Received: 2 February 2021 | Revised: 16 May 2021 | Accepted: 1 June 2021

DOI: 10.1111/exsy.12754

SURVEY ARTICLE

Expert Systems WILEY

Anomaly detection in autonomous electric vehicles using AI techniques: A comprehensive survey

Palak Dixit | Pronaya Bhattacharya | Sudeep Tanwar | Rajesh Gupta

Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, India

Correspondence
Sudeep Tanwar, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India-382481.
Email: sudeep.tanwar@nirmauni.ac.in, sudeep149@rediffmail.com

Abstract

The next wave in smart transportation is directed towards the design of renewable energy sources that can fuel automobile sector to shift towards the autonomous electric vehicles (AEVs). AEVs are sensor-driven and driverless that uses artificial intelligence (AI)-based interactions in Internet-of-vehicles (IoV) ecosystems. AEVs can reduce carbon footprints and trade energy with peer AEVs, smart grids (SG), and roadside units (RSUs). It supports green transportation vision. However, the sensor information, energy units, and user data are exchanged through open channels, and thus, are susceptible to various security and privacy attacks. Thus, AEVs can be remotely operated and directed by malicious entities that can propagate false updates to the peer nodes in IoV environment. This can cause the failure of components, congestion, as well as the entire disruption of IoV network. Globally researchers and security analysts have addressed solutions that pertain to specific security requirements, but still, the detection and classification of malicious AEVs is a widely studied topic. Malicious AEVs exhibit an anomaly behavior that differentiates them from normal AEVs, and thereby, the detection of anomalous AEVs and classification of anomaly type is required. Motivated from the aforementioned facts, the survey presents a systematic outlook of AI techniques in anomaly detection of AEVs. A solution taxonomy is proposed based on research gaps in the existing surveys, and the evaluation metrics for AI-based anomaly detection are discussed. The open challenges and issues in AI deployments are discussed and a case study is presented on anomaly classification through a weighted ensemble technique. Thus, the proposed survey is designed to guide the manufacturing industry, AI practitioners, and researchers worldwide to formulate and design accurate and precise mechanisms to detect anomalies.

KEYWORDS
anomalous classes, anomaly detection, artificial intelligence, autonomous electric vehicles, deep learning, machine learning, reinforcement learning

1 | INTRODUCTION

Rapid urbanization has shifted the focus of smart cities to look for sustainable solutions in intelligent transportation systems. The shift has revolutionized the automobile sector to move towards the utilization of renewable energy sources fuel generation such as thermal power plants, wind energy, and photo-voltaic cells. Currently, the automobile sector is trying to reduce carbon footprints and looking for green energy-based

solutions. Thus, the shift has been attributed towards novel AEVs design, and emerged as a key player in the intelligent transportation systems for mid and high-segment customers. As per the market survey, the global sale of AEVs is predicted to 26.95% million units by the end of 2030 (Berckmans et al., 2017). The growth is attributed to the improved operational and maintenance cost, low carbon waste, fewer fuel costs per unit, and health benefits of AEVs over the traditional non-renewable counterparts. The advantages of AEVs adoption over the non-renewable sources is presented in Figure 1. As depicted in the figure, the adoption of AEVs over traditional diesel and petrol variants has promising benefits in terms of low fuel consumption, reduction of accidents, eco-friendly usage, automated driving through embedded sensor controls, low power and battery consumption, and improved path planning through continuous updates from peer AEVs, rapid charging from charging stations, and low emission rate. Statically, AEVs have a 16kWh T-shaped lithium-ion battery, which is a key-energy exchange driver. Compared to petrol-diesel driven vehicles, AEVs have a low-fuel emission rate up to 22% over non-renewable counterparts. This is evident as they can emit 22% less carbon dioxide than diesel and 28% less than petrol, which contributes to green-energy-based solutions. Power consumption is also less as it's 194 Wh/km. Pollution is also drastically decreased by 37% over non-AEV models. In the case of safety and accidents, collisions are mitigated from 4.4% to 2.6%, which is almost half. Thus, the breakthrough drives the modern smart automobile industry.

AEVs are incorporated with network communication and driving sensors that communicate with roadside units (RSUs), charging stations, and smart grids (SG) on the internet of vehicles (IoV)-based ecosystems (Singh, Singh, & Bhattacharya, 2021). They communicate with IoV nodes and other peer AEVs through wireless charging adapters through directed short-range communications, which is IEEE *802.11p* standard for wireless high-speed communication of AEVs with IoV nodes without the external involvement of cellular links. The communication operates in close proximity to AEV nodes. It provides means of energy exchange through vehicle-to-anything (V2X) links (vehicle-to-vehicle [V2V], vehicle-to-infrastructure [V2I] and vehicle-to-grid [V2G] links). Moreover, AEVs are equipped with advanced technologies and are embedded with low-powered mechanical control systems that allow energy harvesting (EH) through built-in firmware and sensor components. Through EH, the ambient energy of IoV nodes is captured and based on motion dynamics and material quality of AEVs, the AEV controllers, devices, and solid-state circuitry units are charged. It increases the lifetime of AEVs body, chassis, and engine parts and improves the vehicle's rotational and motion movements. Moreover, EH reduces the periodic wireless charging of AEVs from charging stations and grid environments. It allows AEVs to have more resilient control to interact with peer nodes in IoV-based ecosystems.

Based on communication requirements, AEVs are broadly classified into fuel-type or network connection types. Fuel type AEVs are battery-operated with plug-in recharging jacks, also termed plug-in hybrid AEVs (PHEVs). Network connection-operated AEVs are categorized as connected or driver-less vehicles. Improved benefits of renewable over the non-renewable variants (coal, petroleum, and natural gas) have lead to a rise in the adoption of EVs in diverse sectors such as agriculture, manufacturing, and transportation (Shaheen et al., 2020). Figure 1 presents the unique characteristics of an AEVs. Figure 2a reflects the AEVs adoption model to various sectors by the year 2030. The AEVs are integrated with micro-controller chips (that control the engine functionality, ABS, suspension, and power steering controls), and sensors (that gather real-time vehicular data from mechanical actions through actuators in V2X ecosystems) (Bhatia et al., 2019). To date, many automobile organizations have manufactured and deployed AEVs and a few of them are shown in Table 1. Modern AEVs are eco-friendly, cheaper, and communicates in IoV with another peer AEVs to collaborate for infotainment and routing controls. This allows AEVs to manage route control, mobility, direction, energy transaction, and message exchanges in IoV. However, the real-time AEV information is captured and collected over open wireless channels, that is, the Internet, which is highly susceptible to various security and privacy attacks such as jamming, eavesdropping, authentication, authorization, synchronization, and distributed DOS (Habeeb et al., 2019). Thus, there is a threat of manhandling the user's privacy in V2X ecosystems.

Apart from security concerns, AEVs are also challenged by individuals (Vehicle drivers/passengers) that are genuinely harmed due to roadside mishaps. In the aftermath, they might even lose their lives in an accident. The mishaps are attributed to driver's carelessness, poor driving abilities, and roadside inconsistencies by other entities in IoV (S. Singh, 2015). Moreover, security attacks by malicious intruders

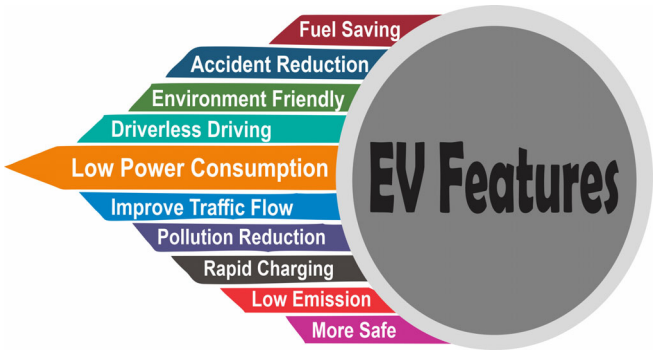

FIGURE 1 Characteristics of EVs

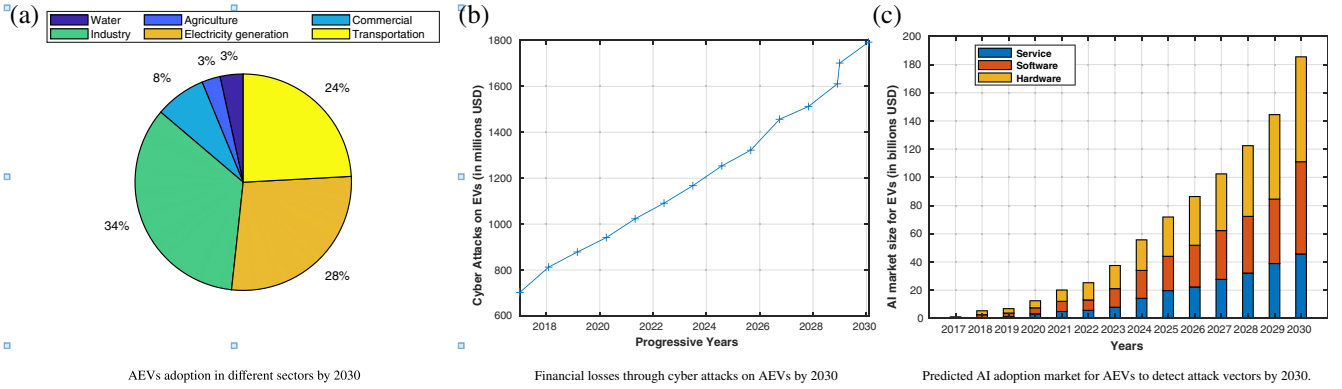

FIGURE 2 AEVs global market forecast and AI adoption to detect anomalies. (a) AEVs adoption in different sectors by 2030. (b) Financial losses through cyber attacks on AEVs by 2030. (c) Predicted AI adoption market for AEVs to detect attack vectors by 2030

include energy drain of AEVs, false message updates in IoV, forged certificates. The attacks are possible as AEVs communicate through open wireless channels, and thus communication details are intercepted by the adversary. Waqas et al. (2020) presented a new category of security threat in AEVs, termed as a rogue attack, where the adversary pretends to be a legitimate AEV. Thus, identification and classification of such malicious and anomalous AEVs is critical. Anomalous AEVs refer to the deviation of AEV from its predicted normal behaviour. Anomalous AEVs should be detected in the IoV ecosystem, and based on observed behaviour, are required to be classified with target labels. The problem is defined as anomaly classification, where the classes are labelled into specific categories, and through artificial intelligence (AI)-based learning methods, the accuracy of classes is predicted (Azzaoui et al., 2020). For the same, reinforcement learning (RL)-based techniques are highly suitable that can classify anomalous rogue classes through the captured channel state information. Different links like V2V, V2I and V2G are examined, and the performance is evaluated based on false alarm and misdirection rates compared against threshold values of the RL algorithm.

Thus, as discussed above, AI-based anomaly detection and classification study is important to drive a secure and trusted AEV environment. Additionally, the vehicle glitch or natural conditions influence the traffic well being also. Another kind of vehicle has been presented to improve street traffic security, known as an autonomous vehicle (AV), which empowers a driving mechanization framework to supplant human drivers to control the vehicle with better acknowledgment and driving abilities (Gupta et al., 2020; Shukla et al., 2020). Besides, AVs can speak with other vehicles, frameworks, and walkers as they are empowered with the V2X correspondence innovation. In this manner, the AVs, once generally sent, are relied upon to decrease human blunders, improve traffic stream, and eventually upgrade by and large wellbeing and experience of street clients (Cui et al., 2019). In this survey, the AVs are also considered as AEVs, that is, self-driving AEVs (Gupta, Tanwar, Kumar, et al., 2020). In anomaly detection, a typical need while analyzing datasets is to distinguish instances of normal behaviour and drift behaviour (Chandola et al., 2007). In such cases, outliers might be present due to induced training errors by AI models in AEV data. Such models are correctly predicted by Hawkins (1980) who have defined exception as a perception that digresses so remarkably from different perceptions as to stimulate doubt that an alternate system created it. These autonomous AEVs redefine the vehicle's business environment as the gigantic information generated by the vehicles themselves. Aggressors have shifted their focus towards the hack of information associated/generated with/by autonomous AEVs, which lead them to control the entire vehicle and incapacitate it also (Habeeb et al., 2019; Osman et al., 2019). Table 2 present various security vulnerabilities associated with specific EV components along with possible AI techniques to minimize its effect. Also, Figure 2b shows the financial losses of the owner or company due to cyberattacks on autonomous AEVs.

Anomaly Detection in autonomous AEVs stays a fundamental and broad research branch because of its boundless use in a huge scope of applications. AEVs are generally integrated with $\approx$ 40–80 ECUs, which continuously record the external environmental conditions (explosive information). Such information is beneficial for decision-making and requires highly computational techniques and infrastructure for processing. The autonomous AEVs are not much computed intensive that makes it difficult to deal with big computational data. A solution to the aforementioned issue, the integration of machine learning (ML), deep learning (DL), or RL algorithms is required (Gupta, Tanwar, Tyagi, et al., 2020; Singh, Cha, et al., 2021). Apart from computational complexity issues, security and privacy are also one of the major concerns. Figure 2c shows the year-wise adoption of AI algorithms to detect attack vectors and also observes that the adoption of AI is increasing exponentially over the years.

Motivated from the aforementioned talk, in this paper, the authors present a comprehensive survey on anomaly detection in AEVs using various AI techniques (K. Patel et al., 2020). The authors preferred classification, clustering, generative, discriminative, Q-learning, and deep reinforcement learning (DRL) techniques for anomaly detection.

TABLE 1 A comparative analysis of AEVs manufactured by different automobile industries

AEV brand	Company	Range	Power	Max. speed	Features	Price	Battery
Tiago	Tata	100 km	85 KW and 3 phase AC induction motor	135 km/h	Dual Airbags ABS and EBD as well as Quick charging and regenerative braking system	8–10 lacs	85 KwH
e2o plus	Mahindra	140 km	19 KW and 3 phase AC induction motor	80 km/h	135 L boot space capacity for storing luggage	7.5 lacs	15 KwH
Tigor	Tata	142 km	30 KW and 3 phase AC induction motor	100 km/h	Fast Charging port at the back which can charge within a 90 min as well as 300 L boot space capacity for storing luggage	10 lacs	16.2 KwH
eVerito	Mahindra	140 km	31 KW and 3 phase AC induction motor	86 km/h	Five Seater, automatic transmission, length of 4247 mm, width 1740 mm, with a wheelbase of 2630 mm	10.39 lack	18.5 KwH
e-KUV100	Mahindra	140 km	30.5 KW and 3 phase AC induction motor	186 km/h	It can go 200 km/h in just 9 s	15 lacs	72 KwH
Wagnor Electric	Maruti	200 km	Torque of 113 Nm with a cycle of 4200 rpm	120 km/h	2 charging ports: AC fast charging in 7 h and DC charging in 1 h	7–9 lacs	50 KwH
Kia Soul EV	Kia Motors	391 km	81.5 KW and 3 phase AC induction motor	168 km/h	It has electric power-assist speed-sensing steering with top speed of 105 mph	35 lacs	64 KwH
Nissan leaf	Nissan	363 km	160 KW	150 km/h	It can get charge uptp 80% in just 30 min as well as it can go upto 96 km/h in just 9.9 s	30 lacs	64 KwH
e-tron	Audi	400 km	280 KW	200 km/h	It can generate 30% energy from regenerative braking system	1 crore	95 KwH
Kona	Hyundai	452 km	100 KW	167 km/h	It has 6 airbags for safety as well as it has regenerative braking system. It can get charge in 6 h with AC charger and 80% charge in 57 min with DC charger	25 lacs	39.2 KwH

1.1 | Motivation

1. To date, many researchers across the globe have given their novel solutions for anomaly detection in AEVs using AI techniques. But, there exists no comprehensive survey, which highlights the usage of AI techniques and algorithms (presented by various researchers) for anomaly detection in AEVs on a single platform. This arises the need for a comprehensive survey that disseminates the complete information about AI-based anomaly detection to the readers.
2. The existing surveys are not much focused towards the autonomous EVs, rather more alleviated towards the EV security and charging. By considering this interesting gap, this paper presents a detailed survey on anomaly detection for AEVs.
3. The above-mentioned reasons motivate us to write a comprehensive survey on AI-based anomaly detection in AEVs.

TABLE 2 Security vulnerabilities in AEVs and possible AI techniques

AEV components	Parts	Attack vectors	Attack at EV layered stack	Raised anomalies	Potential security breaches	Detection probability	Possible AI techniques
Chassis	Airbag, chassis, power steering, brakes	Segment-based attacks, eavesdropping attacks	Data-link, network layer	Data packets sent in small header segments to a nearest malicious intruder, and passive channel information gain	Privacy, confidentiality	Low	Bayesian, multi-layer perceptron, and k-means
Audio or video panels	Phone jack, navigation, display units, audio system, Bluetooth	Synchronization, disruption attack, jamming attack	Session, presentation, and application layers	Unauthorized supply of service sets to nearby vehicles, and remote road-side malicious entities, data corruption, unusable formats, incorrect working of infotainment units	Entity and data integrity, location, privacy, authentication	Moderate at low-density areas, and high at high-density areas	RNN, CNN, clustering approaches
Engine	Power sensors, electric battery, controller unit, actuators	Masquerading attack, eavesdropping attack, injection attack, replay attack, DoS attack, bus-off attack	Network and transport layers	Incorrect data insertion through time gaps in sequenced data, data sent later by a malicious intruder, failed authorization to registered services, change of route and navigation sequences, incorrect location updates	Authentication, availability, confidentiality	High	DNN, LSTM, RL
Network communication sensors	Remote navigation, key units, infrared, light/climate, and temperature sensors	Network access, traffic confidentiality, traffic integrity, denial of service attacks	Logical-link control sub-layer, medium-access control sub-layer, network, and transport layer	Access to unauthorized EV information, access to physical units, gaining remote driving controls, unauthorized displays, failed authorization to registered services	Authentication, availability, confidentiality, privacy	High	GAN, Bayesian, RNN, LSTM

1.2 | Research contributions

Following are the major contributions of the paper.

1. The proposed survey identifies the gaps in the existing surveys possessing different AI techniques for anomaly detection in AEVs based on real-time sensor information captured from EVs in the IoV environment.
2. A fine-grained solution taxonomy is proposed to classify anomaly detection techniques considering network, security, and AI-based solutions in the IoV environment. The different schemes in each sub-taxonomy are discussed in context to AEVs for anomaly detection.
3. The open issues and challenges in deploying AI techniques for detecting anomalies in AEVs are discussed. The authors then present an experimental case study based on a weighted ensemble of CNN-LSTM modules to fine-tune and optimize the anomaly classification. The case study suggests an attention mechanism sequence and also presents multiple classifiers to optimize the prediction. The case study is measured for performance indicators like precision, accuracy, and F1-score on the SPMD dataset, as proposed by van Wyk et al. (2020).

1.3 | Scope of the survey

To date, several surveys and methodologies have been conducted by authors across the globe, which considered different features of anomaly detection (Aldweesh et al., 2020; Erfani et al., 2016; Li et al., 2017; H. Wang et al., 2019). This paper presents a comprehensive and organized survey for the outlier detection methods designed between the years 2016 to 2020. Many of them have highlighted the utilization of AI techniques to detect anomalies in AEVs. But, the proposed survey presents a detailed overview of different techniques to handle anomalies in autonomous AEVs. Table 3 shows the comparative study of existing surveys on anomaly detection with the proposed survey concerning the parameters such as architecture presented, anomalies detected, applications targeted, security achieved, AI technique used, and security algorithm used. These parameters clearly show the motivation behind the proposed comprehensive survey.

Erfani et al. (2016) focused on anomaly detection using AI techniques like DBN, one-class support vector machine (SVM) including SVDD, and plan-based one-class SVM and hybrid DBN-SVM. Li et al. (2017) discussed the strategy of power management depends on RL using methods like dynamic programming and Q-learning in plug-in AEVs. Koustubh et al. (2018) covers ANN-based SVDD method to detect anomaly in hybrid AEVs. Aldweesh et al. (2020) focused on intrusion detection security with discriminative and generative approaches in the domain of DL along with a taxonomy of various DL IDS approaches. H. Wang et al. (2019) focused on various outlier detection techniques like statistical-based, distance-based, density-based, clustering-based, graph-based, ensemble-based (ALzubi et al., 2019), learning-based methods including both conventional, and emerging challenges. Chalapathy and Chawla (2019) discussed deep learning models like semi-supervised, unsupervised, hybrid, and One-class neural network along with various DAD techniques. Wu et al. (2020) presented a design scheme for monitoring unmanned surface vehicles through effective path planning and improved motion control paths through embedded sensor units. Shi et al. (2020) proposed model predictive control technique in for AEVs, to optimize energy management and battery fuel. They have considered a non-linear constrained formulation of AEV and presented the optimization as a sequential quadratic problem to derive the control unit function of AEVs.

1.4 | Organization and reading map

Figure 3 shows the organization of the survey. In Section 1, there is a basic introduction of the paper, which includes the motivation and scope of the survey. In Section 2, there is a summary of AEVs, anomaly detection, AI approaches, and application areas. In Section 3, there is a discussion about the review plan and information related to data sources. Sections 4–6 present the taxonomies of network-based, AI-based, and security-based anomaly detection. Section 7 highlights the evaluation metrics, including accuracy, precision, TNR, FPR, and FNR. Section 8 discusses various open issues and challenges in the proposed anomaly detection technique for autonomous AEVs. Section 9 presents the case study. Then, the paper is concluded in Section 10. Table 4 shows the acronyms used in the paper.

2 | BACKGROUND

This section highlights the commonly used concepts of AEVs, anomaly detection, and approaches to identifying and detecting anomalies. Also, it shows how to integrate AI and AEVs.

TABLE 3 Comparative analysis of state-of-the-art surveys with the proposed survey

Ref.	Year	Architecture presented	Anomalies detected	Application targeted	AI technique used	Summarized findings	Pros	Cons
(Erfani et al., 2016)	2016	Hybrid model	High-dimensional and large-scale anomalies	High-dimensional data applications	DBN, one-class SVM	Hybrid DBN-1SVM is faster in training and testing from autoencoder	In the case of high-dimensional and large-scale, these hybrid methods are very efficient	Not able to maintain accuracy of the model if normal behaviour evolves significantly over time
(Koustubh et al., 2018)	2018	Enhanced SVDD	Inaccurate data	HEV	SVDD, ANN	Normal class has 99.56% accuracy and test grid has 98.8% accuracy	Has high accuracy as 99.8% by using classification with k-means while training the ANN model	dynamic selection of kernel functions
(Moustafa et al., 2019)	2019	classical IDS	DoS, Brute force, browser, shell shock, SSL, Botnet, backdoor	Cyber kill chain models	Mobile edge, fog, cloud, IoT			IDS faces challenge for being built in an online and adaptable manner
(Chalapathy & Chawla, 2019)	2019	DHM	Fraud, cyber-intrusion, Log-anomaly, Industrial damage	Anomalous application domains	DHM,OC-NN	Unsupervised models have low robustness for noisy data	Due to pre-training of a model, testing is fast and in supervised approaches	quite expensive in the model training which are based on classification, supervised or semi-supervised techniques
(Miglani & Kumar, 2019)	2019	Traffic flow prediction using hybrid DL	Traffic congestion	AV	CNN, RNN, LSTM, GRU, TDNN, AE, DBM, DBN, RBM, WNN	As compared to an individual model, hybrid structure are found to be more accurate.	Since hybrid approach is used, accuracy is more compare to individual model	Long-term prediction is difficult in traffic prediction
(Aldweesh et al., 2020)	2020	DL based IDS	deep-learning based cyber security	IDSs	AE, RBM, DBN, CNN, RNN, DNN, GAN	DL is efficient for IDS. Proposed approaches rely on the legacy benchmark datasets	Due to different DL frameworks used, high accuracy is achieved	Cannot deal with recent database and real-time scenarios
(Ferrag et al., 2020)	2020	IDS methodology	Cyber security intrusion	different datasets	DNN, RNN, CNN, RBM, DBM, DAE, DBN	DNN has 96.915% TNR,RNN has 91%–98% detection rate, CNN has 97%–99% detection rate	Accuracy of RNN and CNN is pretty high	Didn't suggested the scenarios of attack with given AI approaches
(Kavousi-Fard et al., 2020)	2020	Microgrid	Highly complex and oscillatory data	Wireless sensor network	LUBE, MSOS	Generates efficient result for malicious attacks and fake data injections	Highly accurate against attacks in data integrity	Communication delays may affect microgrid negatively in security and reliability
The proposed	2021	Anomaly detection using AI techniques	Misbehaving and malicious EVs	AEV	CNN, RNN, LSTM, DBN, ANN, DBSCAN, SVM, RL, Q-learning	Presents useful anomaly classification scheme based on network, security, and AI-techniques	Evaluation metrics and open issues of anomaly detection of AEVs are discussed	-

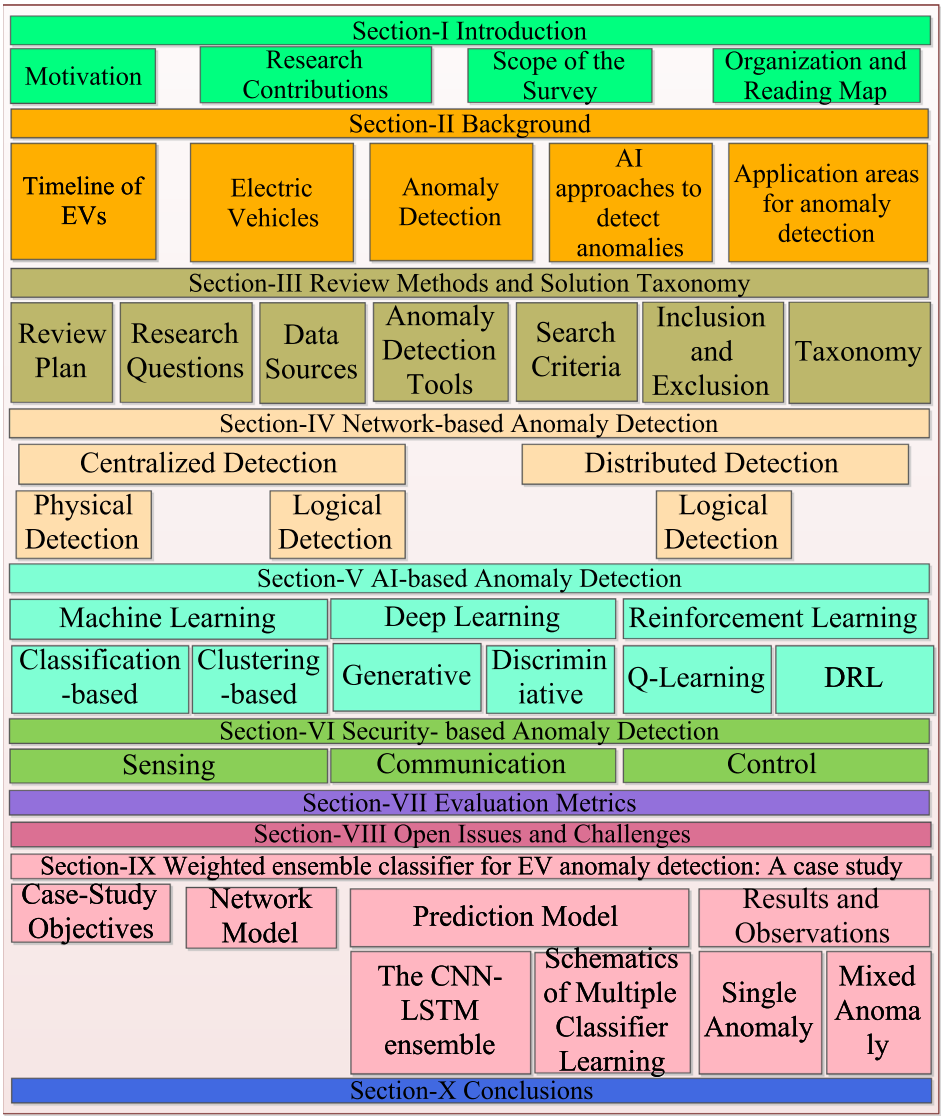

FIGURE 3 Paper organization

2.1 | Timeline of AEVs

In the 1800s, many researchers and innovators worldwide started exploring AEVs powered by a battery component. Then, in 1832, Robert Anderson from Britain has developed the first electric car. Later, Robert Anderson, Henry Ford, and Thomas Edison were started working on developing AEVs, which can run over 100 miles efficiently. Then, in the early 1900s, one-third of all cars in the US were electric, which is fueled by various charging stations. After that, the gasoline models of vehicles took place, but the main focus was on AEVs. By the mid-'20s, that is, 2040, more than half of the vehicles will be battery-driven. Figure 4 shows the timeline of AEVs. As per the Economic Times prediction, by the year 2024, the sale of AEVs in the US will cross 1 million.

During 1920 to 1960, the prevalence of AEVs started decreasing due to Ford's mass-delivered Model T and other gas energized vehicles, alongside far-reaching reception of self-starters, acquainted in 1912 with supplanting stubborn hand wrenches that necessary a great deal of muscle. Then in 1954, Lektro presented the golf cart, which was the first business purpose vehicle. After that, the national union electric corporation did modifications in AEVs. As a part of this, it changes 100 Renault Dauphines to run on battery and these new forms are called "Henney kilowatts". During the 1960s, various organizations, including General Motors and American Motors produced ideal models in light of developing worries about air contamination from people in general, state, and neighbourhood governments.

In the era of 1970 to 1980, the battery-controlled vehicles gets a promotional lift due to the electric lunar roving vehicle of NASA, which was designed and built by innovators of Boeing and GM. Then, in the 1990s, the fixing discharge prerequisites cause automobile organizations to concentrate progressively on elective fuel vehicles. An inventor from GM presented an EV1, which was far efficient than the earlier invented AEVs.

TABLE 4 Acronyms

Acronym	Description
AF	Activation function
AI	Artificial intelligence
ANN	Artificial neural network
CNN	Convolutional neural network
DAD	Deep anomaly detection
DL	Deep learning
DRL	Deep reinforcement learning
DBN	Deep belief network
DBSCAN	Density-based spatial clustering of applications with noise
DoS	Denial of service
DNN	Deep neural network
EV	Electric vehicle
EMS	Energy management strategy
ECU	Electronic control unit
FPR	False positive rate
FNR	False negative rate
HEV	Hybrid electric vehicle
HIDS	Host intrusion detection system
IoT	Internet of things
IoV	Internet of vehicle
IDS	Intrusion detection system
LSTM	Long short-term memory
LUBE	Lower and upper bound estimation
ML	Machine learning
MSOS	Modified symbiotic organisms search algorithm
NIDS	Network intrusion detection system
ODD	Outlier detection datasets
RL	Reinforcement learning
R2L	Remote to local
RNN	Recurrent neural network
RBM	Restricted Boltzmann machine
SVM	Support vector machine
SDN	Software defined network
SVDD	Support vector data description
TP	True positive
TN	True negative
TNR	True negative rate
TPR	True positive rate
U2R	User to root
V2G	Vehicle to grid

So, they developed ≈ 1000 such vehicles and gave them to clients on a rental basis. Along with this, Toyota's Prius and Honda's Insight, as well as Nissan reviews its Altra EV minivan, controlled by lithium-particle batteries. Tesla dispatches the sports car, the first creation of EV with a lithium-ion battery in 2008.

Nissan's Leaf goes on sale in 2010, which became the world's best-selling EV. Then, Tesla adds its Model S sedan, Model X SUV, and lower-priced Model 3. Then, Musk also announces plans to build an electric Semi truck, which will compete with haulers from companies such as

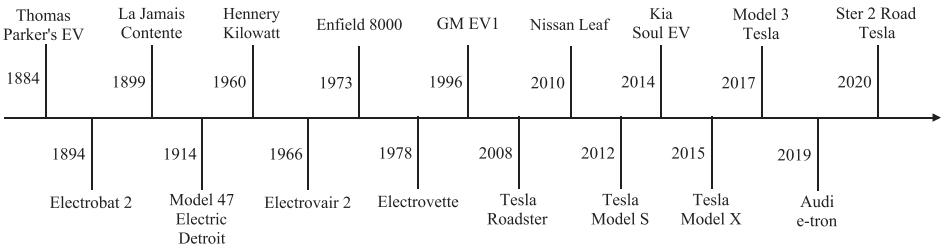

FIGURE 4 Evolution timeline of AEVs

Daimler, maker of Mercedes-Benz luxury cars, and China's BYD, backed by Warren Buffett. China's focus on reducing smog and cutting oil imports makes it the world's biggest EV market, spurring hundreds of local manufacturers and startups to fight for share, including XPeng Motors and SAIC Motor. Echoing La Jamais Contente's 1899 speed record, Volkswagen's I.D. R sets a new record in June 2018 for the century-old pikes peak international hill climb, racing 12.42 miles in 7 min, 57.148 s (in 1916 the winning time was 20 min and 55.6 s). Then, Nissan's Leaf went marked down in 2010 and became the world's top-line EV.

2.2 | Autonomous electric vehicles

AEVs are vehicles, which use one or more electric motors or traction motors instead of an internal combustion engine that generates power by burning a mix of fuel and gases for driving. AEVs are not the same as petroleum product-controlled vehicles, which can get their capacity from a wide scope of sources, including non-renewable energy sources, atomic force, and inexhaustible sources. AEVs are used as a substitute in automobiles to address the issues of pollution in the urban area, the effect of global warming, the greenhouse effect, and depleting natural resources. The power controls the vehicle's wheels utilizing an electric engine.

Recently, the advanced vehicles are outfitted with various modules, for example, in-vehicle systems including motor controls units, body control modules, and cell phone coordination module, which give basic functionalities to control and security of AEVs. These modules should be broken down progressively to distinguish the irregularities in the vehicles, which incorporates abrupt speed up, radar sensors identification, camera detecting, unusual petroleum utilization, unexpected motor disappointment, unseemliness in switching to another lane, and incorrect article recognition. To exploit the same, vehicle recognition is a critical aspect of study in IoV environments. Vehicle recognition allows the capture of live vehicular traffic as framesets. The captured frames are successively collected to form the recognition datasets. To train the models, cold-start-based vehicle model recognition in cross-frame scenarios is greatly employed, with transfer learning technique. In this case, deep and joint adaptation networks are built on top of convolutional neural nets, like *AlexNet and ResNet*, to build a better model that achieves higher accuracy (H. Wang et al., 2020). Tian et al. (2020) presented object detection models through application of off-the-shelf detectors. In the scheme, model training is presented based on ground truth labels. An adaptive approach is presented for cross-domain vehicle detection that captures the image and feature space requirements. The features are fed to generative adversarial models, and detection accuracy is improved.

2.3 | Anomaly detection

The identification of anomalies is a significant issue that has been examined under different research zones and application areas. It is a process to identify the patterns in given data that behave differently than the expected behaviour. Commonly, these odd things have the capability of getting converted into an issue, for example, the basic imperfections, mistakes, or fakes. Utilizing AI for anomaly detection helps in upgrading the speed of recognizing such patterns. These non-adjusting designs are regularly alluded to as inconsistencies, anomalies, conflicting perceptions, special cases, variations, or contaminants in different application spaces. Inconsistency discoveries find broad use in a wide assortment of utilizations, for example, intrusion in the network, social insurance, smart urban areas, IoT, misrepresentation recognition, cloud, and considerably more. For instance, a strange traffic design in a system could imply that a hacked system conveys delicate information to an unapproved goal (Habeeb et al., 2019).

2.4 | AI approaches to detect anomalies

Probably the best thing about AI frameworks and ML-based arrangements is that they can learn in a hurry and conveys better and progressively exact outcomes with each cycle. The pipeline of learning procedure is the equivalent for each framework and contains the accompanying

programmed and human-helped stages. The details of the anomaly detection view with the AI approach are depicted in Figure 5. Anomaly detection depends on criteria for detection and approaches to detect an anomaly. Anomaly detection belongs to unsupervised learning, while classification is a part of supervised learning. Classification deals with clusters, and detection deals with the whole data set. In general, an anomaly detection algorithm is assumed to be presented in six domains, namely, threshold-based, statistical-based (outliers and large deviations), nearest-neighbour-based, cluster-based detection, classification-based, and prediction-based anomalies. The basic assumptions associated with each anomaly detection technique are discussed as follows.

1. *Threshold-based*: Such detection techniques presents mathematical relationships among working model and set threshold. If the observed drift is higher than the threshold value, the model tags the behaviour as anomalous. They are simple learning models and consume low computational resources.
2. *Statistical-based*: These models are oriented towards design of models that detect anomalies in test datasets, based on observed deviation patterns in the data. Statistical models are highly skewed towards outlier patterns and tend to have a higher learning rate than threshold-based models.
3. *Nearest-neighbour based*: These models are used to classify abnormal data based on relative similarity indexes, and employ two techniques, the density-based and distance-based detection. The models are trained on the principle that normal data has high density compared to anomalous data patterns.
4. *Cluster-based*: In cluster-based anomaly detection, the results are obtained through unsupervised learning methods. The technique focuses on the specific principle that assumes that maximum samples are normal data in a given population, and only a specific are drifted anomalous data. The models compute the Euclidean, or norm-distance between normal and anomalous data and presents the correlation between the two observed classes.
5. *Classification-based*: In classification-based detection, supervised learning has been used to label the classes as anomalous and normal. However, data labelling and extraction is a fine-art, as incorrect labels reduce the efficiency and accuracy of the model.
6. *Prediction-based*: In prediction-based algorithms, the anomalous classes are compared based on measured data information and the output behaviour, and the algorithm relies on effective pre-training models and are independent of label classification. In the case of AEVs, prediction-based models are a suitable choice as real-time captured data from AEVs are stored in normalized form, which involves cleaning and filling missing attributes in the data. The data, once cleaned, can be used for pre-training purposes, and the accuracy of the model improves as it converges better than cluster-and classification-based approaches.

Based on chosen anomaly detection model, the observed EV sensor specifications might contain both normal and malicious AEVs. The data is normalized into the window boundary and fed to the training model. The features are then extracted from the training sequences, which involves reducing the number of available features and creating new features from present features. The reduced feature set is designed to capture most of the information available with original features. To exploit the same, normally neural nets are designed, employing techniques like stochastic gradient descent and momentum technique at the input layer that consists of the entire feature pool. Then, at the middle layer, the convolutional layer pattern, followed by pooling and softmax layers, will label and extract unique features that correspond to the entire range. Post feature extraction, the data is stored in a feature extraction pool, with specific inputs from label sequences. The anomaly-detection and outlier

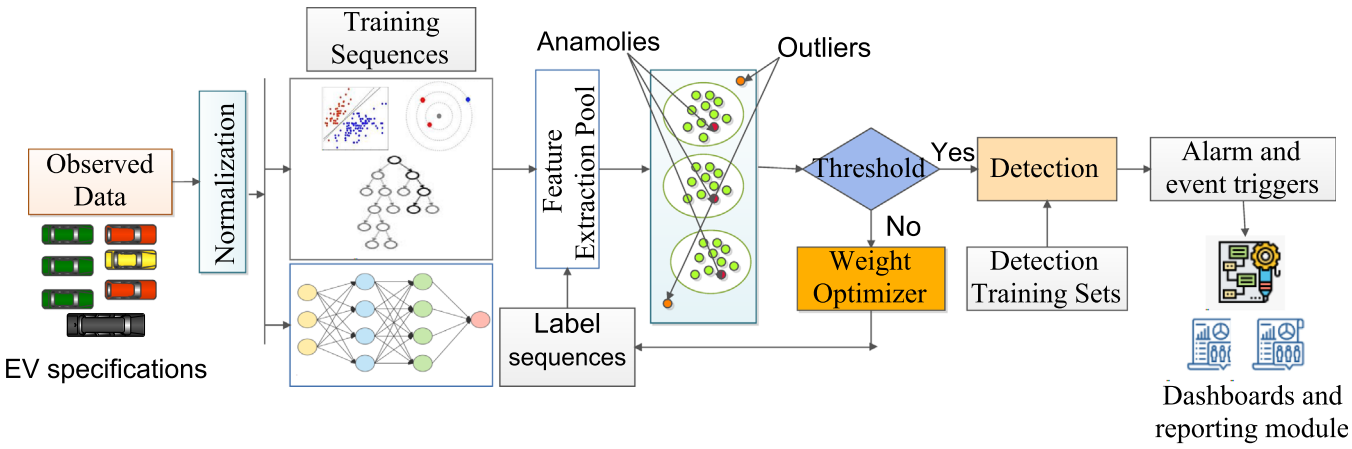

FIGURE 5 A view of anomaly detection using AI techniques

classification models are set up for anomaly and normal classification on the feature pool and presented labelled data. The anomalies are measured as outliers and drifts in data patterns, observed through a threshold value. A weight optimizer presents a feed-backward response that improves the model detection accuracy to optimize the label sequences and improve training rates. If drifts are observed, the AI-based anomaly detection system triggers alarms, and successive reporting is presented to the user. For real-time analytics, a dashboard module is set up to present the drift results through observed plots.

Information models are created dependent on the datasets. A potential peculiarity is raised each time an exchange goes astray from the model. An area master affirms the deviation as an oddity. The framework gains from the activity and expands the information model for future forecasts.

2.5 | Application areas of anomaly detection

Anomaly detection, with its ever-developing interest, has a few applications in wide-running regions. These applications where exception identification is applied are so differing, it is difficult to cover completely in only a single review. So, the authors list and present existing and ongoing application regions in this paper.

1. *Defense and intelligence*: Anomaly detection can be possible in the area of defence and intelligence by doing target detection for defence and military surveillance. It can be done efficiently with help of GUI implementation in which data is collected via sensor.
2. *Fraudulent refunds*: With the help of classification and clustering-based approaches, detecting fraudulent refunds can be possible based on fraudulent activities and transaction refund can be done. K-means is efficient in this case.
3. *Fake news detection*: Anomaly detection can be done by searching words like fake, false, wrong, fake news and some other words proposing individuals are alluding to the news piece as bogus in the case of fake news detection.
4. *Banking Security*: Anomaly detection is useful in Banking security domain to lead business and protect customers as well as organization from potentially wrecking misfortunes.
5. *Medical*: In medicine, Anomaly detection helps by detecting little deviation from normal records or detecting anomalous patient reports which shows sickness flare-ups of patient.
6. *Marketing*: In the area of marketing, Anomaly detection can be helpful by detecting potential security risks at early stage which could put their clients into danger.

3 | REVIEW METHODS AND SOLUTION TAXONOMY

3.1 | Review plan

The presented review starts with exploring and recognizing various research questions (RQ), data sources, anomaly detection tools, search criteria, inclusion and exclusion, quality evaluation, and taxonomy. This survey identified related articles, publications, and various studies. These recognized sources or materials are first checked for their quality, and afterward, just pertinent data is extracted for the given survey.

3.2 | Research questions

This section presents the research questions identified from the existing surveys in the same area and the survey techniques to detect the anomalies. The research questions addressed by this study are as follows.

1. What are AEVs and autonomous AEVs?
2. What is anomaly detection?
3. What are different methods in AI to detect anomalies?
4. What are cyber attacks in the network?
5. How can anomaly detection be carried out in AEVs?
6. How to standardize the anomaly detection techniques to ensure their ease of use?
7. What gives rise to the anomalies and how to identify those?

3.3 | Data sources

Anomaly detection techniques have been applied in various types of data, for example, in ordinary, high-dimensional, streamed, inaccurate, and time-series datasets. In anomaly identification, two types of information are generally thought of and required to assess the exhibition of calculations. They are real-time and manufactured datasets. This present reality datasets can be acquired from freely accessible databases. A few of the datasets, which are used in anomaly detection are as follows.

1. *KDD99 dataset*: This dataset can be used for international knowledge discovery and data mining, bringing the KDD CUP 99 dataset. It establishes the TCPdump data for network congestion. KDD99 generally has five categories of ordinary, DoS, U2R, R2L, and probe. This dataset is highly redundant.
2. *ELKI datasets*: It is a repository that can handle self-assertive dimensionalities and supports uniform and normal distributions. ELKI has an assortment of datasets for anomaly recognition and, furthermore numerous data for OD strategies assessment. These datasets are utilized to examine the presence of a few OD calculations and aspects.
3. *Unsupervised anomaly detection database datasets*: The unsupervised anomaly detection benchmark dataset has been acquired from different sources and is, for the most part, dependent on datasets initially utilized for supervised ML. By distributing these alterations, a correlation of various calculations is currently workable in unsupervised ML for anomaly detection (H. Wang et al., 2019).
4. *ODD*: ODDS gives open access to the whole collection of large datasets related to anomaly detection. Its focus is to provide datasets from various areas and present them under a solitary umbrella for the examination network. ODDS support various kind of datasets such as multidimensional point datasets, time series graph datasets for event detection, time series point datasets for both multivariate as well as univariate kind of data, security datasets like Attack scenario related data, crowded scene video data for anomaly detection (Xiao et al., 2016).
5. *DEFCON datasets*: DEFCON dataset is created in two different adoptions such as DEFCON-8 and DEFCON-10. Anomalies in DEFCON-8 consist mainly of two areas: scanning of ports and overflow of buffer, while DEFCON-10 has mainly two kinds of anomalies: probing and non-probing attacks. Both DEFCON-8 and DEFCON-10 versions are utilized to classifying network anomalies.
6. *UCI benchmark dataset*: The UCI ML repository has several open-access datasets, and numerous object detection strategies utilize the repository to assess the presence of calculations. Most of these datasets are intended for classification strategies. In anomaly detection, the main task is to preprocess the datasets. The anomalies speak to objects in the minor class and all other classes are considered ordinary classes. These datasets are associated with general clustering and classification-related algorithm. These datasets are used in both multivariate and sequential kinds of data (Chandola et al., 2009; Xiao et al., 2016).
7. *TENNESSEE dataset*: In anomaly detection, anomalous tests are either costly to get or hard to describe in these datasets. In this, the ordinary examples can be viewed as positive ones while anomalous tests as negative. At that point, one-class classification can be utilized in anomaly detection. These datasets are normally used with a one-class SVM technique for anomaly detection in AEVs.

3.4 | Anomaly detection tools

Various kinds of tools can be used for anomaly detection and few of them are as follows.

1. *Scikit-learn anomaly detection*: Scikit-learn tool provides an object named *covariance.EllipticEnvelop* for anomaly detection, which uses ML algorithms such as isolation forest with method named as *ensemble.IsolationForest*, local outlier factor (LOF) with method named as *neighbours.LocalOutlierFactor* as well as one-class SVM with method name as *svm.OneClassSVM*.
2. *MATLAB*: It is a user-friendly tool for anomaly detection, which uses ML and DL approaches like one-class SVM, pre-trained AlexNet, and classification.
3. *Rapid Miner*: It uses supervised ML, unsupervised ML, predictive analytics as classification, and association for anomaly detection. Some algorithms such as LOF, COF, LOCI, and LOOP for anomaly detection with Rapid Miner.
4. *Python Outlier Detection (PyOD)*: It is generally utilized for detecting anomalies in multivariate data. It uses algorithms such as angle-based outlier detection (ABOD), k-nearest neighbours detector, isolation forest, histogram-based outlier detection, local correlation integral (LOCI), feature bagging, clustering-based local outlier factor technique.

3.5 | Search criteria

In this criteria, the search begins with the keyword "anomaly detection in electric vehicles" and other keywords as shown in Figure 6. Numerous review papers have not been found by considering the mentioned search string, as it may be possible that the search string is not present either

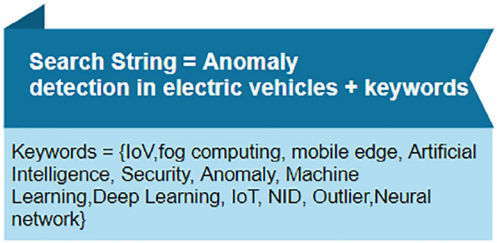

FIGURE 6 Search keywords used to identify relevant literature

in abstract or title. To distinguish such papers, the manual search procedure has been accomplished to identify relevant papers with given keywords in the digital sources such as IEEEXplore, Science Direct, Springer, and Wiley.

3.6 | Inclusion and exclusion

The issue of anomalies, outliers, attacks, etc., are present in various application domains such as video surveillance, SG, transportation, and power grid. Therefore the search string "anomaly detection in electric vehicles" retrieved many irrelevant papers also. At that point, filtration is required based on some inclusion–exclusion parameters such as citations, views, Scopus index, and many more. The review articles, relevant papers, websites, reports, and other resources are also incorporated for more extensive inclusion.

3.7 | Taxonomy

Based on the collected literature and survey methodology, the authors presented a taxonomy of anomaly detection approaches which can be broadly classified into network-based detection (Section 4), AI-based detection (Section 5), security-based detection (Section 6), and it has been shown in Figure 7 in this section. These categories focus on the different methods to detect anomalies in autonomous AEVs. AI plays a vital role in detecting an anomaly in AEVs, so it is discussed in AI-based approaches, mainly classified into DL, ML, and RL and their further classification as shown in the AI-based approach section (Section 5). Then, network-based classification is classified into the centralized and distributed part, which contains cutting-edge technologies such as IoT, cloud, SDN, fog, and edge (Prasad et al., 2019). A detailed description of each existing approach of anomaly detection is discussed in the following sections.

4 | NETWORK-BASED ANOMALY DETECTION

In the current era, network anomaly detection systems (NADSs) are an extensive and widely studied research area. This system combines centralized and distributed approaches of anomaly detection for detecting cyber intrusions in AEVs. Any unwanted or illegal pursuit in a network can be an intrusion. This is also called the attack on the network. These types of attacks are divided into two parts, active and passive attacks. Passive attacks affect the confidentiality of the network, but they do not infringe the system's state. Passive attacks have a comparatively small likelihood of attack detection. Both passive and active scanning is classified as passive attacks. Here the intruder does not truly interact with the system to obtain the required target system data, while in active recognition, an attacker usually performs a port scan. Passive attacks can include social engineering, eavesdropping, analyzing traffic, and port scanning (Taj et al., 2020).

Active attacks infringe the network's confidentiality, integrity, and accessibility. Here, the associate degree interloper attempts to vary target information or info that's en-routing to the targeted system. Associate degree IDS gathers and examines the knowledge from a computer system continuously to observe intrusions. IDS have two main types operating with analyzed data: NIDS and HIDS (Taj et al., 2020). Active attacks violate the network's confidentiality, integrity, and accessibility, therefore ever-changing the targeted system. NIDS examines and verifies network traffic on each layer of the stack for Open Systems Interconnection. It additionally decides and analyzes the planned purpose of traffic for untrusted activities. Both HIDSs and NIDSs can scan traffic at the same time from many devices. NIDS scans the network-wide passing traffic against the threats. If an Associate in Nursing attack is recognized or any uncommon conduct is detected Associate in the Nursing alert is created. Although NIDS scans all departing and inward traffic that would sometimes generate a bottleneck moving the speed of network (Taj et al., 2020).

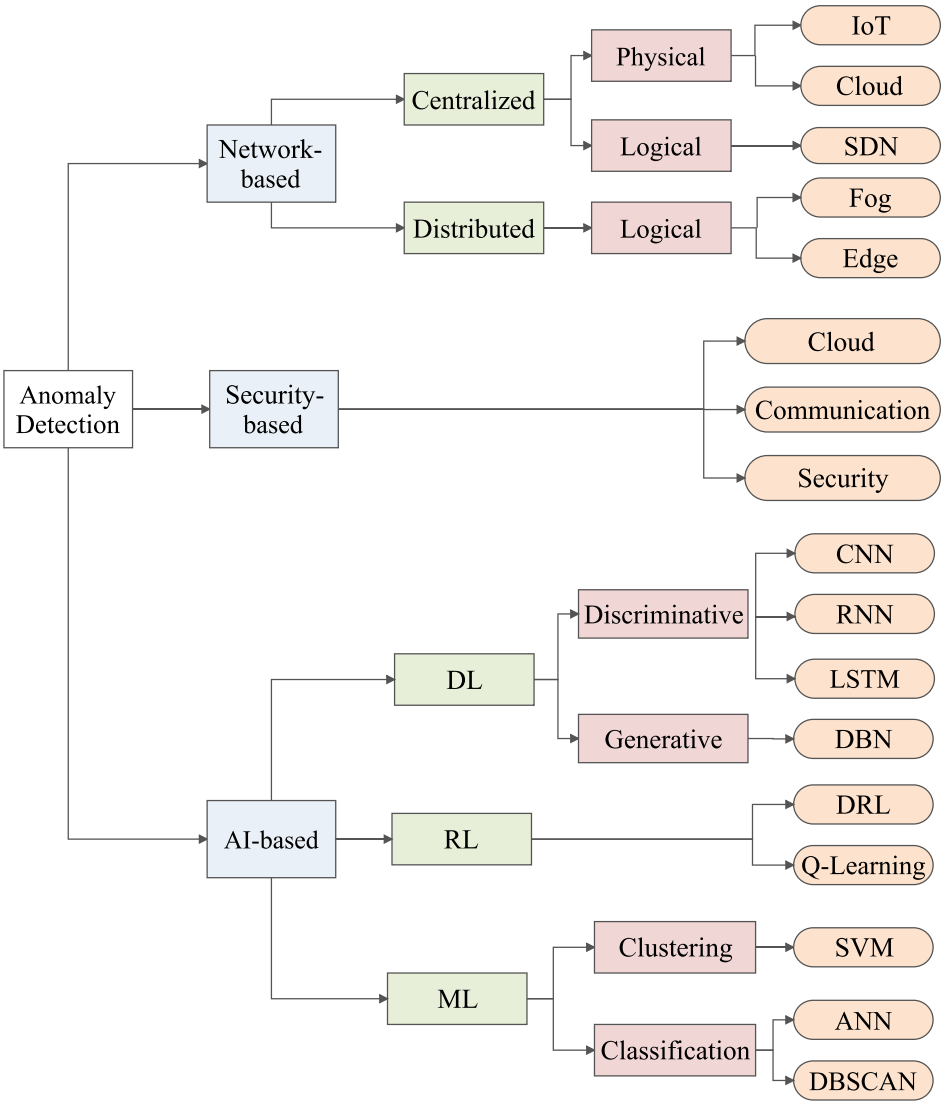

FIGURE 7 Solution taxonomy for anomaly detection

Anomaly-Based IDS uses system features and networks to predict the network-related typical activities. Here, the activities that diversify from the typical and conventional network patterns of traffic would be considered an attack. This IDSs help in revealing intrusive attacks and abnormal operations related to information systems and in a technological environment, which is constantly in evolution. The core objective remains unchanged for identifying the real attacks correctly. Identifying non-attacks adversely and thus, it is an efficient approach to identifying and reacting to malicious networking and computing environments. The conventional signature-based strategy depends on predefined signatures for detecting attacks, whereas anomaly-based IDS do not follow another approach, which helps identify novel attacks. Though, these are having a downside of few amounts of elevations in FP rate, which categorizes valid traffic as attacks. So, a comprehensive review is required to determine the traffic and attack precisely. Therefore, anomaly-based IDS should be implemented with immense research and effective knowledge (Taj et al., 2020). Table 5 shows the comparative analysis of various network-based anomaly detection schemes.

4.1 | Centralized detection

A type of network where all users connect to a central server, which is the acting agent for all communications and handles all the major processing solely. Main components of a Centralized System are (i) node (e.g., Computer and Mobile), (ii) server and (iii) communication link (e.g., Cables and Wi-Fi). The detection can be physical or logical, which are explained as follows.

TABLE 5 Network-based anomaly detection

Paper	Year	IoT	Cloud	SDN	Edge	Fog
(Lee et al., 2011)	2011		Yes			
(Aujla et al., 2016)	2016			Yes		
(Nafi et al., 2016)	2016			Yes		
(Mao et al., 2017)	2017	Yes	Yes		Yes	
(Moustafa et al., 2019)	2018	Yes	Yes		Yes	Yes
(S. Wang et al., 2018)	2018			Yes		
(Hussain et al., 2019a)	2019				Yes	
(Hussain, Du, Imran, et al., 2019)	2019				Yes	
(Ayad et al., 2019)	2019	Yes				
(Moustafa et al., 2019)	2019	Yes	Yes		Yes	Yes
(Taj et al., 2020)	2020		Yes			
(Pacheco et al., 2020)	2020	Yes				Yes
(Al-Garadi et al., 2020)	2020	Yes	Yes			

4.1.1 | Physical detection

1. *Internet-of-Things (IoT)*: It is deployed to secure different applications based on the convergence of smart devices and the Internet. An IoT-enabled IDS should help identify abnormal and suspicious behaviours from physical devices such as sensors and actuators, which are communicating with the Internet. Post-processing techniques play an important role in IoT networks as effective measures can be taken to curb the incorrect alarm rates and help in effective visualization of the network data. In a nutshell, the new NIDSs should be programmed, adapted, and maintained without the extensive need for human interaction (Moustafa et al., 2019).
2. *Cloud-based*: A Cloud is Important for firms that shift workloads and services to public Cloud paradigms such as Amazon Web Services and Microsoft Azure to hedge models of platforms, software, and infrastructures. Existing NIDs are inefficient in detecting and responding to internal malicious activities and they also prove wrong while protecting cloud computing and mobile cloud computing. Internal malicious activities are complex and contain remotely located modules; hence, detecting them is a challenging task. More than that, many virtual machines could be destroyed at data centers of the cloud, tracking normal attack events demand scalable and collaborative IDSs (Moustafa et al., 2019).

4.1.2 | Logical detection

1. *Software-Defined Network (SDN)*: Within the network field, SDN is the most famous and optimistic approach to detect the anomaly. There are some challenges in current hardware-centric networking in terms of innovation and cost. By proposing SDN, overcome of these challenges is possible. It is a fledgling network scenario that breaks down in 3 categories: application, control plane, and data plane (S. Wang et al., 2018). Applications coordinate with a controller at the control plane by means of a northbound interface, while the controller utilizes the southbound interface of the switch for connecting to the data plane. SDN separates the control plane and data plane or logical control and data forwarding to achieve security and resolve the prevailing rigid network system. This rigidity happens due to some protocols, which affects the speed of the network by reducing it. By separating of control plane and data plane, a simple network switch will turn into a forwarding device. SDN is used to combine some cutting-edge technologies such as fog, cloud, big data, edge, and IoT (Farhady et al., 2015).

4.2 | Distributed detection

It is a network that distributes its workload among all the machines present in the network instead of relying on a single centralized server. In this, each node is independent of the other. The components of a decentralized system are nodes and communication links. The anomaly detection in the decentralized system logical, which is further classified into fog and edge. A detailed explanation about the above-mentioned classifications is as follows.

4.2.1 | Logical detection

1. *Edge and Fog-based*: According to Moore's law, a huge number of edge-based devices, along with the extremely high speed in the processor context, will be deployed soon. Nowadays, technology is evolving from centralized mobile computing to mobile edge computing for better reliability (Mao et al., 2017). Mobile edge computing (MEC) is working upon the principle of decentralized systems, network control, and storage. It focuses on executing intensive computation and allows applications at mobile phones, which is critical in the context of latency by collecting the tremendous amount of inactive computation energy and storage space. Due to this, there is an extremely reduction possible in latency and energy consumption (M. Patel et al., 2014). It is located at the edge server. It can detect anomalies with an accuracy ratio between 70% to 96% (Hussain, Du, Zhang, et al., 2019). It is efficient enough with a high rate of accuracy and low rate of FPR to detect anomalies. It is more suitable to detect instant anomaly than long-term anomaly. IDs are usually deployed and executed at the users' proximity or at the network edge to protect and secure the sensitive information/data shared over smartphones, computers, and network systems. In the scenario where the IDSs are employed at the network edges and data security, this option also aids in addressing the various challenges which cloud architecture possesses, such as the processing of large-scale networks, geographic distribution, and high mobility and low-latency. It is important to note that edge architecture in deployment is not an alternative to cloud architecture, but it benefits to cope with the cloud challenges. These architectures adhere to smart data management and a scalable approach towards the NIDS that can grow along with the real-time requirements and in times of suspicious events. Regardless of the many challenges edge computing environment compared to the centralized systems, it is still better in terms of the aforementioned benefits. Integration of heterogeneous service infrastructures and the requirement of synchronizing soft and hard states of multi-tiered architecture possess several issues that need to be looked upon. Distributed norms also involve developing various standards that mention the integration of different infrastructure elements and how the virtual machines can access data/information related to context as well as host (Moustafa et al., 2019).
   Fog Computing extends the Cloud computing paradigm to the edge of the computational network, enabling a wide range of applications and services that exhibit lower latency, better awareness for location services, mobility, and elasticity. Fog computing has been seen to be effective in supporting IoT applications that require predictable latency.

5 | AI-BASED ANOMALY DETECTION

A significant level of clarification on how AI helps to detect anomalies is presented in the following subsections. Table 6 shows the comparative analysis of various existing AI-based anomaly detection schemes.

5.1 | Machine learning

This subsection discusses the classification and clustering-based anomaly detection. The details are now presented in subsections as follows.

5.1.1 | Classification-based

Classification is a two-step process such as training and testing. Generally, classification is utilized to gain proficiency with a model from a collection of labelled data (considered as training dataset) and classify the new data into one of the class labels, also called a testing dataset (Chandola et al., 2009; Sheth et al., 2020). The testing data which does not belong to any of the class labels is considered as an outlier.

1. *Support Vector Machine (SVM)*: SVMs are familiar with the domain containing ordinary occasions utilizing a single class learning technique (Issa & Vasarhelyi, 2011). It is generally used in one class to detect the anomaly. This kind of strategy utilizes one class learning procedure for SVM and gets familiar with an area that comprises the training data (Chandola et al., 2009). For each test data, the essential procedure decides whether the test data falls inside the specified area or not. If a test data falls inside that region, it is considered normal data, and if not falls under that region, it will be considered an outlier (Vapnik, 2013).

5.1.2 | Clustering-based

The measure to detect anomaly depends on the non-part of a data point in any particular cluster, how far or how near from other clusters, and the size of the nearest cluster. The clustering problem correlates with the anomaly detection issue, in which focus either has a place with groups

TABLE 6 AI-based anomaly detection techniques

Paper	Year	Dataset	SVM	ANN	Density based
(Hodge & Austin, 2004)	2004				Yes
(Chandola et al., 2009)	2009		Yes	Yes	Yes
(Gogoi et al., 2011)	2011				Yes
(Jyothsna et al., 2011)	2011		Yes	Yes	
(Zhang, 2013)	2013				Yes
(Xiao et al., 2016)	2016	Yes	Yes		
(Habeeb et al., 2019)	2018		Yes		
(Koustubh et al., 2018)	2018	Yes		Yes	
(Avatefipour et al., 2019)	2019	Yes	Yes		
(H. Wang et al., 2019)	2019	Yes			Yes
(Khan et al., 2019)	2019		Yes		
(Pacheco et al., 2020)	2020			Yes	
Proposed	2021	Yes	Yes	Yes	Yes

or anomalies. Many clustering approaches are present, and few are given as ANN and DBSCAN (Aggarwal, 2013). The most popular unsupervised learning technique is clustering, which works by grouping the data points based on maximum group similarity or distance from other data points. The common procedure for this technique is to choose a representative (or data point) for each group and the new data point is being classified as a member of one of the groups based on the proximity from the representative data point (Tanwar et al., 2020). There can be cases where few data points may not be classified as members of any group and hence, they are termed as outliers, which in turn help us to identify the anomalies from all the data points. Occurrence of intrusion events from raw audit data is clearly observed with this clustering technique and due to which, the efforts needed to tune the IDS is henceforth reduced (Garcia-Teodoro et al., 2009). The description of clustering algorithms is as follows.

1. *Artificial Neural Network (ANN)*: Neural systems are multi-class order methods that comprise of two stages. The initial stage is to prepare a neural system on the named information occasions and becomes familiar with the typical classes, and afterward, new cases are presented. In any case, the occurrence is dismissed by the neural system, then it is named anomaly (Issa & Vasarhelyi, 2011).
2. *Density-based spatial clustering of applications with noise (DBSCAN)*: This clustering algorithm ends up being generally exact in identifying the inconsistencies in this specific framework. It is an incredible, notable calculation in the fields of information mining and AI. DBSCAN is a clustering algorithm based on data densities. To characterize a local density, the number of points inside a predefined specified region of a given data point is utilized (Aggarwal, 2013). This density-based algorithm does partitions of the given data space. The logic behind this is to make the clusters of those points closer to the minimum neighbours and identify those points that do not belong to any clusters and name it as anomalies. Inputs to this algorithm are minimum points and maximum distance. It distinguishes high-density areas which are isolated by low-density regions. It works on three types of points. *Core point*: If the number of points within that particular radius area is greater than a predefined threshold value and has at least minimum points in its radius. *Border point*: It is a point that is not a core point and is within that Epsilon of a core point. *Noise points*: It is a point which is neither core nor the border point (Issa & Vasarhelyi, 2011).

5.2 | Deep learning

With the advent of DL algorithms, various achievements in terms of results have been observed. The state-of-the-art architectures have used supervised as well as unsupervised learning. The usage of commonly known multilayer perceptron through an unsupervised way, mainly the higher-level representations being expressed in simple ones. Different types of neural networks have been found in use, some of them are CNN, DBN, stacked autoencoders (SAE), LSTM (Kumari et al., 2020). These algorithms possess inherent characteristics and they are used for different classification problems. For few decades, there has been a consistent amount of research in computer networks, especially in anomaly detection. Numerous researchers have followed different approaches, but DL perception has been in focus for the last few years (Maimó et al., 2018). Table 7 shows the comparative analysis of various state-of-the-art DL-based anomaly detection schemes with respect to the proposed survey. The description of such supervised and unsupervised learning is as follows in terms of generative and discriminative methods.

TABLE 7 Comparative analysis of various state-of-the-art DL-based anomaly detection schemes with respect to the proposed survey

Paper	Year	CNN	RNN	LSTM	DBN	OC-NN	DHM
(Rodriguez et al., 1999)	1999		Yes				
(Guo et al., 2010)	2010		Yes				
(Krizhevsky et al., 2012)	2012	Yes					
(Erfani et al., 2016)	2016				Yes		
(Nadeem et al., 2016)	2016				Yes		
(Alrawashdeh & Purdy, 2016)	2016				Yes		
(Kwon et al., 2017)	2017		Yes		Yes		
(Yu et al., 2017)	2017	Yes					
(Z. Zhao et al., 2017)	2017			Yes			
(Ergen et al., 2017)	2017			Yes			
(Du et al., 2017)	2017			Yes			
(Vinayakumar et al., 2017)	2017	Yes	Yes	Yes			
(Yin et al., 2017)	2017		Yes				
(Van et al., 2017)	2017				Yes		
(Hundman et al., 2018)	2018			Yes			
(Sugimoto et al., 2018)	2018			Yes			
(Park et al., 2018)	2018			Yes			
(Chawla et al., 2018)	2018	Yes	Yes				
(R. Zhao et al., 2019)	2019	Yes	Yes	Yes	Yes		
(Racki et al., 2018)	2018	Yes					
(Miglani & Kumar, 2019)	2019	Yes	Yes	Yes	Yes		
(Chalapathy et al., 2018)	2019					Yes	
(H. Wang et al., 2019)	2019	Yes			Yes	Yes	Yes
(Ferrag et al., 2020)	2020	Yes	Yes		Yes		
The proposed	2021	Yes	Yes	Yes	Yes	Yes	Yes

5.2.1 | Generative

Generative (or unsupervised) DL architectures can learn automatically from unlabelled raw data to accomplish different tasks. The description of a few of the generative algorithms is as follows.

1. *Deep belief network*: It is a neural network model which contains many hidden layers. It is a composition of stacked multiple RBMs prepared in a layer-wise manner (Aldweesh et al., 2020). These machines are the system of neuron units that are evenly associated. These neurons are settling on choices about whether it's on or off. DBN is a combination of both supervised and unsupervised learning methods. In unsupervised learning, the model is learned in a layered manner connection at once and in supervised learning, it can connect one or more layers at a time for classifying objects (Moustafa et al., 2019).
   The DBN adapts continuously by changing loads with the back-propagation calculation. Its working includes ascertaining the input for every neuron unit initially and this input is the summation of multiplication of all inputs with its corresponding weights (Nadeem et al., 2016). From that point onward, the output of each neuron is determined by utilizing a logistic function. At that point, the error is determined for every neuron. At last, the weights of neurons will be updated. Moreover, DBN is best suitable for dimensionality reduction along with independent classifier at the time of discrimination layer inclusion. Once the pre-training is over, the various aspects of this method can be further tweaked as an intermediary for the DBN log-probability (R. Zhao et al., 2019).

5.2.2 | Discriminative

This approach deals with the labelled dataset for supervised learning to distinguish the patterns for the prediction tasks.

- *Convolutional neural network*: It was used for the purpose of image processing in the initial phase and additionally has been acquainted with natural language processing and speech recognition (R. Zhao et al., 2019). CNN is a multiperceptron ANN, which is motivated by the association of creature visual cortex. It is acquainted to deal with connection among DNN layers. Structure of CNN includes many hidden layers, which comprises of convolutional layer, pooling layers followed by the fully connected layer (Aldweesh et al., 2020). CNN train numerous layers at the output layer to classify high-dimensional data into a collection of classes. The main benefit of CNN is it distributes many weights which contain fewer parameters. Due to this feature, the training process of the CNN model becomes relatively easy with a similar number of hidden layers among all other models. Moreover, a CNN is good to compare to other DL models in the context of required parameters. It uses fewer parameters compare to others with the same depth of other network models. The benefit of this is the complexity reduction and making the learning process of the model faster. CNN is well-suited for handling complex data and due to this, it is helpful for feature extracting as well as classifying the data for anomaly detection.
- *Long short term memory*: Compared to DNN and early RNNs, LSTMs have been appeared to improve the capacity to keep up the memory of long-term dependencies of the feature of a self-loop moulded on setting that permits them to overlook past data notwithstanding collecting it. It is a special type of RNN, which specifically recollect the designs for quite a long term (Miglani & Kumar, 2019). It can deal with time-series data for both the long and short term. It resolves the vanishing gradient problem of RNN (Tian & Pan, 2015). LSTM can handle data such as sequential, temporal, and data with high-complexity (Hundman et al., 2018). It is useful in applications such as text classification, natural language processing, speech recognition, and time series forecasting. In addition, LSTM can be utilized with both supervised and unsupervised learning (Maimó et al., 2018).
- *Recurrent neural network*: It is a feed-forward neural network, which is dynamic. It is suitable well for both supervised as well as unsupervised learning methods. In RNN, the data is associated in a long sequence in a layered manner and the feedback loop is connected to it, which passes the output back to a similar unit related to the following timestamp. There is a cycle between those layers that gives direction and useful for high reliability with the capacity to make an inward memory for logging information of the past data. It is recognized by its capacity to learn consecutive information over timestamps. The configuration of such a neural network is that the output of each unit relies on the present input (Aldweesh et al., 2020). There is no reliance among the present input and previous output of a similar unit. There are two subtypes of RNNs, which are LSTM and GRU (Yin et al., 2017). The RNN model has a single direction stream of data from the input layer to the hidden layer and the combination of the single direction data stream from the previous input to the target output.

5.3 | Reinforcement learning

Now a days, the RL based anomaly detection has emerged as one of the heavily used control strategies for HEV. In general, its strategies relies on the enhanced parameter determinations. Here, the authors discuss the Q-learning and DRL algorithms of RL. Figure 8 shows the graphical view of the working of RL.

5.3.1 | Q-learning

It is a model-free RL technique that learns the state activity esteem work through an association with some conditions. It is famous for its bootstrapping attributes and its strategy does not require any control-arranged model, which stays away from the demonstrating exertion (Xu et al., 2020). Generally, this algorithm changes its state-action value function depends on the predefined estimated state-action value function.

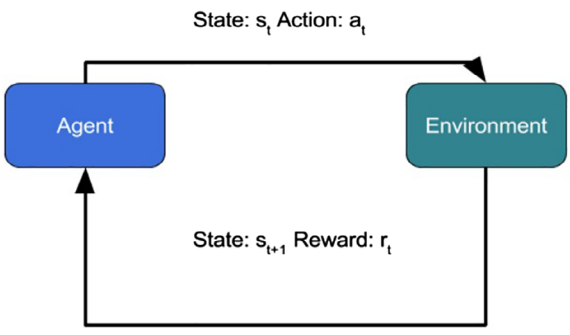

FIGURE 8 Graphical view of RL

5.3.2 | Deep reinforcement learning (DRL)

DRL structure is exceptionally adaptable for enormous state space, which is different from conventional RL. Due to light-weight and less power consumption, DRL is most popular nowadays in the area of RL. Basically DRL is made by integration of reinforcement and deep learning. It is focused on high-dimensional data. It is mainly classified into two phases that are deep Q-learning which is online and the other is a DNN that is offline (Mnih et al., 2013). DNN is received to determine the relationship between each state-activity pair (s, a) of the framework and its value function is Q(s, a) in the offline phase. In this value function, the system begins at state s and it will follow the action along with some fixed strategy from that point. It will get a reward after that. The DRL structure requires a moderately low-dimensional activity space because of the way that at every choice epoch the DRL agent needs to identify all potential activities under present status and perform induction utilizing DNN to determine the ideal Q(s, a) value function.

Table 8 presents the pros and cons of the various AI-based methods for anomaly detection.

6 | SECURITY BASED ANOMALY DETECTION

6.1 | Sensing

It is a layer vulnerable to spoofing and eavesdropping attacks on vehicle sensors, such as inertial or radar sensors. LiDAR/camera, RADAR/Ultrasonic Sensor, GPS/TPMS, and Gyroscopic sensors/countermeasures (El-Rewini et al., 2020).

6.2 | Communication

There are two types of communications in the context of vehicles, which are inter-vehicular and intra-vehicular communications (Tanwar et al., 2018). They both are susceptible to eavesdropping attacks. The communication layer is also at risk of threats that propagate upward from the sensing layer, formed of vehicular sensors (El-Rewini et al., 2020). These vehicular communications take place either in internal mode or external mode between vehicles. Internal mode of vehicle communication happens in the case of the intra-vehicle network. It refers to the communication of ECUs within the system itself. In the case of external vehicular communication, communication happens when a direct connection is established between the vehicles and USBs as well as maintenance tools.

6.3 | Control

A control layer describes the automated vehicular control techniques, such as vehicle speed and steering control (El-Rewini et al., 2020).

TABLE 8 Advantages and disadvantages of AI methods

Method	Advantages	Disadvantages
CNN	Computationally efficient	Requires huge amount of training data
RNN	well-suited for dynamic models	Vanishing Gradient problem, not able to process very long sequence with tanh AF
LSTM	Sufficient for noisy and distributed data	slower than AF like sigmoid, tanh or rectified linear unit
DBN	Sufficient use of hidden layers	Cost inefficient in training a model
ANN	well-suited for parallel multitasks and for non-linear approximation	Not sufficient for solving complex problem
DBSCAN	sufficient for arbitrary shapes and supports in outlier detection	Not compatible with very sparse dataset
SVM	supports high dimensional and unstructured data using Kernel trick	Inefficient for Selection of kernel function to handle unstructured data, high memory consuming
DRL	Suitable for correcting an errors propagated during training phase	Not efficient for large amount of data
Q-Learning	Efficient for less amount of data,	Slower with less rewards at initial states

7 | EVALUATION METRICS

The assessment models rely upon evaluating a confusing matrix as a classification issue. The reason for designing the confusion matrix is to analyze both actual and predicted values. In this case, the confusion matrix is defined by a 2×2 confusion matrix. The terms TP and TN indicate effectively anticipated conditions and FP and FN misclassified ones (Moustafa et al., 2019).

The TP values denote the correctly rejected data points, such as the records that are actually an anomaly and detected as an anomaly. On the contrary, FP are the records that are not an anomaly and are also predicted correctly. The TN are those records of the data set that are actually an anomaly but are predicted as an anomaly. In contrast, the FN shows the records of the anomaly records' dataset but are identified as normal (Moustafa et al., 2019).

1. *Accuracy*
   a. Accuracy refers to the closeness of a measured incentive to a norm or illustrious value. Accuracy = (TN + TP)/(TP + FP + TN + FN) could be a metric that estimates the general percentages of detection associate degree false alarms an IDS model produces, that the general success rate of any IDS, and is computed as: Moustafa et al. (2019)
2. *Precision*
   a. Precision deal with the fraction of relevant instances from the total retrieved instances. Precision = TP / (TP + FP)
3. *TNR*
   a. The TNR likewise called the specificity, is the level of effectively classified ordinary examples of the absolute number of typical vectors. TNR = TN/(TN + FP)
4. *FPR*
   a. FPR is the percentage of normal vectors of the total number of normal vectors misclassified as attacks. FPR = FP/(FP + TN)
5. *FNR*
   a. FNR is the percentage of misclassified attack vectors of the total number of attack instances. FNR = FN/(FN + TP)

8 | OPEN ISSUES AND CHALLENGES

TP anomaly detection techniques are constantly updating nowadays with an objective to make the system secure as well as error-free (Garcia-Teodoro et al., 2009). Though these techniques are of promising nature, yet there exist few significant challenges with regard to anomaly detection. Figure 9 shows the vital research challenges and open issues with regard to anomaly detection.

1. *In-vehicle security*:
   a. In-vehicle security is still a major issue for autonomous AEVs. A vehicle hacking test shows that autonomous AEVs can be effectively remotely controlled by portable applications for various controls. Furthermore, the battery state, area, and other private readings of the vehicle could be acquired by aggressors. Future research should concentrate on shielding AV in-vehicle frameworks from outside frauds.
2. *Data accessibility*:
   a. A typical challenge is the procurement of applicable information. Likewise, this is confinement concerning the accessibility, quality, and organization of the current information impact the presentation of AI calculations. A typical test is the high-dimensionality of the accessible information that contains unimportant and excess data that can affect the arrangement's presentation. Besides, securing a piece of typical preparing information can be troublesome and regardless of whether it is acquired, almost certainly, it may not represent all deviations during activity.
3. *Computational cost*:
   a. Various examinations have concentrated on blending or fusing a few procedures to build the presentation of anomaly discovery, which prompts increment in calculation cost. In this, the utilization of large information alongside the cloud will address the computational cost issue by fusing equal and disseminated preparing, which assists with building various bunches prompting minimization of the calculation cost. The large-scale manufacturing of high chips and processors has to lessen their expenses. Subsequently, usage of this equipment will build the intensity of frameworks that continuously prepare an immense volume of information, bringing about decreasing in computational expense.
4. *Algorithm choice*:
   a. This impacts the capacity to characterize different deficiencies and disappointment modes utilizing AI procedures. Since deficiencies are uncommon, information is costly and regularly different. There is a requirement for melding data from a wide range of viewpoints, including natural history, equipment, programming, and execution, to show antecedents and underlying drivers. As information is delivered in high volumes, scale, and extension, this requires strategies to automate deficiency arrangements.

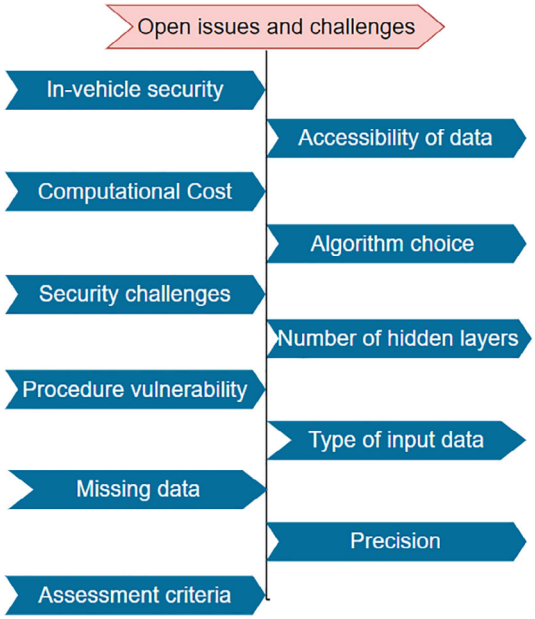

FIGURE 9 Open issues and challenges

5. *Security challenges*:
   a. Flexible associations in brilliant urban areas offer assistance to AEVs and yet present more difficulties. Guaranteeing V2X correspondence security is critical because assaults on AVs could spread to savvy foundations and the other way around. For instance, an assault on the autonomous AEVs could spread to the force matrix foundation through the electric energizing hardware to the utility framework (Cui et al., 2019). Creating secure correspondences and safeguard systems are instances of future research here.
6. *Number of hidden layers*:
   a. The inclusion of too many neurons in the hidden layers may result in overfitting. As well as the use of more hidden layers may result in backpropagation and dimensionality issues. Backpropagated errors drastically decrease after few layers.
7. *Procedure vulnerability*:
   a. Since broken information is uncommon and costly to mark, there is a need to quantify the precision of the outcomes. Contingent upon the conveyance/fluctuation, the computational cost will be enormous. This shows the requirement for researching factual methodologies, for example, Naïve Bayesian, to pick up knowledge on ambiguities associated with the procedure. There will consistently be some vulnerability in the prepared models themselves, the vulnerability in the subsystem, prerequisite definitions, and vulnerabilities in the earth. Further, it is imperative to distinguish the different kinds and manage their belongings separately.
8. *Input data type*:
   a. In a part of any model assembled, the first thing is to investigate the idea of input information. They have different qualities for every data instance, such as factor, attributes, field, and measurement. Every data instance generally falls under the classification of either univariate or multivariate (Habeeb et al., 2019). The differing idea of information makes the abnormality location procedures battle in choosing proper calculation to deal with that specific information. Essentially, anomaly detection strategies will differ depending on the nature of the qualities in that application (Chandola et al., 2009). These issues will be tended to by creating crossover solo AI calculation.
9. *Missing data*:
   a. Sorts of information gathered from different conveyed sensors by means of a correspondence channel incorporate commotion and missing qualities because of the approaching velocity of information (Chandola et al., 2009). Missing data can create high probabilities for raising the bogus positive caution in anomaly detection. An immense amount of random highlights produce clamour in the info information, which sidestep the genuine inconsistencies (Erfani et al., 2016). These issues will be tended to by joining the auto commotion cleaning module in the location system.
10. *Precision*:
    a. Even though the current advances are fit for anomaly detection, the reliance on the result is inconsistent because of the exactness issues. Sometimes, better exactness is delivered at the expense of high computational handling and time (Habeeb et al., 2019). This issue will be tended to by joining continuous large information advancements with hybrid AI calculations, which rise as a meta-learning apparatus to precisely investigate the huge volume of information produced by present-day applications, with less memory and force utilization.

11. *Assessment criteria*:
    a. Given the above challenges, it is critical to assess the answer for quantifiable presentation measurements, for example, runtime execution, recognition rate, adaptability, and so forth (Khan et al., 2019). This brings up a significant issue about how to do quality affirmation of AI arrangements where factors, for example, information quality, highlights, and the calculation pipeline and framework, regularly shift.

9 | WEIGHTED ENSEMBLE CLASSIFIER FOR EV ANOMALY DETECTION: A CASE STUDY

The section presents a case study on anomaly detection of EV based on a multi-stage ensemble with a proposed attention mechanism that couples convolution neural networks (CNN) and long-short term memory (LSTM) to detect real-time sensor anomalies in networked EV communication in IoV ecosystems. The case study is based on findings by Javed et al. (2020), that presents the raised anomalies in AEVs based on real-time sensor measurements. As sensor data are exchanged through open channels, they are subjected to propagation errors caused via channel noise, faulty signals, and injected attack vectors by malicious entities that disrupt propagation updates among EV nodes in IoV might result in accidents, and congested routes. The framed attacks might disrupt the functioning of AEVs and effect controls such as brakes, accelerator, and induce faults in the controller area network (CAN) bus, that hinders the communication with IoV networks. The authors present a multi-stage anomaly detection method with the fusion of CNN and LSTM to handle and process the raised anomalies. As a working principle, the real-time sensor data is streamed and collected in raw data files. The files are then processed in vector form and passed as reading inputs to the sensor processing units (SPUs). The data is then pre-processed, and drift measurements are recorded. A weighted-fine tuning method is proposed based on averaged values obtained from different classifier probabilities to detect anomalies and optimize the ensemble's performance. The details of the case study are presented in Figure 10. The authors now present the schematics of the scheme in the following subsections.

9.1 | Case-study objectives

The proposed case-study presents a scheme with the following objectives.

1. Weight-based coupling of LSTM and CNN is proposed, where LSTM handles a multi-stage attention module, and CNN weights are fine-tuned to detect anomalies in sensor readings highlighted through the attention module of LSTM.
2. For fine-tuning distinct classifiers, a weighted ensemble is proposed that adjusts and equalizes weights, detects anomalies from multiple input streams of captured data, and assigns a vote-based weight to class predictors, and detects the anomalous behaviours of multiple EV users.
3. The considered data-set is from van Wyk et al. (2020), that considers research data from safe pilot deployments SPMD dataset (Safety Pilot Model Deployment Test Conductor Team Report, 2015). To build the dataset, vehicular data is recorded every 100 ms for 2500 vehicular nodes.

9.2 | Network model

The case study considers a IoV sensor network that generates sensor readings from n nodes, deployed on AEVs. The generated readings from n nodes, $\{R_1, R_2, ..., R_n\}$ are arranged in matrix form $M\ p \times q$, where any R_i is represented as tuple information. Based on M, a set of target class T_r

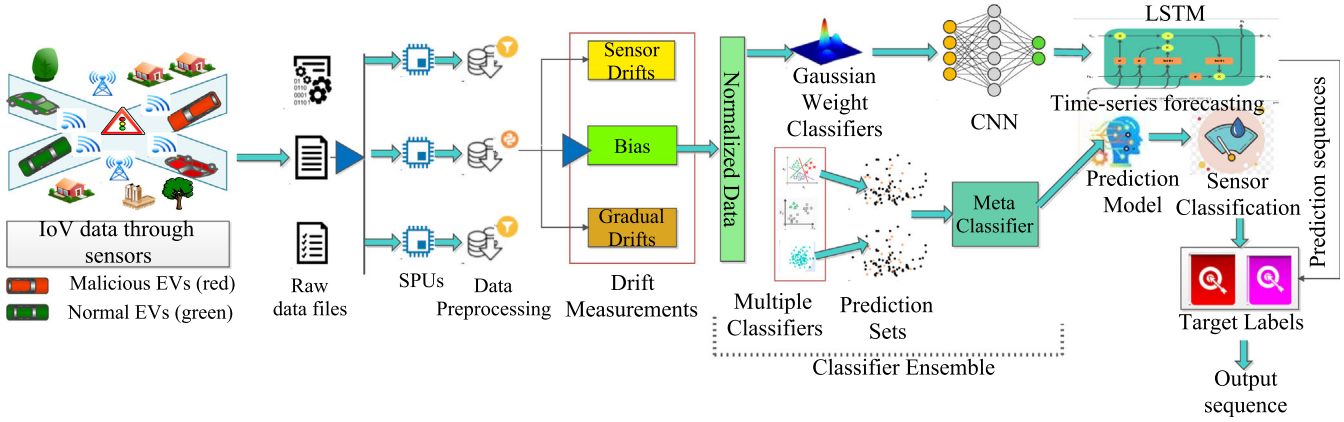

FIGURE 10 Case study of weighted ensemble classifier (Javed et al., 2020)

is defined for sensor readings as {*N*, *I*, *C*, *GD*, *BA*}, where *N* denotes normal, *I* denotes instant *C* represents constant, *GD* denotes gradual drift, and *BA* denotes the bias classes respectively. on T_r, a prediction model is executed that highlights the labels *L* for any mapped target class T_r. A feature matrix *FM* is built on *L* based on labelled instances L_i. On *F*, a normalized scaled feature matrix is computed, denotes as N_F, that scales the features to a maximum and minimum window W_{max}, and W_{min} respectively.

The prediction model N_F considers three features on SPMD dataset of interest obtained from sensors as *speed*, *GPS speed*, and *acceleration*. On these values, anomalous values are added in the dataset to denote {*I*, *C*, *GD*, *BA*} drifts. *I* represents a sudden jump in values of two successive readings R_j, and R_{j+1}. *C* represents shows irregularities in sensor values through co-relation techniques, *GD* represents a small drift in readings from normal values for time period *T*, and *BA* shows a constant offset ϵ to a sensor value at any time instant T_q. These anomalies are added in varying frequency levels to normal values and are fed to prediction models to determine the effect of cyberattacks on the IoV ecosystem.

9.3 | Prediction models

Based on added anomalies, the section presents the fusion of CNN and LSTM to classify the anomaly regions as a single anomaly or mixed anomaly. The details are now presented as follows.

9.3.1 | The CNN-LSTM ensemble

As depicted in Figure 10, an attention-based CNN architecture is designed to determine that takes inputs from dataset, and process them through multiple hidden layers to classify anomalies. To exploit the same, a context vector C_V is defined as $\sum_{n=1}^{T} at_{mn} h_n$, where at_{mn} denotes the attention matrix, and h_n denotes the hidden layer specification. For at_{mn}, a *Softmax* function is defined based on previous data at time ($l-1$), denoted as $Softmax(f_n(h_n, s_{l-1})$, which is the attention weight score to the reading sequence, and h_n is the current state *S*. In the process, the target labels *L* are transformed into {0, 1} sequence based on one-hot encoding, and readings are scaled through scalar functions. Based on the sequence obtained from one-hot method, *L* is shaped as 3*D* function and is fed to the CNN model. From CNN, feature extraction takes place that identifies the anomalous information, and fine-tunes the weight functions. For the same, C_V is utilized and target label prediction is done. To assign weights, a Gaussian weight filter is used that evenly distributes and scales the weights over the region boundary. The extracted features are now fed to the LSTM layer based on current input h_t. For h_t processing, the information is computed from the previous cell h_{t-1}, with *b* as the bias unit. A forget gate f_t is setup as $\sigma(W_f[C_V - s_{t-1}, h_{t-1}] + b_f)$, where σ denotes the sigmoid function. The *tanh* layer is set-up as $tanh(W_l[h_{t-1}, h_t] + b_l$, and values are updated and new context vector N_V is obtained.

9.3.2 | Schematics of multiple classifier learning

In this section, The authors present the idea of multiple classifiers as an ensemble. In the case of multiple classifiers, the idea is to present maximum matched labels to estimate *L*. The predicted results from multiple classifiers are fed into a voting strategy that forms a meta-classifier. The voting scheme is denoted as $argmax(\mathbb{N}(C_1),\mathbb{N}(C_2),...,\mathbb{N}(C_n))$, where $\mathbb{N}(C_i)$ denotes the labelled class with maximum matched features, and highest classification region. The multiple classifiers combine various methods as random forest (RF), AdaBoost, and SVM to form the meta classifier. To exploit the same, we consider that the SPMD dataset contains samples as $S_1, S_2, ..., S_n$. Any S_i is assigned a confidence value C_i. Based on the mapped C_i, two values *Pred*(*i*) and *Target*(*i*) are formed, that denotes the predicted and the target confidence values. For any C_i, *Pred*(*i*) is set to a threshold γ to evaluate *Target*(*i*). Out of total target classes, C_{tot}, the target class labels predicted by C_i are counted as instances. In the case of anomalous data, the count is appended in anomaly class A_c, and other data are presented in normal class A_n. With the highest votes, the classifier that closely matches the target indicates the highest confidence of real match (both anomalous or normal), and has the highest classification confidence. The class outputs are then combined with results of time-series LSTM data to predict the final output sequences, as depicted in Figure 10.

9.4 | Results and observations

In this section, the authors present the obtained results of the case study for the designed weighted ensemble (Javed et al., 2020). The proposed scheme validates the result for anomalous labels {*I*, *C*, *GD*, *BA*}. The observation is based on the pattern suggested by van Wyk et al. (2020). For the CNN model, the detection scheme contains three CNN layers and 5 hidden layers. For bifurcation, the first layer contains 64 neurons and is halved successively in the next two hidden layers. The split for training, validation, and testing purposes is considered as {0.75, 0.10, 0.15}.

To optimize the performance, over-fitting is avoided through *L*2-regularization, with 0.2 dropout probability. For activation, *ReLU* is employed, with a batch size of 200. The model is trained for 200 epochs, with Adam optimizer with the decay of 0.025. At the last layer, a sigmoid function is used to get binary output for C_V. For performance, three evaluation parameters accuracy, precision, and F1-score are computed for single and mixed anomaly types. The observations are now presented as follows.

9.4.1 | Single anomaly

For the observed values of {*I*, *C*, *GD*, *BA*}, the model experiments against another approach *WAVED* for anomaly detection. For *I* type, it is observed that for low anomaly values, the difference in the normal and malicious sensor is less, and hence the variance is lower. As the anomaly is increased in the dataset, the variation increases and signifies risk in node communication in IoV. For *C*, the proposed scheme performs better than *WAVED* scheme at duration $d = 10$, for higher anomalous values. The ensemble also ensures consistency in the obtained F1 and precision scores, compared to the *WAVED* scheme. In case of *GD*, the maximum observed F1 score is 0.9762 for 20 epochs, compared to 0.9759 in the *WAVED* scheme. For *BA*, the performance of both the schemes drops out considerably when the anomaly range increases. The maximum obtained F1-score is 0.9737, for the bias of 0.5. The precision of the scheme is 99.06 compared to 98.87 in the *WAVED* scheme. The increased precision can be accounted for the benefits of higher accuracy of neural nets with large sensor data and precise relationships among complex data sequences. Moreover, the attention sequence computation increases the overall accuracy of the scheme. The comparative analysis is shown in Table 9. As depicted in the figure, the proposed mechanism handles short bursts in bias data gracefully and can easily find out base patterns and classify the normal patterns from the anomalous patterns for given drift values with higher accuracy, compared to the *WAVED* scheme by van Wyk et al. (2020).

9.4.2 | Mixed anomaly

In the case of mixed anomaly sets from {*I*, *C*, *GD*, *BA*}, the performance of the scheme has a maximum F1-score 92.87 for *C* drift at a distance $d = 20$ units. In the case of *BA*, the maximum obtained score is 90.45, which shows the benefits of the combination of multiple classifiers in the prediction sets. The comparative analysis is shown in Table 10. As depicted in the table, it is evident that the proposed scheme outperforms

TABLE 9 Performance metrics of the proposed CNN-LSTM ensemble with the *WAVED* scheme for single anomaly detection (Javed et al., 2020)

Single anomaly against *WAVED* scheme									
		WAVED (%)				Proposed (%)			
Type	Anomaly magnitude	Accuracy	Sensitivity	Precision	F1	Accuracy	Sensitivity	Precision	F1
Instant Anomaly	base+500 * N (0,0.01)	96.82	99.59	98.18	98.26	96.02	99.79	97.86	99.02
Constant Anomaly	base + U (0,5), d = 10	95.56	94.12	98.93	96.46	96.61	95.61	99.28	97.41
Gradual Drift	base + linespace(0,2), d = 10	93.58	91.02	99.51	94.9	94.36	93.09	99.07	95.58
Bias Anomaly	base + U (0,5), d = 10	94.87	92.34	98.87	95.44	96.56	95.74	99.06	97.37

TABLE 10 Performance metrics for mixed anomaly against baseline scheme (Javed et al., 2020; van Wyk et al., 2020)

Mixed anomaly types against baseline scheme				
	Baseline (van Wyk et al., 2020)		Proposed	
Anomaly type	Accuracy	F1	Accuracy	F1
Instant 1000 * N(0,0.01)	91.34	78.11	91.1	77.9
Constant U(0,5), d = 10	95.64	90.43	95.3	90.1
GD linespace(0,4), d = 20	93.61	84.3	92.5	83.3
BA U(0,5), d = 10	96.02	90.45	94.8	89.3

the baseline approaches. The baseline approach involves the use of a Kalman filter (KF) and CNN-KF based ensemble to boost the optimizer weights.

10 | CONCLUSION

Energy sustainability is a key driver in current IoV-based ecosystems. To reduce carbon imprints and ensure renewable and green energy sources, AEVs play a critical role in facilitating energy exchange with peer AEVs, and RSUs in IoV ecosystems. The network-connected AEVs are equipped with sensor units and are connected through wireless infrastructures. The sensors gather real-time data and communicate through open channels and are subject to network-based attacks by malicious injected AEVs in the ecosystem. Recently, AI techniques are heavily employed in IoV ecosystems to monitor and analyze real-time gathered data from sensor units and classify the EV behaviour as normal or anomalous. The survey provides the reader's insights about anomaly detection techniques for AEVs through AI-based approaches. The survey addresses gaps in existing surveys through a detailed study of the associated security vulnerabilities and matching AI techniques to classify anomaly behaviour. A solution taxonomy for AI-leveraged anomaly detection in AEVs is considered. An experimental case study is depicted that combines a weighted ensemble of CNN-LSTM classifier for different infused anomaly types in the SPMD dataset and the optimization in the classifier model. The open challenges and possible solutions are also discussed of integration of AI schemes with real-sensor data.

As part of future work, the authors intend to design a scheme that preserves privacy of exchanged data of AEVs through open channels. We intend to design trusted AI model through which critical and sensitive information can be exchanged in de-identified form. It allows to form an end-to-end solution of information exchange in open channels, as well as increases the accuracy of detection of anomalous AEVs in the IoV ecosystem.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID

Sudeep Tanwar https://orcid.org/0000-0002-1776-4651

REFERENCES

Aggarwal, C. C. (2013). *Proximity-based outlier detection* (pp. 101–133). Springer.

Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, *189*, 105124.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1646–1685.

Alrawashdeh, K., & Purdy, C. (2016, December). *Toward an online anomaly intrusion detection system based on deep learning*. Paper presented at 15th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 195–200.

ALzubi, J. A., Bharathikannan, B., Tanwar, S., Manikandan, R., Khanna, A., & Thaventhiran, C. (2019). Boosted neural network ensemble classification for lung cancer disease diagnosis. *Applied Soft Computing*, *80*, 579–591. https://doi.org/10.1016/j.asoc.2019.04.031

Aujla, G. S, Jindal, A., Kumar, N., & Singh, M. (2016, December). *SDN-based data center energy management system using RES and electric vehicles*. Paper presented at 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6.

Avatefipour, O., Al-Sumaiti, A. S., El-Sherbeeny, A. M., Awwad, E. M., Elmeligy, M. A., Mohamed, M. A., & Malik, H. (2019). An intelligent secured framework for cyberattack detection in electric Vehicles' CAN bus using machine learning. *IEEE Access*, *7*, 127580.

Ayad, A., Zamani, A, Schmeink, A., & Dartmann, G. (2019, October). *Design and implementation of a hybrid anomaly detection system for IoT*. Paper presented at 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp. 1–6.

Azzaoui, A. E., Singh, S. K., Pan, Y., & Park, J. H. (2020). Block5GIntell: Blockchain for AI-enabled 5G networks. *IEEE Access*, *8*, 145918. https://doi.org/10.1109/ACCESS.2020.3014356

Berckmans, G., Messagie, M., Smekens, J., Omar, N., Vanhaverbeke, L., & Van Mierlo, J. (2017). Cost projection of state of the art lithium-ion batteries for electric vehicles up to 2030. *Energies*, *10*(9), 1314.

Bhatia, J., Modi, Y., Tanwar, S., & Bhavsar, M. (2019). Software defined vehicular networks: A comprehensive review. *International Journal of Communication Systems*, *32*(12), e4005. https://doi.org/10.1002/dac.4005

Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. *arXiv preprint arXiv:1901.03407*.

Chalapathy, R., Menon, A. K., & Chawla, S. (2018). Anomaly detection using one-class neural networks. *arXiv preprint arXiv:1802.06360*.

Chandola, V., Banerjee, A., & Kumar, V. (2007). Outlier detection: A survey. *ACM Computing Surveys*, *14*, 15.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*(3), 1–58.

Chawla, A., Lee, B., Fallon, S., & Jacob, P. (2018, February). *Host based intrusion detection system with combined CNN/RNN model*. Paper presented at 2018 Joint European Conference on Machine Learning and Knowledge Discovery in Databases, pp. 149–158, Springer.

Cui, J., Liew, L. S., Sabaliauskaite, G., & Zhou, F. (2019). A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Networks*, *90*, 101823. Recent advances on security and privacy in Intelligent Transportation Systems.

Du, M., Li, F., Zheng, G., & Srikumar, V. (2017, October). *Deeplog: Anomaly detection and diagnosis from system logs through deep learning*. Paper presented at 2017 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1285–1298.

El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. *Vehicular Communications*, *23*, 100214.

Erfani, S. M., Rajasegarar, S., Karunasekera, S., & Leckie, C. (2016). High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning. *Pattern Recognition*, *58*, 121–134.

Ergen, T., Mirza, A. H., & Kozat, S. S. (2017). Unsupervised and semi-supervised anomaly detection with lstm neural networks. *arXiv preprint arXiv: 1710.09207*.

Farhady, H., Lee, H., & Nakao, A. (2015). Software-defined networking: A survey. *Computer Networks*, *81*, 79–95.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419.

Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, *28*(1-2), 18–28.

Gogoi, P., Bhattacharyya, D., Borah, B., & Kalita, J. K. (2011). A survey of outlier detection methods in network anomaly identification. *The Computer Journal*, *54*(4), 570–588.

Guo, F, Polak, J. W., & Krishnan, R. (2010, September). *Comparison of modelling approaches for short term traffic prediction under normal and abnormal conditions*. Paper presented at 13th International IEEE Conference on Intelligent Transportation Systems, pp. 1209–1214.

Gupta, R., Kumari, A., & Tanwar, S. (2020). A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. *Transactions on Emerging Telecommunications Technologies*, e4009. https://doi.org/10.1002/ett.4009

Gupta, R., Tanwar, S., Kumar, N., & Tyagi, S. (2020). Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Computers & Electrical Engineering*, *86*, 106717. https://doi.org/10.1016/j.compeleceng.2020.106717

Gupta, R., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Machine learning models for secure data analytics: A taxonomy and threat model. *Computer Communications*, *153*, 406–440. https://doi.org/10.1016/j.comcom.2020.02.008

Habeeb, R. A. A., Nasaruddin, F., Gani, A., Hashem, I. A. T., Ahmed, E., & Imran, M. (2019). Real-time big data processing for anomaly detection: A survey. *International Journal of Information Management*, *45*, 289–307.

Hawkins, D. M. (1980). *Identification of outliers* (Vol. 11). Springer.

Hodge, V., & Austin, J. (2004). A survey of outlier detection methodologies. *Artificial Intelligence Review*, *22*(2), 85–126. https://doi.org/10.1023/B:AIRE.0000045502.10941.a9

Hundman, K., Constantinou, V., Laporte, C., Colwell, I., & Soderstrom, T. (2018, July). *Detecting spacecraft anomalies using LSTMs and nonparametric dynamic thresholding*. Paper presented at 2018 Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, pp. 387–395.

Hussain, B., Du, Q., Imran, A., & Imran, M. A. (2019). Artificial intelligence-powered mobile edge computing-based anomaly detection in cellular networks. *IEEE Transactions on Industrial Informatics*, *16*(8), 4986–4996.

Hussain, B., Du, Q., Zhang, S., Imran, A., & Imran, M. A. (2019). Mobile edge computing-based data-driven deep learning framework for anomaly detection. *IEEE Access*, *7*, 137656.

Issa, H, & Vasarhelyi, M. A. (2011). *Application of anomaly detection techniques to identify fraudulent refunds*. Available at SSRN 1910468.

Javed, A. R., Usman, M., Rehman, S. U., Khan, M. U., & Haghighi, M. S. (2020). Anomaly detection in automated vehicles using multistage attention-based convolutional neural network. *IEEE Transactions on Intelligent Transportation Systems*, 1–10. https://doi.org/10.1109/TITS.2020.3025875

Jyothsna, V., Prasad, V. R., & Prasad, K. M. (2011). A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, *28*(7), 26–35.

Kavousi-Fard, A., Su, W., & Jin, T. (2020). A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids. *IEEE Transactions on Industrial Informatics*, *17*(1), 650–658.

Khan, S., Liew, C. F., Yairi, T., & McWilliam, R. (2019). Unsupervised anomaly detection in unmanned aerial vehicles. *Applied Soft Computing*, *83*, 105650.

Koustubh, B. P., Nair, V. V., & Kumaravel, S. (2018, February). *Anomaly detection in hybrid electric vehicles using ann based support vector data description*. Paper presented at 2018 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), pp. 14–20.

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. *Commun. ACM*, *60*(6), 84–90. https://doi.org/10.1145/3065386

Kumari, A., Vekaria, D., Gupta, R., & Tanwar, S.. (2020, June). *Redills: Deep learning-based secure data analytic framework for smart grid systems*. Paper presented at 2020 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6.

Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2017). A survey of deep learning-based network anomaly detection. *Cluster Computing*, *22*, 1–13.

Lee, J. H., Park, M. W., Eom, J. H., & Chung, T. M. (2011, February). *Multi-level intrusion detection system and log management in cloud computing*. Paper presented at 13th International Conference on Advanced Communication Technology (ICACT2011), pp. 552–555.

Li, Y., He, H., Peng, J., & Zhang, H. (2017). Power management for a plug-in hybrid electric vehicle based on reinforcement learning with continuous state and action spaces. *Energy Procedia*, *142*, 2270–2275.

Maimó, L. F., Gómez, Á. L. P., Clemente, F. J. G., Pérez, M. G., & Pérez, G. M. (2018). A self-adaptive deep learning-based system for anomaly detection in 5G networks. *IEEE Access*, *6*, 7700–7712.

Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. *IEEE Communications Surveys & Tutorials*, *19*(4), 2322–2358.

Miglani, A., & Kumar, N. (2019). Deep learning models for traffic flow prediction in autonomous vehicles: A review, solutions, and challenges. *Vehicular Communications*, *20*, 100184.

Mnih, V, Kavukcuoglu, K, Silver, D, Graves, A., Antonoglou, I., Wierstra, D., & Riedmiller, M. (2013). Playing atari with deep reinforcement learning. *arXiv preprint arXiv:1312.5602*.

Moustafa, N., Hu, J., & Slay, J. (2019). A holistic review of Network Anomaly Detection Systems: A comprehensive survey. *Journal of Network and Computer Applications*, *128*, 33–55. https://doi.org/10.1016/j.jnca.2018.12.006

Nadeem M, Marshall O, Singh S, Fang X, Yuan X. *Semi-supervised deep neural network for network intrusion detection*. 2016. Kennesaw State University DigitalCommons. https://digitalcommons.kennesaw.edu/ccerp/2016/Practice/2/.

Nafi, N. S., Ahmed, K., Datta, M., & Gregory, M. A. (2016, December). *A novel software defined wireless sensor network based grid to vehicle load management system*. Paper presented at 2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1–6.

NHTSA. (2015). *Safety Pilot Model Deployment Test Conductor Team Report*. Retrieved from https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812171-safetypilotmodeldeploydeltestcondrtmrep.pdf

Osman, M. H., Kugele, S., & Shafaei, S. (2019, December). *Run-time safety monitoring framework for Ai-based systems: Automated driving cases*. Paper presented at 2019 26th Asia-Pacific Software Engineering Conference (APSEC), pp. 442–449.

Pacheco, J., Benitez, V. H., Félix-Herrán, L. C., & Satam, P. (2020). Artificial neural networks-based intrusion detection system for internet of things fog nodes. *IEEE Access*, *8*, 73907–73918.

Park, D., Kim, S., An, Y., & Jung, J. Y. (2018). LiReD: A light-weight real-time fault detection system for edge computing using lstm recurrent neural networks. *Sensors*, *18*(7), 2110.

Patel, K., Mehta, D., Mistry, C., Gupta, R., Tanwar, S., Kumar, N., & Alazab, M. (2020). Facial sentiment analysis using AI techniques: State-of-the-art, taxonomies, and challenges. *IEEE Access*, *8*, 90495–90519.

Patel, M., Hu, Y., Hédé, P., Joubert, J., Thornton, C., Naughton, B., Ramos, J. R., Chan, C., Young, V., Tan, S. J., Lynch, D., Sprecher, N., Musiol, T., Manzanares, C., Rauschenbach, U., Abeta, S., Chen, L., Shimizu, K., Neal, A., … Klas, G. (2014). Mobile-edge computing introductory technical white paper. *White Paper, mobile-edge Computing (MEC) Industry Initiative*, *29*, 854–864. https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf.

Prasad, V., Bhavsar, M., & Tanwar, S. (2019). Influence of montoring: Fog and edge computing. *Scalable Computing*, *20*, 365–376. https://doi.org/10.12694/scpe.v20i2.1533

Racki, D., Tomazevic, D., & Skocaj, D. (2018, March). *A compact convolutional neural network for textured surface anomaly detection*. Paper presented at 2018 IEEE Winter Conference on Applications of Computer Vision (WACV), pp. 1331–1339.

Rodriguez, P., Wiles, J., & Elman, J. L. (1999). A recurrent neural network that learns to count. *Connection Science*, *11*(1), 5–40.

Shaheen, S., Martin, E., & Totte, H. (2020). Zero-emission vehicle exposure within US carsharing fleets and impacts on sentiment toward electric-drive vehicles. *Transport Policy*, *85*, A23–A32.

Sheth, K., Patel, K., Shah, H., Tanwar, S., Gupta, R., & Kumar, N. (2020). A taxonomy of AI techniques for 6G communication networks. *Computer Communications*, *161*, 279–303. https://doi.org/10.1016/j.comcom.2020.07.035

Shi, D., Wang, S., Cai, Y., Chen, L., Yuan, C. C., & Yin, C. F. (2020). Model predictive control for nonlinear energy management of a power split hybrid electric vehicle. *Intelligent Automation & Soft Computing*, *26*(1), 27–39. https://doi.org/10.31209/2018.100000062

Shukla, A., Bhattacharya, P., Tanwar, S., Kumar, N., & Guizani, M. (2020). DwaRa: A deep learning-based dynamic toll pricing scheme for intelligent transportation systems. *IEEE Transactions on Vehicular Technology*, *69*(11), 12510–12520. https://doi.org/10.1109/TVT.2020.3022168

Singh, R., Singh, A., & Bhattacharya, P. (2021). *A machine learning approach for anomaly detection to secure smart grid systems* (pp. 199–213). IGI Global.

Singh S. (2015). *Critical reasons for crashes investigated in the national motor vehicle crash causation survey*. Technical Report.

Singh, S. K., Cha, J., Kim, T., & Park, J. (2021). Machine learning based distributed big data analysis framework for next generation web in IoT. *Computer Science and Information Systems*, *18*, 12–12. https://doi.org/10.2298/CSIS200330012S

Sugimoto, K., Lee, S., & Okada, Y. (2018, March). *Deep learning-based detection of periodic abnormal waves in ECG data*. Paper presented at 2018 Proceedings of the International MultiConference of Engineers and Computer Scientists.

Taj, M. S., Ullah, S. I., Salam, A., & Khan, W. U. (2020). Enhancing anomaly based intrusion detection techniques for virtualization in cloud computing using machine learning. *International Journal of Computer Science and Information Security (IJCSIS)*, *18*(5), 68–78.

Tanwar, S., Vora, J., Kaneriya, S., Tyagi, S., Kumar, N., Sharma, V., & You, I. (2020). Human arthritis analysis in fog computing environment using Bayesian network classifier and thread protocol. *IEEE Consumer Electronics Magazine*, *9*(1), 88–94. https://doi.org/10.1109/MCE.2019.2941456

Tanwar, S., Vora, J., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018). A systematic review on security issues in vehicular ad hoc network. *Security and Privacy*, *1*(5), e39. https://doi.org/10.1002/spy2.39

Tian, Y., & Pan, L. (2015, December). *Predicting short-term traffic flow by long short-term memory recurrent neural network*. Paper presented at 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), pp. 153–158.

Tian, Y., Wang, L., Gu, H., & Fan, L. (2020). Image and feature space based domain adaptation for vehicle detection. *Computers, Materials & Continua*, *65*(3), 2397–2412. https://doi.org/10.32604/cmc.2020.011386

Van, N. T., Thinh, T. N., & Thanh Sach, L. (2017, July). *An anomaly-based network intrusion detection system using deep learning*. Paper presented at 2017 International Conference on System Science and Engineering (ICSSE), pp. 210–214.

van Wyk, F., Wang, Y., Khojandi, A., & Masoud, N. (2020). Real-time sensor anomaly detection and identification in automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *21*(3), 1264–1276. https://doi.org/10.1109/TITS.2019.2906038

Vapnik, V. (2013). *The nature of statistical learning theory*. Springer Science & Business Media.

Vinayakumar, R., Soman, K., & Poornachandran, P. (2017, September). *Applying convolutional neural network for network intrusion detection*. Paper presented at 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1222–1228.

Wang, H., Bah, M. J., & Hammad, M. (2019). Progress in outlier detection techniques: A survey. *IEEE Access*, *7*, 107964.

Wang, H., Xue, Q., Cui, T., Li, Y., & Zeng, H. (2020). Cold start problem of vehicle model recognition under cross-scenario based on transfer learning. *Computers, Materials & Continua*, *63*(1), 337–351. https://doi.org/10.32604/cmc.2020.07290

Wang, S., Wu, J., Zhang, S., & Wang, K. (2018). SSDS: A smart software-defined security mechanism for vehicle-to-grid using transfer learning. *IEEE Access*, *6*, 63967–63975.

Waqas, M., Tu, S., Rehman, S. U., Halim, Z., Anwar, S., Abbas, G., Abbas, Z. H., & Rehman, O. U. (2020). Authentication of vehicles and road side units in intelligent transportation system. *Computers, Materials & Continua*, *64*(1), 359–371. https://doi.org/10.32604/cmc.2020.09821

Wu, D., Liu, Y., Xu, Z., & Shang, W. (2020). Design and development of unmanned surface vehicle for meteorological monitoring. *Intelligent Automation & Soft Computing*, *26*(5), 1123–1138. https://doi.org/10.32604/iasc.2020.012757

Xiao, Y., Wang, H., Xu, W., & Zhou, J. (2016). Robust one-class SVM for fault detection. *Chemometrics and Intelligent Laboratory Systems*, *151*, 15–25.

Xu, B., Rathod, D., Zhang, D., Yebi, A., Zhang, X., Li, X., & Filipi, Z. (2020). Parametric study on reinforcement learning optimized energy management strategy for a hybrid electric vehicle. *Applied Energy*, *259*, 114200.

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, *5*, 21954–21961.

Yu, B., Yin, H., & Zhu, Z. (2017). Spatio-temporal graph convolutional networks: A deep learning framework for traffic forecasting. *arXiv preprint arXiv: 1709.04875*.

Zhang, J. (2013). Advancements of outlier detection: A survey. *ICST Transactions on Scalable Information Systems*, *13*(1), 1–26.

Zhao, R., Yan, R., Chen, Z., Mao, K., Wang, P., & Gao, R. X. (2019). Deep learning and its applications to machine health monitoring. *Mechanical Systems and Signal Processing*, *115*, 213–237.

Zhao, Z., Chen, W., Wu, X., Chen, P. C., & Liu, J. (2017). LSTM network: A deep learning approach for short-term traffic forecast. *IET Intelligent Transport Systems*, *11*(2), 68–75.

AUTHOR BIOGRAPHIES

Palak Dixit is a postgraduate student in the Department of Computer Science and Engineering in the Institute of Technology, Nirma University, Ahmedabad, India. Her research interest lies in the area of energy optimization, blockchain technology, autonomous vehicles, artificial intelligence, and network security.

Pronaya Bhattacharya is is employed as an Assistant Professor with the Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad, India. He has over eight years of teaching experience. He has authored or co-authored 35 research papers in leading SCI journals and top core IEEE ComSoc conferences. Some of his top findings are published in IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, Transactions on Emerging Telecommunications Technologies (Wiley), Future Generation Computer Systems (Elsevier), Journal of Engineering Research (Kuwait University), ACM-MobiCom, IEEE-InfoCom, IEEE-ICC, and IEEE-CITS. His research interests include optical switching, high-performance networking, blockchain, IoT, and deep learning. Mr. Bhattacharya is awarded the best paper award in Springer ICRIC-2019 and COMS2-2021. He is working as a Reviewer of reputed SCI journals IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE NETWORK, IEEE-ACCESS, Transactions on Emerging Telecommunications Technologies (Wiley), International Journal of Communication Systems (Wiley), Optical Switching and Networking (Elsevier), Multimedia Tools and Applications (Springer), Wireless Personal Communications (Springer), and Journal of Engineering Research (Kuwait University). He has also been appointed as the Session Chair in IC4S-2019, IC4S-2020, and IICT-2020, organized by Springer. He is a Lifetime Member of professional societies like ISTE and IAENG.

Dr. Sudeep Tanwar is currently working as a Professor of the Computer Science and Engineering Department at Institute of Technology, Nirma University, India. Dr Tanwar was a visiting Professor at Jan Wyzykowski University in Polkowice, Poland and the University of Pitesti in Pitesti, Romania. Dr Tanwar's research interests include Blockchain Technology, Wireless Sensor Networks, Fog Computing, Smart Grid, and IoT. He has authored 02 books and edited 13 books, more than 200 technical papers, including top journals and top conferences, such as IEEE TNSE, TVT, TII, WCM, Networks, ICC, GLOBECOM, and INFOCOM. Dr Tanwar initiated the research field of blockchain technology adoption in various verticals in 2017. His h-index is 38. Dr Tanwar actively serves his research communities in various roles. He is currently serving the editorial boards of Physical Communication, Computer Communications, International Journal of Communication System, and Security and Privacy. He has been awarded best research paper awards from IEEE GLOBECOM 2018, IEEE ICC 2019, and Springer ICRIC-2019. He has served many international conferences as a member of the organizing committee, such as publication chair for FTNCT-2020, ICCIC 2020, WiMob2019, member of the advisory board for ICACCT-2021, ICACI 2020, workshop co-chair for CIS 2021, and general chair for IC4S 2019, 2020, ICCSDF 2020. Dr Tanwar is a final voting member for IEEE ComSoc Tactile Internet Committee in 2020. He is a Senior Member of IEEE, CSI, IAENG, ISTE, CSTA, and the member of Technical Committee on Tactile Internet of IEEE Communication Society. He is leading the ST research lab where group members are working on the latest cutting-edge technologies.

Rajesh Gupta is a Full-Time Ph.D. Research Scholar in the Computer science and Engineering Department at Nirma University, Ahmedabad, India. He received a Bachelor of Engineering in 2008 from the University of Jammu, India and a Master's in Technology in 2013 from Shri Mata Vaishno Devi University, Jammu, India. He has authored/co-authored some publications (including papers in SCI Indexed Journals and IEEE ComSoc sponsored International Conferences). Some of his research findings are published in top-cited journals (such as IEEE Transactions on Network Science and Engineering, IEEE Networks, Computer Communications, CEE Elsevier, ETT Wiley, IJCS Wiley, IET Communications, Physical Communications Elsevier, Expert System Wiley, etc.) and top-tier conferences (such as IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, IEEE CITS). His research interest includes Network Security, Blockchain Technology, 5G Communication Network, and Machine Learning. He is also a recipient of a Doctoral Scholarship from the Ministry of Electronics and Information Technology, Govt. of India under the Visvesvaraya Ph.D. scheme. He has been awarded IEEE ComSoc Student Travel Grant to attend IEEE ICC 2021 conference which is held in Montreal, Canada. He is a student member of IEEE since 2018.

How to cite this article: Dixit, P., Bhattacharya, P., Tanwar, S., & Gupta, R. (2021). Anomaly detection in autonomous electric vehicles using AI techniques: A comprehensive survey. *Expert Systems*, 1–30. https://doi.org/10.1111/exsy.12754