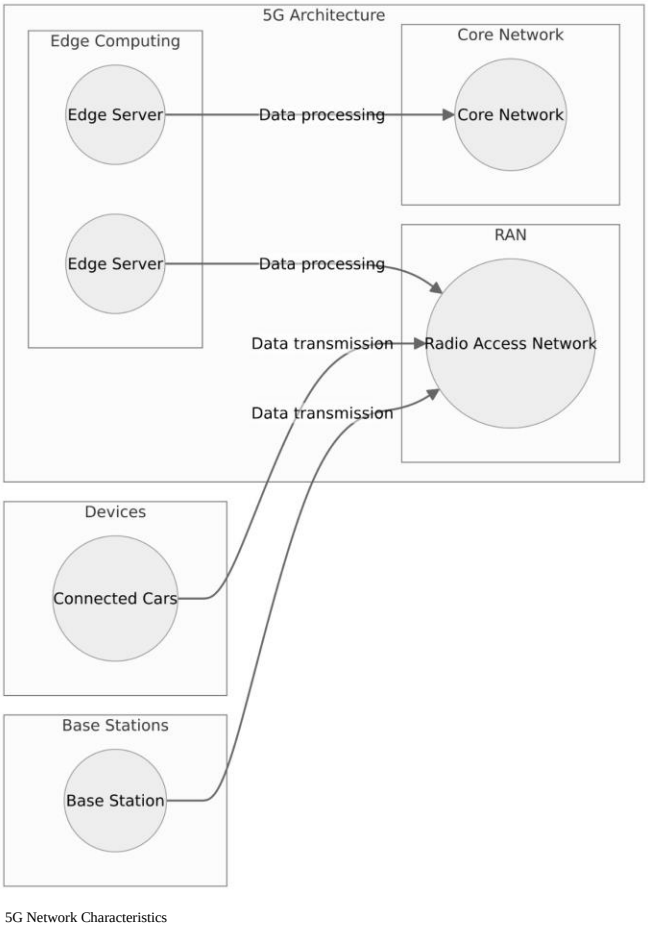

Figure 1: 5G Architecture

Figure 1 shows the basic 5G architecture of connected cars with factors such as edge computing, core network, RAN,devices and the base station

In light of these advancements, this paper aims to explore the impact of 5G networks on the development of connected and autonomous cars. By examining the various ways in which 5G technology influences the capabilities, performance, and Future prospects of these vehicles, we seek to shed light on the transformative potential of this wireless standard. Additionally,[5] we will delve into the challenges and considerations associated with the integration of 5G networks into the transportation ecosystem, addressing issues such as infrastructure requirements, cybersecurity concerns, and regulatory aspects.

3.SUMMARY OF IMPORTANT ACRONYMS

Through this comprehensive review, we hope to provide valuable insights into the interplay between 5G networks and connected and autonomous cars, thereby contributing to the ongoing discourse surrounding the future of transportation. By understanding the implications of 5G technology on the development of these innovative vehicles, stakeholders can make informed decisions and pave the way for a connected, efficient, and safe transportation system of tomorrow. The Impact of 5G on CACs The availability of 5G networks will have a significant impact on the development of CACs. With 5G, CACs can achieve the necessary speeds, latency, and capacity required for safe and efficient operation, making them a more appealing option for consumers and businesses.

3.1 Advantages

- Faster and more reliable communication: 5G networks offer significantly higher data transfer rates and lower latency compared to previous generations.
- Allowing for real-time and seamless communication between vehicles and the surrounding infrastructure.
- This enables a faster exchange of critical information, such as collision warnings, traffic updates, and road conditions, enhancing overall safety and efficiency.
- Extensive. Reliable communication allows for the accurate transmission of sensor data, aiding precise decision-making.
- Increased network capacity integrates more vehicles and infrastructure, improving traffic management.
- Mission-critical applications receive top priority, ensuring reliable emergency functions

3.2 Enhanced V2V and V2I communication

5G networks provide a more robust platform for V2V and V2I communication. This allows vehicles to share information With each other and with the infrastructure, facilitating coordinated actions, efficient traffic management, and optimized navigation. It also enables the implementation of cooperative driving techniques, such as platooning, where vehicles travel closely together to reduce aerodynamic drag

The key characteristics of 5G networks, such as high speed, low latency, and high capacity. The bars represent the relative value of each characteristic, with speed being the highest at 20 times faster than 4G, latency being 10 times lower, and capacity being 100 times greater.

Support for autonomous driving: The low latency and high bandwidth of 5G networks are essential for the deployment of autonomous driving technologies. Connected and autonomous vehicles require constant and reliable connectivity to access real-time data, such as high-definition maps, traffic information, and sensor inputs from the surrounding environment. 5G

networks provide the necessary infrastructure for these vehicles to communicate effectively and make split-second decisions[2] leading to safer and more efficient autonomous driving experiences.

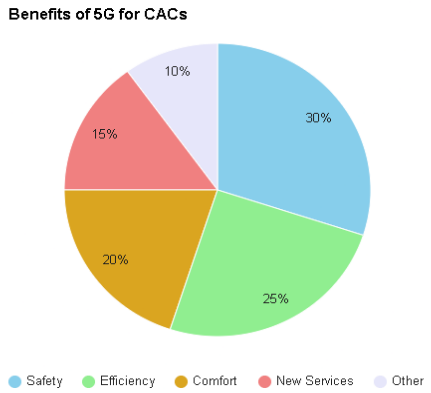

Figure 2: Benefits of 5G for CACs

Figure 2 depicts The pie chart slices represent the percentage of each benefit, with safety being the largest at 30%, followed by efficiency at 25%, comfort at 20%, new services at 15%, and other benefits at 10%.

3.3 Disadvantages

- Infrastructure requirements and deployment costs: The implementation of 5G networks requires a significant investment in infrastructure, including the installation of new base stations and network equipment. The deployment costs associated with building the necessary infrastructure can be substantial, posing financial challenges for automotive manufacturers, service providers, and governments.

- Network coverage and reliability: While 5G networks promise faster and more reliable connectivity, achieving comprehensive network coverage in all areas can be a challenge. Rural and remote regions may have limited access to 5G networks, which could hinder the widespread adoption of connected and autonomous cars. Additionally, disruptions in network reliability and stability can impact the performance and safety of connected vehicles, highlighting the need for robust and redundant network infrastructure.

- Cybersecurity concerns: With the increased connectivity and data exchange in 5G-enabled connected cars, cybersecurity becomes a critical concern. The complex network architecture and a large number of connected devices increase the potential attack surface for malicious actors. Protecting vehicles and the entire ecosystem from cyber threats, such as unauthorized access, data breaches, and remote vehicle manipulation,[8] requires robust security measures and constant updates to address emerging vulnerabilities.

4. RELATED SURVEYS ON 5G-BASED AUTONOMOUS VEHICLES

The emergence of 5G networks as a groundbreaking technology brings numerous transformative aspects that will revolutionize industries.[14] This section provides an in-depth overview of the impact of connected and autonomous cars, highlighting key features and benefits.

An essential characteristic of 5G is its ability to deliver high data rates, enabling fast communication between devices. With multi-gigabit per second (Gbps) download speeds, connected and autonomous cars can transfer data swiftly. Real-time information exchange between vehicles, infrastructure, and other devices in the transportation ecosystem is facilitated.

5G networks offer remarkably low latency, ensuring minimal delay in data transmission. This instantaneous response time enhances the safe and reliable operation of connected and autonomous cars, enabling quick decision-making and reactions to traffic conditions. Reduced latency enhances vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, improving safety and efficiency.

Another significant feature is the support for massive device connectivity. 5G networks seamlessly accommodate numerous connected devices simultaneously, enabling cooperative driving. Vehicles can coordinate actions, share traffic updates, and optimize routes to reduce congestion, enhancing traffic flow.

Additionally, 5G introduces network slicing, dividing a physical network into virtual networks. Customizable slices with specific requirements, such as bandwidth and security, cater to different applications. Critical applications can be allocated high-priority[7] slices, ensuring uninterrupted and reliable operation

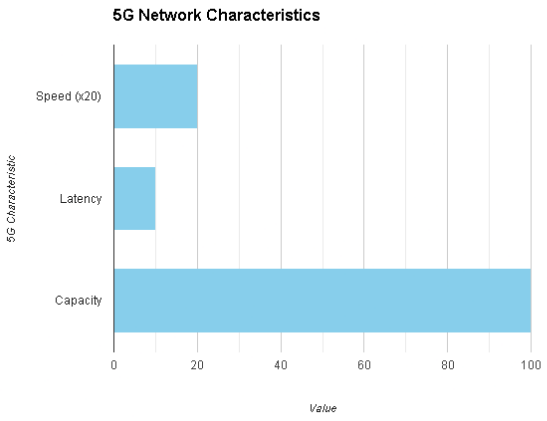

Figure 3: 5G Network Characteristics

Figure 3 describes the 5G network characteristics such as speed, latency, capacity against values.

4.1 Vehicle-to-Infrastructure(V2I) Communication: It is revolutionizing the transportation industry, and the advent of 5G networks has further accelerated its potential. With its high-speed and low-latency capabilities, 5G technology is poised to transform how vehicles interact with the surrounding infrastructure, creating a seamless and efficient transportation ecosystem. In our review paper titled "The Impact of 5G Networks on the Development of Connected and Autonomous Cars," we delve into the various applications of 5G in V2I communication and highlight its profound influence.

One of the key areas where 5G networks shine is traffic signal optimization.[15] By leveraging real-time data transmission, vehicles can communicate with traffic signals and exchange vital information. This two-way interaction enables intelligent signal control systems to dynamically adjust signal timings based on traffic flow, minimizing congestion and improving overall traffic efficiency. With 5G's ultra-fast speeds and minimal latency, these interactions can occur seamlessly and instantaneously, ensuring smooth and uninterrupted traffic flow.

Intelligent transportation systems represent another significant application of 5G in V2I communication. These systems rely on the exchange of data between vehicles, infrastructure, and even pedestrians to enhance safety, efficiency, and convenience on the road. 5G networks provide the necessary bandwidth and reliability to support the vast amount of data generated by connected and autonomous vehicles. This data includes real-time traffic updates, road condition information, and even predictive analytics, empowering vehicles to make informed decisions and optimize their routes for the most efficient travel experience.

Additionally, 5G facilitates the remote monitoring and control of connected and autonomous vehicles. With its low-latency communication capabilities, it becomes possible to remotely access and manage various aspects of a vehicle's operations. This includes monitoring the vehicle's performance,[17] conducting over-the-air software updates, and even remotely controlling certain functions when necessary. By harnessing the power of 5G, manufacturers, and fleet operators can ensure the safety and efficiency of their vehicles without the need for physical intervention.

5. SECURITY

Given the potential for manipulation and fraud, security emerges as a concern of critical when handling the smart cards, particularly when they hold monetary value. To protect from unauthorized access, the implementation of both user identification and access control becomes imperative in distributed computer systems. Smart cards offer varying security features to address this challenge, including authentication, encryption using single and triple DES algorithms, MAC checksums, and it uses secret codes like PINs. These measures contribute to enhancing overall security during the implementation of smart card systems[9].

5.1 Protective capabilities of the network's security measures

Data communication. should be adequately protected either through the system's design or the implementation of network protocols that prevent tampering and maintain the overall system security. Physical security measures can be implemented to secure the card terminal. For example, if the card terminal is integrated into a wall, the card security is ensured by utilizing equipment such as a smart card reader with a mechanized shutter[6]. Additionally, the communications connection and smart card reader can be physically safeguarded by placing them in a secure location. These measures contribute to protecting the integrity and confidentiality of system and its associated data.

5.2 Fundamental Security Concepts

Security is of utmost importance in a smart card system due to various factors. Upholding the principles of irrefutability, data consistency, identity verification, and verification are critical components of ensuring a secure environment[10]. These principles help to establish trust, prevent the denial of actions or transactions, maintain data accuracy and consistency, verify the identity of users, and validate the reliability of the system's operations[3]. By adhering to these methodologies, a smart card system can safeguard against unauthorized access, protect sensitive information, and maintain the overall security and reliability of the system.

These ideas are brought from various encryption algorithms used by smart cards. A single mechanism may occasionally be able to offer many security services. For instance, a digital signature can offer non-repudiation, source authentication, and data integrity[11]. Public key infrastructure (PKI) is important because it offers the policies and processes needed for creating secured information exchange, which is required for the majority of these security needs.

PKI (Public Key Infrastructure) utilizes data scrambling to ensure privacy, electronic certificate for verification purposes, and digital signatures to demonstrate the integrity of transactions performed by the originator without interruption or error. The upcoming sections will delve into the processes employed in smart cards to enforce these fundamental principles.

6. PRIVACY

The concept of safeguarding message exchanged between two parties from third-party interference is known as privacy. However, additional research on privacy and security is required before designing a card capable of preserving such confidentiality. This is because of heightened risk of privacy breaches when a person's smart card contains a larger amount of unique and personal information. Nonetheless, smart cards currently possess a diverse range of applications, and as they continue to shrink in size, become more affordable, and gain enhanced capabilities, their ability to support even more functions increases significantly.

Privacy is ensured using symmetrical and asymmetrical cryptography. Various procedures are required depends on card application. Numerous algorithms were implemented. is not conceivable despite the abundance of physical resources

It is common that a single algorithm will be universally employed. Currently, the widely adopted symmetric key cryptography algorithm is DES (FIPS 46-3), or potentially triple-DES (ANSI X9.17), while RSA is commonly utilized for asymmetric cryptography. Although it is unlikely to occur anytime soon, there might be future initiatives to replace DES with the more advanced AES (FIPS 196) algorithm

- Symmetrical Cryptography: Symmetrical cryptography employs A single key is used to encrypt plain text into enciphered text and to decode enciphered text back into plain text[12]. Cryptography with symmetry is called symmetrical because it uses the same. To encode and decode the communication the key is used. The DES algorithm is a fast method that may be utilized with smart card software. (FIPS 46-3) [13]. The conventional method for securely distributing keys to cards is to write a des key at the time of card personalization. Asymmetrical cryptography, which is described below If this is not achievable
- Asymmetrical Cryptography: In their article "New Directions in Cryptography," published in 1976, initially proposed separating the encryption/decryption key rather than using a single key for both functions. This concept is now recognized as asymmetrical cryptography. Two keys are used in asymmetric cryptography: one to encrypt plain text and the other to decrypt it. These are connected mathematically. The communication with only one key can be unlocked using a different key. RSA is popular asymmetrical cryptography algorithm[12].

This is used by credit card firms for authentication. Data encryption is rarely utilized. Asymmetric cryptography is also employed for this purpose. Asymmetrical encryptions are frequently used to safely transfer the key from one party to another. Asymmetric encryption is used for data transfer if both participants should know of the DES key. This action enhances the presentation.

6.1 Verification

Verification is the method of determining a person's identification. In reality, it provides clarification or confirmation that a person or object is indeed the entity it claims to be. For instance, Ram needs to be certain that Sham is the processor of the key before accepting a communication from him. This requires a procedure known as authentication.

Certificates: The authority that issues the certificate guarantees that the certificate's holder is who they claim to be. if the securely signed message contains a copy of the certificate holder's public key and other details about certificate holder. The recipient of the communication can then be certain that the key is trust-worthy[16].

The helpful action before using a card is verifying the cardholder's identification. If two parties wish to start a business, they must be certain of each other's identity. We can use verbal and visual cues to identify other people. To confirm that the person being impersonated is actually that person, secure communication technology.is used.

- Security codes: Security codes typically refers to a sequence of four or five digits. that is attached to the smart card. Cardholder commits this number to memory. PIN is securely kept. Digital content and functions on the chipcard can be secured until access from the outside world is permitted. Due to the excessive number of chip card applications, it will take some time until the proper pin code is available. As a result, people will need to memorize more and more pin numbers. Keep in mind that 15–20 distinct Security codes are challenging for everyone and could result in someone writing the secured number on the card. The initial merit of having a PIN was lost, which is why subsequent attention to security measures has focused on biometric as a method of recognizing a person.

- Biometrics: The science of quantifying characteristics is called biometrics. Users find it difficult to remember numeric pass codes and secret phrases. a determining component influencing the betterment of biometrics is this reluctance. Additionally, since many people share pin numbers, they are not identifiable uniquely, whereas biometrics can identify a real person since they are the following biological characteristics can be measured:
    - Signature
    - Fingerprint
    - Voiceprint
    - Hand geometry
    - Eye retina

6.2 Real-Time Data Processing

The Crucial Role of 5G Networks in Revolutionizing the Development of Connected and Autonomous Cars In recent years, the remarkable advancements in 5G networks have paved the way for a transformative era in the development of connected and autonomous cars. The unparalleled combination of high data rates and ultra-low latency offered by 5G has revolutionized the capabilities of these vehicles, particularly in terms of real-time data processing. This critical aspect has propelled the automotive industry into a new realm of possibilities, enabling enhanced functionalities that were once merely speculative. One of the key advantages of 5G networks is their ability to facilitate efficient data exchange and processing in connected and autonomous cars. With the exponential growth of data generated by sensors, cameras, and various other sources within the vehicle ecosystem, the need for rapid and seamless communication has become paramount.[19] The exceptional bandwidth and reduced latency of 5G networks allow for the instantaneous transmission of vast amounts of data, facilitating real-time decision-making processes and empowering vehicles to navigate through complex scenarios with unparalleled accuracy and safety. Real-time navigation is a prime example of how 5G networks have transformed the automotive landscape.

Traditional Additionally, manufacturers and developers must adopt a security-by-design approach, embedding cybersecurity principles into the very fabric of connected and autonomous cars.[22]

6.3 Cybersecurity

The rapid advancement of technology has revolutionized the automotive industry, particularly with the emergence of connected and autonomous cars. These vehicles, equipped with state-of-the-art features and capabilities, rely heavily on seamless connectivity to enhance their performance, efficiency, and overall user experience. However, this increased connectivity also introduces a myriad of cybersecurity challenges that need to be addressed to ensure the safety and integrity of these vehicles and their passengers. At the forefront of these challenges is the impact of 5G networks on automotive cybersecurity, a topic of great significance in the realm of connected and autonomous cars. With the deployment of 5G technology,[20] vehicle networks are expected to experience unprecedented levels of connectivity, speed, and responsiveness. While this promises a range of exciting possibilities, it also opens up potential vulnerabilities that malicious actors could exploit. In the context of 5G-enabled vehicle networks, it becomes crucial to examine the potential risks and vulnerabilities that may arise. The sheer complexity of these networks, with numerous interconnected devices and systems, increases the attack surface for cyber threats. Adversaries may attempt to exploit vulnerabilities in the underlying infrastructure, compromising the integrity of critical systems, such as steering, braking, and acceleration. Such attacks could have devastating consequences, leading to accidents, property damage, or even loss of life. [21] To mitigate these risks, a comprehensive set of countermeasures must be implemented. These countermeasures encompass both preventive and reactive measures to ensure the security of 5G-enabled vehicle networks. Preventive measures may include robust encryption protocols, secure authentication mechanisms, and intrusion detection systems.

6.3.1 Safety Dimension

According to certain surveys, users' concerns about security have grown, and this has been identified as one of the main aim of technology aspect. In this study “degree to which person feels that security is important to them and believes that by using smart card is secured” is the definition of security. Strengthening system security will safeguard uses perception of the systems overall quality. security control may help to safeguard systems holistic content.[1] Superiority by preserving the availability, confidentiality and integrity of the material[18].

6.3.2 Enhanced Driver Assistance Systems (EDAS):

This have experienced significant advancements with the emergence of 5G networks, as they provide a robust and reliable infrastructure to support the development of connected and autonomous cars. The impact of 5G on ADAS functionalities is profound, paving the way for a new era of automotive innovation. Cooperative perception stands out as one of the key features enabled by 5G networks. By leveraging the ultra-low latency and high bandwidth capabilities of 5G, connected cars can communicate and share real-time sensor data, enhancing their perception capabilities. This cooperative perception allows vehicles to create a comprehensive and accurate understanding of the surrounding environment, thereby increasing safety and enabling more effective decision-making. Moreover, 5G networks facilitate cooperative manoeuvering, enabling vehicles to communicate and coordinate with each other on the road. This cooperative manoeuvering takes ADAS to a new level, as vehicles can synchronize their actions, such as lane changes or merging, to optimize traffic flow and improve overall [23]

7. CONCLUSION

Users this review paper has provided a comprehensive overview of the impact of 5G networks on the development of connected and autonomous cars. The research findings have emphasized the tremendous potential of 5G technology in transforming the automotive industry and expediting the realization of fully autonomous vehicles. The key benefits offered by 5G, such as high data rates, ultra-low latency, extensive device connectivity, and network slicing, empower a wide array of applications and scenarios in the context of connected and autonomous cars. However, the successful integration of 5G in this domain necessitates addressing several critical challenges concerning network infrastructure, spectrum allocation, deployment strategies, interoperability, and cybersecurity. To fully harness the potential of 5G networks in shaping the future of transportation, further research and collaboration among industry stakeholders are imperative. By tackling these challenges collectively, we can unlock the full transformative power of 5G and drive the advancement of connected and autonomous cars toward a safer and more efficient transportation ecosystem

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude and appreciation for the invaluable support and contributions provided by the esteemed research team at the Department of Computer Science And Engineering, AIET. Their expertise and dedication have played a vital role in the successful completion of this review paper titled "The Impact of 5G Networks on the Development of Connected and Autonomous Cars." The collaboration and insights shared by the research team have significantly enhanced the quality and depth of this study. Their extensive knowledge in the field of electrical engineering and their commitment to advancing the understanding of 5G networks and their influence on connected and autonomous cars have been instrumental in shaping the content of this paper. The author extends their heartfelt thanks to each member of the research team for their unwavering support and their contributions, which have undoubtedly enriched the outcomes of this research endeavor.

REFERENCES

[1] A. Manfreda, K. Ljubi, and A. Groznik, "***Autonomous vehicles in the smart city era: An empirical study of adoption factors important for millennials***," International Journal of Information Management, p. 102050, 2019.

[2] C. Ravi, A. Tigga, G. T. Reddy, S. Hakak, and M. Alazab, "***Driver identification using optimized deep learning model in smart transportation***," ACM Transactions on Internet Technology, 2020.

[3] K. Jadaan, S. Zeater, and Y. Abukhalil, "***Connected vehicles: an innovative transport technology***," Procedia Engineering, vol. 187, pp. 641–648, 2017.

[4] Z. Wadud, D. MacKenzie, and P. Leiby, "***Help or hindrance? the travel, energy and carbon impacts of highly automated vehicles,***" Transportation Research Part A: Policy and Practice, vol. 86, pp. 1–18, 2016.

[5] J. Sachs, G. Wikstrom, T. Dudda, R. Baldemair, and K. Kittichokechai, "***5g radio network design for ultra-reliable low-latency communication***," IEEE network, vol. 32, no. 2, pp. 24–31, 2018.

[6] M. M. d. Silva and J. Guerreiro, "***On the 5g and beyond***," Applied Sciences, vol. 10, no. 20, p. 7091, 2020.

[7] A. Rasouli and J. K. Tsotsos, "***Autonomous vehicles that interact with pedestrians: A survey of theory and practice***," IEEE transactions on intelligent transportation systems, vol. 21, no. 3, pp. 900–918, 2019.

[8] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, ***"Evolution of v2x communication and integration of blockchain for security enhancements***," Electronics, vol. 9, no. 9, p. 1338, 2020.

[9] S. Rahmadika, K. Lee, and K.-H. Rhee, "***Blockchain-enabled 5g autonomous vehicular networks***," in 2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC). IEEE, 2019, pp. 275–280.

[10] D. Reebadiya, T. Rathod, R. Gupta, S. Tanwar, and N. Kumar, "***Blockchain-based secure and intelligent sensing scheme for autonomous vehicles activity tracking beyond 5g networks,***" Peer-to-Peer Networking and Applications, pp. 1–18, 2021.

[11] L. Nkenyereye, B. Adhi Tama, M. K. Shahzad, and Y.-H. Choi, ***"Secure and blockchain-based emergency driven message protocol for 5g enabled vehicular edge computing***," Sensors, vol. 20, no. 1, p. 154, 2020.

[12] J. Chen, W. Wang, Y. Zhou, S. H. Ahmed, and W. Wei, ***"Exploiting 5g and blockchain for medical applications of drones***," IEEE Network, vol. 35, no. 1, pp. 30–36, 2021.

[13] G. Kakkavas, A. Stamou, V. Karyotis, and S. Papavassiliou,***"Network tomography for efficient monitoring in sdn-enabled 5g networks and beyond: Challenges and opportunities,"*** IEEE Communications Magazine, vol. 59, no. 3, pp. 70–76, 2021.

[14] C. Benzaid and T. Taleb, "***Ai-driven zero touch network and service management in 5g and beyond: Challenges and research directions,***" IEEE Network, vol. 34, no. 2, pp. 186–194, 2020.

[15] M. Liyanage, Q.-V. Pham, K. Dev, S. Bhattacharya, P. K. R. Maddikunta, T. R. Gadekallu, and G. Yenduri, ***"A survey on zero touch network and service (zsm) management for 5g and beyond networks,***" Journal of Network and Computer Applications, p. 103362, 2022.

[16] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "***A review on safety failures, security attacks, and available countermeasures for autonomous vehicles,"*** Ad Hoc Networks, vol. 90, p. 101823, 2019.

[17] A. M. Malla and R. K. Sahu, "***Security attacks with an effective solution for dos attacks in vanet***," International Journal of Computer Applications, vol. 66, no. 22, 2013.

[18] S. S. Manvi and S. Tangade, "***A survey on authentication schemes in vanets for secured communicatio***n," Vehicular Communications, vol. 9, pp. 19–30, 2017.

[19] L. B. Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "***A survey of security and privacy in connected vehicles***," in Wireless sensor and mobile ad-hoc networks. Springer, 2015, pp. 217–247.

[20] S. Zhang, Y. Lin, Q. Liu, J. Jiang, B. Yin, and K.-K. R. Choo, "***Secure hitch in location based social networks***," Computer Communications, vol. 100, pp. 65–77, 2017.

[21] M. Raya and J.-P. Hubaux, "***Securing vehicular ad hoc networks,"*** Journal of computer security, vol. 15, no. 1, pp. 39–68, 2007.

[22] B. G. Stottelaar, "***Practical cyber-attacks on autonomous vehicles***," Master's thesis, University of Twente, 2015.

[23] C. Bockelmann, N. Pratas, H. Nikopour, K. Au, T. Svensson, C. Stefanovic, P. Popovski, and A. Dekorsy, "***Massive machine-type communications in 5g: Physical and mac-layer solutions***," IEEE Communications Magazine, vol. 54, no. 9, pp. 59–65, 2016.