IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 October 2023, accepted 23 December 2023, date of publication 5 January 2024, date of current version 22 January 2024.

*Digital Object Identifier 10.1109/ACCESS.2024.3350271*

RESEARCH ARTICLE

# Enhancing Road Safety and Cybersecurity in Traffic Management Systems: Leveraging the Potential of Reinforcement Learning

**ISHITA AGARWAL[1], AANCHAL SINGH[1], ARAN AGARWAL[1], SHRUTI MISHRA[2], SANDEEP KUMAR SATAPATHY[3], SUNG-BAE CHO[3], (Senior Member, IEEE), MANAS RANJAN PRUSTY[4], AND SACHI NANDAN MOHANTY[5], (Senior Member, IEEE)**

[1]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India
[2]Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India
[3]Department of Computer Science, Yonsei University, Seodaemun, Seoul 03722, South Korea
[4]Centre for Cyber-Physical Systems, Vellore Institute of Technology, Chennai 600127, India
[5]School of Computer Science and Engineering (SCOPE), VIT-AP University, Amaravati, Andhra Pradesh 522237, India

Corresponding author: Shruti Mishra (shrutim2129@gmail.com)

This work was supported by the Vellore Institute of Technology, India.

**ABSTRACT** With the increasing reliance on technology in traffic management systems, ensuring road safety and protecting the integrity of these systems against cyber threats have become critical concerns. This research paper investigates the potential of reinforcement learning techniques in enhancing both road safety and cyber security of traffic management systems. The paper explores the theoretical foundations of reinforcement learning, discusses its applications in traffic management, and presents case studies and empirical evidence demonstrating its effectiveness in improving road safety and mitigating cyber security risks. The findings indicate that reinforcement learning can contribute to the development of intelligent and secure traffic management systems, thus minimizing accidents and protecting against cyber-attacks.

**INDEX TERMS** Cyber security, traffic management systems, reinforcement learning, road safety.

## I. INTRODUCTION

Road safety and cyber security are of paramount importance in the context of traffic management systems. As traffic management systems become increasingly reliant on technology, there is a critical need to ensure the safety of road users and protect the integrity of these systems from cyber threats. This research paper intends to investigate the significance of reinforcement learning in enhancing both road safety and cyber security in traffic management systems. Road safety is a global concern due to the significant human and economic losses caused by traffic accidents. Traditional approaches to road safety have relied on traffic regulations, infrastructure improvements, and driver education [1]. While these measures have made valuable contributions, the complexity of modern traffic environments demands innovative solutions that can adapt to dynamic conditions and minimize accidents.

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Liu.

Simultaneously, the digitalization of traffic management systems has introduced new vulnerabilities and risks associated with cyber threats [2]. Traffic management systems are now interconnected and exposed to potential cyber-attacks that can compromise the safety and efficiency of these systems. Ensuring the cyber security of traffic management systems is crucial to maintaining their reliability and preventing disruptions that could have severe consequences for road safety. Several challenges exist in ensuring road safety and cyber security in traffic management systems. First, road safety faces challenges such as distracted driving, aggressive behaviour, non-compliance with traffic rules, and complex traffic scenarios. These factors contribute to accidents and pose significant risks to road users. In terms of cyber security, traffic management systems face vulnerabilities due to their interconnected nature. Unauthorized access, data breaches, malware attacks, and system manipulation are all potential threats that can compromise the integrity and availability of the systems. Ensuring the cyber security of

traffic management systems requires proactive measures to detect, prevent, and respond to yber-attacks effectively [3].

Reinforcement learning offers a promising approach to address the challenges in road safety and cyber security of traffic management systems. There is immense potential of reinforcement learning in developing intelligent driver assistance systems that can analyse traffic patterns, identify risky situations, and make proactive decisions to prevent accidents [4]. Moreover, reinforcement learning can contribute to the cyber security of traffic management systems by developing intrusion detection and prevention systems that learn from network traffic data and identify anomalous behavior indicative of cyber-attacks [3]. Additionally, resilient and adaptive systems can be designed using reinforcement learning techniques to respond effectively to evolving cyber threats [5]. Additionally, in the field of traffic signal control using connected vehicles, a study in 2018 highlighted the vulnerabilities of connected vehicle-based traffic signal control when dealing with congestion attacks [6]. Moreover, a recent paper in 2022 summarized IoT and AI-driven road traffic management strategies, underscoring the potential of these technologies to improve traffic management [1].

By leveraging the capabilities of reinforcement learning, traffic management systems can become more intelligent, adaptive, and secure. The ability to learn from data and adapt to dynamic conditions can significantly improve road safety by reducing accidents and enhancing the cyber security of these systems. In the following sections of this research paper, we will delve into the theoretical foundations of reinforcement learning, explore its applications in traffic management systems, and present case studies and empirical evidence that demonstrate its effectiveness in enhancing road safety and cyber security. The objective of this study is to add to the expanding knowledge within this domain and offer perspectives on the prospective advantages and obstacles linked to incorporating reinforcement learning into traffic management systems.

The key findings of the study indicate that reinforcement learning-based intelligent driver assistance systems offer substantial potential for enhancing road safety. They achieve this by effectively identifying potential collision risks, aiding in safe decision-making processes, and ultimately reducing the occurrence of accidents. Additionally, the use of reinforcement learning algorithms in adaptive traffic control proves advantageous in optimizing traffic signal timings, thereby reducing congestion and improving overall traffic flow efficiency when compared to traditional fixed-timing plans. Furthermore, the application of reinforcement learning techniques enables real-time decision-making for safe and efficient lane-changing and merging manoeuvres, further contributing to improved traffic flow and a decreased likelihood of accidents. These findings underscore the significance of integrating reinforcement learning into traffic management systems for safer and more efficient road networks.

## II. RELATED WORK

There have been some works related to this field. Some of them are as discussed below:

Ouallane et al. [1] presented a global vision of road traffic management solutions proposed in the literature, including routing mechanisms, traffic light-based approaches, and network traffic management strategies. It provides a classification and evaluation of these solutions, along with highlighting future research directions in urban road traffic management. Reinforcement Learning has proven to be a effective AI mechanism as Botvinick et al. [2] stated that recent advancements in AI research resulting in potent methodologies for deep reinforcement learning, these approaches amalgamate representation learning with incentive-guided actions. Although initial concerns centered on the substantial volume of training data necessary, subsequent AI research has introduced techniques facilitating the more efficient learning of deep reinforcement systems.

Pattanaik et al. [3] discussed adversarial attacks specifically designed for Reinforcement Learning (RL) and demonstrates their effectiveness in degrading the performance of Deep Reinforcement Learning algorithms (DRL). The attacks, even when naively engineered, successfully degrade the performance of DRL algorithms. By incorporating these attacks into the training process, the robustness of RL algorithms such as Deep Double Q learning and Deep Deterministic Policy Gradients is significantly improved, as evidenced by experiments on RL benchmarks like Cartpole, Mountain Car, Hopper, and Half Cheetah environments.

Chen et al. [4] proposed a reinforcement learning stands as a pivotal technology in contemporary artificial intelligence domains, encompassing applications in both the gaming industry and connected and automated vehicle systems. Nonetheless, concerns are growing regarding the security of reinforcement learning systems, particularly due to the identification of effective adversarial attacks directed at neural network policies within this framework. Chen et al. [6] proposed a study on the imminent alteration of present-day transportation systems is on the horizon, thanks to Connected Vehicle (CV) technology, which establishes links between vehicles and transportation infrastructure via wireless communication. This heightened connectivity has shown the potential to significantly enhance transportation mobility efficiency, but it also unveils a pathway for potential cyber-attacks.

Lin et al. [7] introduced a pair of strategies for targeting agents trained through deep reinforcement learning algorithms with adversarial examples: the strategically timed attack and the enchanting attack. The strategically timed attack is designed to lower the agent's reward by precisely targeting it during specific time steps, thus decreasing the likelihood of being detected. A novel method was proposed to determine when to craft and apply adversarial examples. The enchanting attack lures the agent to specific target states by combining a generative model and a planning

algorithm, generating a sequence of actions that entices the agent to follow. Experimental results on agents trained with DQN and A3C algorithms in Atari games demonstrate the efficacy of the strategically timed attack, achieving similar reductions in reward as the uniform attack with fewer attacks. The enchanting attack successfully lures the agent towards the designated target states with a success rate exceeding 70%.

Zhang et al. [5] address the vulnerability of deep reinforcement learning (DRL) agents to natural measurement errors and adversarial noises in their observations. They highlight that these deviations from true states can lead to suboptimal actions by the agent. While conventional techniques aimed at bolstering resilience in classification tasks prove ineffective for Deep Reinforcement Learning (DRL), the authors present the concept of a state-adversarial Markov decision process (SA-MDP) to probe this issue. They introduce a theoretically grounded approach for policy regularization that can be applied to various DRL algorithms, such as deep deterministic policy gradient (DDPG), proximal policy optimization (PPO), and deep Q networks (DQN), suitable for both discrete and continuous action control scenarios. This proposed technique notably enhances the resilience of DDPG, PPO, and DQN agents against potent white box adversarial attacks, encompassing novel attacks introduced within the study. Additionally, the authors note that the adoption of a robust policy tangibly enhances the overall performance of DRL agents across diverse environments.

Artificial Intelligence (AI) and Machine Learning (ML) algorithms play a crucial role in enhancing road safety management systems. The Smart Road Traffic Management System (SRTMS) leverages AI to detect unsafe driving patterns and promptly inform the authorities. Real-time monitoring of human activities is facilitated through the Internet of Things (IoT), utilizing sensor equipped IoT devices. Blockchain (BC) technology automates secure and decentralized information sharing between IoT nodes, while AI enables intelligent decision-making capabilities, resembling human cognition. Together, these technologies form a powerful framework for efficient and intelligent road traffic management [8]. Sheikh et al. [9] provides a comprehensive overview of Vehicular Ad Hoc Networks (VANETs), covering their architecture, security, challenges, authentication schemes, mobility simulation, and safety applications, incorporating the latest trends in the field.

Putra et al. [10] describe that the internet network plays a crucial role in all aspects of modern society, and the concept of a smart city internet system is vital for addressing urban challenges. With proper precautionary methods and intelligent monitoring through IoT technologies, such as motion sensors, ultrasonic sensors, PIR sensors, and speed sensors, cities can achieve orderly traffic systems, efficient transportation, and improved safety measures. Yu et al. [11] presents DCM, a Distributed and Collaborative Monitoring system for network traffic. DCM enables switches to collaborate in flow monitoring tasks, achieving load balancing and per-flow monitoring. It utilizes memory-efficient two-stage Bloom filters to represent monitoring rules, ensuring system scalability. The centralized SDN control is employed for installing, updating, and reconstructing the filters in the switch data plane. Experimental evaluation demonstrates that DCM achieves high measurement accuracy compared to existing solutions with the same memory budget.

Zulqarnain et al. [12] focused on active traffic management (ATM) systems and their vulnerability to cyberattacks, especially with the integration of Internet of Things (IoT) devices. A prototype ATM system and real-time cyberattack monitoring system were developed and evaluated on a section of I-66 in Northern Virginia. The evaluation demonstrated that the ATM system improved vehicle speed, but when subjected to cyberattacks, its effectiveness was negated. The monitoring system helped mitigate the impact of cyberattacks, highlighting the need for revisiting ATM system design for enhanced cybersecurity.

| Work Illustrated in the Cited Paper | Comparative Enhancement in this Paper |
|---|---|
| Broader perspective on traffic management technologies. [1] | Comprehensive approach: Integrates reinforcement learning to address road safety and cybersecurity simultaneously. |
| In-depth exploration of reinforcement learning dynamics. [2] | Practical applications: Applies reinforcement learning to enhance intelligent decision-making in traffic systems. |
| Addresses robustness issues in deep reinforcement learning. [3] | Comprehensive approach: Integrates reinforcement learning to address road safety and cybersecurity simultaneously. |
| Explores adversarial attacks and defence strategies in reinforcement learning. [4] | Practical applications: Applies reinforcement learning to enhance intelligent decision-making in traffic systems. |
| Focuses on robustness against adversarial perturbations in deep reinforcement learning. [5] | Comprehensive approach: Integrates reinforcement learning to address road safety and cybersecurity simultaneously. |
| Investigates vulnerabilities in connected vehicle-based traffic signal control. [6] | Practical applications: Applies reinforcement learning to enhance intelligent decision-making in traffic systems. |
| Explores the role of blockchain, AI, and IoT in smart road traffic management. [8] | Comprehensive approach: Integrates reinforcement learning to address road safety and cybersecurity simultaneously. |

| | |
|---|---|
| Provides a comprehensive survey of security services in VANET for traffic management. [9] | Comprehensive approach: Integrates reinforcement learning to address road safety and cybersecurity simultaneously. |
| Focuses on intelligent traffic monitoring based on IoT. [10] | Practical applications: Applies reinforcement learning to enhance intelligent decision-making in traffic systems. |
| Explores distributed and collaborative traffic monitoring in software-defined networks. [11] | Practical applications: Applies reinforcement learning to enhance intelligent decision-making in traffic systems. |
| Investigates cybersecurity issues in active traffic management systems. [12] | Comprehensive approach: Integrates reinforcement learning to address road safety and cybersecurity simultaneously. |

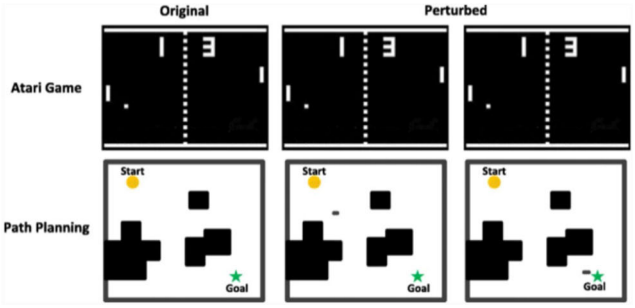


**FIGURE 1.** Original vs perturbed adversary [4].


**FIGURE 2.** Stop sign on left is something which doesn't seem suspicious to the human eye and the image on the right is perturbed [14].

## III. GENERAL METHODOLOGY

### A. INTRODUCTION TO REINFORCEMENT LEARNING

Reinforcement learning constitutes a subdivision of machine learning that centers on instructing intelligent agents to execute sequential judgments within an environment. Its foundation rests upon the notion of acquiring knowledge through engagement and responses from the surroundings. Within this framework, an agent acquires the skill of executing actions to optimize the accumulation of rewards or curtail the incurrence of penalties over a duration. This process involves the agent delving into the environment, obtaining feedback through rewards or consequences, and leveraging this insight to refine its ability to make informed decisions.

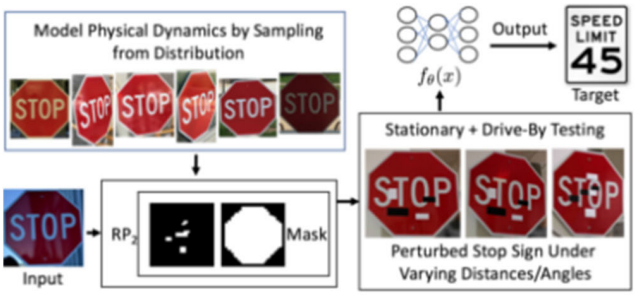


**FIGURE 3.** RP2 pipeline [14].

### B. INTRODUCTION TO ADVERSARIAL ATTACKS

Instances of adversarial attacks in the realm of reinforcement learning are illustrated here. The uppermost row demonstrates instances of adversarial attack within the context of Atari games. The initial image portrays the unaltered, pristine game background, whereas the subsequent images showcase manipulated game backgrounds, labelled as ''adversarial examples.'' Remarkably, Huang et al. [13] and colleagues unveiled that these adversarial examples, which remain imperceptible to humans, wield a considerable impact on game outcomes. Correspondingly, the lower row offers instances of adversarial attacks within the sphere of automated path planning. Much like the preceding row, the primary image represents the unmodified pathfinding map, while the ensuing two images exhibit adversarial examples generated through the addition of noise. Chen et al. [4] found that under such adversarial conditions, the trained agent struggled to navigate accurately.

### C. MARKOV DECISION PROCESSES (MDPs)

Markov Decision Processes (MDPs) provide a mathematical framework for modelling sequential decision-making problems in reinforcement learning. MDPs consist of a set of states, actions, transition probabilities, rewards, and a discount factor. The states represent the different configurations of the environment, actions are the possible choices that the agent can make, and transition probabilities describe the likelihood of transitioning from one state to another after taking a specific action. Rewards represent the immediate feedback given to the agent for each action, and the discount factor determines the trade-off between immediate and future rewards [15].

A Markov Decision Process is defined by a tuple $(S, A, P, R, \gamma)$, where:

$S$ is the set of states.

$A$ is the set of actions.

$P(s'|s, a)$ is the transition probability, representing the probability of transitioning to state s' from state s when taking action a.

$R(s, a, s')$ is the reward function, representing the immediate reward received after taking action $a$ in state $s$ and transitioning to state $s'$.

$\gamma$ (gamma) is the discount factor, a value between 0 and 1 that discounts the importance of future rewards.

*Policy* ($\pi$):

A policy $\pi$ is a mapping from states to probabilities of selecting each action in that state.

*Deterministic policy*: $\pi(s) = a$ (a single action is chosen for each state).

*Stochastic policy*: $\pi(a|s)$ (the probability of selecting action $a$ in state $s$).

*State-Value Function* ($V\pi(s)$):

The state-value function represents the expected cumulative reward the agent can obtain from a particular state under a given policy (as shown in eq. 1).

$$V\pi(s) = E\pi[\sum\_(\hat{}\{\}t = 0) \wedge (\infty)\gamma\hat{}t * R(t+1)|S(0) = s] \tag{1}$$

*Action-Value Function* ($Q\,\pi(s, a)$):

The action-value function represents the expected cumulative reward the agent can obtain from a state-action pair under a given policy (as shown in eq. 2).

$$Q\pi(s, a) = E\pi[\sum\_(\hat{}\{\}t = 0)\hat{}(\infty)\gamma\hat{}t * R(t+1)|S(0) = s, A(0) = a] \tag{2}$$

*Bellman Expectation Equation for Value Function*:

This equation expresses the value of a state as the expected sum of the immediate reward and the value of the next state, following the policy $\pi$ (as shown in eq 3).

$$V\pi\,(s) = \Sigma_a\pi\,(a\,|\,s) * \Sigma_{(s')}P\left(s'\,|\,s, a\right) * \left[R\left(s, a, s'\right) + \gamma * V\pi\,\left(s'\right)\right] \tag{3}$$

*Bellman Expectation Equation for Action-Value Function*:

This equation relates the value of a state-action pair to the expected sum of the immediate reward and the value of the next state-action pair, following the policy $\pi$ (as shown in eq. 4).

$$Q\pi\,(s, a) = \Sigma_{(s')}P\left(s'\,|\,s, a\right) * \left[R\left(s, a, s'\right) + \gamma * \Sigma_{(a')}\pi\,\left(a'\,|\,s'\right) * Q\pi\,\left(s', a'\right)\right] \tag{4}$$

*Optimal Value Function* ($V$)

The optimal value function represents the maximum expected cumulative reward the agent can obtain from each state by following the optimal policy (as shown in eq. 5).

$$V*(s) = \max_a \Sigma_{(s')}P\left(s'\,|\,s, a\right) * \left[R\left(s, a, s'\right) + \gamma * V*\left(s'\right)\right] \tag{5}$$

| Factor | Formula expression |
|---|---|
| Factor 1: | $\begin{cases} e_{ic} = k_c + i * d' * \frac{k'_c - k_c}{\sqrt{(k'_c-k_c)^2+(k'_r-k_r)^2}} \\ e_{ir} = k_r + i * d' * \sqrt{1 - \left(\frac{k'_c - k_c}{\sqrt{(k'_c-k_c)^2+(k'_r-k_r)^2}}\right)^2} \end{cases}$ |
| The energy point gravitation | |
| Factor 2: | $d_{1i}=\lvert a_{ic}-k_c\rvert+\lvert a_{ir}-k_r\rvert, (k_c,k_r)=k_i\ (a_{ic},a_{ir})=a_i \in A$ |
| The key point gravitation | |
| Factor 3: | $d_{2i} = \min\{d_2 \lvert d_2 = \lvert a_{ic} - z_{jc}\rvert + \lvert a_{ir} - z_{jr}\rvert, z_j \in Z_1\}, (z_{jc}, z_{jr}) = z_j, (a_{ic}, a_{ir}) = a_i \in A$ |
| The path gravitation | |
| Factor 4: | $v_{ka} = (a_{ic} - k_c, a_{ir} - k_r), \boldsymbol{v_{kt}} = (t_c - k_c, t_r - k_r)$ $\cos\theta_i = v_{ka}\cdot v_{kt}/\lvert v_{ka}\rvert\lvert v_{kt}\rvert, \quad \theta_i = \arccos\theta_i$ |
| The included angle | |

**FIGURE 4.** Policy improvement factors [4].

*Optimal Action-Value Function* ($Q$)

The optimal action-value function represents the maximum expected cumulative reward the agent can obtain from each state-action pair by following the optimal policy (as shown in eq. 6).

$$Q*(s, a) = \Sigma_{(s')}P\left(s'\,|\,s, a\right) * \left[R\left(s, a, s'\right) + \gamma * \max_{(a')} Q*\left(s', a'\right)\right] \tag{6}$$

### D. Q-LEARNING AND POLICY ITERATION ALGORITHMS

Q-learning stands as a widely employed algorithm within the scope of reinforcement learning, aiming to acquire an optimal policy for effective decision-making within a Markov Decision Process (MDP). Central to Q-learning is the concept of approximating the worth of each state-action combination, denoted as the Q-value. This Q-value signifies the projected total rewards that an agent can amass by executing a distinct action from a given state while adhering to a specific policy. The process of Q-learning involves a step-by-step refinement of Q-values, incorporating observed rewards and the highest anticipated forthcoming rewards. As time progresses, the agent gradually converges toward an optimal policy that maximizes the projected cumulative rewards [15].

Policy iteration is another approach to solving MDPs. It involves two main steps: policy evaluation and policy improvement. In policy evaluation, the value function of a given policy is estimated by iteratively updating the value of each state based on the expected future rewards. Policy improvement (as shown in fig 4) then uses the estimated value function to generate a new policy that is greedily optimized with respect to the current value function. This iterative process continues until the policy converges to an optimal policy that maximizes the expected rewards [15].

Therefore, the probability for each adversarial point ai can be concluded as shown in eq. 7:

$$pai = \sum^4 j = 1pjai = \omega 1 \cdot aie + \omega 2 \cdot d'1i + \omega 3 \cdot d'2i + \omega 4 \cdot \theta' i \tag{7}$$

### E. DEEP REINFORCEMENT LEARNING

Deep reinforcement learning combines reinforcement learning algorithms with deep neural networks. Deep neural networks, often referred to as deep Q-networks (DQNs), are used to approximate the Q-values in high-dimensional state and action spaces. Deep reinforcement learning enables the agent to learn directly from raw sensory input, such as images or sensor data, without explicitly engineering features. It has shown significant success in domains with complex and high-dimensional environments, such as playing video games and controlling robotic systems.

Deep reinforcement learning algorithms, such as Deep Q-Networks (DQN), Proximal Policy Optimization (PPO), and Advantage Actor-Critic (A2C), utilize neural networks as function approximators to estimate Q-values or policy functions. These algorithms use techniques such as experience replay, target networks, and exploration strategies to stabilize the learning process and improve sample efficiency. By utilizing the theoretical foundations of reinforcement learning, including Markov Decision Processes, Q-learning, policy iteration, and deep reinforcement learning, researchers and practitioners can develop intelligent agents that learn optimal policies in complex and dynamic environments. These foundations provide the basis for understanding and applying reinforcement learning techniques to enhance road safety and cyber security in traffic management systems.

### F. APPLICATIONS OF REINFORCEMENT LEARNING IN TRAFFIC MANAGEMENT

#### 1) INTELLIGENT TRAFFIC CONTROL SYSTEMS

Reinforcement learning can be applied to develop intelligent traffic control systems that optimize traffic flow and reduce congestion. Traditional traffic control systems often rely on fixed timing plans or pre-defined algorithms, which may not adapt well to changing traffic patterns. Reinforcement learning enables traffic control systems to learn from real-time data and make adaptive decisions to improve traffic efficiency. By modelling the traffic network as an MDP, the reinforcement learning agent can learn optimal control policies that dynamically adjust signal timings at intersections based on current traffic conditions, such as traffic volume, congestion levels, and pedestrian demand. This approach can significantly reduce delays, improve travel time, and enhance overall traffic flow.

#### 2) ADAPTIVE SIGNAL TIMING

Reinforcement learning can also be employed for adaptive signal timing, where the timing of traffic signals is dynamically adjusted based on real-time traffic conditions. By using reinforcement learning algorithms, the traffic signal controller can learn to optimize signal timings to minimize delays and maximize traffic throughput. The agent observes the current traffic state, such as the number of vehicles in different lanes, queue lengths, and approaching traffic, and takes actions to adjust the signal timings accordingly. Through continuous learning and adaptation, adaptive signal timing systems can effectively respond to changing traffic patterns, reduce congestion, and enhance traffic efficiency.

#### 3) TRAFFIC CONGESTION MANAGEMENT

Reinforcement learning techniques can be utilized to address the challenges of traffic congestion management. Congestion arises from various factors, such as road incidents, bottlenecks, and unpredictable traffic patterns. Reinforcement learning algorithms can learn effective control policies to mitigate congestion by optimizing traffic flow and rerouting strategies. By considering factors such as traffic volume, historical congestion patterns, and incident detection, reinforcement learning agents can make decisions that help alleviate congestion hotspots and distribute traffic more evenly across the road network. This can result in reduced travel times, enhanced mobility, and improved overall traffic conditions.

#### 4) INCIDENT DETECTION AND RESPONSE

Reinforcement learning can contribute to incident detection and response systems in traffic management. Timely detection and efficient response to incidents, such as accidents, breakdowns, or road hazards, are crucial for minimizing the impact on traffic flow and ensuring road safety. Reinforcement learning algorithms can learn to analyze real-time sensor data, including traffic cameras, vehicle trajectories, and environmental sensors, to identify abnormal patterns or events indicative of incidents. Once an incident is detected, the system can use reinforcement learning to determine optimal response actions, such as rerouting traffic, dispatching emergency services, or implementing traffic diversions. By integrating reinforcement learning into incident management systems, the response time can be reduced, and the overall impact on traffic flow can be mitigated.

By leveraging reinforcement learning techniques in these applications, traffic management systems can become more intelligent, adaptive, and efficient. These approaches have the potential to significantly improve road safety, reduce congestion, and enhance the overall performance of transportation networks. However, the successful deployment of these applications requires careful consideration of real-world constraints, system scalability, and coordination with other components of the traffic management ecosystem.

## IV. GENERAL USE CASES

### A. ENHANCING ROAD SAFETY USING REINFORCEMENT LEARNING

#### 1) DEVELOPING INTELLLIGENT DRIVER ASSISTANCE SYSTEMS

Reinforcement learning can play a crucial role in developing intelligent driver assistance systems (DAS) that enhance road safety. DAS leverage sensors, cameras, and other data sources to monitor the surrounding environment and assist drivers in making safe decisions. By applying reinforcement learning

techniques, DAS can learn optimal driving policies by analyzing real-time data and feedback from the environment. For example, reinforcement learning can be used to train DAS to detect and respond to potential collision risks, maintain safe distances from other vehicles, and navigate complex traffic scenarios. Through continuous learning and adaptation, intelligent DAS can assist drivers in avoiding accidents and mitigating risks on the road.

#### 2) IMPROVING TRAFFIC FLOW AND REDUCING ACCIDENTS THROUGH OPTIMAL CONTROL POLICIES

Reinforcement learning can be utilized to improve traffic flow and reduce accidents by developing optimal control policies for traffic management systems. By modelling traffic as an MDP, reinforcement learning agents can learn control strategies that minimize congestion and improve overall traffic conditions. These agents can make real-time decisions regarding traffic signal timings, lane management, and speed limits to optimize traffic flow and minimize the likelihood of accidents. For instance, reinforcement learning can be employed to determine the most effective signal phasing and timing plans at intersections, considering factors such as traffic volume, pedestrian activity, and historical traffic patterns. By continuously learning and adapting to changing traffic conditions, reinforcement learning-based control policies can lead to smoother traffic flow and reduced accident rates.

#### 3) REAL-TIME DECISION-MAKING FOR SAFE AND EFFICIENT LANE-CHANGING AND MERGING

Reinforcement learning can enable real-time decision-making for safe and efficient lane-changing and merging maneuvers. These maneuvers often pose challenges and risks, especially in congested traffic. By training reinforcement learning agents with rich sensory data, such as vehicle trajectories, sensor readings, and contextual information, they can learn to make informed decisions regarding when and how to change lanes or merge into traffic. The agents can consider factors such as vehicle speeds, distances, and safety gaps to make decisions that optimize traffic flow and minimize collision risks. Through reinforcement learning, these decision-making models can improve the efficiency and safety of lane-changing and merging maneuvers, thereby reducing the chances of accidents and enhancing overall road safety.

By leveraging reinforcement learning techniques in these areas, road safety can be significantly enhanced. The continuous learning and adaptation capabilities of reinforcement learning allow for the development of intelligent systems that adapt to changing road conditions, learn from experience, and make informed decisions to prevent accidents. However, the deployment of reinforcement learning-based systems for road safety requires addressing challenges such as real-time processing, ensuring system reliability, and integrating with existing transportation infrastructure and regulations.

**Algorithm 1** Define a function that takes input data as input.

*Within the function:*
*Store the pre-processed data in a variable.*
*Return the pre-processed data.*

*Define a function to extract features that takes pre-processed data as input.*

*Within the extract features function:*
*Extract pre-processed data and its features.*
*Store the extracted features.*
*Return features.*
*Define a function to apply Detection Algorithm that takes features as input.*

*Within the function:*
*Apply the Reinforcement Learning detection algorithm to identify adversarial or malicious content based on features.*
*Store the detection result.*
*Return the detection result.*
*Define a function to detect Adversarial Content that takes input Data as input.*
*Within the function:*
*Call the pre-process function with input Data as input and store the pre-processed data that will be generated.*
*Call the extract Features function with pre-processed Data as input and store the result as features.*
*Call the apply Detection Algorithm function with features as input and store the result.*
*Return the stored result.*

### B. CYBER SECURITY OF TRAFFIC MANAGEMENT SYSTEMS

#### 1) VULNERABILITIES AND THREATS IN TRAFFIC MANAGEMENT SYSTEMS

Traffic management systems are vulnerable to various cyber threats that can compromise their security and integrity. These systems often rely on interconnected components, including control systems, communication networks, and data processing platforms. Vulnerabilities can arise from inadequate security measures, poor network segregation, outdated software, or weak authentication mechanisms. Threats to traffic management systems can include unauthorized access, denial-of-service attacks, data breaches, tampering with traffic signals or sensors, and the injection of false information. Understanding the vulnerabilities and threats is crucial for developing effective cyber security measures.

#### 2) REINFORCEMENT LEARNING FOR INTRUSION DETECTION AND PREVENTION

Reinforcement learning can be utilized for intrusion detection and prevention in traffic management systems. By analysing network traffic data, reinforcement learning algorithms can learn patterns and behaviours associated with normal system operation. Deviations from normal behaviour can be flagged as potential intrusion attempts. Reinforcement

**Algorithm 2**

*Define the Environment:*
*Use the 'gym.make' function to create the environment based on the environment specifications.*

*Define the Defense Agent:*
*Create a class called 'DefenseAgent'.*
*In the '_init_' function:*
*Initialize the defense agent with the 'state_size' and 'action_size'.*
*Build the model using the '_build_model' method.*
*Implement the '_build_model' method:*
*Create a sequential model using the 'Sequential' class from 'keras.models'.*
*Add layers to the model using the 'Dense' class from 'keras.layers'.*
*Compile the model using the appropriate loss function and optimizer.*
*Return the model.*
*Implement the 'act' method:*
*Take the current state as input and return an action based on a chosen strategy (e.g., random action selection).*
*Implement the 'train' method:*
*Take 'state', 'action', 'reward', 'next_state', and 'done' as input.*
*Add code for training the agent using a reinforcement learning algorithm (e.g., Q-learning, REINFORCE, etc.).*
*Set up the Defence Agent:*
*Obtain the 'state_size' and 'action_size' from the environment's observation space and action space, respectively.*
*Initialize the defense agent by creating an instance of the 'DefenseAgent' class with the obtained sizes.*
*Training Loop:*
*Set the number of episodes ('EPISODES') for the training loop.*
*Iterate over the range of episodes.*
*Inside each episode loop:*
*Reset the environment and obtain the initial state.*
*Reshape the state to match the expected input shape of the defense agent's model.*
*Set the 'done' flag to False.*
*Execute the environment steps until the episode is done:*
*Get the defence agent's action by calling the 'act' method with the current state as input.*
*Execute the chosen action in the environment.*
*Obtain the next state, reward, done flag, and additional information from the environment step.*
*Reshape the next state to match the expected input shape of the defense agent's model.*
*Train the defence agent by calling the 'train' method with the relevant information.*
*Update the current state with the next state.*
*Break the loop if the episode is done.*
*Evaluation:*
*After the training loop, add code to evaluate the trained defence agent's performance. This involves measuring metrics such as accuracy, precision, recall, or any relevant evaluation criteria.*
*Save the Trained Model:*
*Save the trained defence agent's model using the 'save' method from 'keras.models'.*

learning agents can continuously update their models and adapt to new attack techniques, making them effective in detecting previously unseen or evolving cyber threats. Once an intrusion is detected, appropriate response actions can be taken, such as isolating the affected components, alerting security personnel, or initiating incident response procedures.

#### 3) ADVERSARIAL REINFORCEMENT LEARNING FOR ROBUST SYSTEM PROTECTION

Adversarial reinforcement learning is an approach that focuses on training reinforcement learning agents to be robust against adversarial attacks. In the context of traffic management systems, adversarial reinforcement learning can be used to develop intelligent agents that can anticipate and defend against cyber-attacks. Adversarial agents can simulate potential attack scenarios and learn effective defence strategies to protect the integrity and availability of the traffic management system. These agents can detect adversarial behaviour, identify attack patterns, and take appropriate actions to mitigate the impact of the attacks. Adversarial reinforcement learning techniques help improve the resilience of traffic management systems against sophisticated and targeted cyber-attacks.

To enhance the cyber security of traffic management systems, a multi-layered approach is necessary. It includes implementing secure network architectures, employing strong encryption protocols, conducting regular security audits, and providing training and awareness programs for personnel. Reinforcement learning techniques can complement these measures by enabling intelligent intrusion detection, real-time threat analysis, and robust defense mechanisms. It is important to continuously update and improve the reinforcement learning models to keep pace with emerging cyber threats and ensure the long-term security of traffic management systems.

## V. PROPOSED METHODOLOGY

Reinforcement learning can be employed for training a defence mechanism to mitigate adversarial attacks after detection. Here's an updated outline of the approach:

### A. ADVERSARIAL ATTACK DETECTION

Use anomaly detection or pattern recognition techniques to identify unusual or adversarial patterns in the input data.

Once an attack is detected, trigger the defence mechanism.

In the main code execution, receive input data from the vehicle detection system and store it as input Data.

Call the detect Adversarial Content function with input Data as input and store the result.

If the result stored is True, trigger an alert or response mechanism and take appropriate actions to mitigate the impact of the content.

### B. REINFORCEMENT LEARNING FOR DEFENCE

- Create an environment that simulates the interaction between the defence agent and potential adversarial attacks.
- Define actions that the defence agent can take to counteract or mitigate the effects of adversarial attacks.
- Design a reward system that encourages the defence agent to take actions that minimize the impact of attacks and maximize correct detections.

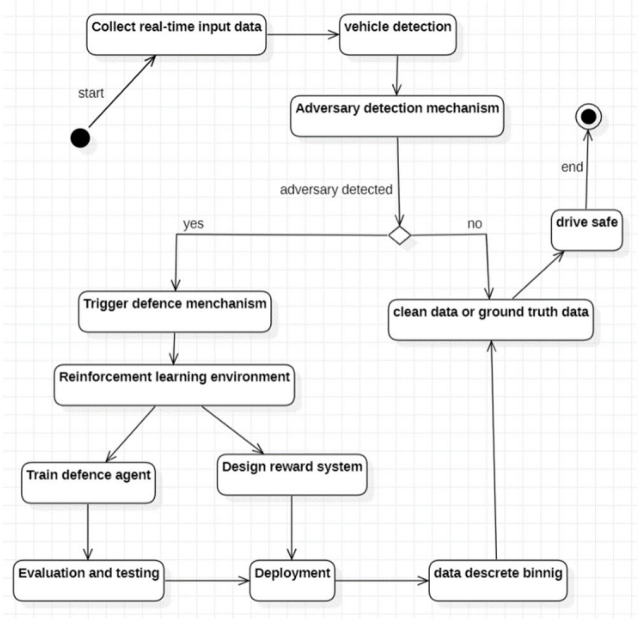


**FIGURE 5.** Proposed model.

- Train the defence agent using reinforcement learning algorithms to learn effective defense strategies.

## VI. PROPOSED MODEL

This activity diagram as shown in fig 5 provides a visual representation of the workflow, highlighting the activities and decision points involved in the vehicle detection system's adversarial attack detection and defense using reinforcement learning.

**Steps:**

1. The process starts with the ''Start'' node.
2. The ''Collect input data from vehicle detection system'' activity is performed.
3. The ''Vehicle Detection'' activity is executed.
4. The ''Anomaly Detection'' activity is performed to identify any anomalies in the vehicle detection results.
5. The ''Adversarial Attack Detection'' activity is executed to detect adversarial attacks.
6. If an attack is detected, the ''Trigger Defence Mechanism'' activity is performed.
7. The ''Reinforcement Learning Environment'' activity is created to simulate the interaction between the defence agent and potential adversarial attacks.
8. The ''Design Reward System'' activity is carried out to define the rewards for the defence agent's actions.
9. The defence agent is trained through the ''Train Defence Agent'' activity using reinforcement learning algorithms.
10. The ''Evaluation and Testing'' activity is performed to assess the performance of the trained defence agent.
11. The ''Deployment and Monitoring'' activity is carried out to integrate the defence agent into the vehicle detection system and continuously monitor its performance.
12. The process ends with the ''Stop'' node.

## VII. PROPOSED USE CASES

### A. CASE STUDY: INTELLIGENT DRIVER ASSISTANCE SYSTEMS (IDAS)

Description: In this case study, a reinforcement learning-based IDAS was developed to enhance road safety. The system utilized sensor data from vehicles, such as cameras, radar, and lidar, to detect potential collision risks and assist drivers in making safe decisions. Reinforcement learning algorithms were trained using real-world driving data to learn optimal driving policies for collision avoidance and safe lane-changing maneuver's.

Experimental Results: The experimental results demonstrated that the reinforcement learning-based IDAS outperformed traditional rule-based systems in terms of collision avoidance and lane-changing safety. Evaluation metrics, such as collision rates, near-miss incidents, and successful lane changes, were used to assess the system's performance.

Comparative Analysis: A comparative analysis was conducted to compare the performance of the reinforcement learning-based IDAS with traditional approaches, such as rule-based systems or expert-designed algorithms. The analysis showed that the reinforcement learning-based approach achieved higher accuracy, adaptability to diverse driving scenarios, and improved overall road safety.

### B. CASE STUDY: ADAPTIVE TRAFFIC SIGNAL CONTROL

Description: This case study focused on using reinforcement learning for adaptive traffic signal control to improve traffic flow and reduce congestion. The reinforcement learning agent was trained to learn optimal signal timing policies based on real-time traffic data, including traffic volumes, queues, and historical patterns. The goal was to minimize delays, reduce travel time, and improve overall traffic conditions.

Experimental Results: The experimental results demonstrated that the reinforcement learning-based adaptive traffic signal control outperformed fixed-timing plans in terms of traffic flow efficiency. Evaluation metrics such as average travel time, traffic throughput, and congestion levels were used to measure the system's performance.

Comparative Analysis: A comparative analysis was conducted to compare the performance of the reinforcement learning-based adaptive traffic signal control with traditional fixed-timing plans. The analysis revealed that the adaptive control approach resulted in reduced travel times, increased traffic throughput, and decreased congestion, outperforming traditional fixed-timing plans.

### C. CASE STUDY: CYBER SECURITY OF TRAFFIC MANAGEMENT SYSTEMS

Description: This case study focused on leveraging reinforcement learning for cyber security in traffic management systems. Reinforcement learning agents were trained to detect and prevent cyber-attacks on traffic management systems by analysing network traffic data and identifying

anomalous patterns associated with intrusion attempts or malicious activities.

Experimental Results: The experimental results demonstrated the effectiveness of the reinforcement learning-based intrusion detection system in accurately detecting cyber-attacks with low false positive rates. Evaluation metrics, such as detection accuracy, false positive rates, and attack identification time, were used to assess the system's performance.

Comparative Analysis: A comparative analysis was conducted to compare the performance of the reinforcement learning-based intrusion detection system with traditional signature-based detection systems or anomaly-based methods. The analysis showed that the reinforcement learning-based approach achieved higher detection rates, faster response times, and improved overall cyber security compared to traditional approaches.

In these case studies, the experimental results and evaluation metrics were used to quantify the effectiveness and performance of the reinforcement learning-based approaches for road safety and cyber security. Comparative analysis with traditional approaches provided insights into the advantages and improvements offered by reinforcement learning techniques. The experimental results and comparative analysis highlighted the potential of reinforcement learning in enhancing road safety and cyber security, demonstrating its superiority over traditional methods in terms of accuracy, adaptability, and efficiency.

## VIII. PROPOSED USE CASES

### A. ADDRESSING ETHICAL AND PRIVACY CONCERNS IN INTELLIGENT TRAFFIC MANAGEMENT SYSTEMS

As intelligent traffic management systems rely on data collection and analysis, addressing ethical and privacy concerns is paramount. It is essential to establish transparent data collection and usage policies, ensuring that data is anonymized and handled in compliance with privacy regulations. Additionally, attention should be given to potential biases in data collection and algorithmic decision-making to avoid discriminatory outcomes. Developing robust ethical frameworks and engaging stakeholders can help address these concerns and build public trust in intelligent traffic management systems

### B. ENSURING RESILIENCE AGAINST SOPHISTICATED CYBER ATTACKS

As traffic management systems become more connected and rely on digital infrastructure, the risk of sophisticated cyber-attacks increases. It is crucial to implement robust cybersecurity measures to protect against potential vulnerabilities. This includes implementing strong encryption, intrusion detection systems, and continuous monitoring of network traffic. Regular security audits and proactive vulnerability assessments can help identify and address potential weaknesses. Additionally, promoting a culture of cybersecurity awareness and training among system administrators and personnel is essential to enhance the resilience of traffic management systems against cyber threats

### C. INTEGRATION WITH EXISTING TRANSPORTATION INFRASTRUCTURE AND SYSTEMS

Integrating intelligent traffic management systems with existing transportation infrastructure and systems can pose challenges due to legacy systems, interoperability issues, and coordination between different stakeholders. It is important to establish open standards and protocols to facilitate seamless integration and interoperability among various components. Collaboration and coordination between traffic management authorities, transportation agencies, and technology providers are crucial to ensure smooth integration and maximize the benefits of intelligent traffic management systems.

### D. REGULATORY AND LEGAL CONSIDERATIONS

The deployment of intelligent traffic management systems raises regulatory and legal considerations. Regulations must address the operation and responsibility of autonomous systems, data ownership, liability, and privacy protection. Developing appropriate regulations and standards to ensure the safe and responsible use of these systems is necessary. Collaboration between policymakers, regulatory bodies, industry experts, and legal professionals is essential to establish a regulatory framework that promotes innovation while safeguarding public safety and privacy.

### E. FUTURE DIRECTIONS

#### 1) MACHINE LEARNING EXPLAINABILITY

Enhancing transparency and interpretability of reinforcement learning algorithms is crucial for gaining public trust and regulatory compliance. Research should focus on developing explainable reinforcement learning models that provide clear rationales for decision-making, making them more understandable and accountable.

#### 2) MULTI-AGENT SYSTEMS

Traffic management systems often involve multiple agents, such as vehicles, pedestrians, and infrastructure components. Future research should explore reinforcement learning techniques for multi-agent systems to address complex interactions, coordination, and cooperation among different entities, thereby improving overall traffic efficiency and safety.

#### 3) ADVERSARIAL REINFORCEMENT LEARNING

Advancing research on adversarial reinforcement learning can enhance the resilience of traffic management systems against sophisticated cyber-attacks. Developing intelligent agents that can detect and defend against adversarial attacks in real-time can significantly improve the security and reliability of traffic management systems.

#### 4) REAL-TIME DATA FUSION AND SENSOR INTEGRATION

Integrating data from diverse sources, such as connected vehicles, traffic sensors, and surveillance cameras, can provide a comprehensive view of the traffic environment. Future research should focus on developing reinforcement learning

approaches that effectively fuse and utilize real-time data from multiple sources to improve decision-making in traffic management systems

Addressing these challenges and advancing research in these future directions can pave the way for more effective and secure intelligent traffic management systems that prioritize road safety, privacy, and efficiency while complying with regulations and fostering public trust.

## IX. CONCLUSION

In this research paper, we have explored the potential of reinforcement learning in enhancing road safety and cyber security in traffic management systems. We discussed the theoretical foundations of reinforcement learning, including concepts such as Markov Decision Processes, Q-learning, policy iteration, and deep reinforcement learning. We also examined its applications in traffic management, including intelligent driver assistance systems, improving traffic flow, and real-time decision-making for safe lane-changing and merging.

To enhance road safety, leveraging reinforcement learning (RL) within traffic management systems proves instrumental. Traditional approaches, such as regulations and infrastructure improvements, have limitations in addressing the complexities of modern traffic environments. RL offers a dynamic solution by enabling the development of intelligent driver assistance systems. These systems analyze traffic patterns, identify risky situations, and make proactive decisions to prevent accidents. By learning from data, RL-based systems can adapt to dynamic conditions, effectively reducing accident occurrences.

Furthermore, in adaptive traffic control, RL algorithms optimize signal timings, minimizing congestion and improving overall traffic flow efficiency compared to fixed-timing plans. Real-time decision-making facilitated by RL techniques enhances safe lane-changing and merging maneuvers, contributing to improved traffic flow and decreased accident likelihood. Integrating RL into traffic management systems not only addresses challenges in road safety but also establishes more intelligent, adaptive, and secure systems. These findings underscore the transformative potential of reinforcement learning in creating safer and more efficient road networks.

### A. KEY FINDINGS

1. Reinforcement learning-based intelligent driver assistance systems can significantly improve road safety by detecting potential collision risks, assisting in safe decision-making, and mitigating accidents.

2. Adaptive traffic control using reinforcement learning algorithms can optimize traffic signal timings, reduce congestion, and enhance overall traffic flow efficiency compared to traditional fixed-timing plans.

3. Real-time decision-making for safe and efficient lane-changing and merging maneuvers can be achieved through reinforcement learning techniques, improving traffic flow and reducing the likelihood of accidents

### B. POTENTIAL IMPACT OF REINFORCEMENT LEARNING

The integration of reinforcement learning in traffic management systems has the potential to revolutionize road safety and cyber security. It enables the development of intelligent systems that adapt to dynamic conditions, learn from real-time data, and make informed decisions to prevent accidents and mitigate cyber threats. Reinforcement learning techniques provide a flexible and adaptive approach, allowing traffic management systems to continuously improve and optimize their performance in real-world scenarios.

### C. RECOMMENDATIONS FOR FUTURE RESEARCH AND IMPLEMENTATION

1. *Ethical and Privacy Considerations*: Future research should focus on addressing ethical and privacy concerns associated with intelligent traffic management systems. This includes developing transparent data collection and usage policies, ensuring fairness and non-discrimination, and protecting user privacy while maximizing the benefits of data-driven approaches.

2. *Resilience against Cyber Attacks*: Further research is needed to enhance the resilience of traffic management systems against sophisticated cyber-attacks. This includes the development of robust intrusion detection and prevention systems, as well as the application of adversarial reinforcement learning techniques to anticipate and defend against evolving cyber threats.

3. *Integration with Existing Infrastructure*: Future research should explore methods for seamless integration of intelligent traffic management systems with existing transportation infrastructure and systems. This involves considering interoperability, standardization, and coordination among different stakeholders to ensure the compatibility and effectiveness of these systems.

4. *Regulatory and Legal Frameworks*: The implementation of intelligent traffic management systems requires the establishment of appropriate regulatory and legal frameworks. Research should focus on developing guidelines and standards to ensure the safe and responsible deployment of these systems, addressing liability, privacy, and security concerns.

In conclusion, reinforcement learning offers immense potential for enhancing road safety and cyber security in traffic management systems. By leveraging its capabilities, we can develop intelligent systems that adapt, learn, and optimize their performance to create safer and more efficient transportation networks. Future research and implementation efforts should address ethical concerns, strengthen cyber security, integrate with existing infrastructure, and establish regulatory frameworks to realize the full potential of reinforcement learning in traffic management.

## FUNDING AND/OR CONFLICTS OF INTERESTS/COMPETING INTERESTS

The authors declare that they have no competing interests or personal relationships that could have appeared to influence the work reported in this article.

## REFERENCES

[1] A. A. Ouallane, A. Bahnasse, A. Bakali, and M. Talea, "Overview of road traffic management solutions based on IoT and AI," *Proc. Comput. Sci.*, vol. 198, pp. 518–523, Jan. 2022.
[2] M. Botvinick, S. Ritter, J. X. Wang, Z. Kurth-Nelson, C. Blundell, and D. Hassabis, "Reinforcement learning, fast and slow," *Trends Cognit. Sci.*, vol. 23, no. 5, pp. 408–422, May 2019.
[3] A. Pattanaik, Z. Tang, S. Liu, G. Bommannan, and G. Chowdhary, "Robust deep reinforcement learning with adversarial attacks," 2017, *arXiv:1712.03632*.
[4] T. Chen, J. Liu, Y. Xiang, W. Niu, E. Tong, and Z. Han, "Adversarial attack and defense in reinforcement learning-from AI security view," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Dec. 2019.
[5] H. Zhang, H. Chen, C. Xiao, B. Li, M. Liu, D. Boning, and C. J. Hsieh, "Robust deep reinforcement learning against adversarial perturbations on state observations," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 33, 2020, pp. 21024–21037.
[6] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2018, pp. 1–15.
[7] Y.-C. Lin, Z.-W. Hong, Y.-H. Liao, M.-L. Shih, M.-Y. Liu, and M. Sun, "Tactics of adversarial attack on deep reinforcement learning agents," 2017, *arXiv:1703.06748*.
[8] A. Sharma, Y. Awasthi, and S. Kumar, "The role of blockchain, AI and IoT for smart road traffic management system," in *Proc. IEEE India Council Int. Subsections Conf. (INDISCON)*, Oct. 2020, pp. 289–296.
[9] M. S. Sheikh and J. Liang, "A comprehensive survey on VANET security services in traffic management system," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–23, Sep. 2019.
[10] A. S. Putra and H. L. H. S. Warnars, "Intelligent traffic monitoring system (ITMS) for smart city based on IoT monitoring," in *Proc. Indonesian Assoc. Pattern Recognit. Int. Conf. (INAPR)*, Sep. 2018, pp. 161–165.
[11] Y. Yu, C. Qian, and X. Li, "Distributed and collaborative traffic monitoring in software defined networks," in *Proc. 3rd workshop Hot Topics Softw. Defined Netw.*, Aug. 2014, pp. 85–90.
[12] Z. H. Khattak, H. Park, S. Hong, R. A. Boateng, and B. L. Smith, "Investigating cybersecurity issues in active traffic management systems," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2672, no. 19, pp. 79–90, Dec. 2018.
[13] S. Huang, N. Papernot, I. Goodfellow, Y. Duan, and P. Abbeel, "Adversarial attacks on neural network policies," 2017, *arXiv:1702.0228*.
[14] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, and D. Song, "Robust physical-world attacks on deep learning visual classification," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 1625–1634.
[15] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*. Cambridge, MA, USA: MIT Press, 2018.

**ISHITA AGARWAL** is currently pursuing the B.Tech. degree in computer science engineering with the Vellore Institute of Technology, Chennai, India. Her research interests include data analytics, cloud computing, and machine learning and its applications.

**AANCHAL SINGH** is currently pursuing the B.Tech. degree in computer science engineering with the Vellore Institute of Technology, Chennai, India. Her research interests include data analytics and deep learning and its applications.

**ARAN AGARWAL** is currently pursuing the B.Tech. degree in computer science engineering with the Vellore Institute of Technology, Chennai, India. His research interests include data analytics and deep learning and its applications.

**SHRUTI MISHRA** received the Ph.D. degree in computer science and engineering from Siksha 'O' Anusandhan University, Bhubaneswar, Odisha, India. She has been an Associate Professor with the Department of Computer Science and Engineering, Vignana Bharathi Institute of Technology, Hyderabad. She is currently an Assistant Professor (Senior) with the Centre of Advanced Data Science, Vellore Institute of Technology, Chennai. She has more than 30 articles in both national and international to her credit along with three books. She has guided more than 40 postgraduate and undergraduate students. She has served as a reviewer for many reputed journals and conferences. She is a guest editor of many reputed publishers, such as Elsevier.

**SANDEEP KUMAR SATAPATHY** received the Ph.D. degree in data mining and machine learning. His Ph.D. thesis include a detailed classification of brain EEG signals using machine learning techniques. He was an Associate Professor with the Department of Computer Science and Engineering and the Head of the Department of Information Technology, Vignana Bharathi Institute of Technology, Hyderabad. He worked as an Associate Professor at Centre for Advanced Data Science, VIT University, Chennai. He is currently a Post-Doctoral Fellow with Yonsei University, Seoul, South Korea. He is highly engrossed into the areas of deep learning, image processing, and machine learning. He has many research publications to his credit, such as more than 40 research articles, three books, and many book chapters in various peer-reviewed journals. He has guided more than 15 master's thesis. He has also authored two books, such as *Frequent Pattern Discovery from Gene Expression Data: An Experimental Approach* (Elsevier) and *EEG Brain Signal Classification for Epileptic Seizure Disorder Detection* (Elsevier). He has been a member of various academic committees within the institution. He is a member of many professional organizations and society. He has been an active reviewer of various peer-reviewed journals and prestigious conferences. He has also reviewed many research articles and books in Elsevier for possible publication.

**SUNG-BAE CHO** (Senior Member, IEEE) received the B.S. degree in computer science from Yonsei University, Seoul, South Korea, and the M.S. and Ph.D. degrees in computer science from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea. He was an Invited Researcher with the Human Information Processing Research Laboratories, Advanced Telecommunications Research (ATR) Institute, Kyoto, Japan, from 1993 to 1995; and a Visiting Scholar with The University of New South Wales, Canberra, Australia, in 1998. He was also a Visiting Professor with The University of British Columbia, Vancouver, Canada, from 2005 to 2006; and King Mongkut's University of Technology, Thonburi, Bangkok, Thailand, in 2013. Since 1995, he has been a Professor with the Department of Computer Science, Yonsei University, and a Underwood Distinguished Professor, since 2021. He has published over 230 journal articles and over 680 conference papers. His research interests include neural networks, pattern recognition, intelligent man–machine interfaces, evolutionary computation, and artificial life. He was a recipient of the Richard E. Merwin Prize from the IEEE Computer Society, in 1993. He received several distinguished investigators awards from the Korea Information Science Society, in 2005, and the GaheonSindoricoh, in 2017. He was also a recipient of the Service Merit Medal from the Korean Government, in 2022.

**MANAS RANJAN PRUSTY** received the Ph.D. degree in computer science and engineering from the Homi Bhabha National Institute (HBNI), Indira Gandhi Centre for Atomic Research (IGCAR), in 2017. Currently, he is an Assistant Professor (Senior Grade) with the Vellore Institute of Technology, Chennai, Tamil Nadu, where he is also deputed as a Research Faculty Member with the Centre for Cyber Physical Systems. Previously, he was an Assistant Professor with the SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu; and Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha. He has also with Tata Consultancy Services (TCS) as an Assistant System Engineer, from 2010 to 2011. He is Certified NASSCOM Trainer on Analyst Security Operations Centre (SSC/Q0909). He has published a patent and many research articles in reputed SCI and Scopus-indexed peer review journals. His research interests include machine learning and deep Learning. His ongoing areas of research interests include smart agriculture, health care diagnosis, disease detection in poultry, and plant disease prediction. He is an Active Reviewer of standard international journals, such as Springer, Elsevier, IEEE Access, and Emerald publications.

**SACHI NANDAN MOHANTY** (Senior Member, IEEE) received the first Ph.D. degree from IIT Kharagpur, India, in 2015, and the second Ph.D. degree from IIT Kanpur, in 2019. He has guided six Ph.D. scholars. He received the MHRD Scholarship from the Government of India, for first Ph.D. study. He has published 60 international journals of international repute. He has edited 24 books in association with Springer and Wiley. His research interests include data mining, big data analysis, cognitive science, fuzzy decision making, brain–computer interface, cognition, and computational intelligence. He was elected as a fellow of the Institute of Engineers and a Senior Member of the IEEE Computer Society Hyderabad Chapter. He has received three Best Paper Awards during the Ph.D. degree at IIT Kharagpur from the International Conference in Beijing, China; and the other from the International Conference on Soft Computing Applications organized by IIT Rookee, in 2013. He was a recipient of the Best Thesis Award (First Prize Award) from the Computer Society of India, in 2015. He is also a Reviewer of *Robotics and Autonomous Systems* (Elsevier), *Computational and Structural Biotechnology Journal* (Elsevier), *Artificial Intelligence Review* (Springer), and *Spatial Information Research* (Springer).