International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 11 ǁ November 2023 ǁ PP. 06-13

Emerging Security Solutions in Transportation Systems

Preetha S, Mahalakshmi B S, Nalini M K,
Pavan Deshpande, Vasudev Chandra, Pranav S Tippimath
*[*1,2,3,4.]Department of Information Science & Engineering, B.M.S. College of Engineering, VTU, India*
E-mail: preetha.ise@bmsce.ac.in

Abstract
The future of detecting threats and preventing attacks in transportation holds great potential with advancements in technology and the expertise of trained personnel. Surveillance systems will be enhanced through the integration of intelligent video analytics, facial recognition and sensors enabling real-time detection of suspicious activities. Artificial intelligence and machine learning algorithms will play a crucial role in analyzing vast amounts of data, identifying patterns and proactively identifying threats. Physical security measures will leverage innovations in access control systems such as biometric authentication and smart locks while the integration of Internet of Things (IoT) devices will enable real-time monitoring of critical infrastructure. Trained security personnel will continue to be essential in detecting threats that automated systems may oversight and effective training programs, information sharing networks will ensure their expertise remains conversant. Collaboration among government agencies, transportation authorities, technology providers and security experts will be key in developing comprehensive security frameworks that address evolving threats. This paper explores emerging security solutions in transportation, addressing challenges posed by technological advancements. Investigation of IoT, 5G technologies, autonomous vehicles, critical infrastructures, identifying vulnerabilities and proposing remedies are done. Study emphasizes advanced technologies like deep learning and intrusion detection systems to sustain security measures. It also highlights the importance of response and recovery strategies within critical infrastructures. Overall, this research aims to enhance transportation security and contribute to secure and resilient infrastructures.

Keywords: *Transportation Systems, Security, Gaussian, Canny, Video frames, Lane Detection*

Date of Submission: 20-10-2023 Date of acceptance: 03-11-2023

I. INTRODUCTION

Transportation systems are vital for the efficient movement of people, goods, and services. However, increasing complexity and interconnectedness of these systems have given rise to new security challenges. Emerging technologies such as intelligent transportation systems (ITS) connected and autonomous vehicles (CAVs) and unmanned aerial vehicles (UAVs) have transformed the transportation landscape but have also introduced vulnerabilities that need to be addressed. The need for innovative security solutions in transportation has become imperative. These solutions aim to protect critical infrastructure, enhance passenger safety, and ensure integrity of transportation networks. Cybersecurity is a key aspect with a focus on securing communication protocols, preventing cyber-attacks, and safeguarding data privacy. Physical security measures play a crucial role in protecting transportation infrastructure against threats such as terrorism, vandalism, and sabotage. Access control systems, surveillance technologies and perimeter protection measures are employed to mitigate risks. Risk assessment and management are fundamental to developing effective security strategies. By identifying vulnerabilities conducting threat modeling and implementing risk mitigation measures, transportation systems can be made more resilient to potential security incidents. Intelligent transportation systems leverage technology to optimize traffic flow, improve safety and enhance efficiency. However, they also present security challenges such as secure communication between vehicles and infrastructure, data privacy concerns, and system resilience. Connected and autonomous vehicles bring numerous benefits but also require robust security measures. Securing vehicle communication, detecting and preventing intrusions, ensuring secure over-the-air updates and implementing strong authentication mechanisms are critical for protecting CAVs against cyber threats.

In the event of security incidents or disruptions, effective emergency response and recovery strategies are essential. Incident management frameworks, contingency planning, crisis communication and post-incident analysis help mitigate the impact and facilitate quick recovery. Regulatory and policy considerations play a vital role in shaping transportation security. International standards, privacy regulations, collaboration between stakeholders and the development of supportive legal frameworks are necessary for the successful implementation

of security solution. Study explores the emerging security solutions in transportation covering various aspects such as cybersecurity, physical security, risk assessment, ITS, CAVs, emergency response and regulatory considerations. By understanding the challenges and opportunities in transportation security, stakeholders can work towards building resilient and secure transportation systems for the future.

II. RELATED WORKS

A comprehensive survey of reports have helped in gaining few insights which have provided a valuable understanding and meaningful implication for further analysis. Through extensive analysis and careful considerations, conclusions and sub-divisions are as mentioned below.

2.1 Basic definition and working

Frustaci, Mario [1] discussed the need to address standardized security protocols, device diversity, and infrastructure vulnerabilities within the IoT ecosystem. Study emphasized the importance of securing IoT systems to ensure the privacy, integrity, and trustworthiness of IoT devices, networks, and data. In [2] Kumar, Sathish Alampalayam and Tyler Vealey provided a basic definition of the IoT as a network of interconnected devices that communicates and exchanged data. Security threats and vulnerabilities that arise in IoT environments, such as unauthorized access, data breaches, and compromised device integrity were observed. A proposal for potential solutions, including cryptographic techniques and secure communication protocols, to mitigate these security risks and ensure the protection of IoT systems and their data was done. The need for a comprehensive and proactive approach to IoT security to address emerging challenges and secure the IoT ecosystem effectively was emphasized.

Parkinson, Simon [3] focuses on the cyber threats faced by autonomous and connected vehicles and discuss the future challenges associated with them. A comprehensive understanding of the subject matter by defining autonomous and connected vehicles as vehicles equipped with advanced technologies that enable self-driving capabilities and seamless connectivity with external systems was provided. Study examined the potential cyber threats encountered by vehicles, including unauthorized access, manipulation of control systems, and privacy breaches. It highlighted the need for robust security measures to safeguard the integrity and safety of autonomous and connected vehicles, emphasizing the importance of secure communication protocols, intrusion detection systems, and encryption techniques. Future challenges were addressed that arise as the technology evolves and stress the significance of ongoing research and advancements in cybersecurity to ensure the protection and reliability of autonomous and connected vehicles in the face of emerging cyber threats.

Aslan, O¨ mer[4] and Khan, Rabia[5] provides a comprehend review of cyber security vulnerabilities, threats, attacks and solutions across various domains. It defined cyber security as the protection of systems, networks and data from unauthorized access, damage or disruption. It explored landscape of cyber security including different types of vulnerabilities and potential threats that organizations face. Study discussed various attack vectors such as malware, social engineering, insider threats, and highlighted the importance of implementing effective security measures to mitigate risks. Also presented a survey on the security and privacy of 5G technologies. Study defined 5G as the fifth generation of wireless communication technology, enabling faster data transmission and low-latency connections. Potential security and privacy challenges associated with 5G net- works and presents potential solutions, recent advancements, and future directions to address these concerns were also discussed. Need for robust security measures, encryption protocols, and user authentication mechanisms to ensure the integrity and confidentiality of data transmitted over 5G networks was emphasized. Overall, both papers contribute to understanding the complexities of cyber security and the specific challenges related to 5G technologies, providing insights into potential vulnerabilities, threats, and solutions.

2.2 Security Challenges in Emerging Technologies

Gonza´lez-Granadillo [6] and Elliott et. al [7] explored the unique security challenges posed by the adoption of 5G networks. It discusses potential threats such as network slicing vulnerabilities, privacy concerns with increased data collection and challenges related to securing IoT devices within 5G networks. Potential solutions and recent advancements in 5G security, including authentication mechanisms, encryption protocols, and network segmentation was presented. They also focuses on the analysis, trends and usage of SIEM systems in critical infrastructures. Security challenges faced by organizations in managing and monitoring security events within complex infrastructures was highlighted. Discussion related to the need for advanced threat detection, response capabilities, integration of diverse security data sources and efficient analysis of security events to ensure timely incident response and mitigation was done.

Sakiz, Fatih, and Sevil Sen [8] focused on Vehicular Ad Hoc Networks (VANETs) and Internet of Vehicles (IoV). Study discussed the vulnerabilities of these systems to various attacks, including message falsification, node misbehavior, and location privacy breaches. Critical need for robust security mechanisms to

protect the integrity, confidentiality, and availability of communications within VANETs and IoV was highlighted. Exploration of different attack detection mechanisms such as trust-based approaches, anomaly detection and digital signature verification was done. Additionally, research addressed the challenges of real-time detection in highly dynamic vehicular environments and the trade-offs between security and system performance. By presenting an in-depth analysis of attacks and detection mechanisms, this paper contributes to the advancement of secure ITS, paving the way for the development of ef fective countermeasures and ensuring the reliability and trust worthiness of future intelligent transportation systems.

Chowdhury, Mashrur, Mhafuzul Islam [9] discusses several security challenges associated with this emerging technology. They highlight the risks related to unauthorized access and control, emphasizing the need for robust authentication and authorization mechanisms to prevent malicious actors from manipulating or disrupting vehicle operations. The authors also address the potential vulnerabilities arising from the connectivity of vehicles to external networks, including the risk of cyber-attacks targeting the vehicle's communication systems and infrastructure. Additionally, challenges of ensuring the privacy of personal and sensitive data collected by connected vehicles and the need for effective data protection measures were also discussed. Lee, Nikolaev, and Jacobson [10] focused on security challenges in air transportation. Various security threats such as hijacking, sabotage and in- sider attacks was explored. Importance of implementing effective screening procedures, surveillance systems, and access control measures to safeguard airports and aircraft was mentioned. Need for collaboration among stakeholders including airlines, airport authorities and security agencies to develop comprehensive security strategies and enhance the resilience of air transportation systems was highlighted. Overall, both studies shed light on the critical security challenges faced by connected and automated vehicles as well as the aviation industry providing insights into the measures required to mitigate these risks and ensured safety and security of these domains.

2.3 Incident Response and Recovery in Critical Infrastructures

Study in [11-12] emphasizes the need for effective intrusion detection mechanisms to detect and respond to potential security breaches in IoT systems. It highlights the importance of timely incident response including alert generation, incident analysis and appropriate actions to mitigate the impact of intrusions. Similarly, focused on the security of intelligent connected vehicles and emphasized the significance of response strategies to address attacks effectively. It discussed various techniques such as anomaly detection, behavior analysis and encryption mechanisms that aid in detecting and responding to attacks in connected vehicle environments. Additionally emphasized the importance of recovery mechanisms such as system restoration, data backup and resilience planning to restore critical infrastructure functionality after an incident. By implementing robust response and recovery practices, critical infrastructures can enhance their ability to mitigate cyber threats, minimize downtime, and ensure continuity of essential services.

Gupta, Anunay discusses the advancements and potential of Unmanned Aerial Vehicles (UAVs) in future transportation systems was done in [13]. While the primary focus was on the benefits and challenges of UAV integration, it indirectly highlights the importance of response and recovery in critical infrastructures. As UAVs become increasingly prominent in transportation, it is crucial to address the potential risks and vulnerabilities associated with their use. In the context of response and recovery in critical infrastructures, it is necessary to establish robust incident management strategies including real-time monitoring, early detection of anomalies or security breaches and swift response mechanisms. Furthermore development of resilient infrastructure, backup systems and redundancy measures can help mitigate the impact of disruptions and facilitate efficient recovery. By incorporating effective response and recovery plans, stakeholders can enhance the overall security and resilience of critical infrastructure systems, ensuring their ability to adapt and recover from adverse events or attacks.

Factors that contribute to downgrade truck crashes using a logistic regression approach was explored by Moomen, Milhan and Mahdi Rezapour [14]. While the primary focus of the study is on identifying influential factors, it indirectly emphasized the significance of response and recovery in critical infrastructures, particularly in the context of transportation systems. When a downgrade truck crash occurs, it can lead to severe disruptions in transportation networks, impacting both the safety of individuals and the functioning of critical infrastructures. Effective response and recovery strategies are crucial to minimize the consequences of such incidents. This involves timely emergency response, traffic management and restoration of affected infrastructure. Furthermore, implementation of proactive measures such as regular maintenance, monitoring systems, and contingency plans can help prevent downgrade truck crashes and ensure a swift recovery in case of an event. By focusing on response and recovery in critical infrastructures, stakeholders can work towards enhancing the safety and resilience of transportation systems, ultimately reducing the impact of downgrade truck crashes and ensuring the efficient functioning of vital infrastructure components.

Lo´pez-Aguilar and Pablo [15] conducts a comprehensive analysis of information security and privacy issues in railway transportation. While the primary focus of the study was on identifying and evaluating security

and privacy challenges, it indirectly highlights the importance of response and recovery in critical infrastructures, specifically within the context of railway transportation systems. When security incidents or privacy breaches occur in railway systems, it can disrupt operations, compromise passenger safety and potentially lead to financial and reputational damages. Therefore, an effective response and recovery framework is crucial to mitigate the impacts of such incidents. This includes timely detection and response to security breaches, incident management, restoration of services and the implementation of preventive measures to minimize future risks. Also, collaboration among various stakeholders such as railway operators, government authorities, and cybersecurity experts is essential to ensure a coordinated and efficient response to security and privacy incidents. By emphasizing the importance of response and recovery in critical infrastructures, study underscores the need for robust security measures, proactive monitoring systems and well-defined incident response protocols to safeguard railway transportation systems, protect passenger information and maintain the resilience and reliability of railway infrastructure.

III. PROPOSED LANE DETECTION SYSTEM

A system for detecting threats and preventing attacks in transportation envisions a future where advanced technologies and human expertise are seamlessly integrated is proposed. It involves implementation of intelligent surveillance systems with advanced video analytics for real-time threat detection. Artificial intelligence and Machine learning algorithms play a vital role in analyzing data and identifying patterns to proactively identify potential threats. Trained security personnel work in tandem with technology, leveraging their expertise to detect intricate threats that automated systems may not detect. Collaboration among stakeholders will be crucial, fostering the development of comprehensive security frameworks that address evolving threats and ensure the safety and security of transportation systems.

3.1 Lane Detection System Architecture

System architecture is shown in figure 1. Prediction phase identifies the left and right borders of lane depending on far and near range. Vertical profile detection detects the near and far ranges. Lane marking point extracts the left and right ends of the lane. Initially it makes the prediction for both left and right lane borders. When it detects the near linear line it updates and it shifts to far range linear detection for further updating process. Later it detects left and right boundaries and updates its result.

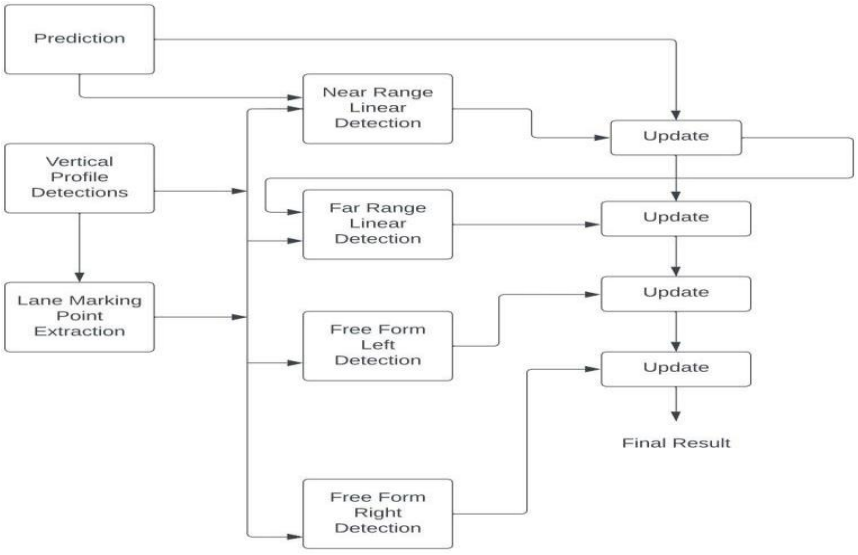

Figure 1: System Architecture for Lane detection

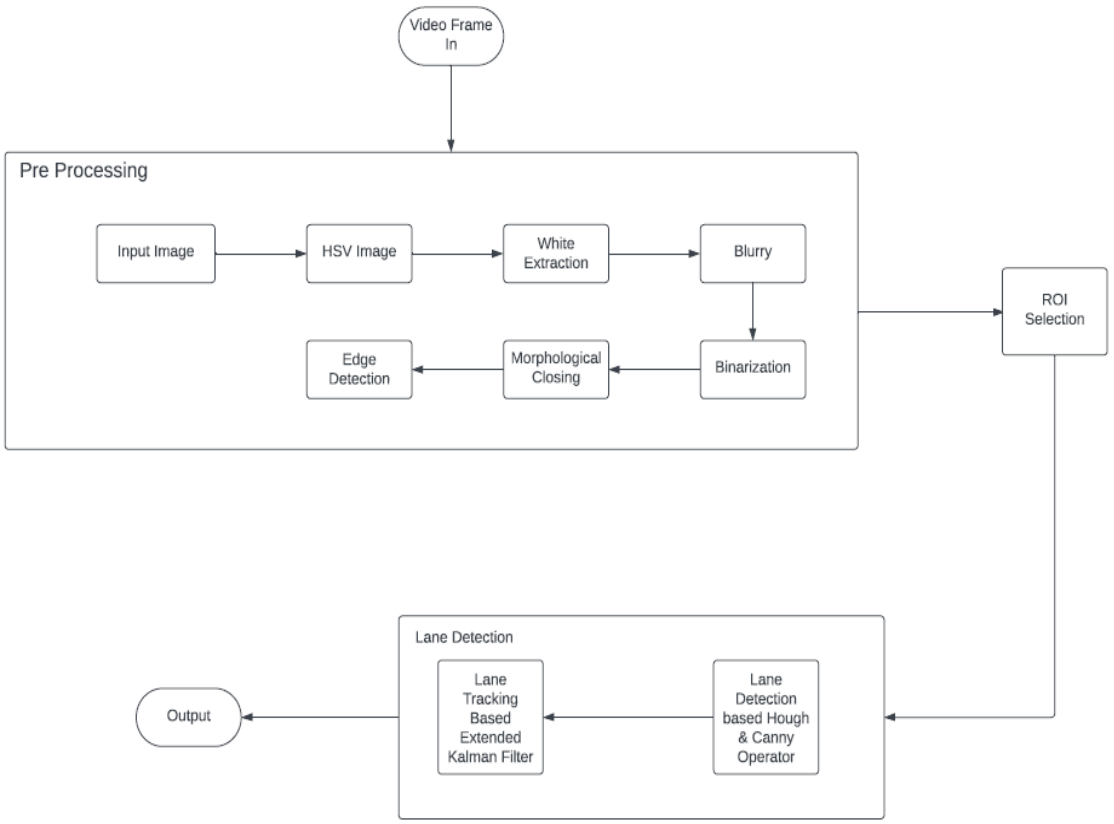

Figure 2: Flowchart for Video frames

Figure 2 shows the flowchart of video frames. In the preprocessing pipeline for video frame analysis, the input image is first converted to the Hue saturation value (HSV) color space. Subsequently, a series of image processing steps including white object extraction, blurring, binarization, morphological closing, and edge detection are applied to enhance the visual information for further analysis. If suitable region of interest is selected appropriately then further lane detection process is done based on Hough & Canny operator and Kalman filter to obtain final result.

3.2 Algorithm

3.2.1 Functionalities

canny(image): Converts the input image to grayscale, applies Gaussian blur, and performs Canny edge detection.
display_lines(image, lines): Draws detected lines on a black image and returns it.
region_of_interest(image): Masks a region of interest in the input image defined by a polygon, returning the masked image.
Open a video file using OpenCV's VideoCapture and set up a loop to process each frame.
Within the loop:

-> Read a frame from the video.
-> Apply the canny function to detect edges.
-> Define a region of interest using the region_of_interest function.
-> Use the Hough Line Transform (cv2.HoughLinesP) to detect line segments in the region of interest.
-> Average and extrapolate the detected line segments using the average_slope_intercept function
-> Draw the detected lines on a black image using the display_lines function.

Combine the original frame with the line image to visualize the detected lines.
Display the result, and continue processing frames until the 'q' key is pressed.
Release the video capture and close all OpenCV windows when the loop is exited.
An average_slope_intercept function is executed for averaging and extrapolating the detected line segments.

3.2.2 Implemented Code snippets

```
def canny(image):
gray = cv2.cvtColor(image, cv2.COLOR_RGB2GRAY)
blur   = cv2.GaussianBlur(gray, (5, 5), 0)
canny = cv2.Canny(blur, 50, 150)       return canny
def display_lines(image, lines): line_image = np.zeros_like(image) if lines is not None:
for x1,y1,x2,y2 in lines:
cv2.line(line_image, (x1, y1), (x2, y2), (255, 0, 0), 10)
return line_image
def region_of_interest(image): height = image.shape[0] polygons = np.array([
[(200, height), (1100, height), (550, 250)]])
Mask = np.zeros_like(image) cv2.fillPoly(mask, polygons, 255)
masked_image = cv2.bitwise_and(image, mask) return masked_image

cap = cv2.VideoCapture("test2.mp4") while(cap.isOpened()):
_, frame = cap.read() canny_image = canny(frame)
cropped_image = region_of_interest(canny_image)
lines = cv2.HoughLinesP(cropped_image, 2, np.pi/180, 100, np.array([]), minLineLength=40, maxLineGap=5)
averaged_lines = average_slope_intercept(frame, lines) line_image = display_lines(frame, averaged_lines)
combo_image = cv2.addWeighted(frame, 0.8, line_image, 1, 1) cv2.imshow("result", combo_image)
if cv2.waitKey(1) & 0xFF == ord('q'): break
   cap.release() cv2.destrouAllWindows()
```

IV. METHODOLOGY

Building a Model: Building a Deep Learning Model for Lane Detection in Transportation

Data Collection: Collect a large dataset of annotated images or videos specifically focused on lane detection in transportation. This dataset should include diverse scenarios, lighting conditions, weather conditions and road types.

Data Preprocessing: Preprocess the collected dataset by resizing, normalizing and augmenting the images to improve model's performance and generalization.

Model Selection: Choose a suitable deep learning architecture for lane detection such as Convolutional Neural Networks (CNNs) or Fully Convolutional Networks (FCNs). Popular architectures for lane detection include U-Net, SegNet and ENet.

Model Training: Split the dataset into training and validation sets. Use the training set to train deep learning model by optimizing its weights and biases. Use techniques like stochastic gradient descent (SGD) and backpropagation to minimize the loss function.

Hyper parameter Tuning: Experiment with different hyper- parameter settings such as learning rate, batch size, number of layers and kernel sizes to find the optimal configuration that maximizes the model's performance.

Model Evaluation: Evaluate the trained model's performance on the validation set using appropriate evaluation metrics such as Intersection over Union (IoU), mean average precision (mAP) or pixel accuracy. Adjust the model and hyper- parameters if necessary to improve its performance.

Model Testing: Test the trained model on an independent test dataset or real-world scenarios to assess its robustness and generalization capabilities. Measure its accuracy, precision and recall in lane detection tasks.

Fine-tuning and Transfer Learning: Consider fine-tuning of pre-trained deep learning model on specific transportation related datasets or transfer learning from related tasks such as object detection or semantic segmentation to enhance the model's performance and speed up training.

Model Deployment: Deploy the trained deep learning model into a real-time or near real-time system for lane detection in transportation. Optimize the model's inference time to achieve fast and efficient lane detection.

Continuous Improvement: Continuously update and refine the deep learning model by incorporating new data retraining with additional annotated samples and fine-tuning are the safer road networks. Collaboration and data sharing among industry partners and researchers are essential for advancements in this field. Transparent documentation and reporting support knowledge exchange. Deep learning-based lane detection models have the potential to revolutionize transportation, enhancing safety and efficiency for all road users.

Evaluation Metrics: Define appropriate evaluation metrics to assess the model's performance such as lane detection accuracy, false positive, false negative rates and runtime efficiency.

Integration with Transportation Systems: Integrate the lane detection model into existing transportation systems, such as Advanced Driver Assistance Systems (ADAS), autonomous vehicles or Traffic management systems to improve safety, navigation and traffic flow.

Real-time Monitoring and Adaptation: Implement real-time monitoring of lane detection performance using feedback mechanisms. Continuously monitor and adaptation of the model to changing environmental conditions like lighting changes, construction zones or adverse weather.
Collaboration and Data Sharing: Foster collaboration with industry partners, transportation authorities and researchers to share annotated datasets, models and insights. Encourage the development of standardized benchmarks for evaluating lane detection models in transportation.
Documentation and Reporting: Document the model development process including data collection, preprocessing steps, architecture details, training parameters and evaluation results. Prepare comprehensive reports and documentation to communicate the model's capabilities and limitations.
Gaussian Blur: is a function used for image filtering and smoothing. It applies a Gaussian blur to an image by convolving it with a Gaussian kernel. Gaussian blur helps reduce noise and smoothens the image by averaging the pixel values with their neighboring pixels. The extent of blurring is controlled by the kernel size and standard deviation of the Gaussian distribution. Gaussian Blur is often applied as a preprocessing step before performing other image analysis tasks to enhance the quality of the image and remove unwanted noise.
Canny: is an edge detection algorithm and is widely used for identifying significant edges in an image while minimizing noise and false detections. Canny edge detection algorithm consists of several steps. It starts with noise reduction by applying a Gaussian blur to the image. Later calculates the gradient magnitude and direction to determine the strength and orientation of edges. Non-maximum suppression is applied to retain only local maxima in the gradient magnitude. Double thresholding is used to classify pixels as strong edges, weak edges, or non-edges. Finally, edge tracking by hysteresis is performed to connect weak edges to strong edges and form continuous edge contours. The output of the canny edge detection algorithm is a binary image where the detected edges are represented as white pixels.

These steps help in developing a robust deep learning model for lane detection in transportation. This model can contribute to improve road safety, enhance navigation systems and enable the deployment of autonomous vehicles in transportation networks. In conclusion the development of deep learning models for lane detection in transportation shows promising improvement in road safety and navigation systems. Models utilizing techniques such as Convolution Neural Networks (CNN) or Fully Convolution Networks (FCN) and leveraging annotated datasets offer accurate and reliable lane detection capabilities. Integration into transportation systems allows for real-time monitoring. Figure 3 shows the lane detection for secure transportation

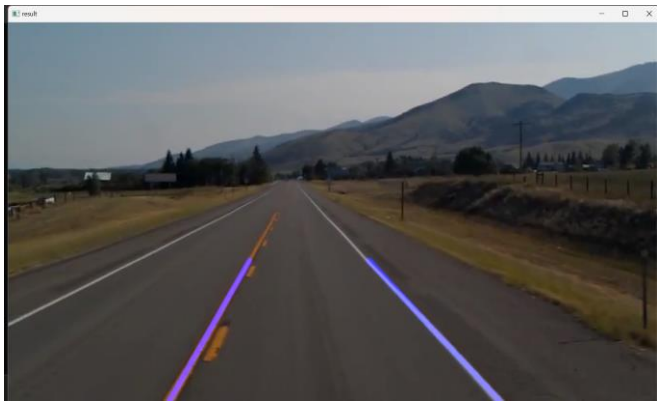

Figure 3: Secure Lane Detection

V. OBSERVATIONS

Research on Emerging Security Solutions in Transportation has shed light on the critical importance of addressing security challenges in the rapidly evolving transportation sector. The analysis of various domains including IoT, 5G technologies, connected vehicles, critical infrastructures and others has highlighted the vulnerabilities and risks associated with these emerging technologies. Study has emphasized the urgent need for proactive measures to mitigate security threats and protect transportation systems from potential cyber-attacks. It has stressed the significance of developing robust intrusion detection systems implementing effective attack prevention mechanisms and establishing efficient incident response strategies. The integration of advanced technologies such as artificial intelligence and machine learning are promising in enhancing security measures.

Furthermore, research has underscored the importance of comprehensive security frameworks that encompass authentication, encryption, access control and data privacy measures. Continuous monitoring, threat intelligence sharing and security awareness training have been identified as crucial elements in staying ahead of evolving cyber threats. Collaboration among stakeholders, including policymakers, researchers, industry experts,

and technology providers, has been emphasized as a key factor in addressing security concerns in a coordinated and holistic manner. This collaboration will facilitate the development and adoption of emerging security technologies, industry standards and best practices.

By implementing the recommendations outlined in this research, transportation systems can strengthen their resilience to ensure safe and secure integration of emerging technologies. Realization of the potential benefits offered by these technologies while mitigating the associated security risks and safeguarding the integrity and reliability of transportation infrastructure are enabled. It is imperative for organizations and policymakers to prioritize security in transportation systems to protect passengers, ensure smooth operation of transportation networks and safeguard critical infrastructures. Continued research, innovation and collaboration will be essential in developing and implementing effective security solutions that adapt evolving threat landscape. Research has highlighted the pressing need to address security challenges in transportation and to provide insights into potential solutions. By taking a proactive and comprehensive approach to security, transportation systems can navigate the emerging landscape with confidence, resilience, and a commitment to safeguard well-being and security of all stakeholders involved.

VI. CONCLUSIONS

Future technological and human solutions for detecting threats and preventing attacks in transportation holds immense promise for enhancing the security and safety of transportation systems. The combination of advanced technologies such as AI, computer vision, biometrics, and cybersecurity measures, along with human expertise and proactive approaches can significantly improve threat detection capabilities.

Intelligent surveillance systems, threat detection in autonomous vehicles, biometric authentication, cybersecurity measures, crowd monitoring, and proactive threat intelligence are key applications that highlight the potential of these solutions. By harnessing the power of technology and human collaboration, creation of a resilient transportation systems that are secure, capable of effectively mitigating threats and attacks are solution to ensure secured and safe transportation systems.

REFERENCES

[1]. Frustaci, Mario, et al. "Evaluating critical security issues of the IoT world: Present and future challenges." IEEE Internet of things journal 5.4 (2017): 2483-2495.
[2]. Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016.
[3]. Parkinson, Simon, et al. "Cyber threats facing autonomous and connected vehicles: Future challenges." IEEE transactions on intelligent transportation systems 18.11 (2017): 2898-2915.
[4]. Aslan, Ömer, et al. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions" Electronics 12.6 (2023): 1333.
[5]. Khan, Rabia, et al. "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions." IEEE Communications Surveys & Tutorials 22.1 (2019): 196-248.
[6]. González-Granadillo, Gustavo, Susana González-Zarzosa, and Rodrigo Diaz. "Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures." Sensors 21.14 (2021): 4759.
[7]. Elliott, David, Walter Keen, and Lei Miao. "Recent advances in connected and automated vehicles." journal of traffic and transportation engineering (English edition) 6.2 (2019): 109-131.
[8]. Sakiz, Fatih, and Sevil Sen. "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV." Ad Hoc Networks 61 (2017): 33-50.
[9]. Chowdhury, Mashrur, Mhafuzul Islam, and Zadid Khan. "Security of connected and automated vehicles." arXiv preprint arXiv: 2012.13464 (2020).
[10]. Lee, Adrian J., Alexander G. Nikolaev, and Sheldon H. Jacobson. "Protecting air transportation: a survey of operations research applications to aviation security." Journal of Transportation Security 1 (2008): 160-184.
[11]. Zarpelão, Bruno Bogaz, et al. "A survey of intrusion detection in Internet of Things." Journal of Network and Computer Applications 84 (2017): 25-37.
[12]. Dibaei, Mahdi, et al. "Attacks and defences on intelligent connected vehicles: A survey." Digital Communications and Networks 6.4 (2020): 399-421.
[13]. Gupta, Anunay, et al. "Advances of UAVs toward future transportation: The state-of-the-art, challenges, and opportunities." Future transportation 1.2 (2021): 326-350.
[14]. Moomen, Milhan, Mahdi Rezapour, and Khaled Ksaibati. "An investigation of influential factors of downgrade truck crashes: A logistic regression approach." Journal of traffic and transportation engineering (English edition) 6.2 (2019): 185-195.
[15]. López-Aguilar, Pablo, et al. "Information Security and Privacy in Railway Transportation: A Systematic Review." Sensors 22.20 (2022): 7698.