IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

# Privacy and Security Issues and Challenges in 5g Enabled Vehicular Networks

[1]Rajesh Kumar, [2]Ankita Sharad, [3]Sanjay Babu Jaiswal,[4]Vivek Kumar Singh, [5]Smriti Kumari

[1,2]M.Tech. Student, [3,4,5]B.Tech. Student

[1,2]Department of IT, [3,4,5]Department of CSE

[1,2]NIT Raipur, Chhattisgarh, India, [3,4,5]IIIT Senapati, Manipur, India

***Abstract :*** In recent time utmost of the workshop are now done with the help of internet and several other services. From many decades' internet services becomes so cheap that utmost of the peoples can go it. In the advancements in the field of vehicular communication lots of big companies are producing vehicles. Tone- driving buses are one exemplifications of the 5g enabled or internet enabled services in which buses can do machine literacy and predicts the accurate and comfort route from itself without doing accident and other road blockages. Tone- driving buses are some of the exemplifications of this big assiduity period for 5g enables vehicular networks. This paper did a relative investigation or different 3g, 4g, and 5g enabled vehicular networks and ultimately this paper bandied the security and isolation aspects for it. This paper has argued the substantially videotape streaming services and vehicular services in 5G enabled vehicular networks. This paper also proposed an approach for assuring sequestration and security by integrating block chain technology to it. The first member will argue about intro and alternate member will argue about Affiliated workshop and growth of vehicular networks communication. Third member will bandy about System model and in fourth member Result analysis will be done and grounded on result analysis conclusion be given in fifth portion and in this member future realm will also be argued.

***IndexTerms*** **- Generation Partnership Program (3GPP). Long Term Evolution (LTE). Wireless Access for Vehicular Environment (WAVE). Vehicle to all/ Everything(V2X). 5th generation (5G). Millimeter wave (MM wave). On-Board Equipment (OBE). Block Chain. Proof of Work (PoW). Proof of Stack (PoS).**

## I. INTRODUCTION

Recent generation of technological enhancement within side the discipline of vehicular verbal exchange got here to some extent in which many agencies at the moment are concerning on this discipline. Tesla, Tata, CMU Navlab, Bosch, PSA [1] Peugeot Citroen, Mercedes Benz, Continental self-reliant car, Google Cars, Renault, Toyota, Audi, and lots of extra motors agencies at the moment are constructing self-using motors a few are in prototype segment and a few are in trying out the segment. Tesla unveils its porotype for self-using motors on 20 October 2020. And even google and a few huge Indian vehicle agencies now coming to this discipline additionally. In this sort of verbal exchange, Wi-Fi connectivity is furnished amongst all peripheral gadgets which are utilized in shipping structures like roadside gadgets, pedestrians, and passengers. This era may be divided into categories. Short variety verbal exchange (SRC) that's centered to a few devoted places and the following is long time evolution(LTE)-primarily based totally car to all, something is probably feasible to hook up with the car (i.e. V2X or LTE) [5]. this trendy implementation of those methods is described with the aid of using IEEE 802. eleven and IEEE 1609 requirements. These requirements are applied in backward days with WAVE (Wireless Access for Vehicular Environment) and now whilst 3g and 4g got here now it's been applied with the aid of using cell technology and combine with them. Integration of LTE primarily based totally [2] V2X will make massive area implantation and may use excessive velocity with potential and it is able to be deployed with accuracy which could guarantee protection and safety of passengers overusing on the avenue. Qualcomm and Tesla have already made their avenue map for LTE primarily based totally V2X [3] devise for vehicular verbal exchange. fifth-generation(5G) [4] helps the velocity and place cowl for those V2X vehicular communications. Because of 5G, excessive-velocity connections, ultra-low latency, and excessive bandwidth can make certain promising V2X services. Although there may be many benefits of vehicular verbal exchange the usage of 5g, however, there are numerous researches finished is that this discipline which tells approximately protection and safety worries for it. Many kinds of research are finished in 2g primarily based totally [6] vehicular connectivity with enhancement 3g primarily based totally and 4g primarily based totally is likewise mentioned with the aid of using many researchers however because of 5g is current and nonetheless in beneath Neath path segment so privatives and safety problems aren't so mentioned with the aid of using many researchers. This paper did a safety and privatizes issue associated with a 5g vehicular verbal exchange. This paper additionally mentioned approximately enhancing video great over 5G community vehicular community.

## II. RELATED WORK

5th generation (5G) technology is capable of offering ubiquitous computing [7] to all vehicles with ultra-low latency and high bandwidth with low cost energy [11]. This makes it easy to integrate with vehicular communication. some vehicles are having 2g, 3g, and 4g integration with them which supports variety of applications associated with them, this 5g can easy integrate with them and some additional modules is needed to fully utilize this technology. One major enhancement done in this field on video quality improving in wireless network has been done.

### 2.1 Connectivity with Antenna in 5G in vehicular networks

5th generation technologies are working in the range of two ranges. Frequency [6] range 1(FR1) and Frequency Range 2(FR2) [8]. One is from 450MHz to 6GHz which also includes the LTE frequencies. The second 24.25GHz [9] to 52.6 GHz whereas 6 GHz sometimes called as FR1 and FR2 is sometimes called as mm Wave [10].

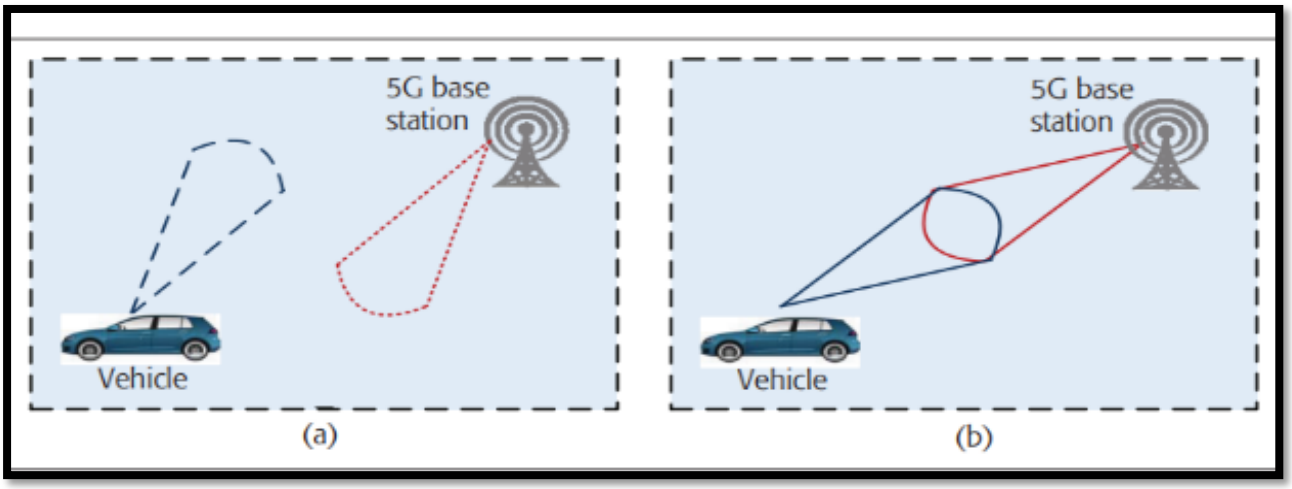


Figure 1: Connectivity with directional antenna; (a) without directional connectivity, (b) with directional connectivity.

In 5g technologies these frequencies are working in short ranges [12] so to experience its maximum speed we need to install many stations so that in combination it provides high speed. These above figure depicts that when vehicle is moving it can be connected with either directional and the other is non directional. If vehicle is configured with direction antenna [13], then it's very difficult to be connected with 5g but if its configured with directional 5g services will keep working until its connected.

### 2.2 5G enabled video streaming architecture for vehicular networks

For the entertainment purpose most of the passengers use music streaming services [14]. So to ensure they get lag free music while driving in the car in parallel to it car need to focus for safety purpose also. While driving car both safety and entertainment requires [15]. In this architecture music is transferring through cloud server to local network gateway then it transmits to local are transmitter finally it is received by our vehicle receiver. It needs to be cleared from server side while listening music up to fixed decibel sound must be there so that neither music is too low nor it should be more than some point so that it not generates any noise.

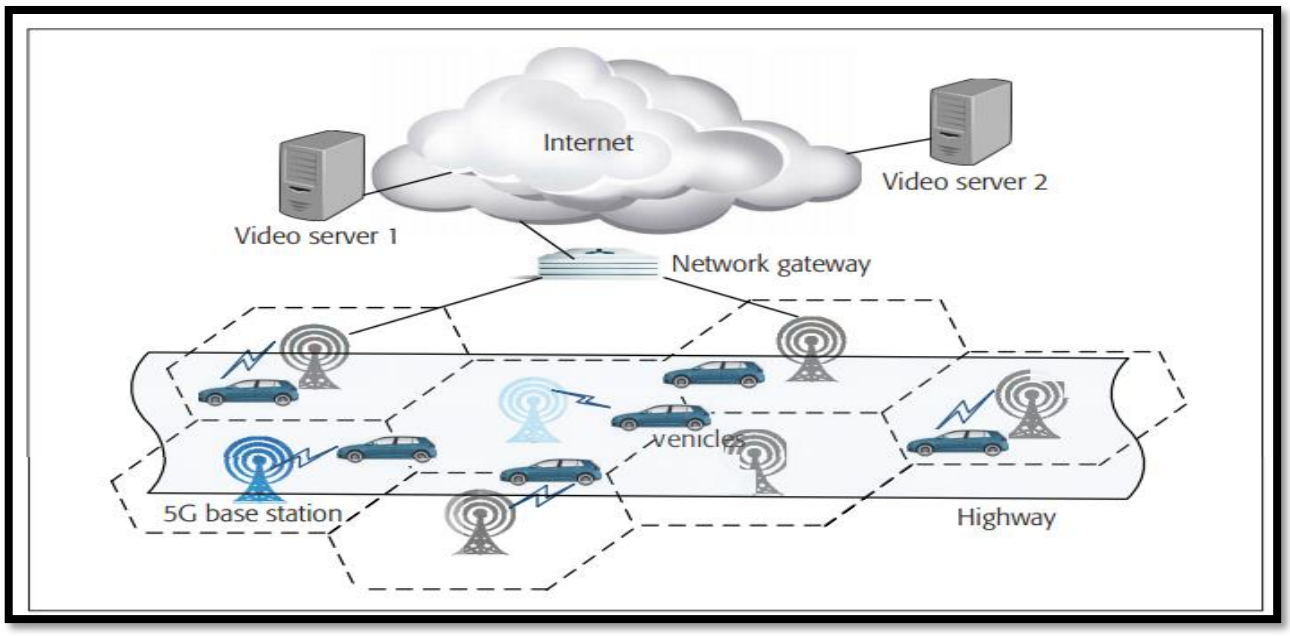


Figure 2:Video Streaming structure 5g enabled vehicular communications

### 2.3 Buffer system for vehicular networks

On 5G platform to improve the video playing experience a buffer system has been implemented at base station of mm Wave to load required video content from the cloud and load the video data in each base station where mobile is roaming inside vehicle. In this video delay can be negotiated because all data is already being stored to nearest base station and these data can be accessed until vehicle is moving in that base station area.

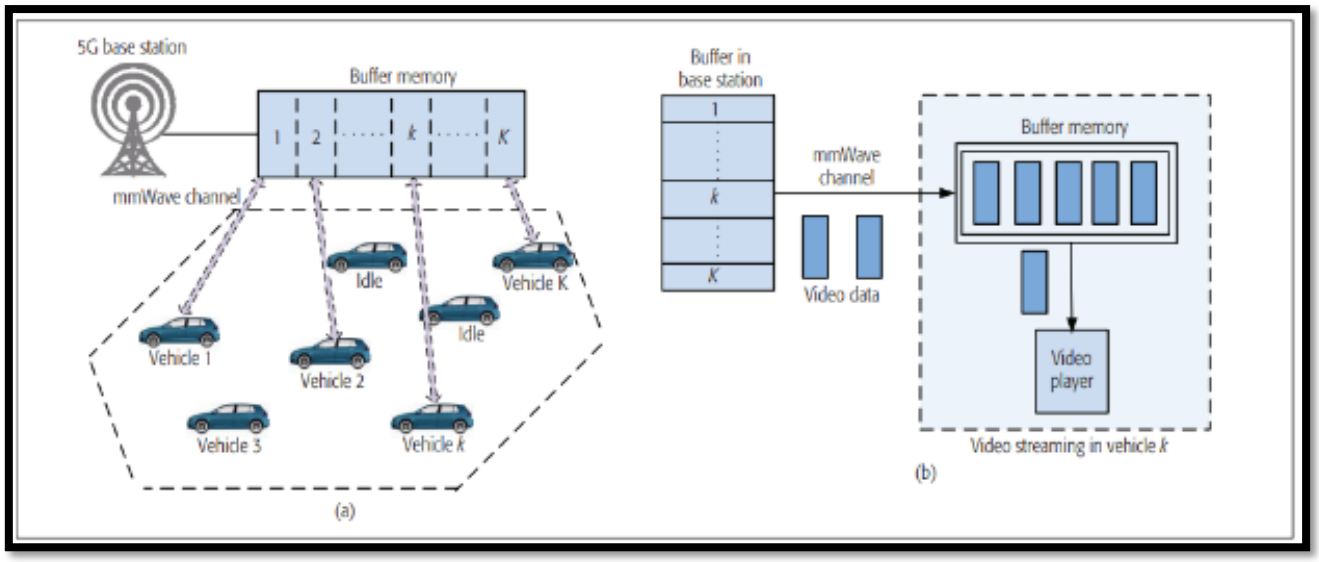


Figure 3:Double-buffer system for 5G enabled vehicular networks: a) buffer system at an mm Wave base station; b) buffer system at each vehicle.

## III. SYSTEM MODEL

In previous year Tesla launched their prototype for their Autonomous driving car and many other company also launched their self-driving cars and in future many company is also going to launch. In recent trending everyone is willing to be in self-driving cars because everyone is thinking that the artificial intelligence (AI) and machine learning (ML) can reduce the risk of accidents in different ways. Because of the AI and ML road accidents may reduce and it's having many other advantages also, therefore many big companies are now moving towards self-driving cars business. Autonomous self-driving cars has many advantage but at the same time its having many privacy and security concerns also. This segment of paper will discuss its privacy and security concerns so that it can be either completely removed or make it less.

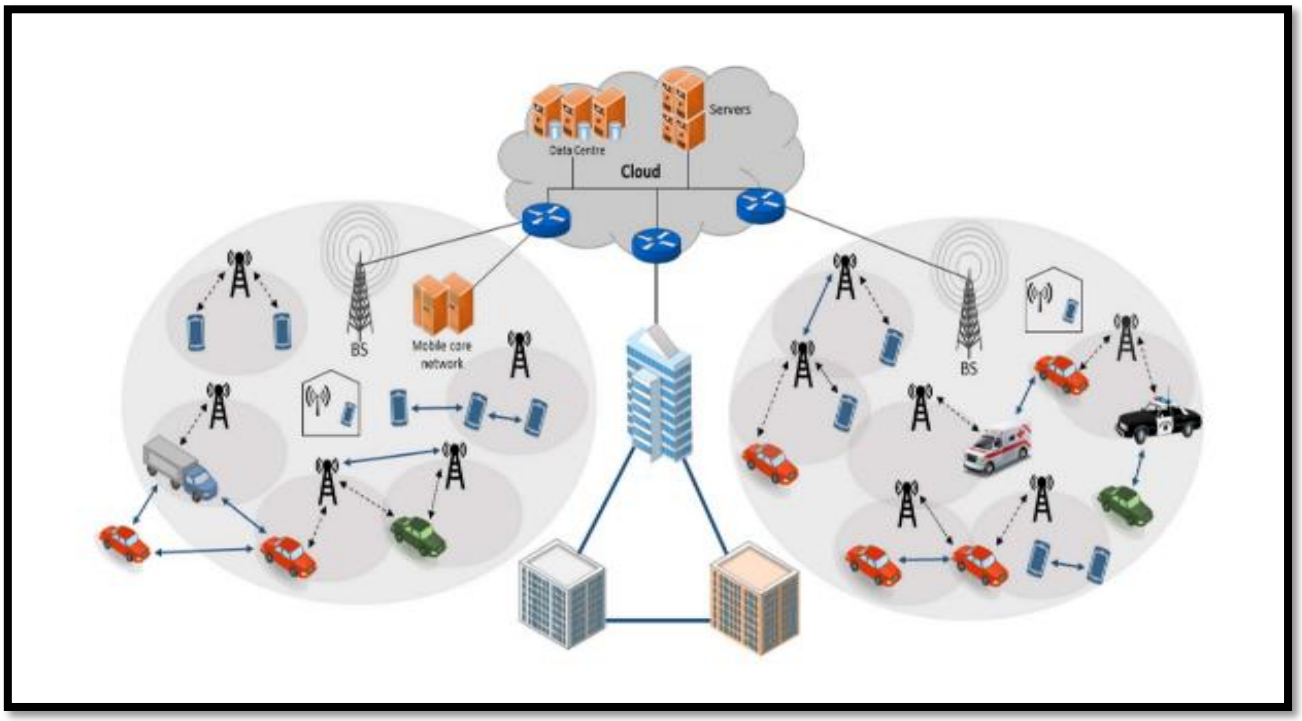


Figure 4: Architecture for the 5th generation(5G) vehicular communication

## *Security*

The security concerns related to it is mainly related to integrity, resistance to replay attack, confidentiality and authenticity.

### 3.1 Integrity

Data which has shared among V2X and other peripheral devices connected over self-driving networks must be integrated. means whatever the server responds for any request that data must be received by the self-driving car. The data which are shared among V2X and other peripheral devices should be integrity protected. The communication and shared data between V2X and OBE must be integrity protected. The transmission among V2X with other V2X with same and other systems also should be integrity protected. Suppose an algorithm says to take right turn when there is a right turn board but due to data integrity or data alteration if it can go to right side here might be possibility for accident or any other worse case. So data integrity mist be there in autonomous self-driving vehicular network.

### 3.2 Confidentiality

The data which are being used for autonomous driving and other stuffs as online audio and videos streaming which has been used for entertainment for drivers and other passengers in the car must be confidential like car coordinates car owner location info and many other data which cannot be leaked to anyone due to any data breach or any internal insider threat. The transmission of the data between 2 different V2X should be very confidential. The transmission of OBE's identity should be confidential and must be very protected. The transmission of data from OBE to v2x systems and other peripheral connected devices must be confidential. Other means for data confidential is the way we can make use of different types of encryption technique, safe and secured password protected data and even hybrid block chain configuration also.

### 3.3 Authenticity

The data which has been shared among all devices over vehicular network for proper autonomous self-driving vehicles is accessed by authentic person or authentic organizers only. The V2X network entities is able to authenticated OBE and all other confidential data. unauthentic access to any confidential data will make a major threat to any device over vehicular network communication.

### 3.4 Replay attack

This is a very special type of man in the middle attack in which a very special V2X device sending a data to server for responds let's say image/maps or geolocation data but in middle someone monitor the data and make a delay for it so that our algorithm is not able to perform better at time. There might be a possibility that man in the middle can alter data and send data which might be suspicious and can occur accident or any other unwanted stuffs. The transmission between V2X networks and networks entities and among other OBE shall be protected from replays.

### 3.5 proposed system

For ensuring privacy and security aspects in 5G enabled vehicular networks we have proposed a block chain based technology to integrate with it. we all know adding a block to block chains require a approval from other blocks that's make it more secured and adding and removing any vehicle from this network again needs most the cars proof of works or any other consensus mechanism based proof.

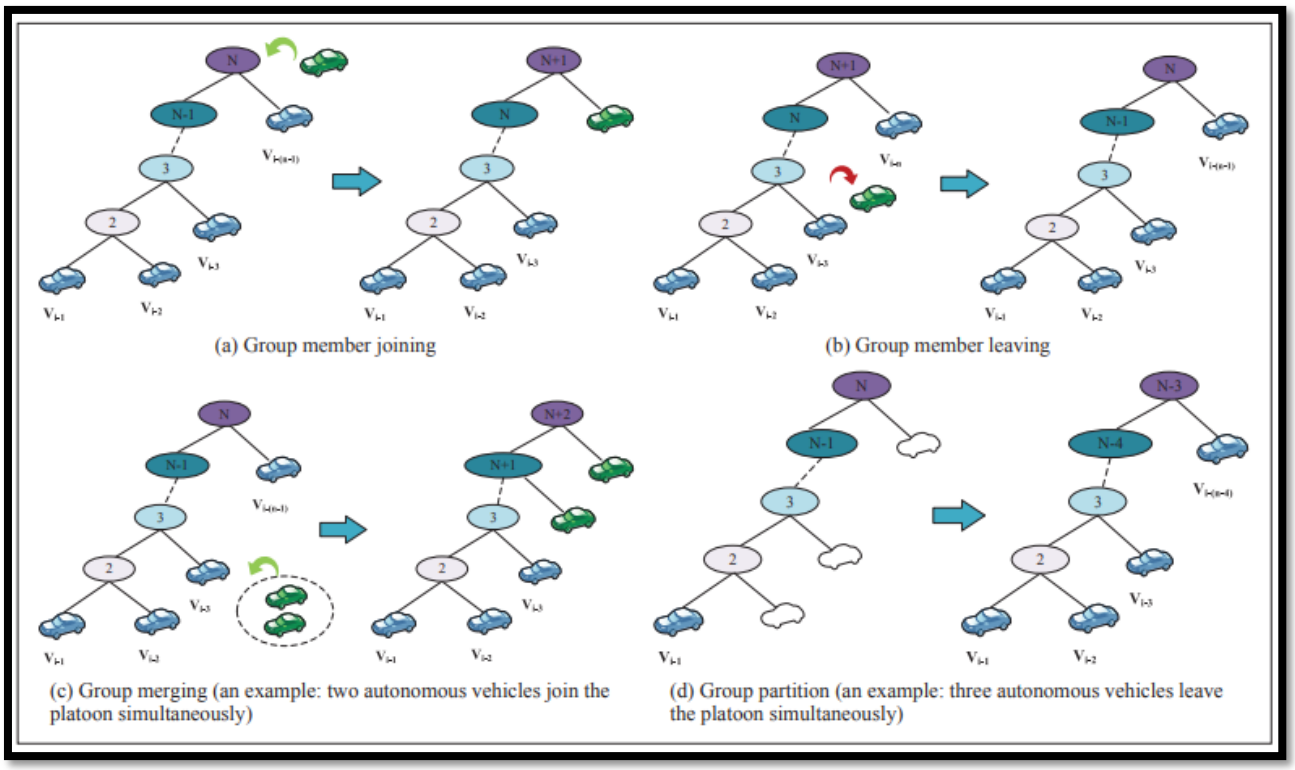


Figure 5: configuration of block chain technology to vehicular network a basic proposed work

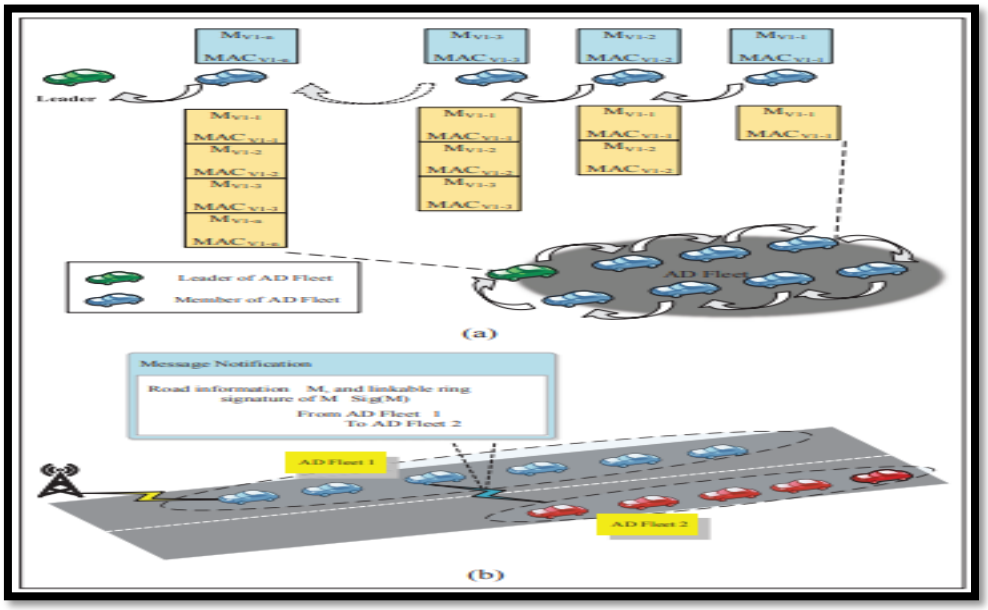


Figure 6: Working of block chain for vehicular network

## IV. RESULT ANALYSIS

In double buffered system it has been clearly seen that while increasing the number of devices the delay is going to be added. but it's less as compare to base station buffer solution. So by making a buffered technique especially double buffered system we can improve both music and autonomous driving techniques smoother and accident free. This graph shows the result for music experience and buffering.

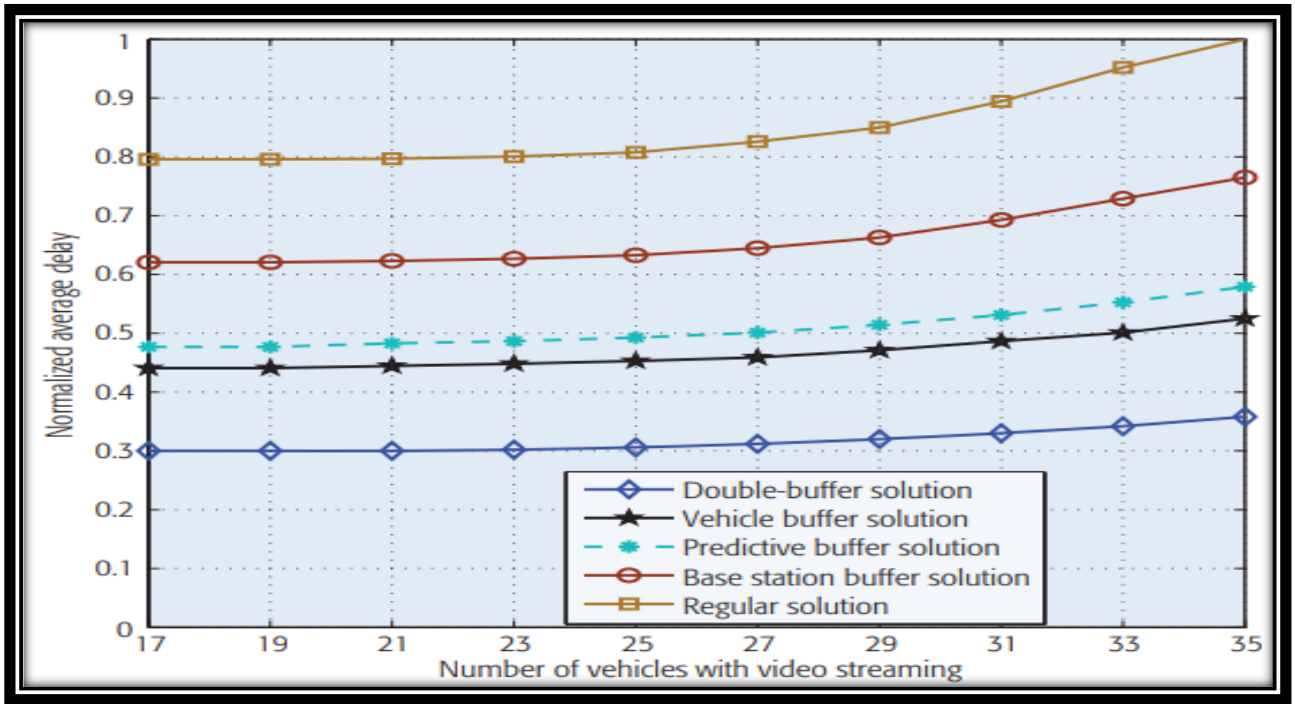


Figure 7:Delay of video streaming in 5G enabled vehicular networks.

**Block chain based implementation for vehicular network**

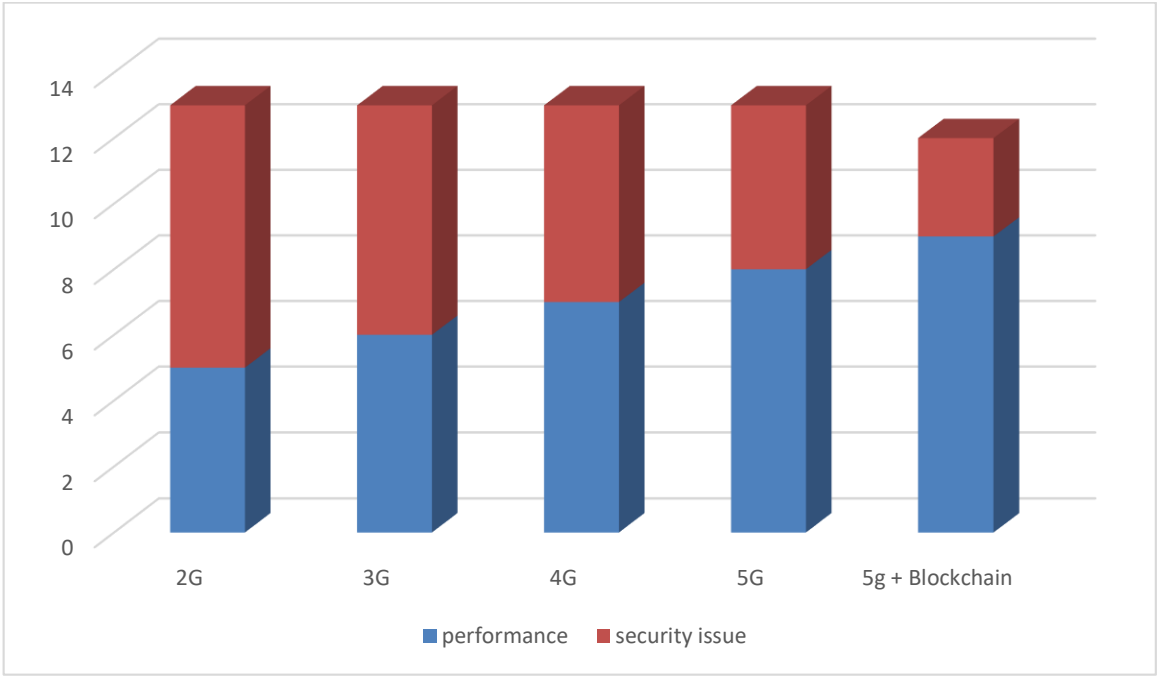


Figure 8: Analysis of performance vs security and privacy concerns for different generations

**Consistency of video streaming in 5g network**

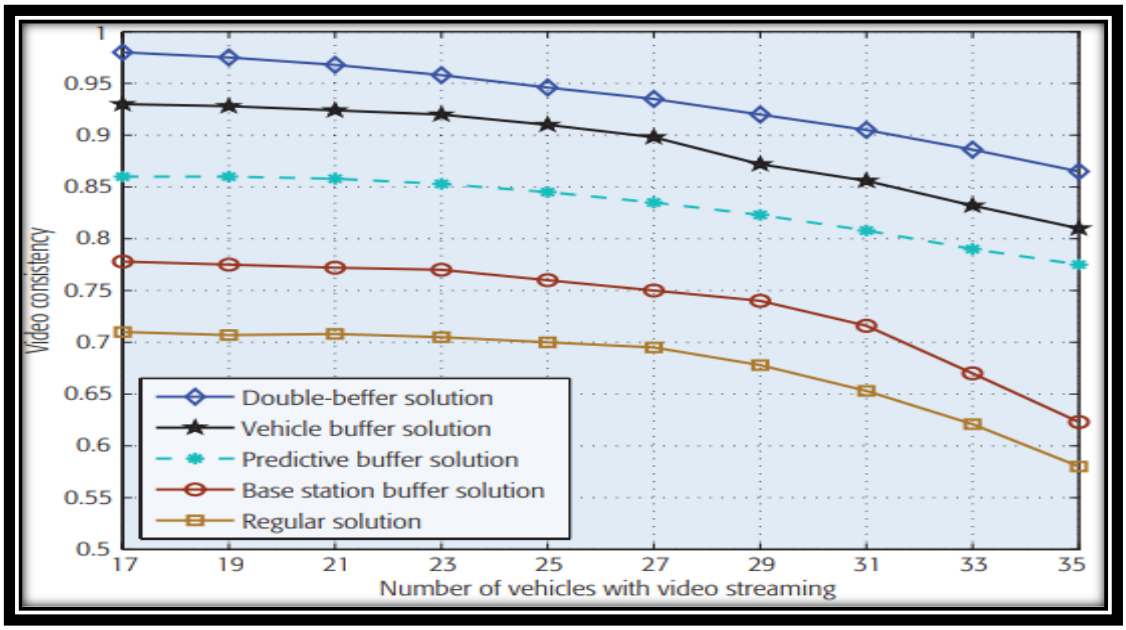


Figure 9:Video consistency in 5G enabled vehicular networks.

## V. Conclusion

This paper analysis shows the complete systematic security and privacy issues in 5g enabled vehicular networks. For understanding privacy and security aspects this paper has studied about architecture for 5g enabled vehicular networks. Then after this paper has discussed security and privacy scenarios for V2X in LTE which is used in 3GPP. This paper has also covered wide topic for improving video streaming over 5g vehicular network. This paper as proposed some techniques for improving video streaming over 5g network which shows better result and same thing is being applied for vehicular communication in 5g enabled network for autonomous movement of vehicles. To ensures privacy and security in 5G enabled vehicular networks we have proposed a block chain based technique which helps to ensure privacy and security for it. cloud and making a new group of cars t new ledger is done based on block Chan technology so that attacks can be tolerated and privacy and security preserves.

## REFERENCES


**[1]** Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," IEEE Trans. Intelligent Transportation Systems, 2018.

**[2]** S. Karnouskos and F. Kerschbaum, "Privacy and Integrity Considerations in Hyperconnected Autonomous Vehicles," Proc. IEEE, vol. 106, no. 1, 2018, pp. 160–70.

**[3]** K. Katsaros and M. Dianati, "A Conceptual 5G Vehicular Networking Architecture," 5G Mobile Commun., 2017, pp. 595–623.

**[4]** N. Cheng et al., "Big Data Driven Vehicular Networks," IEEE Network, 2018. [5] 3GPP TS 33.185, "Security Aspect for LTE Support of Vehicle-to-Everything (V2X) Services," Rel. 15, 2018.

**[5]** T. H. Luan et al., "Social on the Road: Enabling Secure and Efficient Social Networking on Highways," IEEE Wireless Commun., vol. 22, no. 1, Feb. 2015, pp. 44–51.

**[6]** Z. Yang et al., "Blockchain-Based Decentralized Trust Management in Vehicular Networks," IEEE Internet of Things J., 2018.

**[7]** V. Kolesnikov et al., "Practical Multi-party Private Set Intersection from Symmetric-key Techniques," Proc. 2017 ACM SIGSAC Conf. Computer and Commun. Security, 2017, pp. 1257–72.

**[8]** C. Lai et al., "SEGM: A Secure Group Management Framework in Integrated VANET-Cellular Networks," Vehic. Commun., vol. 11, 2018, pp. 33–45.

**[9]** C. Lai et al., "Secure Group Communications in Vehicular Networks: A Software-Defined Network-Enabled Architecture and Solution," IEEE Vehic. Tech. Mag., vol. 12, no. 4, 2017, pp. 40–49.

**[10]** H. J. Jo, I. S. Kim, and D. H. Lee, "Reliable Cooperative Authentication for Vehicular Networks," IEEE Trans. Intelligent Transportation Systems, vol. 19, no. 4, 2018, pp. 1065–79.

**[11]** E. Fujisaki, "Sub-Linear Size Traceable Ring Signatures without Random Oracles," Cryptographers' Track, RSA Conf., 2011, pp. 393–415.

**[12]** P. J. Fernandez et al., "Securing Vehicular IPv6 Communications," IEEE Trans. Dependable and Secure Computing, vol. 13, no. 1, 2016, pp. 46–58.

**[13]** F. Boeira et al., "Effects of Colluding Sybil Nodes in Message Falsification Attacks for Vehicular Platooning," IEEE Vehic. Net. Conf., 2017, pp. 53–60.

**[14]** A. Akhunzada and M. K. Khan, "Toward Secure Software Defined Vehicular Networks: Taxonomy, Requirements, and Open Issues," IEEE Commun. Mag., vol. 55, no. 7, July 2017, pp. 110–18.

**[15]** R. Kumar, J. Lachure and R. Doriya, "Use of Hybrid ECC to enhance Security and Privacy with Data Deduplication," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), 2021, pp. 934-941, doi: 10.1109/ICESC51422.2021.9532948.

**[16]** Rajesh Kumar, Varun Pramod Bhartiya,Dhananjay Singh,Pavan Rathoriya,Jagmohan Sahu,"PALM PRINT RECOGNITION AND AUTHENTICATION USING DIGITAL IMAGE PROCESSING", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.9, Issue 12, pp.b486-b493,14 December 2021

**[17]** Rajesh Kumar,Harsh Sinha,Ankita Sharad,Rupali Sahu,"A Case Study on Software Defect Prediction", International Research Journal of Engineering and Technology (IRJET),e-ISSN: 2395-0056,p-ISSN: 2395-0072,Volume.8,Issue 12,pp.1348-1352,30 December 2021