[1] **Venkata Lakshmi Namburi**

# Dynamic Adaptive Security Framework for Software-Defined Autonomous Vehicles in Edge Computing Environments

Journal of Electrical Systems

***Abstract:*** - Security and accountability must be prioritized in the ever-increasing deployment of autonomous vehicles (AVs). This work aims to suggest an all-encompassing strategy for addressing these challenges. Our primary contribution will be to enhance cybersecurity by implementing a solid mechanism for identifying authorized users within AVs in response to the increasing importance of speaker identification. An ensemble-based strategy that makes use of speaker verification techniques is offered as a means of preventing the threat of voice spoofing. This approach ensures that user commands are genuine. Furthermore, in the event of incidents involving autonomous vehicles, there is a requirement for precise accountability and the distribution of liability liabilities. We propose a novel application of blockchain technology to address this issue. This application makes it possible to create an event recording system that guarantees transparent and tamper-proof records. EC-CAVs, connected autonomous vehicles powered by edge computing, have the potential to meet the growing demand for intelligent transportation on a worldwide scale. Any number of advantages, including proactive vehicle monitoring, traffic management, and services that offer completely autonomous driving, could result from incorporating such advances into transportation ecosystems. When deploying EC-CAVs, there must be strict adherence to safety and security protocols to avoid any possibility of vehicle immobilization, road accidents, data leaks, or other problems. A standard attack taxonomy for the EC-CAVs ecosystem will be derived from this study's current and future cyber threats investigation. This article presents the EC-CAV reference architecture. The following part provides an in-depth analysis of security measures that can ensure passengers' safe and secure transportation from one place to another by utilizing an ecosystem of EC-CAVs.

***Keywords:*** Autonomous vehicle, Software-defined vehicle, Edge computing environments.

## Introduction

Emerging as a potentially transformative technology, autonomous and self-driving vehicles can reshape the transportation landscape [1]. Among the many advantages offered by these vehicles are better road safety, more satisfying user experiences, greater mobility, and proactive driving capabilities. Autonomous cars encompass a wide range of levels of automation, with levels 2 to 4 being the most prevalent. This is illustrated in Figure 1. The increase in automation at these levels highlights how important it is for cars and people to communicate seamlessly. Significant milestones have been reached in autonomous vehicle (AV) technology, such as a blind individual being able to travel unaccompanied in a Google self-driving car in Austin [2]. In addition to other achievements, these successes demonstrate that autonomous vehicles have the potential to provide users with impairments with enhanced mobility and independence.

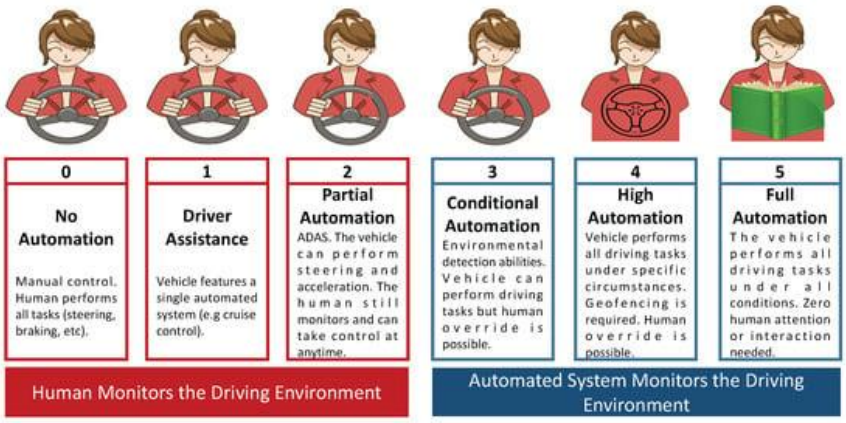


**Figure 1.** Levels of vehicle automation.

[1] Research Scholar, B.E.S.T Innovation University (BESTIU), Software Systems Engineer, Danlaw Inc. Michigan USA. venkatanamburi91@gmail.com

**Background and Motivation**

Several concerns have been raised regarding the safety of autonomous vehicles (AVs) when they are operating on public roads. Accidents on the road could be caused by autonomous vehicles (AVs) if the system fails to function properly. Among the 130 accidents involving autonomous vehicles that occurred between July 2021 and May 2022, according to the National Highway Traffic and Safety Administration (NHTSA) [3].

Significant public attention was drawn to several other prominent accidents that used autonomous vehicles. While the bus was travelling at a speed of fifteen miles per hour (or twenty-four kilometres per hour), a Google self-driving car was travelling at a low speed of two miles per hour (or three kilometres per hour); this caused the collision that occurred in 2016. In 2017, there was another incident with a Tesla Model S involving a collision with a bicyclist over 80 years old. This type of accident highlights the critical need for trustworthy solutions regarding autonomous vehicles (AVs) to safeguard road users from threats like these.

In addition, research has demonstrated that these occurrences have resulted in an unfavourable perception of technology among the general population [4].

Responsibility is yet another issue that arises in connection with autonomous vehicles. When an AV crashes, it might be hard to tell who was at blame—whether it was with another AV, a regular automobile, or even a person. In the case of an accident involving an autonomous vehicle, how can the parties involved be fairly and adequately compensated?

To determine who is responsible for an accident, it is critical to have access to trustworthy accident forensics [5]. Misunderstandings and disagreements regarding liability may result from this. In some cases, individuals may even fabricate evidence to escape being held accountable. Can we record these instances so that they may be investigated later and we can become aware of what took place? In addition, what measures can we take to guarantee that these documents are accurate and cannot be altered in any way? The study's objective includes a blockchain-inspired accident, an ensemble speaker identification system, and a method for recording events that ensures the collection of verifiable and trustworthy forensics.

Speaker identification refers to identifying the people who operate an audiovisual device through speech. Speaker identification systems can distinguish and categorize individuals by using several spectral features intrinsic to human speech [6]. The reliability and precision of speaker recognition in AVs are crucial for solving specific issues and ensuring that interactions between humans and cars are safe and effective. Speaker identification is vital because it allows vehicles to differentiate between drivers, passengers, and other external actors speaking to the vehicle (Figure 2). Furthermore, authorized personnel can more easily obtain and keep exclusive access with speaker identification. Reliable speaker recognition systems are becoming increasingly important in autonomous vehicles because of the number of accidents and incidents involving these vehicles [7]. When considering the available facts, this becomes much more apparent. Conversely, they stress the significance of speaker recognition systems that are strong enough to provide dependable and smooth interactions between humans and autonomous cars. Figure 2 shows how a speaker identification system can limit the capabilities and number of people allowed to operate an autonomous vehicle.

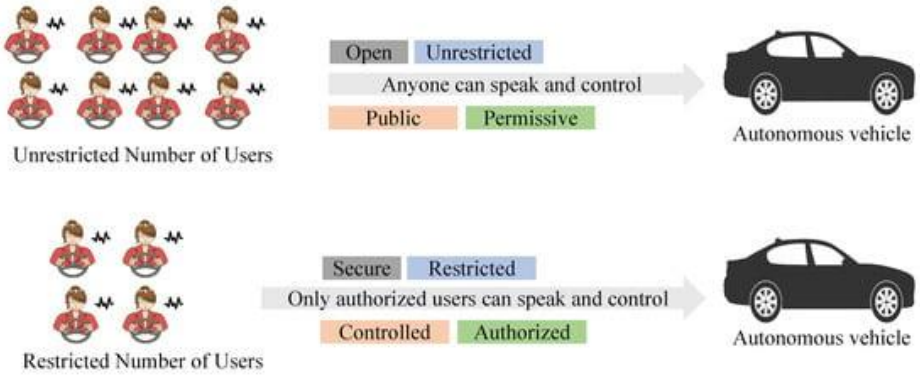


**Figure 2.** A speaker identification device is used to limit the number of people allowed to use an autonomous vehicle.

Speaker identification systems must be concerned about their vulnerability to speech spoofing attacks. This type of attack occurs when an adversary attempts to imitate the voice of a legitimate speaker in order to give commands to the vehicle. This can be accomplished by speech synthesis or voice conversion. This could put both autonomous vehicles and people who utilize roads in danger. Figure 3 provides a visual representation of such a scenario.

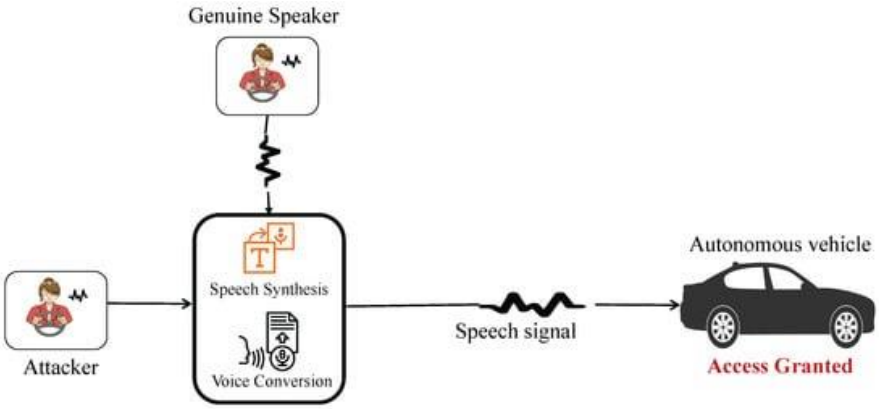


**Figure 3.** The impact of voice spoofing on autonomous vehicles.

Regarding autonomous vehicles, security becomes an essential problem beyond interactions with individuals. Improving the safety and traceability of autonomous vehicles is one use of blockchain technology, which gained traction because of cryptocurrencies [8]. Blockchain technology is perfect for creating trustworthy and decentralized data records because it cannot be altered. As a result, the dangers of data manipulation and illegal access are mitigated [9]. To make autonomous car systems more trustworthy, blockchain technology is being used to secure data storage and access control. This helps to address potential weaknesses and improves the system's overall reliability [10].

**Related works**

The following part presents a literature overview of speaker recognition approaches designed for autonomous vehicles and in-vehicle communication systems. We also examine past research on voice spoofing and event recording systems for autonomous vehicles assisted by blockchain technology.

***Speaker Identification***

There has been a lot of research on the speaker identification problem, but it still has its unique challenges [11]. The development of speaker identification models that are both highly accurate and computationally efficient is a fundamental obstacle that must be overcome. As a consequence of this, researchers have extensively investigated various speech characteristics and made use of machine learning (ML) approaches, achieving remarkable outcomes. Speaker identification has also been studied in audiovisual devices (AVs) [12]. The main reference point was using microphone arrays for speaker localization and identification [13]. Another study looked at using conventional machine learning techniques to identify speakers in AVs. To detect speakers in AVs, researchers looked at an artificial neural network (ANN) method [14]. Having trustworthy speaker identification models for AV equipment is a crucial finding of these studies.

Building a robust machine learning model for speaker identification requires considering data type, machine learning method, and feature extraction approach.

When identifying a speaker, distinguishing elements of their speech is essential, especially when considering aspects such as gender and linguistic traits. When it comes to voice recognition and speaker identification tasks, the characteristics utilized most frequently are known as Mel frequency cepstral coefficients (MFCCs). They have a high level of robustness and have been successfully employed in various speech-related tasks, including speaker identification, emotion recognition, and speech recognition. MFCC traits are effective in speaker recognition systems, as evidenced by several research, including [15].

Gamma tone cepstral coefficients, on the other hand, are more resistant to noise than noise-free cepstral coefficients (MFCCs), which is why they are the favoured choice for speaker recognition tasks [16]. Another

characteristic frequently utilized for speaker identification is pitch, which has been used to improve speaker identification performance, for example [17]. A more reliable speaker identification system was developed in [17] with a hybrid feature that included both pitch and MFCC. Since this is the case, it is essential to determine which characteristics are most appropriate for speaker identification. Furthermore, there is still a substantial worry regarding identifying the most robust machine learning model for speaker identification [18]. To successfully develop a real-time speaker identification system, it is vital to consider models with either a low computational complexity or a low memory footprint.

***Voice Spoofing***

Refinement of features, machine learning models, or resource-intensive approaches have been the primary focus of previous research endeavours linked to speaker identification. Despite this, the vulnerability of these systems to voice spoofing assaults is a crucial aspect that has frequently been put to the rear of the pack. This weakness's potential to jeopardize security and accountability is not insignificant. Numerous research initiatives have sought to combat spoofing by investigating various tactics. Using neural networks for post-processing voice samples has become the focus of attention in specific situations. These networks have been fine-tuned to reduce the dissimilarity between the characteristics that distinguish authentic and counterfeit utterances [19].

An impostor's attempts to transform their voice into a convincing rendition lead to artefact estimations. An alternative approach that takes artefact estimations into account is this one. This analysis was based on the assumption that all changed speech samples would display artefacts.

Undertaking the task of subsampling spoken frames before commencing spoofing detection techniques was the primary focus of the research researchers [20] carried out.

Similar to the previous example, reference [21] mapped out a similar path by converting speech characteristics into a novel collection of characteristics that makes it easier to recognize numerous spoofing assaults. Machine learning-based approaches have also proven useful in the fight against spoofing. To enhance the detection accuracy for real-world incidents of undetected voice spoofing attacks, a one-class learning technique was employed in the context of [22]. According to the studies that were found, more research has been done on the concept of ensemble learning.

The paper details an ensemble learning approach, combining deep neural networks with traditional machine learning techniques [23]. The model's predictions are combined using logistic regression.

Reference [24] utilized a comparable strategy to create a set of ML models that differentiate between speaker identification systems and attacks that use speech faking. To combat voice replay attacks, an ensemble model was developed and compared to other machine learning classifiers, including K-nearest neighbour (KNN) and support vector machines (SVMs) [25]. This method had a significant influence on the research solution we applied. This method is based on the premise that it combines multiple proven effective models in detecting phoney audio. The models that comprise this ensemble have been hand-picked to enhance overall performance by strengthening each other's capabilities.

**The AI-powered development life cycle in autonomous vehicles**

In this section, we will look at the big picture of the development life cycles of autonomous cars powered by artificial intelligence. These aspects may also be applied to other fields beyond autonomous vehicles.

**Model Training and Deployment**

Training and deployment of artificial intelligence models in autonomous cars is a methodical process that typically consists of numerous steps, including the following:

*Data Collection and Preprocessing:* The process of collecting a massive amount of data from sensors located in the real world, existing datasets, and other sources, such as synthetic datasets. First, the data must be cleaned and preprocessed to make it acceptable for machine learning models.

*Model Training:* This refers to the pattern extraction models used to understand structures and patterns in the data. Neural networks, deep learning, and natural language processing are some examples of learning models that are

used [26]. The models are trained to attain an accuracy target in specific situations or general abstract circumstances, like pattern extraction during live vehicle deployment.

*Model Generation:* This alludes to the various models of decision-making. Utilizing trained models is essential for carrying out certain decision-making activities, functions, or modules that rely on learned patterns. These models can use a wide variety of structures. There are many types of neural networks; some examples are decision trees, random forests, regression trees, deep layers, and ensemble learning.

*Code Refinement and Optimization:* In order to enhance the quality, readability, and functionality of the code that was generated, it should be refined. Post-generation processing is performed to ensure that the code complies with coding standards, conventions, and requirements.

*Quality Assessment:* The code generated should be evaluated to determine whether it is valid, efficient, and adheres to the planned features. Testing, debugging, and validation processes are all included in this process.

*Integration and Deployment:* The model must be incorporated into a more extensive system currently being developed to implement autonomy. Various approaches should be employed to install and test the software program that integrates the new model, including software-in-the-loop, hardware-in-the-loop, human-in-the-loop, and others. There should also be an emphasis on using simulation, controlled courses, and limited public road environments. Some models undergo ongoing training to enhance their learning capabilities, even after they have been put into production.

A systematic approach like this one could benefit automated vehicles' perception, planning, controls, and Human-Machine Interface (HMI) subsystems by establishing confidence levels for each model being developed and used in these areas.

**An overview of Edge computing-based connected autonomous vehicles.**

Computing at the network's Edge has the potential to become a significant technology for processing the enormous amount of data that autonomous vehicles (CAVs) would create every second of their operation. This is done to improve these vehicles' speed, safety, and reliability. The EC paradigm can be described as a computing platform that is distributed and decentralized [27]. This allows for data processing to occur at or very close to the point where it was generated. It is being done to resolve restrictions encountered in centralized computing platforms, and this is done by processing data closer to its point of origin. The delay in processing data, the loss of data due to inadequate connectivity, and network traffic congestion are all examples of these limitations.

Regarding Edge computing-based networked autonomous cars, Liu et al. [28] proposed a straightforward tier-topology as a solution. Figure 4 is a graphical illustration of the three tiers: cloud servers, RSUs as Edges, and CAVs as devices involved in the networking infrastructure.

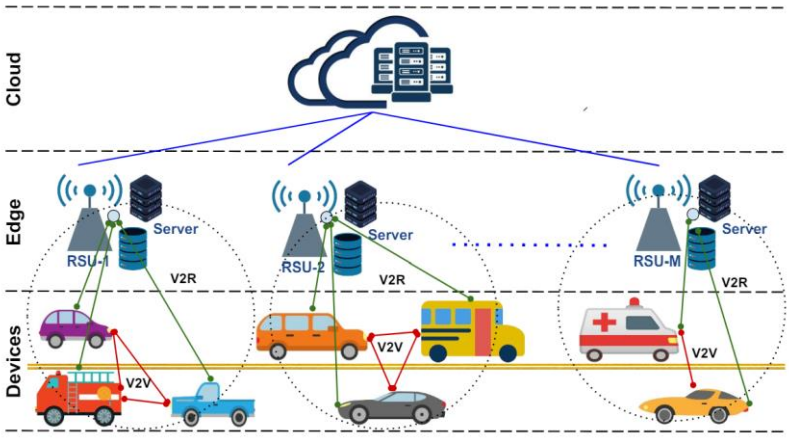


Fig. 4. A simplified tier-topology of Edge computing-based connected autonomous Vehicles.

• Devices typically denote CAVs. Electronic control units (ECUs), onboard diagnostic ports (OBDs), controller area networks (CANs), global positioning systems (GPSs), light detection and ranging (LiDARs), radio detection

and ranging (Radars), cameras (image sensors), and many more devices allow CAVs to sense traffic and environmental conditions in real-time. Connected autonomous vehicles (CAVs) can exchange data with one another and other CAVs in the area via V2V and vehicle-to-roadside unit (RSU) communication. Furthermore, CAVs are equipped with embedded computing and data storage capabilities, allowing them to carry out essential activities on a local level. Therefore, CAVs are capable of being referred to as prosumers, which means that in addition to being a data consumer, they are also a data producer [29]. At this level, the tasks that are carried out are as follows: 1) data sensing and collection, 2) data interchange, and 3) data processing to carry out the activities that have been allocated [30].

• Roadside Equipment (RSE) Connecting devices and cloud systems, this area is known as the Edge and comprises RSUs, networking resources, and servers [31]. Additionally, RSUs enable sophisticated processing of raw data uploaded by devices and real-time data analysis after the data has been transferred to the cloud. To ensure that autonomous vehicles (CAVs) run well, they offer services such as video streaming, traffic control, and trail routing. Offloading computations, outsourcing tasks, caching data, and making software administration procedures possible are all made possible by edge computing [32]. 1) The gathering, filtering, aggregation, and cleansing of local area information; 2) The analysis of local data with broad area information; 3) The processing of real-time data; and 4) The low-latency reaction to CAVs are the tasks that are carried out at this tier. Regarding automated driving, the Edge can be utilized to achieve high-performance standards.

• The cloud uses powerful and efficient servers and storage devices to process and store data uploaded by edge devices. Cloud-based systems can be utilized for data processing tasks at the application level and long-term storage, typically less time-sensitive [33]. Services in the cloud are offered to facilitate centralized management and controls, which in turn allows for optimal decision-making.

## Conclusions

In this study, an EC-CAVs reference architecture was published. Cloud, Edge, and CAV technologies were the three tiers that made up this design. To create a standard attack taxonomy, it is necessary to analyze the reference architecture that describes both existing and future cyberattacks on the EC-CAVs that are being developed. To ensure that transportation is safe and secure, we looked at different security techniques that may be used to protect the ecosystem of EC-CAVs, including the hardware, the network, and the software. The obstacles that need to be overcome and the research that needs to be done to build a security solution that is foolproof for EC-CAVs were discussed.

## References


1. Njoku, J.N.; Nwakanma, C.I.; Kim, D.S. Evaluation of Spectrograms for Keyword Spotting in Control of Autonomous Vehicles for The Metaverse. In Proceedings of the Conference of the Korean Institute of Communications and Information Sciences (KICS), Seoul, Republic of Korea, 20–25 May 2022; Volume 78, pp. 1777–1778. [**Google Scholar**]
2. Njoku, J.N.; Anyanwu, G.O.; Igboanusi, I.S.; Nwakanma, C.I.; Lee, J.M.; Kim, D.S. State-of-the-Art Object Detectors for Vehicle, Pedestrian, and Traffic Sign Detection for Smart Parking Systems. In Proceedings of the 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19–21 October 2022; pp. 1585–1590. [**Google Scholar**] [**CrossRef**]
3. Rajabli, N.; Flammini, F.; Nardone, R.; Vittorini, V. Software Verification and Validation of Safe Autonomous Cars: A Systematic Literature Review. *IEEE Access* **2021**, *9*, 4797–4819. [**Google Scholar**] [**CrossRef**]
4. Halsey, A., III; Laris, M. *Blind Man Sets Out Alone in Google's Driverless Car*; The Washington Post: Washington, DC, USA, 2016. [**Google Scholar**]
5. Pitts, W. *12 Self-Driving Cars Crashed in Arizona in the Last Year*; 12News: Phoenix, AZ, USA, 2022. [**Google Scholar**]
6. Lee, D. *Google Self-Driving Car Hits a Bus*; BBC: London, UK, 2016. [**Google Scholar**]
7. Bevilacqua, M. *Cyclist Killed by Tesla Car with Self-Driving Features*; The Bicycling: London, UK, 2017. [**Google Scholar**]
8. Chougule, A.; Chamola, V.; Sam, A.; Yu, F.R.; Sikdar, B. A Comprehensive Review on Limitations of Autonomous Driving and its Impact on Accidents and Collisions. *IEEE Open J. Veh. Technol.* **2023**, 1–20. [**Google Scholar**] [**CrossRef**]
9. Penmetsa, P.; Sheinidashtegol, P.; Musaev, A.; Adanu, E.K.; Hudnall, M. Effects of the autonomous vehicle crashes on public perception of the technology. *IATSS Res.* **2021**, *45*, 485–492. [**Google Scholar**] [**CrossRef**]

10. Oham, C.; Michelin, R.A.; Jurdak, R.; Kanhere, S.S.; Jha, S. WIDE: A witness-based data priority mechanism for vehicular forensics. *Blockchain Res. Appl.* **2022**, *3*, 100050
11. Nasr, M.A.; Abd-Elnaby, M.; El-Fishawy, A.S.; El-Rabaie, S.; Abd El-Samie, F.E. Speaker identification based on normalized pitch frequency and Mel Frequency Cepstral Coefficients. *Int. J. Speech Technol.* **2018**, *21*, 941–951. [**Google Scholar**] [**CrossRef**]
12. Zhao, X.; Wang, D. Analyzing noise robustness of MFCC and GFCC features in speaker identification. In Proceedings of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 7204–7208. [**Google Scholar**] [**CrossRef**]
13. Ayoub, B.; Jamal, K.; Arsalane, Z. Gammatone frequency cepstral coefficients for speaker identification over VoIP networks. In Proceedings of the 2016 International Conference on Information Technology for Organizations Development (IT4OD), Fez, Morocco, 30 March–1 April 2016; pp. 1–5. [**Google Scholar**] [**CrossRef**]
14. Leu, F.Y.; Lin, G.L. An MFCC-Based Speaker Identification System. In Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 27–29 March 2017; pp. 1055–1062. [**Google Scholar**] [**CrossRef**]
15. Totakura, V.; Vuribindi, B.R.; Reddy, E.M. Improved Safety of Self-Driving Car using Voice Recognition through CNN. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1022*, 012079. [**Google Scholar**] [**CrossRef**]
16. Guo, H.; Meamari, E.; Shen, C.C. Blockchain-inspired Event Recording System for Autonomous Vehicles. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 218–222. [**Google Scholar**] [**CrossRef**]
17. Sun, S.; Tang, H.; Du, R. A Novel Blockchain-Based IoT Data Provenance Model. In Proceedings of the 2022 2nd International Conference on Computer Science and Blockchain (CCSB), Wuhan, China, 28–30 October 2022; pp. 46–52. [**Google Scholar**] [**CrossRef**]
18. Rewatkar, H.R.; Agarwal, D.; Khandelwal, A.; Upadhyay, S. Decentralized Voting Application Using Blockchain. In Proceedings of the 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 18–19 June 2021; pp. 735–739. [**Google Scholar**] [**CrossRef**]
19. Ahamed, N.N.; Vignesh, R. A Build and Deploy Ethereum Smart Contract for Food Supply Chain Management in Truffle—Ganache Framework. In Proceedings of the 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 17–18 March 2023; Volume 1, pp. 36–40. [**Google Scholar**] [**CrossRef**]
20. Sharan, R.V.; Abeyratne, U.R.; Swarnkar, V.R.; Porter, P. Automatic Croup Diagnosis Using Cough Sound Recognition. *IEEE Trans. Biomed. Eng.* **2019**, *66*, 485–495. [**Google Scholar**] [**CrossRef**]
21. Jahangir, R.; Teh, Y.W.; Nweke, H.F.; Mujtaba, G.; Al-Garadi, M.A.; Ali, I. Speaker identification through artificial intelligence techniques: A comprehensive review and research challenges. *Expert Syst. Appl.* **2021**, *171*, 114591. [**Google Scholar**] [**CrossRef**]
22. Sardar, V.M.; Shirbahadurkar, S.D. Speaker identification of whispering speech: An investigation on selected timbrel features and KNN distance measures. *Int. J. Speech Technol.* **2021**, *21*, 545–553. [**Google Scholar**] [**CrossRef**]
23. Guglani, J.; Mishra, A. Automatic speech recognition system with pitch dependent features for Punjabi language on KALDI toolkit. *Appl. Acoust.* **2020**, *167*, 107386. [**Google Scholar**] [**CrossRef**]
24. Marques, I.; Sousa, J.; Sá, B.; Costa, D.; Sousa, P.; Pereira, S.; Santos, A.; Lima, C.; Hammerschmidt, N.; Pinto, S.; et al. Microphone Array for Speaker Localization and Identification in Shared Autonomous Vehicles. *Electronics* **2022**, *11*, 766. [**Google Scholar**] [**CrossRef**]
25. Njoku, J.N.; Nwakanma, C.I.; Lee, J.-M.; Kim, D.S. Multi-Feature Concatenation for Speech Dependent Automatic Speaker Identification in Maritime Autonomous Vehicles. In Proceedings of the 2nd International Conference on Maritime IT Convergence (ICMIC 2023), Jeju Island, Republic of Korea, 23–25 August 2023; Volume 2, pp. 103–106.
26. D. Sabella, H. Moustafa, P. Kuure, S. Kekki, Z. Zhou, A. Li, C. Thein, E. Fischer, I. Vukovic, J. Cardillo, et al., "Toward fully connected vehicles: Edge computing for advanced automotive communications," 5G Automot. Assoc. (5GAA), White Paper, vol. 230, 2017.
27. F. Arena and G. Pau, "When edge computing meets iot systems: Analysis of case studies," China Communications, vol. 17, no. 10, pp. 50–63, 2020
28. L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular edge computing and networking: A survey," Mobile Networks and Applications, vol. 26, no. 3, pp. 1145–1168, 2021.
29. K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," IEEE access, vol. 8, pp. 85714–85728, 2020.
30. B. Fritzsche, "Revealing the invisible-information visualization in the internet of things era," the Internet of Things Era, vol. 18, 2015.
31. J. Chang et al., "An overview of usdot connected vehicle roadside unit research activities." https://rosap.ntl.bts.gov/view/dot/34763, 2017. online web resource.

32. R. Morabito, V. Cozzolino, A. Y. Ding, N. Beijar, and J. Ott, “Consolidate iot edge computing with lightweight virtualization,” IEEE network, vol. 32, no. 1, pp. 102–111, 2018.
33. S. Taherizadeh, A. C. Jones, I. Taylor, Z. Zhao, and V. Stankovski, “Monitoring self-adaptive applications within edge computing frameworks: A state-of-the-art review,” Journal of Systems and Software, vol. 136, pp. 19–38, 2018