Securing Autonomous Vehicles: Leveraging Blockchain for Enhanced AV Safety

Abstract—**In a smart society where every detail operates intelligently, managing the intelligent transportation system is necessary to reduce traffic jams, decrease the number of traffic accidents, and, most importantly, allocate parking spaces appropriately. The foundational technology for protecting numerous applications that are real-time and their data is blockchain. One industry where automakers are eager to embrace the use of distributed ledgers in autonomous vehicles or platforms is the automotive industry. By doing so, they hope to enhance their goods, customer pleasure, and other useful experiences. The purpose of this research is to determine the security and use of blockchain technology in self-driving cars. The applications and significance of sensors, architectures and network needs, vehicle kinds, driving modes, vehicle targets and tracking strategies, intelligent agreements, smart handling of data, and use cases relevant to particular industries are all examined in the context of blockchain technology. While the advancement of fully autonomous cars is hindered by attacks such as men-in-the-middle, imitating of the GPS system, denial-of-service, sniffing, and many more, the adjoining autonomous sector is expanding at a faster rate than self-driving cars. Most of the research focuses on a single point of failure in a central system. The architecture, security, and difficulties of blockchain technology are covered in relation to autonomous cars in this study.**

Index Terms—**Autonomous Vehicles, Sensors, Blockchain, Sensor and Network Security,**

I. Introduction

AVs have received a lot of attention in recent years, both in academia and in industry as well as intelligent transportation networks. AVs are predicted to be integrated into our daily lives in a variety of ways, including autonomous drone shipment systems, driverless cars, guided automated vehicles in warehouses, and autonomous home assistant gadgets. Self-driving cars are rapidly advancing; they use a mix of sensors, actuators, machine learning infrastructure, and complicated and powerful algorithms to deploy software and drive between locations without human intervention. The incorporation of computer systems and the automation of mechanical and manual tasks have enhanced vehicle features. E. Yurtsever [1] et. al states that driver assistance systems are becoming more common in new automobiles. Adaptive cruise control, lane-departing warning systems, and self-parking systems are examples of useful features. The introduction of self-driving vehicles heralds a new era in the automobile industry, promising increased safety and economy. However, these cars are prone to errors, and there have been numerous accidents in recent years. The complexity of AVs and their subsystems creates vulnerabilities that unethical behavior can easily exploit. Examples include compromised or hijacked communication channels, cyber-attacks and risks, and command injection attacks. To address these problems, it is necessary to provide robust and secure alternatives to an autonomous system. Blockchain technology can address security concerns due to its immutability, decentralized and distributed network approach, transparency, enhanced security through cryptography, robust consensus-building framework, and faster transaction settlements, among other features.

Although blockchain technology integration into autonomous vehicle security remains in its infancy, further research and development initiatives should produce novel solutions that eventually improve the security and safety of autonomous cars. Distributed shared ledgers, cryptography, the use of consensus techniques for process validation, and smart contacts are the primary contributions. Wang [2] et al. explored the blockchain technology approach for safe content distribution in vehicle social networks as an example of modern development. In this case, vehicular social networks in a multi-party setting are the focus of the POR consensus protocol. By changing the simulation time, a safe delivery ratio-based analysis is performed. An extensive examination of assaults and weaknesses in autonomous systems was prepared by Jahan [3] et al. This work has produced theoretical talks on the recent developments in autonomous systems development as well as attack classifications. There is discussion of several AVs, their characteristics, and current advancements. A thorough analysis of blockchain-based solutions for V2X connectivity security was carried out by Shrestha [4] et al. Blockchain and 5G technology solutions supply the security elements, and integrations are the topic of discussion.

II. Research Method

- This work has carefully searched the literature to identify current blockchain-based AV systems as well as suggested strategies. This work also covers new applications of blockchain technology to enhance the experience of driving an autonomous vehicle. Additionally, steps are made for feature-based analysis and design or study.
- Various AVs have been investigated in this paper, and the significance of blockchain technology in addressing challenges related to distributed decision-making, coordination, and data security has been covered.
- As a result, industry use-cases for AGVs are covered. Along with exploring a reward-based blockchain system for automated guided cars, the article also discusses the significance of blockchain technology for automated guided vehicles, as well as the main issues, solutions, benefits, and drawbacks in a real-time setting. investigat-

ing how blockchain technology can be applied to current smart city issues.

III. Architecture Of an Autonomous Vehicle

The architecture of an autonomous vehicle combines actuators for vehicle control, decision-making algorithms, and sensor arrays for environment awareness. Together, these systems can navigate, foresee difficulties, and carry out driving tasks without the need for human assistance. Resilience and efficiency in architecture are essential for secure and dependable autonomous transportation.

A. Sensors and Vision System

Car sensing may be divided into two sections. They are exteroceptive and proprioceptive sensors. The former detects the car's surroundings, whilst the latter senses the car's inside. Internal vehicle examples include wheel speed, inertia measurement, and driver attention. The modern visual sensing capacity adds an eye to the car's autonomous driving. To produce high-quality 2D and 3D representations, creating 3D technology integrates optical, image, and software technologies. Innovative features of the best-in-class optical systems with tilt and picture-generating unit (PGU) technologies include selective dimming, curved surfaces, improved optics management, center displays with HS haptics, and a new interior rearview e-mirror that allows switching from mirror mode to display mode. Cuma [5] et. al shows a vision chip, or SoC, is a crucial component of an automated vehicle's 360-degree perspective. The image processing technique is computed using pictures from numerous smart CMOS cameras. Consequently, the automobile can identify people, departure lanes, and other impending obstructions. Its output controls numerous control devices in the vehicle, including the steering wheel, brakes, and accelerator. We can attain these controls thanks to the Renesas MCU's power. The chip includes concurrent image analysis and rendering to replace the picture signal in each camera's CPU. The automatic parking system and advanced driver assistance technology are examples of vehicle automation technology. The R-Car V3H system-on-chip processor has been released by Renesas Electronics Corporation.

In level 3 and level 4 autonomy of automated cars, the SoC handles artificial intelligence and computer vision applications. It can execute irrevocable emergency braking, expressway and congestion piloting, as well as remote parking. Its dual image signal processor handles techniques like Dense Stereo Disparity, Dense Optical Flow, and Object Classification. So much so that the SoC has a convolutional neural network block to speed up deep learning operations. It handles stereo front camera optimization with its IMP-X5 + image recognition engine, enhancing its performance five times at only 0.3 W. The lightweight system on chip has the ability of managing cognitive activities such as driving and parking the vehicle independently using its 3D surround vision.

B. Sensor Integration

Sensors will play a major role in Autonomous vehicle as Sensors are critical to an automated driving system's view of its surroundings, and the use and efficacy of various incorporated sensors can directly decide the safety and practicality of automated driving cars. Sensor calibration is the cornerstone of every autonomous system and its component sensors, and it must be done accurately before sensor fusion and obstacle identification can be applied. We will use four types of sensors.

Cameras, which serve as the visual sensors of autonomous vehicles, provide high-resolution picture capture, color identification, and road sign interpretation. They give a complete view for guidance and safety monitoring when strategically placed on the front, back, sides, and inside. Cameras are very cheap, and with the right software, they can identify both mobile and static impediments in their range of vision, as well as offer high-resolution photographs of their surroundings. These skills enable the vehicle's perception system to recognize road signs, traffic lights, road lane markings, and obstacles in the case of road traffic vehicles, and a variety of other items in the case of off-road vehicles. Barzaghi [6] states that an AV's camera system may use monocular cameras, binocular cameras, or an assortment of both. The monocular camera system, as the name suggests, employs a single camera to capture a succession of pictures. Traditional RGB monocular cameras are essentially more limited than stereo cameras in that they lack native depth information, though depth information can be calculated using complex algorithms in some applications or more advanced monocular cameras using dual pixel autofocus hardware. As a result, two cameras are frequently put side by side in autonomous cars to form a binocular camera system.

LIDAR (Light Detection and Ranging) sensors, which use laser beams to build comprehensive 3D maps, are used for exact object detection. Multiple units, placed on prominent areas such as the roof, cover diverse perspectives, ensuring a complete portrayal of the surroundings. Due to its performance characteristics such as evaluation range and precision, durability to surrounding changes, and high scanning speed (or refresh rate), typical devices in use nowadays can record up to 200,000 points per second or further, covering 360 rotation and a vertical field of view of 30 degrees. The wavelengths of today's cutting-edge LiDAR sensors used in AVs are typically 905 nm (nanometers)—the safest form of laser (Class 1), with lower water absorption than, say, 1550 nm wavelength sensors previously used. According to a study, 905 nm devices can deliver improved resolution of point clouds in bad weather circumstances such as fog and rain. However, 905 nm LiDAR systems are still somewhat subject to fog and precipitation: Vargas [7] et.al states that extreme weather conditions such as fog and snow can reduce sensor performance by 25 percent.

Ultrasonic sensors, which generate sound waves, give close-range data for parking and maneuvering. They are placed on the front, rear, and side bumpers to supplement the long-range detecting abilities of other sensors.

GPS (Global Positioning System) antennae on the roof provide real-time position data, which aids navigation precision. GPS, when combined with additional sensors, improves the general comprehension of the vehicle's location relative to the surroundings.

C. Sensor Fusion

Sensor fusion is a critical component of most autonomous systems, such as self-driving automobiles on the road and autonomous Unmanned Ground Vehicles (UGV). It combines data from numerous sensing modalities to decrease detection uncertainty and overcome the limitations of individual sensors functioning alone. Furthermore, Yeong [8] et. al shows that sensor fusion aids in the development of a consistent model capable of properly perceiving the surroundings in a variety of environmental situations. Camera and radar fusion, for example, may offer high-resolution pictures as well as the relative speeds of identified obstacles in the perceived scene. To track and record both authorized and illegal vehicle behavior, vehicle numbers, driver details, path situations, information about the environment, insurance, and maintenance data acquired by the IoT sensor fusion network are stored in a distributed ledger and blockchain network. Blockchain technology can be used in IoT to decrease single points of failure and to store and analyze IoT data in a safe and effective manner. The peer-to-peer architecture of the blockchain is seen to offer a possible remedy for problems with bottlenecks and single points of failure. The appropriate blockchain authorities can locate the hacked IoT sensor and take immediate action against the perpetrators if they manipulate an IoT sensor.

D. Vehicle Communications

The AV operates in phases: vision (sensors), communication (Vehicle-to-Everything), and movement (actuators) and (V2X) technology. The goal of vehicle-to-vehicle (V2V) communication is to wirelessly transfer pertinent information across vehicles to improve driving efficiency and safety. Cellular network infrastructures are used when vehicles use vehicle-to-vehicle (V2V) multimedia services. By employing real-time updates on road conditions, intelligent transportation systems enable better controlled vehicle-to-roadside, or V2R, connectivity. Autonomous vehicles (AVs) rely on vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communications to efficiently interact with their environment. Vehicles can communicate with other cars, the infrastructure, people, and even the outside world thanks to these communication technologies. Zorkany [9] et. al states that V2V communication allows cars to communicate with other vehicles in real time, sharing information like heading, position, and speed. For safety applications like cooperative merging, emergency braking, and accident avoidance, this information is essential. Vehicles and other infrastructure components can communicate using V2X communication, including traffic lights and road signs. As a result, there can be less congestion, better traffic flow, and dynamic traffic management. Vehicle-to-vehicle communication (V2X) enables access to environmental data, including pollution levels, road conditions, and weather. AVs can adjust their driving style based on this knowledge.

E. Levels of Automation

Fully automated driving systems in autonomous cars come in a variety of forms and degrees, making it possible to fix the appliance if one of its parts breaks down. Although there are currently several classifications for AVs, they are not very different from one another. A unified framework for describing the six degrees of autonomous driving has been created by the SAE [48]. Wishart [10] et. al describes six degrees or levels of driving automation, ranging from 0 (totally manual) to 5 (fully independent), are what define SAE.

- No Automatic Driving (Manual Control) - Level 0 : Most cars on the road today are level 0 or manually operated. While it may temporarily interfere and send out alerts, the automated system lacks long-term vehicle control.
- Driver Assistance (Hands-on) - Level 1 : It is automation at its most basic level. One automated device that helps the driver with steering and acceleration (also known as cruise control) is installed in Level 1 cars.
- Hands-off Partial Driving Automation—level 2 : The cars have the highest level of autopilot functionality among end-user cars and can steer and control speed. Despite being able to "hand-off" the steering wheel thanks to the supervising driver technology, the driver is still responsible for the car.
- Automatic Conditional Driving (Eyes Off) – Level 3 : With Level 3 technology, drivers may maintain the vehicle's stability on the road without having to focus their attention on the road or the steering wheel. Alternatively, consumers can watch movies, play games, and read messages on their smartphones. The sole requirement is that you remain in your car.
- High Automation Of Driving (Mind Off) - Level 4 : According to the SAE categorization system, cars that need human intervention are rated as level 4 even in terms of safety. They can do all driving duties on their own, freeing the driver to relax or sleep. At this point, cars are capable of operating without human help on their own (except from when they reach their destination).
- Complete Automation (Optional Steering Wheel) - Level 5 : Most autonomous cars aim for full startup automation. This is the moment at which human interaction is never necessary, not even in the most difficult environments, like dirt tracks. To put it briefly, Level 5 vehicles solely carry passengers and lack a driver.

IV. SECURITY PROBLEMS ON AUTONOMOUS VEHICLES

Sensor systems are a major component of autonomous vehicles' (AVs) navigation and key decision-making processes. The global positioning system (GPS) is one of the most important of these since it can provide accurate geolocation, speed, and chronological data, independent of the vehicle's location on Earth and the weather. Khan [11] et. al states that

GPS is susceptible to possible security breaches just like any other highly developed technological system.

Attacks using Spoofing: In these situations, opponents simulate authentic GPS signals with fake signals. Once the AV receives these false signals, it interprets them as genuine, leading to an erroneous location calculation.

Attacks known as jamming: In these attacks, the attacker uses gadgets that broadcast signals at the same frequency as GPS signals to obstruct the real signals. The GPS receiver's capacity to determine its geolocation is hampered by this interference, which prevents it from connecting to the actual GPS signals.

Meaconing Attacks: In these attacks, GPS signals are intercepted and then purposefully delayed before being retransmitted. The GPS receiver may miscalculate its position because of this behavior.

Attacks known as replays include intercepting GPS signals and sending them again at a different time or place. The GPS receiver may calculate the location or time incorrectly because of this activity.

Autonomous vehicles' LiDAR systems may be subject to security breaches, which could have detrimental effects on traffic safety. The following are instances of how security breaches on LiDAR sensors may materialize in actual autonomous vehicles:

Attacks known as "spoofing": These occur when adversaries produce fake signals that resemble the real signals that LiDAR sensors detect, leading the autonomous vehicle to misread its environment. For instance, to make a victim's AV stop or brake violently, an attacker could place a fictitious obstruction next to the front of the vehicle.

Cyber-level attacks: Even in the absence of situational awareness, attackers can tamper with sensor data by breaching the LiDAR system. Road safety may suffer because of impaired perception and navigation in multisensory autonomous vehicles.

Electromagnetic interference (EMI): The time-of-flight circuits that comprise contemporary LiDAR systems are impacted by EMI, which can impair LiDAR sensors. This could make it harmful for road safety if the AV recognition system misidentifies or misclassifies objects and perceives immaterial impediments.

Adversarial objects: Under some circumstances, attackers can produce adversarial objects that elude LiDAR-based detection systems. An attacker could, for instance, build an item that seems regular to a human viewer but is incorrectly classified through the LiDAR system, leading to inaccurate decisions by the AV.

V. Blockchain

A. Block in Blockchain

The primary component of a blockchain is a block, which is essentially an account of every transaction that has occurred. You may think of a block as a link in a chain. The tens of thousands of blocks that make up the blockchain network are constantly changing. The block is significant since it is nearly impossible to hack. It would be like a bank robber taking all the bank's records along with the money, if that were feasible. Bitcoin miners receive BTC, or bitcoins, for both their contributions to the solution seeking process and their successful solutions to challenging mathematical equations.

B. Blockchain Architecture

The design of blockchain revolves around a decentralized system where information is stored across a network of computers instead of a central authority. Gururaj [12] et. al states to think of it like a digital ledger that keeps track of transactions, but instead of being managed by a single entity, it's distributed among many computers, forming a chain of blocks. Each block contains data, like a list of transactions, and is linked to the previous block, ensuring a continuous chain. All participants in the network, called nodes, have a copy of this chain, making it transparent and resistant to tampering. Transactions are secured through cryptographic methods, ensuring that only authorized users can make changes. These transactions are verified by network participants, who reach an agreement on their validity through mechanisms like Proof of Work or Proof of Stake. Blockchain networks come in two main types: public and private. Public blockchains, like Bitcoin and Ethereum, are open to anyone to join and participate in transactions. On the other hand, private blockchains limit access to authorized users, offering more control over who can interact with the network. Smart contracts are a key feature of blockchain technology, enabling automated and programmable transactions. These contracts execute predefined actions when specific conditions are met and are deployed on platforms like Ethereum. In essence, blockchain combines decentralized consensus, cryptographic security, and smart contracts to create a secure, transparent, and tamper-proof system for recording transactions across a network of participants.

C. Components of Blockchain

The different components associated with a typical blockchain are

- Cryptographic Encryption: Blockchain uses various cryptographic encryption methods like one way hash function, Merkel trees and public key encryption to ensure a secure and transparent environment.
- P2P network: P2P network is used for the discovery of a new peer and sharing data in a peer to peer fashion.
- Rules of validation: A common set of rules are established for validating a user and allowing access to the network.
- Ledger: The ledger maintains a list of transactions which are bundled together in blocks, which are cryptographically linked.
- Consensus Mechanism Algorithm: It is a type of algorithm that decides a chronology of transactions in scenarios where a dishonest transaction is suspected (adversarial environment).

D. Advantages Over Traditional Security Solutions

Blockchain has many advantages over traditional security solutions, some of which are as follows:

Conventional methods for storing and protecting data are incredibly centralized, suggesting a single point of failure. This implies that any hostile external attack, such malware or brute-force hacking, on a central server may cause all or some of the data to be lost. Depending on the kind of data saved on the system, information loss could pose a threat to entire economies and enterprises that rely on antivirus software.

Storage based on blockchain technology is impenetrably safe from outside threats like hacking. Data loss is very low because all blockchain nodes save the same data. This means that sensitive data, like user identity and autonomous vehicle communication, is ideal for security and storage on the blockchain. It is vital that the data stored on the blockchain be accurate. Accessing and editing any data recorded on the blockchain would be nearly hard without network-wide notification and consensus. Consequently, users may operate a reliable and safe environment and rely on the blockchain as an indicator of truth, all without requiring mutual trust or familiarity.

The decentralized, transparent structure established by blockchain technology fosters confidence among network users. AVs can consist of insurance companies or workshops that collaborate to record data about transactions and other shared data via blockchain technology. Because of this feature of the blockchain, every user has equal access to the data that is recorded, and any modification needs approval from all users. Every member of the blockchain-based network maintains, computes, and updates new entries to keep the distributed ledger current. By communicating with one another, every node maintains internal security. It enables you to track the data's ownership, record, and origin. The user may view how old and new copies of the same information were replaced using timestamps and cryptographic proofs thanks to the blockchain. Any change made to the blockchain cannot be undone.

The capacity to update information is decentralized in blockchain, while traditional storage methods for data are centralized because of their client-server architecture. Blockchain technology preserves the preceding block of data indefinitely while maintaining an unchangeable chain of documents and transactions. This guarantees that the chain's history can be independently verified and traced back to the source of every new block.

VI. ADDRESSING SECURITY PROBLEMS OF AVs THROUGH BLOCKCHAIN

Recently, several research have suggested combining blockchain technology with autonomous vehicles. Pokhrel and Choi [13], for instance, suggested an AV design based on blockchain technology. This concept makes advantage of FL to protect data privacy while simultaneously enhancing vehicle communication effectiveness. A mathematical structure is suggested here. Using FL parameters and blockchain technology, this framework facilitates the development of a controllable network. Block size, block arrival rate, data repetition limit, and frame size are some of these factors. This work has highlighted several issues with the suggested model that calls for forward-thinking research.

In the event of an assault or compromise to vehicle operations, Rowan [14] et al. presented a secure method of inter-vehicle communication using side channels including visual light and ultrasonic audio. This method confirms the position and guards against attacks. The handshake protocol restricts side channel flow to 176 bits to create safe communication. Physical side channels and blockchain technology are used for the data sharing between manufacturers and untrusted cars. Using symmetric encryption and message-passing authentication keys, the side channels enable direction-based safe transfer between vehicles.

As AV will become more and more common, the most important issue which will be faced by the existing IOT networks is scalability and associated security breaches. Increased in no of AVs will result in growth in the number of devices connected to the IOT network. This will result in overlapping authentication issues, associated authorization problems and miscommunications between the different nodes in the network, resulting in a bottleneck. Thus, huge investment would be required for the servers which are suitable for very large-scale information exchange to avoid server downtime.

Extremely high dependance on IOT devices is an area which needs to be addressed with the increment of number of AVs. IOT devices are prone to DDOS attacks and usage of blockchain technology can eliminate this issue. With blockchain, there is no possibility of a single point of failure-based attack because blockchain is entirely auditable and transparent. Blockchain also uses a distributed database and multiple ways of authentication and identification of connected devices.

As AVs will become more popular, they will become more prone to unauthorized and unethical sensory or network related attacks. AS hackers are becoming more and more skillful, surely within someday they will use low cost easily available devices like flipper zero to tamper with the overall integrity of AV. Usage of blockchain technology can help to develop a Blackbox like device where all sensory, mechanical, physical and network related interactions of an AV will be recorded in a transparent ledger like system which are not at all tamper able. This will not only help in increasing the overall security of the AV, but also will supply necessary forensics evidence in cases of theft, mishaps etc.

Every AV used to communicate with each other and to the infrastructure using a vehicular ADhoc network. Since autonomous vehicles were experimental until a few years ago, most of the work done on the vehicular networks was through a global VANET. But in recent days with the increase of the number of AVs and with public access of AVs in many countries, Zafar [15] et. al states that, it has become the need of the hour to implement a decentralized regional VANET instead of the global VANET. First, we must identify the weak links in the blockchain and address them accordingly. The areas of vulnerability are .. delay between two blocks, increase in random block sizes and an insecure connection between two blocks. The solutions are.. We must decrease the time delay of information exchange between two blocks giving unauthorized agents a reduced timeframe of attack. We must make the block sizes as small as possible to avoid the possibility of bottlenecks. If there is no delay during the time of information exchange the chances of the information losing its integrity becomes very less. The advantage of using small block sizes is that they can be encrypted in a much more secure way, resulting in an increase of data integrity.

One of the most important issues of all networks related attack is a scenario where the hacker or the attacker gains control of 51 percent of the entire network components. in case of AVs this attack may prove to be extremely serious in nature as it can deliver the entire control of the car to an unknown attacker. The car will no longer remain under the control of the driver or the owner and can result in manifold mishaps. The ownership of the car can be compromised by tampering the relevant information. The car can be driven from a remote location paving the way for malicious personal attacks. It can cause issues of terrorism and compromise with national security. Tampering with car data can also lead to blind any forensic investigation as well as financial fraud on car insurance and costs. In the context of blockchain, Amin [16] states that, it is possible to fend off a '51 percent attack', much like how one side in a tug-of-war might be forced to re-balance when the other starts pulling too strongly. We can bring blockchains back into balance by changing the game's rules or banding together to oppose the more powerful party. An attacker may be severely slowed down or removed from the action entirely by using these tactics. It's critical to keep in mind that conducting a '51 percent attack' necessitates a sizable amount of time, effort, and cash commitment. Furthermore, if successful, it might destroy the cryptocurrency's value, which would hurt the attacker in the end.

VII. Conclusion

By developing a secure and dependable approach utilizing the signals for transmitting factor of the current car to neighboring vehicles as well as the developing field of autonomy and intellectual development of transport systems, the authors of the paper proposed employing Blockchain technology to increase security. The literature examines an autonomous vehicle's design, vision system, sensor integration, and inter-vehicle communication. It focuses on weaknesses in sensor systems, such as GPS and LiDAR, and suggests using blockchain technology to solve these problems. It describes different ways that AV navigation and safety might be compromised by cyberattacks on GPS and LiDAR, such as spoofing, blocking, meaconing, and replays. It also talks about how blockchain technology might improve AV security by guaranteeing data integrity, blocking unwanted access, and facilitating open record-keeping.

Blockchain is a suitable alternative to conventional centralized safety measures for AV system security because of its decentralized construction, encryption protection, and smart contracts. To handle the growing number of AVs, the paper highlights the necessity of creating a decentralized regional Vehicular Ad hoc Network (VANET), addressing issues like latency between blocks and unsecured connections. It also draws attention to the possibility of a '51 percent attack' on the blockchain network, which may jeopardize antivirus control and present grave security risks. The paper does, however, offer countermeasures to these attacks, such as altering the rules and encouraging network users to cooperate.

The report's conclusion emphasizes how crucial it is to include blockchain technology into antivirus (AV) systems to improve security, prevent illegal access, and guarantee the integrity of data flow. Through vulnerability mitigation and the utilization of blockchain's built-in security features, autonomous vehicles (AVs) can function with increased safety and efficacy in the dynamic transportation environment.

References

[1] E. Yurtsever, J. Lambert, A. Carballo and K. Takeda, "A Survey of Autonomous Driving: Common Practices and Emerging Technologies," in IEEE Access, vol. 8, pp. 58443-58469, 2020, doi: 10.1109/ACCESS.2020.2983149.

[2] Y. Wang, Z. Su, K. Zhang, and A. Benslimane, "Challenges and solutions in autonomous driving: A blockchain approach," IEEE Netw., vol. 34, no. 4, pp. 218–226, Jul. 2020.

[3] F. Jahan, W. Sun, Q. Niyaz, and M. Alam, "Security modeling of autonomous systems: A survey," ACM Comput. Surv., vol. 52, no. 5, pp. 1–34, Oct. 2019.

[4] 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, Aug. 2020

[5] Cuma, M.U., Dükünlü, Ç. and Yirik, E., 2023. Smart Driver Behavior Recognition and 360-Degree Surround-View Camera for Electric Buses. Electronics, 12(13), p.2979.

[6] Barzaghi, L., 2023. Sensors' Architecture Definition for Energy Consumption Reduction in Urban Battery Electric Vehicles (Doctoral dissertation, Politecnico di Torino).

[7] Vargas, J., Alsweiss, S., Toker, O., Razdan, R. and Santos, J., 2021. An overview of autonomous vehicles sensors and their vulnerability to weather conditions. Sensors, 21(16), p.5397.

[8] Yeong, D.J., Velasco-Hernandez, G., Barry, J. and Walsh, J., 2021. Sensor and sensor fusion technology in autonomous vehicles: A review. Sensors, 21(6), p.2140.

[9] El Zorkany, M., Yasser, A. and Galal, A.I., 2020. Vehicle to vehicle "V2V" communication: scope, importance, challenges, research directions and future. The Open Transportation Journal, 14(1).

[10] Wishart, J., Como, S., Forgione, U., Weast, J., Weston, L., Smart, A. and Nicols, G., 2020. Literature review of verification and validation activities of automated driving systems. SAE Int. J. Connect. Autom. Veh, 3, pp.267-323.

[11] Khan, S.Z., Mohsin, M. and Iqbal, W., 2021. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. PeerJ Computer Science, 7, p.e507.

[12] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," IEEE Trans. Commun., vol. 68, no. 8, pp. 4734–4746, Aug. 2020.

[13] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. Mc Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," 2017, arXiv:1704.02553.

[14] Zafar, F., Khattak, H.A., Aloqaily, M. and Hussain, R., 2022. Carpooling in connected and autonomous vehicles: current solutions and future directions. ACM Computing Surveys (CSUR), 54(10s), pp.1-36.

[15] Amin, M.R., 2020. 51 percent attacks on blockchain: a solution architecture for blockchain to secure iot with proof of work.