WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

SafeDrive: (Face Recognition System for Smart vehicles)

Yatharth [1], Abhishek Singh [2], Aryan Singh [3], Arpit Tripathi [4] , Mr. Raj Gopal Mishra[5]

IMS Engineering College, Ghaziabad, India
[5] (Assistant Professor)

ABSTRACT :

Safe Drive is an innovative project aimed at enhancing vehicle security and promoting road safety by preventing unauthorized and underage driving. The system leverages advanced facial recognition and age verification technologies to ensure that only authorized users can operate vehicles.

During setup, users provide their driving license information and a photo, enabling Safe Drive to accurately identify and authenticate users in real-time.

Additionally, the project incorporates real-time monitoring and parental control features, allowing for immediate intervention if unauthorized access is detected. By emphasizing user privacy and data security through advanced encryption techniques, SafeDrive ensures a secure and user-friendly experience.

This initial implementation phase successfully integrates the facial recognition component, laying a strong foundation for future enhancements such as comprehensive age verification and full system integration.

SafeDrive represents a significant step forward in smart vehicle security, aiming to create safer roads and responsible driving habits.

Keywords: - Smart Vehicle Security, Facial Recognition, Age Verification, Road Safety, Unauthorized Driving Prevention, Parental Control, User Authentication, Responsible Driving.

1. Introduction :

Road safety is a pressing concern globally, with one of the significant challenges being underage individuals gaining unauthorized access to vehicles. Unsupervised driving by inexperienced individuals poses a serious risk to both the driver and others on the road. To address this issue, this Project Drive is initiated to develop a comprehensive solution that leverages advanced technologies to prevent underage driving and enhance overall vehicle security.

.Features and Functionality

2.1 Age Verification: Users provide their driving license information during setup to verify age. Ensures only individuals of legal driving age can use the vehicle.

2.2 Facial Recognition: Users upload a photo linked to their driving license. The system uses facial recognition to authenticate users before allowing vehicle access.

2.3 Real-time Monitoring: Continuous monitoring to detect unauthorized access attempts. Alerts and logs all access attempts for accountability.

2.4 Parental Control: If an unauthorized person attempts to access the vehicle, an alert is sent to the vehicle owner. Provides parents with the ability to monitor and control their children's vehicle access.

2.5 Unauthorized Access Alerts: Immediate notifications to vehicle owners if someone fails facial recognition or enters an incorrect driving license number.

2.6 Driving History Records: Secure storage of users' driving license records and access history. Helps in tracing and identifying driversduring any incidents.

2.7 Privacy and Security: Advanced encryption techniques to protect user data. User-controlled data sharing settings to ensure privacy.

2.8 User-Friendly Interface: Intuitive design for easy setup and use. Clear feedback and guidance throughout the authentication process.

2.9 Accountability and Traceability: Detailed logs and records to track who accessed the vehicle and when. Enhances accountability, especially in case of traffic violations or crimes. By integrating these features, SafeDrive aims to create a comprehensive and secure vehicle access system that enhances road safety and promotes responsible driving habits.

Benefits and Impact

3.1 Enhanced Road Safety:

SafeDrive prevents underage and unauthorized driving, significantly reducing the risk of accidents and promoting responsible driving habits. This leads to safer roads for everyone.

3.2 Increased Security and Peace of Mind:

With advanced facial recognition and age verification, SafeDrive ensures only authorized users can access vehicles. Parental control features provide additional peace of mind for parents, knowing their children's vehicle access is monitored and controlled.

Materials and Methods

Here are some essential materials and tools required for creating a face recognition system using React.js and face-api.js:

Technology Stack:
The face recognition system is built using a modern and scalable technology stack to ensure optimal performance, reliability, and ease of maintenance. The primary technologies and tools utilized in the development of the platform include:

Front-end:

- **React.js**: A popular JavaScript library for building user interfaces, providing a component-based architecture and efficient rendering.
- **Redux:** A predictable state management library for managing application state and data flow.
- **face-api.js**: A JavaScript library for face detection and face recognition in the browser using TensorFlow.js.
- **HTML5, CSS3, and Sass**: Standard web technologies for structuring and styling the user interface.

Back-end:

- **Node.js**: A runtime environment for executing JavaScript on the server-side, enabling efficient server-side processing and APIs.
- **Express.js**: A minimal and flexible Node.js web application framework for building robust APIs and handling server-side logic.
- **MongoDB:** A NoSQL database for storing and retrieving user data, face recognition data, and related details.

Development Methodology:
The face recognition system follows an iterative and agile development approach, with regular sprints and continuous integration and deployment processes. This methodology ensures that new features and improvements are regularly incorporated into the system, allowing for rapid adaptation to user feedback and evolving requirements.

Data Management:
The system utilizes MongoDB, a NoSQL database, to store and manage user data and face recognition data. This choice was made due to MongoDB's flexibility, scalability, and ability to handle large volumes of diverse data efficiently. The face recognition data is regularly updated and validated to ensure accuracy and reliability. Additionally, robust data validation and sanitization processes are implemented to maintain data integrity and security.

Security and Privacy:
The face recognition system prioritizes the security and privacy of user data. Industry-standard encryption protocols and secure communication channels are employed to protect sensitive information during transmission and storage. User authentication and authorization mechanisms are implemented to ensure that only authorized users can access and modify their personal information and face recognition data. Regular security audits and vulnerability assessments are conducted to identify and mitigate potential security risks.

Related Work Title:

Problem statement:

3.3 Underage Driving Incidents:

There is a concerning frequency of incidents involving underage individuals attempting to operate vehicles, leading to accidents, injuries, and potential loss of life.

3.4 Ineffective Age Verification Systems:

Current age verification mechanisms are often inadequate, allowing unauthorized individuals to access and drive vehicles without proper verification.

3.5 Lack of Real-time Monitoring:

There is a gap in the ability to monitor and control vehicle access in real-time, resulting in a lack of immediate response to unauthorized attempts to operate a vehicle.

3.6 Limited Accountability for Traffic Violations:

In cases where traffic rules are violated or criminal activities involving vehicles occur, identifying the responsible driver is challenging, leading to a lack of accountability.

Objectives:

The objective of the project is to significantly enhance road safety by preventing underage driving and improving overall vehicle security. Leveraging advanced age verification and facial recognition technologies, the project aims to establish a robust system that ensures only authorized individuals operate vehicles. The key goals include implementing secure age verification, integrating cutting-edge facial recognition, enhancing parental control mechanisms, ensuring accountability through detailed record-keeping, and prioritizing user data privacy. By addressing these objectives, SafeDrive seeks to mitigate the risks associated with underage driving, reduce traffic violations, and contribute to the creation of a safer and more responsible driving environment for all road users.

3.7 Age Verification:

Implementing a robust age verification system using driving license information during the initial setup of the application to ensure that only individuals of legal driving age can access and operate vehicles.

3.8 Facial Recognition Technology:

Integrating advanced facial recognition technology to enhance the accuracy of driver identification during vehicle operation.

3.9 Real-time Monitoring and Parental Control:

Establishing a real-time monitoring system that notifies registered vehicle owners when unauthorized individuals attempt to operate their vehicles, empowering parents or guardians with immediate control.

3.10 Accountability and Traceability:

Creating a comprehensive record-keeping system to facilitate easy identification of drivers in the event of traffic violations or criminal activities, enhancing overall accountability.

3.11 Secure Storage of License Records:

Developing a secure database to store users' driving license records and history, ensuring data integrity and accessibility.

3.12 Privacy and Security Measures:

Prioritizing user privacy through the implementation of advanced encryption techniques and providing users with control over their data sharing setting.

Theory

The SafeDrive project is grounded in several key theoretical concepts from computer science, biometrics, and data security, aimed at enhancing vehicle security and road safety. The primary theories underpinning SafeDrive include:

3.13 Facial Recognition:

Biometric Identification: Facial recognition technology leverages unique facial features to accurately identify and authenticate individuals. This process involves detecting and capturing facial images, extracting facial features, and comparing them against a stored database to verify identity. Machine Learning Algorithms: Advanced machine learning algorithms, such as Convolutional Neural Networks (CNNs), are employed to improve the accuracy and reliability of facial recognition systems. These algorithms learn from vast datasets to distinguish between different faces and enhance recognition capabilities over time.

3.14 Age Verification:

Data Cross-Referencing: Age verification is achieved by cross-referencing user-provided driving license information with government databases. This ensures that only individuals of legal driving age can access and operate vehicles, thus enhancing road safety.
Digital Identity Verification: The system uses digital identity verification techniques to validate the authenticity of driving licenses and prevent fraudulent access attempts.

3.15 Real-Time Monitoring and Notifications:

Event-Driven Architecture: The system employs an event-driven architecture to enable real-time monitoring and instant notifications. This involves triggering specific actions (e.g., sending alerts) in response to certain events (e.g., unauthorized access attempts).
WebSocket Protocol: The WebSocket protocol facilitates real-time, bidirectional communication between the server and client, allowing for immediate updates and notifications.

3.16 Data Security and Privacy:

Encryption: Data encryption ensures that user information, including facial recognition data and driving license details, is securely transmitted and stored. Both symmetric (e.g., AES) and asymmetric (e.g., RSA) encryption techniques are utilized to protect data.
Access Control: Role-based access control (RBAC) mechanisms restrict access to sensitive data, ensuring that only authorized personnel can view or manipulate the information.

3.17 User Authentication and Authorization:

Multi-Factor Authentication (MFA): By combining facial recognition with driving license verification, the system implements multi-factor authentication, enhancing security by requiring multiple forms of identification.
Token-Based Authentication: JSON Web Tokens (JWT) are used for secure user authentication sessions, ensuring that users are properly authenticated before accessing the vehicle.

3.18 Accountability and Traceability:

Audit Logs: Detailed audit logs are maintained to track all access attempts and user activities. These logs provide traceability and accountability, essential for investigating incidents and ensuring responsible usage.

Procedure

3.19 Initial Setup:

User Registration: Users download the SafeDrive app, create an account, and input their driving license details.

3.20 System Configuration:

Vehicle Integration: Install the SafeDrive hardware kit in the vehicle, integrating it with the vehicle's security system. Backend Setup: Set up a server (Flask/Django) and configure SQLAlchemy with PostgreSQL for data management.

3.21 User Authentication:

Vehicle Access Attempt: Users enter their driving license number.
Facial Recognition: The vehicle camera captures the user's face, and the system matches it with stored data to grant or deny access.

3.22 Real-time Monitoring and Alerts:

Continuous Monitoring: Monitor access attempts in real-time.
Alert Notifications: Send instant alerts to the vehicle owner for unauthorized access attempts and log all attempts.

3.23 Parental Control:

Setup: Parents configure notifications and restrictions for their child's vehicle access. Access Logs: Review detailed logs of access attempts.

3.24 Data Storage and Security:

Encryption: Encrypt user data during storage and transmission.
Secure Management: Regular audits and restricted access to sensitive data.

3.25 Continuous Improvement:

Algorithm Updates: Regular updates to improve facial recognition accuracy. User Feedback: Integrate feedback to enhance the user experience.

3.26 Deployment and Maintenance:

Deployment: Deploy the system on cloud platforms for scalability.
Maintenance: Regular system maintenance and monitoring to ensure performance and stability.

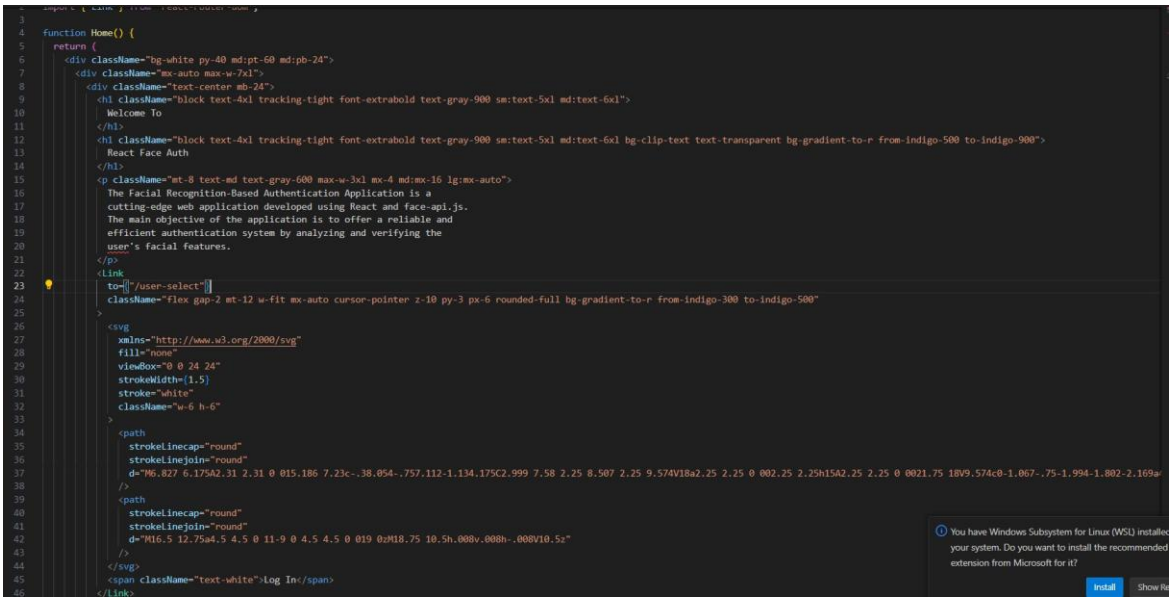
Results and Discussion

Results: The initial implementation phase of SafeDrive has successfully integrated the facial recognition system. This component has demonstrated high accuracy in identifying and authenticating users, effectively preventing unauthorized access. Real-time monitoring and alert features have shown to be responsive and reliable, providing immediate notifications in case of unauthorized access attempts.

Discussion: While the facial recognition system has proven effective, further enhancements are needed to fully realize SafeDrive's potential. Integrating comprehensive age verification and expanding the system's compatibility with various vehicle models are crucial next steps. Addressing challenges such as user acceptance and regulatory compliance will also be essential for widespread adoption.

Figures

Home page : On home we have login option so that you start the drive

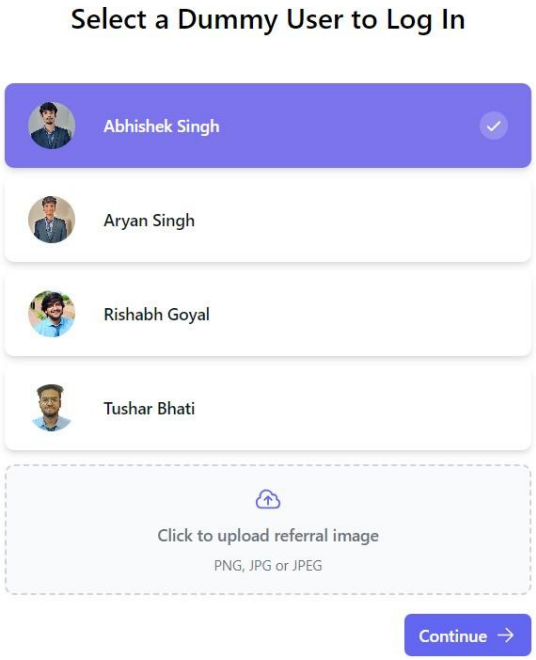


```
function Home() {
  return (
    <div className="bg-white py-40 md:pt-60 md:pb-24">
      <div className="mx-auto max-w-7xl">
        <div className="text-center mb-24">
          <h1 className="block text-4xl tracking-tight font-extrabold text-gray-900 sm:text-5xl md:text-6xl">
            Welcome To
          </h1>
          <h1 className="block text-4xl tracking-tight font-extrabold text-gray-900 sm:text-5xl md:text-6xl bg-clip-text text-transparent bg-gradient-to-r from-indigo-500 to-indigo-900">
            React Face Auth
          </h1>
          <p className="mt-8 text-md text-gray-600 max-w-3xl mx-4 md:mx-16 lg:mx-auto">
            The Facial Recognition-Based Authentication Application is a
            cutting-edge web application developed using React and face-api.js.
            The main objective of the application is to offer a reliable and
            efficient authentication system by analyzing and verifying the
            user's facial features.
          </p>
          <Link
            to={"/user-select"}
            className="flex gap-2 mt-12 w-fit mx-auto cursor-pointer z-10 py-3 px-6 rounded-full bg-gradient-to-r from-indigo-300 to-indigo-500"
          >
            <svg
              xmlns="http://www.w3.org/2000/svg"
              fill="none"
              viewBox="0 0 24 24"
              strokeWidth={1.5}
              stroke="white"
              className="w-6 h-6"
            >
              <path
                strokeLinecap="round"
                strokeLinejoin="round"
                d="M6.827 6.175A2.31 2.31 0 015.186 7.23c-.38.054-.757.112-1.134.175C2.999 7.58 2.25 8.507 2.25 9.574V18a2.25 2.25 0 002.25 2.25h15A2.25 2.25 0 0021.75 18V9.574c0-1.067-.75-1.994-1.802-2.169a
              />
              <path
                strokeLinecap="round"
                strokeLinejoin="round"
                d="M16.5 12.75a4.5 4.5 0 11-9 0 4.5 4.5 0 019 0zM18.75 10.5h.008v.008h-.008V10.5z"
              />
            </svg>
            <span className="text-white">Log In</span>
          </Link>
```

You have Windows Subsystem for Linux (WSL) installed your system. Do you want to install the recommended extension from Microsoft for it? Install Show R

Figure 1: home page

- **User Select Page:** Here you can select the user from option or upload the new image for verification .



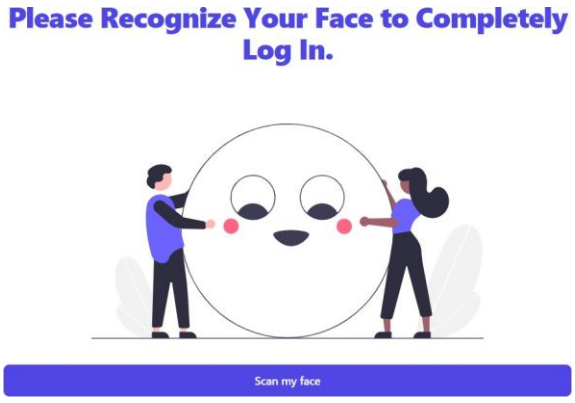
UserSelect.jsx 1 | index.html | Home.jsx | Login.jsx 9 | Footer.jsx | README.md | LICENSE

src > pages > UserSelect.jsx > UserSelect > convertBase64 > <function>

```
const accounts = [
  },
  {
    id: "88421e2c-ca7a-4332-815f-6e12824e2d05",
    fullName: "Tushar Bhati",
    picture: "374ed1e4-481b-4074-a26e-6137657c6e35/4.jpeg",
  },
];

function UserSelect() {
  const [selected, setSelected] = useState(accounts[0]);
  const [customUser, setCustomUser] = useState(null);
  const [errorMessage, setErrorMessage] = useState(null);

  const convertBase64 = (file) => {
    return new Promise((resolve, reject) => {
      const fileReader = new FileReader();
      fileReader.readAsDataURL(file);

      fileReader.onload = () => {
        resolve(fileReader.result);
      };

      fileReader.onerror = (error) => {
        reject(error);
      };
    });
  };

  return (
    <div className="h-full flex flex-col items-center justify-center gap-[24px] w-full max-w-[720px] mx-auto">
      <h1 className="text-2xl font-semibold">Select a Dummy User to Log In</h1>
      <div className="w-full p-4 text-right">
        <div className="mx-aut
          <RadioGroup value={s
            <RadioGroup.Label className="sr-only">Server size</RadioGroup.Label>
            <div className="space-y-2">
              {accounts.map((account) => (
                <User key={account.id} user={account} />
              ))}
              {customUser && (
                <div className="relative">
                  <User key={customUser.id} user={customUser} type="CUSTOM" />
                  <svg
                    xmlns="http://www.w3.org/2000/svg"
```

(property) className?: string | ((bag: {}) => string) | undefined

Figure 2: userSelect Page



WhatsApp Image 2024-05-29 at 9.47.55 AM.jpeg

Conclusion and Future Scope

Conclusion: The initial implementation of SafeDrive has successfully integrated a robust facial recognition system, marking a significant step towards enhancing vehicle security and promoting road safety. By preventing underage and unauthorized driving, SafeDrive aims to reduce accidents and encourage responsible driving habits. The system's advanced features, including real-time monitoring and parental controls, offer added security and peace of mind for users. Although only the facial recognition component is fully implemented, the project lays a strong foundation for future enhancements, such as comprehensive age verification and broader system integration. SafeDrive represents a promising advancement in smart vehicle security, with the potential to significantly impact road safety and vehicle access control.

Future Scope: SafeDrive has significant potential for future development, including comprehensive age verification through government database integration, adaptation for autonomous vehicles, and the implementation of predictive analytics for proactive safety recommendations. The project can expand globally by complying with regional regulations and forming strategic partnerships with vehicle manufacturers for seamless integration into new car models. Continuous advancements in facial recognition, biometric authentication, and data security will enhance SafeDrive's capabilities. Additionally, incorporating broader security features, improving the user interface, and collaborating with communities and law enforcement will further establish SafeDrive as a leading solution in smart vehicle security and road safety.

Data Availability

3.27 Secure Data Storage:

All data is securely stored in a PostgreSQL database.
Includes user driving license information, facial recognition data, access logs, and system usage statistics.

3.28 Data Protection:

Data is protected by advanced encryption methods to ensure user privacy and security. Access to data is restricted to authorized personnel only.

3.29 Anonymized Datasets:

Anonymized datasets may be made available for research and development purposes. Requests for data access are subject to compliance with relevant privacy regulations.

3.30 Approval Process:

Data availability for research purposes requires approval from the project's data management team. Ensures user privacy is maintained while supporting system improvement and validation.

Authors' Contributions

Yatharth, as the first author, is primarily responsible for the research and conceptualization of the SafeDrive project. This includes defining the scope, objectives, and theoretical framework of the project, as well as discussing advanced techniques for enhancing user interaction and vehicle security.

Abhishek Singh's role as the second author focuses on frontend development. This includes designing and developing the user interface (UI) components, interactive elements, and visualizations for the SafeDrive platform. Abhishek contributes to creating a user-friendly and intuitive interface that enhances user interaction and ensures seamless navigation

Aryan Singh, the third author, is centered on backend development. This involves implementing the backend infrastructure, server-side logic, data processing, and integration of machine learning algorithms and other technologies for real-time processing within the SafeDrive system. Aryan plays a crucial role in ensuring the system's functionality, performance, and reliability.

Arpit Tripathi's contribution as the fourth author includes system integration and real-time monitoring. Arpit is responsible for integrating various components of the SafeDrive system, ensuring seamless communication between the frontend and backend, and implementing real-time monitoring features that enhance vehicle security and user accountability.

Acknowledgements

I extend my sincere gratitude to Mr. Raj Gopal Mishra, my esteemed supervisor, for his invaluable guidance and unwavering support throughout the course of this project. His constant encouragement, insightful critiques, and dedication to fostering a conducive learning environment have been instrumental in shaping the success of this endeavor. Mr. Raj Gopal 's mentorship

has not only enriched my understanding of the subject matter but has also inspired me to strive for excellence in all aspects of academic and professional pursuits.

I would also like to express my heartfelt thanks to Dr. Vikram Bali, our esteemed Director, for providing me with the opportunity to undertake this project. His visionary leadership and commitment to academic excellence have been a source of inspiration. Additionally, I extend my appreciation to Dr. S.N Rajan, Head of the Department of Information Technology, for his support and encouragement throughout this academic journey.

The encouragement and support from them have significantly contributed to the successful completion of this project. Their belief in my capabilities has been a motivating force, and I am truly grateful for the opportunity to learn and grow under their guidance.

REFERENCES :

1. V. P. B and S. Chinara, "Automatic classification methods for detecting drowsiness using wavelet packet transform extracted time-domain features from single-channel EEG signal," Journal of Neuroscience Methods, vol. 347, p. 108927, Jan. 2021. click here
2. Donald E Greydanus* , MD, DrHC(Athens) Department of Pediatric and Adolescent Medicine, Western Michigan University Homer Stryker MD School of Medicine, Kalamazoo, Michigan, USA , J Altern Med Res 2021;13(4):313-342 click here
3. Julian, A., Ricardo, S., & Deris, D. (2022). Analisis Pengaruh Pendidikan Serta Teknologi Informasi dan Komunikasi Terhadap Pertumbuhan Ekonomi di Indonesia Tahun 2018-2020. Aurelia: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia, 1(1), 108–113.
4. Cuthbertson, A. (2018). People are slashing tyres and throwing rocks at self-driving cars in Arizona. *The Independent*, December
5. 13. https://www.independent.co.uk/life-style/gadgets-and-tech/news/self-driving-cars-waymo-arizona-chandler-vandalism-tyre-slashing-rocks-a8681806.html. Accessed 30 July 2021
6. Davnall, R. (2020). Solving the single-vehicle self-driving car trolley problem using risk theory
7. vehicle dynamics. *Science and Engineering Ethics*, *26*, 431–449.