Engineering Applications of Artificial Intelligence 129 (2024) 107667

Contents lists available at ScienceDirect

Engineering Applications of Artificial Intelligence

journal homepage: www.elsevier.com/locate/engappai

Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems

Hamed Alqahtani [a], Gulshan Kumar [b,*]

[a] Assistant Professor, College of Computer Science, King Khalid University, Saudi Arabia
[b] Associate Professor, Department of Computer Applications, Shaheed Bhagat Singh State University, Ferozepur (Punjab), India

ARTICLE INFO

Keywords:
Anomaly identification
Cybersecurity
Privacy
Safety
Sustainability in EnFV security
Sustainable transportation
Threat detection

ABSTRACT

This paper delves into the transformative role of machine learning (ML) techniques in revolutionizing the security of electric and flying vehicles (EnFVs). By exploring key domains such as predictive maintenance, cyberattack detection, and intelligent decision-making, the study uncovers pivotal insights that will shape the future of this technology.

From a theoretical perspective, ML emerges as a cornerstone for fortifying EnFV safety, offering real-time threat detection, predictive maintenance capabilities, and enhanced anomaly detection. In practical terms, ML-based solutions are envisioned as instrumental in preventing cyberattacks, reducing downtime, and improving overall safety.

The research contributions of this study encompass a comprehensive overview of ML applications in EnFV security, identification of challenges, and paving the way for future research directions. While acknowledging research limitations, particularly the need for real-world implementation, the study emphasizes the crucial yet underexplored ethical considerations in ML for EnFV security. Future research suggestions focus on Explainable AI techniques, real-time ML algorithms for resource-constrained environments, and privacy-preserving ML techniques, aiming for a transparent, efficient, and privacy-aware integration of ML in EnFV security. By addressing key security challenges, ML can potentially revolutionize the EnFV domain, paving the way for a future of efficient, sustainable, and connected transportation systems.

1. Introduction

The dynamic evolution of transportation technology has brought forth a transformative era marked by the rise of electric and flying vehicle (EnFV) systems, positioned to reshape global travel dynamics (Sanguesa et al., 2021; Bharathidasan et al., 2022). In line with global objectives such as Sustainable Development Goals (SDGs) and net-zero targets (Lipu et al., 2022; Jayachandran et al., 2022), the International Energy Agency (IEA) reported a record-breaking year in 2022, with electric car sales surpassing 10 million, reflecting a substantial 55% increase from 2021 (IEA, 2022). This exponential growth, depicted in Fig. 1, underscores the transformative potential of EnFVs in enhancing efficiency, mitigating environmental impact, and expanding mobility (Mohamed et al., 2023; Javed et al., 2021a).

However, amid these advancements, a critical challenge surfaces: ensuring the security of these sophisticated, interconnected systems (Heidari et al., 2023; Sanguesa et al., 2021). This review paper intricately explores the nexus between security and emerging transportation technologies, with a dedicated focus on the application of machine learning techniques, aligning with the broader global objectives for sustainable and secure advancements in transportation.

In the contemporary landscape, the fusion of artificial intelligence (AI) and transportation technology has unlocked a realm of possibilities, from self-driving electric vehicles navigating city streets to unmanned aerial vehicles (UAVs) soaring through the skies (Chriki et al., 2021). However, this convergence also introduces an array of vulnerabilities and potential risks that extend beyond the physical realm. As vehicles become more intelligent and interconnected, they become susceptible to cyber threats, data breaches, and malicious interventions. In light of this intricate interplay, reinforcing security measures becomes paramount to ensure the seamless integration and secure operation of EnFV systems. Machine learning (ML), a potent subset of AI, emerges as a beacon of hope in the endeavor to bolster transportation security (Heidari et al., 2023; Srivastava et al., 2021). Its capacity to learn from data, identify anomalies, and make real-time informed decisions positions it as a robust tool for countering evolving threat landscapes. By harnessing the potential of these technologies, we

* Corresponding author.
E-mail address: gulshanahuja@gmail.com (G. Kumar).

https://doi.org/10.1016/j.engappai.2023.107667
Received 22 August 2023; Received in revised form 19 November 2023; Accepted 4 December 2023
Available online 8 December 2023

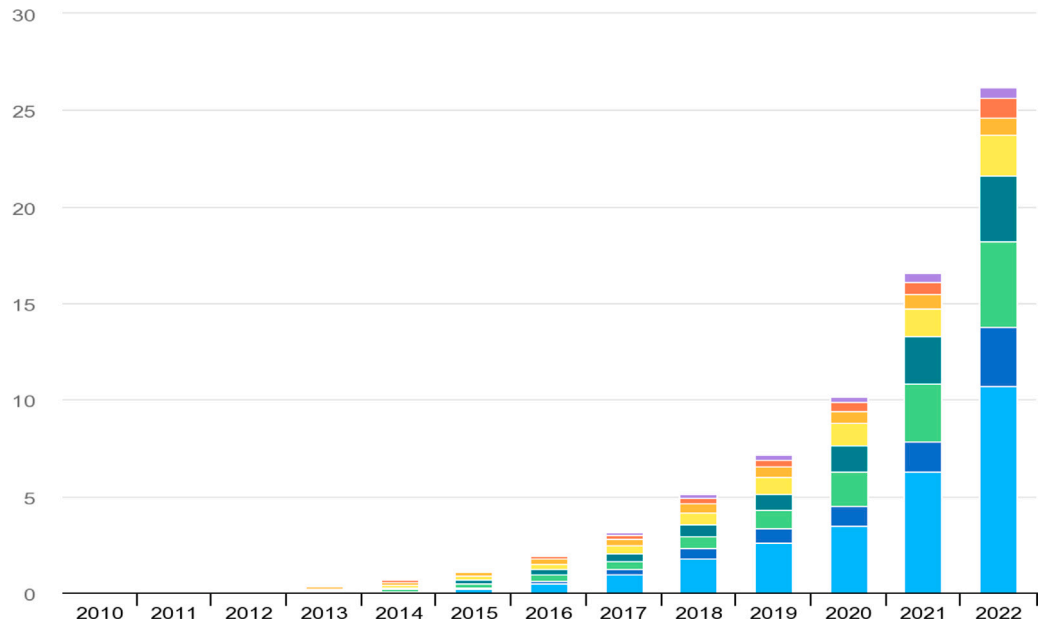

Fig. 1. Global electric car stock from 2010 to 2022 (IEA, 2022).

can not only pinpoint vulnerabilities and preempt potential risks but also engineer adaptive security systems capable of responding to novel and unforeseen challenges.

Various ML-based approaches have been developed in the existing literature to enhance transport security, particularly for EnFVs. However, a comprehensive review of these techniques is lacking. This paper aims to fill this gap by extensively reviewing the current literature on ML-based cyberattack detection and mitigation for EnVs. Through a systematic review, the authors analyze and compare the strengths and limitations of the cited research papers, facilitating the identification of research gaps and opportunities for further exploration. The methodology employed in this paper aims to contribute valuable insights into future research directions in the dynamic field of ML-based security for EnFVs. Major contributions of this study include:

1. Identifying the potential of machine learning techniques in enhancing transportation security for electric and flying vehicles.
2. Providing a comprehensive review of the existing literature on machine learning-based cyberattack detection and mitigation for electric and flying vehicles.
3. Highlighting the research gaps in the field and offering opportunities for further investigation and advancement.
4. Presenting a comparative analysis of the different machine learning techniques and their effectiveness in addressing transportation security challenges.
5. Proposing a framework for integrating machine learning techniques into transportation security systems for electric and flying vehicles.
6. Providing insights into the future directions of research in this field.

The subsequent sections of this paper are organized as follows: Section 2 provides an overview of EnFV systems and their security, aiming to offer readers a comprehensive grasp of the subject matter. Section 3 delves into security challenges faced by EnFV systems, exploring potential vulnerabilities and associated risks. Moving on to Section 4, the paper discusses the applications of ML in transportation security, highlighting how ML techniques can enhance EnFV system security. In Section 5, the paper explores future directions and emerging trends in EnFV system security, discussing potential advancements and research areas shaping the domain's future. Finally, Section 6 concludes the paper by summarizing key findings and underlining the importance of addressing security challenges in EnFV systems.

2. EnFV systems and their security

The landscape of transportation technology is undergoing a significant transformation driven by rapid advancements in EnFV systems. EVs have emerged as a promising alternative to traditional internal combustion engine vehicles, offering benefits such as reduced emissions, improved energy efficiency, and quieter operation (Bharathidasan et al., 2022). At the same time, the concept of flying vehicles, once relegated to science fiction, is steadily becoming a reality with the development of electric vertical takeoff and landing (eVTOL) aircraft. The spectrum of EV systems encompasses various modes, including electric cars, buses, bikes, and scooters. These systems utilize electric power sources like batteries and fuel cells to propel vehicles, contributing to a reduced carbon footprint associated with transportation. The proliferation of EVs heralds a paradigm shift in urban mobility, paving the way for a greener and more sustainable future (Escorcia-Gutierrez et al., 2023). On the horizon, the potential of flying vehicles holds the promise of reshaping urban transportation even further. eVTOL aircraft, driven by electric propulsion systems, can alleviate traffic congestion and enable efficient point-to-point travel within urban and suburban environments. With advanced aerodynamics and vertical takeoff capabilities, these vehicles are poised to revolutionize the concept of air mobility.

As EnFV systems become increasingly interconnected and reliant on software-driven functionalities, the vulnerability to cyber threats and malicious attacks escalates (Dey and Khanra, 2020). Consequently, this review paper delves into the intricate domain of security within the context of EnFV systems. It explores ML's indispensable role in fortifying these systems against potential threats. By enhancing security measures, these technologies ensure the seamless integration of groundbreaking EnFV technologies into our daily lives.

2.1. Significance of security in transport technological advancements

The realm of transportation technology, encompassing EVs and FVs (such as drones and flying taxis), presents a distinct array of security challenges (Kateb and Ragab, 2023). The interconnected nature of these vehicles with digital networks and their autonomous capabilities creates potential vulnerabilities that malicious actors could exploit. The repercussions of security breaches extend beyond vehicle operators and passengers; they could impact critical infrastructure, public safety, and

erode trust in these transformative technologies (Al-Rubaye et al., 2023; Adil et al., 2020).

The importance of security in transportation technology is multifaceted. Firstly, it encompasses passenger safety as compromised security of electric and flying vehicles could lead to accidents, endangering passengers and pedestrians (Kulkarni et al., 2023; Da Silva et al., 2022). Robust security measures are crucial to prevent unauthorized access, cyberattacks, and manipulation of controls that could jeopardize safety. Secondly, data privacy is paramount as these vehicles collect and transmit sensitive data, necessitating protection against unauthorized access and breaches to preserve passenger privacy and prevent data misuse. Thirdly, integrating such vehicles into existing transportation networks requires safeguarding critical infrastructure like charging stations and communication networks to prevent disruptions and impacts on urban infrastructure. Lastly, public trust in the security and reliability of EnFV systems is essential for their successful adoption; significant security incidents could hinder technological development and widespread acceptance of these transformative technologies.

2.2. Role of ML in enhancing security

In the rapidly evolving landscape of EnFV systems, prioritizing robust security measures is of utmost importance. As transportation technology advances, integrating ML methods emerges as a transformative strategy to bolster security protocols and counter potential threats (Kulkarni et al., 2023; Shaukat et al., 2020e). ML, a subset of AI, excels in recognizing patterns, anomaly detection, and intelligent decision-making through data analysis (Berger et al., 2018). This positions ML as a potent tool to tackle intricate security challenges. ML algorithms swiftly identify deviations from norms by utilizing historical and real-time data from vehicle operations, communication networks, and external environments. Intrusion detection systems (IDSs) powered by ML autonomously flag unauthorized access or suspicious behaviors, enabling swift response and mitigation tactics. Amidst the journey toward increased vehicle autonomy and connect[illegible], the insights from ML contribute to predictive maintenance strateg[illegible] By analyzing data trends and historical performance, these techniques forecast potential vulnerabilities and maintenance needs, preemptively mitigating risks and ensuring vehicle safety.

Numerous research efforts have been invested in using ML in vehicle [illegible]ecurity by integrating it with emerging technologies such as cloud [illegible]nd fog computing. For example, Mohammed et al. (2022) presented a cost-efficient and secure vehicular fog cloud computing (VFCN) comprising a mobility-aware multi-scenario offloading phase (MAMSOP) to address mobility and offloading costs. The work aimed to execute applications with minimal delays and costs securely. For security considerations, a scheme based on fully-homomorphic encryption was proposed, encrypting and decrypting data locally and involving computations on encrypted data rather than decrypting it into its original form. Given most applications' deadline and mobility constraints, a fully polynomial-time approximation scheme (FPTAS) based search task scheduling (STS) was proposed to ensure the execution of all applications within their specified constraints. STS-FPTAS aimed to determine delay and cost-aware scheduling into knapsack-aware resources, where the knapsack allowed all tasks to be allocated to the available length of resources. The results indicated that the proposed work optimized costs by 40% compared to existing systems. The authors enhanced their research in Mohammed et al. (2023) by proposing a homomorphic federated learning-enabled pedestrian and vehicle detection system named HMFLS. The system utilized fog nodes and cloud servers to collect real-time data and train ML models for pedestrian and vehicle detection. HMFLS incorporated homomorphic encryption, enabling computations on encrypted data without decryption, ensuring privacy and confidentiality. The system employed Generative Adversarial Networks and VGG19 to train pedestrian and vehicle images and extract features. The study demonstrated that HMFLS outperformed existing schemes regarding security accuracy, resource leakage, and vehicle and pedestrian detection processing time. The system also included an Android-based application for easy integration into vehicles and mobile phones. The authors discussed the challenges in existing pedestrian and vehicle detection systems and presented the contributions of the proposed HMFLS. The performance of the system was evaluated through simulations. They highlighted the advantages of HMFLS in terms of security, efficiency, and integration capabilities. Similarly, Lakhan et al. (2023) explored the challenges and issues faced in sustainable transport applications, such as battery power consumption and execution accuracy. Recognizing the limitations of existing decision support methods, a fuzzy-based energy-efficient decision support system (FBEES) was proposed to address these challenges. FBEES aimed to minimize energy consumption, delay, and cost while enhancing scheduling accuracy. The system employed ubiquitous fog servers to offload data from vehicles for processing. Simulation results demonstrated that FBEES outperformed existing energy, cost, delay, and accuracy methods for sustainable transport applications. The article also delved into related work in the field and presented the problem formulation, proposed algorithm, and performance evaluation. Abo Mosali et al. (2022) explored the autonomous landing of unmanned aerial vehicles (UAVs) on moving platforms, comparing the effectiveness of traditional control theory and reinforcement learning (RL) in UAV control. The authors proposed an adaptive multi-level quantization-based RL model to address the delay issue induced by deep neural networks through quantizing continuous actions and states. The model underwent evaluation and demonstrated superiority over state-of-the-art approaches, as evidenced by a lower root mean square error (RMSE). The study emphasized the significance of autonomous landing in diverse UAV applications and outlined the challenges associated with landing on moving targets. Given its capacity to handle non-linearity and the absence of accurate plant models, RL was deemed a suitable control algorithm for this task. Yassine and Stanulov (2024) presented an overview of ML algorithms used to predict air passenger traffic flow in the aviation industry. The authors discussed the challenges faced by the industry and the potential benefits of employing ML for prediction purposes. They compared the performance of three algorithms – Long Short-Term Memory (LSTM), Support Vector Regression Machine (SVRM), and Random Forest (RF) – utilizing a dataset of passenger numbers at Oslo Airport Gardermoen. The LSTM model demonstrated the highest generalization ability, exhibiting the lowest Mean Squared Error (MSE) and Root Mean Squared Error (RMSE) on the testing dataset. The authors also deliberated the complexity, stability, and predictive capabilities of each model in anticipating fluctuations in passenger numbers.

Key goals of research utilizing ML techniques to enhance security in the ENFV domain include (Bithas et al., 2019):

1. Efficiency
    - Real-time Threat Detection and Response: Employ ML to analyze sensor data in real time, enabling swift detection and response to threats, thereby preventing potential attacks.
    - Automated Anomaly Detection: Utilize ML for automated identification of anomalous behavior in EnFV systems, serving as an early warning system for potential security threats.
    - Adaptive Security Mechanisms: Develop adaptive security mechanisms using ML to learn from new threats and dynamically adapt to changing attack patterns, ensuring continuous and evolving protection for EnFV systems.
2. Sustainability
    - Reduced Energy Consumption: Apply ML to optimize EnFV systems for energy efficiency, thereby reducing their overall environmental impact.

- Extended Battery Life: Utilize ML to predict and extend the battery life of EnFVs, minimizing the need for frequent charging and enhancing overall sustainability.
- Predictive Maintenance: Employ ML for predictive maintenance, accurately anticipating when EnFV components require replacement, reducing downtime, and lowering maintenance costs.

3. Connectivity

- Secure Vehicle-to-Everything (V2X) Communication: Implement ML to secure V2X communication, which is crucial for enabling secure information exchange between EnFVs and other infrastructure components.
- Privacy-Preserving Data Sharing: Develop privacy-preserving data sharing mechanisms using ML, allowing EnFVs to share information without compromising privacy or security.
- Resilient Communication Networks: Leverage ML to design resilient communication networks capable of withstanding cyberattacks and disruptions, ensuring continuous connectivity for EnFV systems.

By achieving these goals, research in ML for EnFV security aims to enhance the efficiency, sustainability, and connectivity of EnFVs, contributing to a safer and more secure transportation system for all.

2.3. Scope and objectives of the study

This review paper focuses on exploring the complex domain of security issues within EnFV systems, emphasizing the role of ML techniques in enhancing security against potential threats. The paper aims to comprehensively analyze the security challenges faced by EnFV systems, uncovering vulnerabilities and risks that could compromise their integrity. It also investigates the application of ML for improving security, covering areas like intrusion detection, cyberattack mitigation, and predictive maintenance. The paper's scope encompasses various security-related topics within EnFV systems, offering insights into their multifaceted intersection with transportation technology and cybersecurity.

In employing a mixed-methods research approach for this study on transportation security, potential threats to validity need careful consideration to ensure the robustness and reliability of the study findings. One potential threat is the inherent subjectivity introduced by the qualitative component, which the researchers' interpretations and biases may influence. Efforts will be made to mitigate this threat by maintaining transparency in the research process and employing multiple researchers for data analysis to enhance the reliability of qualitative insights. Additionally, the generalizability of the quantitative results to broader populations could be compromised if the sample size is not sufficiently representative. To address this, a well-defined sampling strategy will be implemented, ensuring diversity and relevance to the broader context of transportation security. Furthermore, the timing of data collection in the qualitative and quantitative phases may introduce temporal discrepancies, impacting the alignment of findings. This challenge will be mitigated by careful planning and coordination to synchronize data collection points, minimizing the risk of temporal bias. Despite these potential threats, a meticulous and thoughtful approach will be adopted to enhance the internal and external validity of the mixed-methods study, thereby strengthening the overall reliability and validity of the research outcomes.

3. Security challenges in EnFV systems

Amidst the swift progress in transportation technology, ensuring the security of EnFV systems has become a pivotal issue. This segment explores the complex security challenges embedded within these novel transportation modes. These challenges encompass the dynamic and multifaceted threat landscape encompassing cyber and physical risks and the vulnerabilities inherent to EnFV systems.

3.1. Threat landscape in transportation technology

The rapid evolution of transportation technology, particularly in the domain of EnFVs, has brought about transformative possibilities while also introducing a complex and evolving threat landscape (Bharathidasan et al., 2022; Sanguesa et al., 2021). This landscape demands careful consideration to establish robust security measures that protect passengers, infrastructure, and the broader transportation ecosystem. As EnFVs become increasingly integrated into daily life, traditional security concerns are compounded by emerging digital threats, with cybercriminals, hacktivists, and even nation-state actors exploiting software, communication networks, and control mechanisms to compromise the integrity, availability, and safety of EnFV systems (Marinho and Holanda, 2023). The heavy reliance on interconnected digital systems in EnFVs introduces vulnerabilities to cyberattacks like malware, ransomware, and denial-of-service attacks that can disrupt critical functions and compromise data. At the same time, privacy concerns arise from the abundance of data-gathering technologies, putting personal information at risk (Dey and Khanra, 2020; Kateb and Ragab, 2023; Sani et al., 2022; Berger et al., 2018). The intricate supply chain of EnFVs also poses risks, with potential points of compromise ranging from hardware components to third-party software, highlighting the need to ensure the security of every element involved in production and operation (Heidari et al., 2023; Shaukat et al., 2021a). Moreover, the pace of technological advancement often outstrips the development of security awareness and best practices, creating gaps that attackers can exploit due to insufficient understanding of potential threats and effective mitigation strategies (Mohamed et al., 2023; Javed et al., 2021b).

3.2. Vulnerabilities of EnFV systems

The rapid progression of EnFV systems has yielded transformative advantages. Yet, it has also introduced significant security challenges that demand attention to guarantee these technologies' secure and dependable operation. This section delves into the inherent vulnerabilities within EnFV systems. Firstly, EnFV systems heavily rely on intricate software-defined architectures governing diverse vehicle functions, including propulsion, energy management, navigation, and communication (Da Silva et al., 2022; Thakur et al., 2021). This software reliance amplifies vulnerability to cyber threats, potentially enabling unauthorized access, manipulating vehicle behavior, and compromising essential safety features. Secondly, seamless communication between vehicles, infrastructure, and components is pivotal for efficient EnFV operation (Sindhwani et al., 2020). However, these communication networks are susceptible to eavesdropping, interception, and unauthorized access, which could disrupt vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, leading to accidents and traffic congestion. Thirdly, while remote access and control of EnFVs enhance convenience and fleet management, they pose a substantial security risk. Unauthorized entry into vehicle systems could result in unauthorized use, theft, or manipulation by malicious entities, endangering passengers and bystanders alike (Tran et al., 2023). Additionally, the array of sensors embedded in EnFVs, like LiDAR, cameras, and GPS, are susceptible to manipulation, spoofing, or jamming. These vulnerabilities can cause erroneous navigation, compromised situational awareness, and potential accidents (Miao et al., 2020). Moreover, the intricate global supply chains manufacturing EnFVs expose them to potential hardware compromises. Counterfeit or malicious components could be integrated, leading to unforeseen vulnerabilities or failures that are challenging to detect (Li et al., 2020b). Lastly, since EnFVs generate substantial data encompassing location details, vehicle performance metrics, and passenger preferences, ensuring data privacy is paramount (Sani et al., 2022). This safeguards against unauthorized tracking, profiling, and misuse of sensitive information.

3.3. Potential risks to passengers and infrastructure

As EnFV systems continue to advance and integrate into modern transportation networks, they bring forth potential risks impacting passengers and critical infrastructure. These risks encompass several dimensions. Firstly, passenger safety remains a priority, with concerns spanning technical malfunctions, system failures, and accidents during various phases of operation (Raj et al., 2021; Bylykbashi et al., 2020). Secondly, the heavy reliance on software and communication systems exposes EnFVs to cybersecurity threats, including hacking and data breaches, which could compromise safety and operational integrity (Li et al., 2022; Lu et al., 2020). Thirdly, vulnerabilities in the charging and takeoff/landing infrastructure could result in disruptions, affecting charging processes and causing cascading effects (Adil et al., 2020; Kulkarni et al., 2023). Introducing flying vehicles also poses challenges to air traffic management, necessitating considerations like collision avoidance and coordination (Vanitha and Ganapathi, 2020; Qureshi et al., 2023; Reddy et al., 2021). Furthermore, the proliferation of sensors and data collection mechanisms raises privacy concerns, potentially infringing upon individuals' privacy rights. Lastly, the environmental impact, despite EVs' green reputation, includes ecological concerns from battery production and disposal and potential noise pollution and energy consumption associated with flying vehicles (Mohamed et al., 2023).

3.4. Need for advanced security solutions

As the realm of transportation technology, propelled by the integration of EnFV systems, undergoes rapid evolution, the call for robust security measures becomes increasingly urgent. The complex interplay between innovative technologies and sophisticated cyber threats highlights the essential requirement for advanced security solutions to safeguard passengers, infrastructure, and the overall transportation ecosystem (Meyer et al., 2021; Putri et al., 2021). Unlike conventional transportation modes, EnFV systems harbor unique vulnerabilities stemming from intricate software integration, interconnected networks, and the proliferation of sensors and data-sharing mechanisms. While these technologies enhance transportation functionality, they expose systems to a broad spectrum of potential threats (Marinho and Holanda, 2023). A key challenge is the risk of unauthorized access and control over vital vehicle functions. Exploiting software or communication vulnerabilities, malicious actors could seize control over an EV or FV, resulting in hazardous scenarios like unauthorized control access, remote manipulation, or complete takeover. Moreover, the reliance on wireless communication and data sharing introduces the potential for eavesdropping, data tampering, and unauthorized data access (Chen and Shi, 2019). This exposes sensitive passenger and operational data to cybercriminals seeking to exploit communication channel weaknesses. The potential fallout of successful attacks on EnFV systems, including accidents, service disruptions, financial losses, and erosion of trust in emerging transportation technologies, further emphasizes the imperative for advanced security solutions.

4. ML applications in transportation security

This segment delves into diverse ML strategies with the potential to reshape the security landscape of EnFV systems. It overviews these methodologies and their practical deployment in fortifying transportation technology. The focus is on specialized IDSs for EnFVs, underscoring their role in thwarting unauthorized access. Furthermore, the text explores anomaly detection in vehicle behavior, a tool for identifying irregularities that could signify emerging threats or system glitches. Additionally, the discourse encompasses the use of ML in detecting and countering cyberattacks, spotlighting its rapid responsiveness to adversarial actions. Beyond defence, the section elucidates ML's contribution to predictive maintenance, ensuring seamless vehicle operations through data-powered foresight.

4.1. Overview of ML techniques

ML has become a potent tool across diverse domains, including transportation security. ML methods leverage data-driven strategies to analyze patterns, predict outcomes, and detect anomalies, bolstering the security of EnFV systems (Chen and Chen, 2019; Mohamed et al., 2023). This section offers an overview of crucial ML techniques within transportation security.

Supervised learning involves training algorithms on labeled datasets to recognize patterns and relationships. This is used for tasks like intrusion detection, aiding in identifying unauthorized access attempts and malicious activities within vehicle systems (Heidari et al., 2023; Said et al., 2023; Sharma and Bora, 2022). Unsupervised learning identifies hidden patterns without predefined labels, supporting anomaly detection by recognizing deviations from normal EnFV behavior, indicative of security breaches (Mohamed et al., 2023). Semi-supervised learning combines aspects of both, valuable when labeled data is limited, improving IDS by identifying new attack patterns with limited labeled data (Sani et al., 2022). Supervised learning algorithms, such as support vector machines (SVMs) and random forests, typically have higher time complexities than unsupervised learning algorithms, such as k-means clustering and anomaly detection. This is because supervised learning algorithms require training on labeled data, which can be time-consuming, especially for large datasets (Shaukat et al., 2020c). For instance, the K-Nearest Neighbors (KNN) algorithm exhibits a time complexity of O(n), making it computationally efficient, particularly for smaller datasets. On the other hand, SVM have a time complexity of $O(n\hat{2})$, which can be manageable for moderate-sized datasets but may pose challenges for larger ones. Random Forest, a popular ensemble learning technique, also carries a time complexity of $O(n\hat{2})$. Neural Networks, known for their capacity to model complex relationships, have a higher time complexity of $O(n\hat{3})$, significantly making them computationally demanding as the dataset size increases. When implementing machine learning methods for cyberattack detection, it is crucial to consider the trade-off between model accuracy and computational efficiency, selecting algorithms based on the specific requirements and scale of the applications (Gopi et al., 2022; Kanti et al., 2023). Mohamed et al. (2023) discussed the increased use of AI and ML to bolster EV security. While the adoption of AI and ML in this context is growing, understanding their precise applications remains incomplete. Their review of existing literature identifies common trends and themes, revealing the use of AI and ML to enhance EV information security through authentication, intrusion detection, and attack prevention. Prominent ML algorithms include DL and neural networks, with an emerging integration of blockchain technology. The review found that approximately 75% of studies focus on intrusion detection, while authentication and attack prevention make up 20% and 5% respectively. Integrating these ML techniques into EnFV security frameworks holds significant potential in strengthening defense mechanisms against threats.

4.1.1. Use cases of ML for improving EnFV security

ML has already demonstrated its effectiveness in improving EnFV security. Several specific examples are described below.

1. Anomaly detection in EnFV sensor data: Machine learning algorithms can analyze sensor data from EnFVs, such as engine temperature, battery voltage, and wheel speed, to detect anomalies that may indicate a potential security threat (Dixit et al., 2022; Hsieh et al., 2021; Pace et al., 2022). For instance, sudden sensor readings or unexpected pattern fluctuations could signal an attempt to manipulate the vehicle's systems or exploit vulnerabilities.
2. Threat detection in EnFV network traffic: ML models can analyze network traffic generated by EnFVs to identify malicious activities, such as unauthorized access attempts, data exfiltration, or

attempts to compromise control systems (Shaukat et al., 2020c; Marinho and Holanda, 2023). ML can detect and prevent intrusions by analyzing network patterns and anomalies before they can cause harm.
3. Predictive maintenance for EnFV components: ML can be used to analyze historical data on EnFV components, such as battery health, motor performance, and wear and tear indicators, to predict when these components are likely to fail (Theissler et al., 2021; Zahra et al., 2021). This predictive maintenance capability allows for proactive replacement of components before they lead to malfunctions or safety hazards.
4. Secure vehicle-to-everything (V2X) communication: ML can play a crucial role in securing V2X communication, which enables EnFVs to exchange information with other vehicles, infrastructure, and pedestrians (Lipu et al., 2022). ML models can analyze V2X messages to detect malicious data injections, spoofing attempts, or attempts to disrupt communication channels.
5. User behavior analysis for EnFV security: ML can analyze user behavior patterns, such as driving habits, access patterns, and interaction with vehicle systems, to identify anomalies that may indicate unauthorized usage or compromised user accounts (Xiao et al., 2019). This behavioral analysis can help prevent unauthorized access and misuse of EnFVs.

These examples illustrate how ML improves EnFV security by providing real-time threat detection, predictive maintenance, and enhanced secure communication. As ML techniques advance, their impact on EnFV security will grow.

4.1.2. Factors affecting ML-based EnFV security solutions

Several factors can impact the effectiveness, reliability, and acceptability of ML-based security solutions as below (Rasool et al., 2022; Shaukat et al., 2020d).

1. Data Quality: Data quality is a critical factor in ML, as it directly affects the performance and generalizability of ML models. In the context of EnFV security, data quality issues can manifest in various forms:
   - Incompleteness: Missing or incomplete data can lead to biased or inaccurate models, potentially overlooking important patterns or anomalies.
   - Inaccuracy: Errors or inconsistencies in data can introduce noise into the training process, resulting in less reliable models for detecting genuine threats.
   - Bias: Bias in the underlying data can lead to biased models that unfairly discriminate against certain groups or conditions.

   Addressing data quality issues requires careful data collection, cleaning, and preprocessing. This may involve data imputation, outlier detection, and bias mitigation strategies.
2. Algorithmic Complexity: ML algorithms can range from simple linear models to complex deep neural networks. While complex algorithms can capture intricate patterns and relationships in data, they also introduce challenges:
   - Interpretability: Complex models can be difficult to understand, making it challenging to identify their strengths and weaknesses, interpret their decisions, and debug potential errors.
   - Overfitting: Complex models may overfit to the training data, becoming overly specific and failing to generalize well to new or unseen data.
   - Computational Cost: Training and running complex models can be computationally expensive, requiring significant hardware resources and increasing deployment complexity.

   Researchers explore techniques like model simplification, regularization, and interpretability to address these challenges. These techniques balance model complexity and interpretability, ensuring that models are practical and understandable.
3. Ethical Considerations: The application of ML in EnFV security raises ethical concerns that need to be carefully considered:
   - Privacy: EnFVs collect vast amounts of personal and sensitive data, including location, driving habits, and biometric information. ML models that analyze this data must adhere to strict privacy principles and protect user confidentiality.
   - Transparency and Accountability: ML models can make decisions with significant implications for safety and security. It is crucial to ensure that these decisions are transparent, explainable, and accountable, allowing affected individuals to understand why decisions were made and seek recourse if necessary.
   - Fairness and Non-discrimination: ML models should not perpetuate biases or discrimination present in the underlying data or training process. Employing bias detection and mitigation techniques is essential to ensure fair and equitable security measures.

   Addressing these ethical considerations requires a multi-pronged approach involving technical safeguards, clear ethical guidelines, and ongoing education and awareness campaigns.

4.2. Intrusion detection systems for EnFVs

In enhancing the security of EnFV systems, IDS play a pivotal role by actively monitoring and pinpointing unauthorized access, unusual behavior, and potential cyber threats (Park et al., 2020; Wu et al., 2019). As these vehicles become more interconnected and reliant on intricate networks and software, the demand for robust intrusion detection mechanisms becomes increasingly crucial. ML techniques have emerged as potent tools for creating intelligent and adaptive IDS capable of real-time detection and response to security breaches (Shrestha et al., 2021). Algorithms like neural networks, decision trees, and support vector machines enable the identification of subtle patterns indicative of unauthorized access or malicious activity by analyzing data from vehicle sensors, communication channels, and software interactions. By learning the normal behavior of the vehicle system, the IDS can then recognize deviations signifying intrusion attempts.

ML-based IDS offer several advantages over traditional rule-based systems within EnFV networks (Bangui and Buhnova, 2021; Berger et al., 2018). These advantages encompass adaptability to evolving attack methods and changes in normal behavior, real-time detection capabilities providing instant alerts and responses to potential threats, proficiency in identifying intricate patterns that might be missed by rule-based approaches, reduction of false positives through continuous learning, and automation of the intrusion detection process, easing the burden on human operators and facilitating swift threat responses. However, ML-based IDS also encounter challenges: DL models, while potent, might lack transparency and interpretability, highlighting the need for explainable decisions to foster trust.

1. Effective ML relies on abundant, high-quality training data accurately representing normal and abnormal behavior.
2. The limited computational resources of EnFVs require the development of lightweight yet effective ML models for intrusion detection.
3. Adversarial attacks could manipulate IDS through evasion tactics, necessitating research into robustness and defense mechanisms.

4.2.1. Case studies

In recent years, numerous ML based IDS have emerged for EnFV networks. Da Silva et al. (2022) conducted a systematic mapping study focused on UAVs to combat increasing threats, analyzing 56 research studies. They explored taxonomy, detected intrusions, ML approaches, UAV swarm applicability, and development standardization, identifying gaps and future directions for UAV security. Similarly, Wu et al. (2019) discussed the unique constraints of in-vehicle networks (IVNs) and surveyed IDS designs for IVNs, highlighting limitations and comparing optimization objectives. Sani et al. (2022) investigated privacy preservation techniques in the context of EVs, emphasizing the significance of securing private data when using ML and DL models. They examined scenarios for enhancing data security and surveyed privacy-preserving ML/DL methods for modern EVs, concluding with the growing interest and ongoing research in EV optimization.

Kosmanos et al. (2020) concentrated on security within dynamic wireless charging for EVs, introducing an IDS utilizing ML to counter spoofing attacks in Inter-Vehicle Communication (IVC) networks. This IDS identifies spoofing attackers in the wireless charging system and achieved accuracy exceeding 90%, aided by a unique metric called Position Verification using Relative Speed (PVRS), which improved accuracy by 6%. Their study also highlighted that combining ML algorithms through data fusion outperforms individual algorithms. Similarly, Avatefipour et al. (2019) addressed security vulnerabilities in EVs' Controller Area Network (CAN) bus due to the absence of message authentication. They proposed an anomaly detection model utilizing a modified one-class support vector machine (SVM) along with the Modified Bat Algorithm (MBA) for optimization. This model aimed to detect abnormal behavior in CAN traffic that may indicate cyberattacks and surpassed other techniques like Isolation Forest and conventional one-class SVM. The researchers employed logged CAN traffic data from a normal EV operation to train the model, demonstrating that their proposed model, incorporating MBA-enhanced one-class SVM, excelled in accurately detecting anomalies.

Narayanan et al. (2015) introduced a Hidden Markov model (HMM), a stochastic model following the Markov property, to identify unusual states in real vehicle operational data. The essence of utilizing an HMM is to treat the vehicle's motion as a sequence of interconnected events, where each event's occurrence depends on the preceding one, similar to Markovian processes. Alshammari et al. (2018) highlighted the CAN protocol, essential for efficient data transmission within vehicles. However, CAN lacks source and destination authentication, making it susceptible to message injection attacks that disrupt system operations. To address these issues, they proposed machine learning (ML) techniques, particularly K-Nearest Neighbors (KNN) and SVM algorithms, for clustering and classifying intrusions in Vehicle Ad-Hoc Networks (VANETs). Detection involves analyzing offset ratios and time intervals between message requests and responses in the CAN protocol. The paper emphasizes the significance of intelligent IDSs in modern connected vehicles to counter diverse attacks that can jeopardize vehicle performance, safety, and property. The study presents a CAN bus IDS tailored for intrusion detection, capable of identifying Denial of Service (DoS) and Fuzzy attacks. The research employed datasets for both attack types, yielding favorable outcomes with KNN and SVM algorithms.

Loukas et al. (2019) addressed the growing concern of cyber and cyber–physical threats to vehicles, highlighting the necessity of intrusion detection techniques to counter these risks. They presented a unified IDS taxonomy that could be universally applied to all vehicle types, offering guidance for researchers across diverse fields to contribute to a comprehensive vehicle IDS framework. This work advocated for the integration of ideas from various vehicle contexts, proposing solutions that encompass both cyber and physical audit features, a range of design architectures, and evaluations under more realistic conditions against a broader array of attacks. ElKashlan et al. (2023) introduced a classifier algorithm that utilizes ML techniques to identify malicious traffic within IoT environments. Using an actual IoT dataset, the study evaluated different classification algorithms, addressing both binary and multiclass traffic models. By implementing this algorithm within an IoT-based IDS tailored for EV charging stations, the system achieved improved stability and mitigation of potential cyberattacks that could disrupt daily operations. The paper underscored the vulnerability of the EV charging station ecosystem to a variety of attacks targeting IoT systems, emphasizing the importance of accurate and efficient detection methods. The proposed ML-IDS algorithm exhibited effectiveness in identifying diverse attack types, particularly excelling in anomaly detection and classification, as evidenced by its superior accuracy, precision, recall, and F-1 score using the IoT23 dataset.

Hsieh et al. (2021) developed an intrusion detection model for In-Vehicle Networks (IVNs) that employs a VGG16 classifier DL model to learn attack behavior characteristics and classify threats. The model's effectiveness is validated using a dataset from the Hacking and Countermeasure Research Lab (HCRL), encompassing various vehicle communication attacks. Their proposed classifier's performance is compared to the XGBoost ensemble learning approach for threat identification in IVNs. The evaluation includes accuracy, precision, recall, and F1-score metrics. Results show that the VGG16 and XGBoost classifiers achieve high accuracy rates for classification tasks. In a separate study, Suriya and Vijay Shankar (2022) introduced an innovative approach that combines deep learning-based IDS with chaotic generators to enhance EV Supply Equipment (EVSE) system security. Their IDS utilizes Gated Recurrent Units (GRU) and incorporates Enhanced Chaotic Scroll Attractor keys (ECSA) as countermeasures. This research introduces a unique dataset depicting EVSE under various attack scenarios, develops a high-accuracy GRU-based IDS, and designs enhanced chaotic encryption schemes to counter attacks. The study employs algorithm-centric metrics and key-centric metrics to comprehensively evaluate the system's performance, demonstrating its superiority over existing methods and its potential to bolster the security of Internet-enabled EVSE systems.

Berger et al. (2018) investigated the security of interconnected systems in modern vehicles, particularly vulnerabilities within the CAN bus. They examined the potential for cyberattacks as vehicles become more connected and evaluated the use of ML, including basic techniques like One-Class SVM, to detect anomalies in CAN bus data. Bangui and Buhnova (2021) focused on integrating Intelligent Transportation Systems (ITS) with emerging network technologies for smarter cities, considering the fusion of VANETs with UAVs to enhance connectivity. They highlighted security challenges in both VANETs and UAVs that advanced ML techniques, such as DL, can address. Hoang et al. (2019) examined a wireless relaying system involving a UAV acting as a relay against an active eavesdropper during authentication. They utilized one-class SVM and K-means clustering to build predictive models and generate datasets from wireless signals, demonstrating OC-SVM's stability and K-means clustering's performance against higher transmission power. Li et al. (2018) explored secure communication involving a transmitter, receiver, and adversarial UAV executing attacks. They proposed a Q-learning-based power control algorithm using non-cooperative game theory to adaptively counter UAV attacks, successfully reducing attack rates and enhancing system secrecy capacity, even with imperfect channel estimation. Xiao et al. (2018) focused on improving communication performance in VANETs by countering smart jammers. Traditional anti-jamming methods like frequency hopping are often ineffective due to VANETs' mobility and network scale. The proposed solution involved using UAVs as relays to transmit messages from onboard units (OBUs), enhancing communication reliability. The UAV strategically relayed messages to better radio transmission RSUs when the serving RSU is interfered or jammed. A game-theoretical approach modeled the interactions between the UAV and smart jammers, where the UAV decides on relaying messages, and jammers adjust their actions based on observed strategies. The study

derives Nash equilibria for the UAV relay game, determining optimal strategies considering transmit cost and channel conditions. The paper introduces a UAV relay strategy based on hotbooting policy hill climbing, aimed at resisting jamming without needing comprehensive knowledge of VANET and jamming models. Simulations showed that this strategy effectively reduces bit error rates and enhances VANET utility compared to a Q-learning-based approach.

Abbaspour et al. (2016) focused on creating a secure control system for UAVs to detect fault data injection (FDI) attacks that endanger UAV safety and functionality. Their proposed method utilized an adaptive neural network combined with an embedded Kalman filter (EKF) to identify FDI attacks in UAV sensors. This approach, specifically designed for cyber-attacks on UAV attitude sensors, provided real-time detection capabilities for sudden and gradual attacks, bolstering UAV resilience against cyber threats. Similarly, Chen and Chen (2019) investigated the vulnerability of UAV communications to privacy attacks arising from the broadcast of location data. Their ML-based approach demonstrated how an attacker could use ML techniques to decrypt UAV messages when possessing both plaintext and ciphertext, emphasizing the susceptibility of UAV messages. The study recommended further exploration into network coding-based encryption schemes for enhancing UAV communication security.

Perumalla et al. (2023) introduced the OAOFS-MLIDS technique for enhancing security in the Internet of Drones (IoD) network through intrusion detection. This method involves preprocessing data with minimal–maximal normalization, utilizing the OAOFS approach for feature subset selection, and applying the Coyote Optimization Algorithm (COA) combined with XGBoost for intrusion classification. In a separate study, Praveena et al. (2022) proposed a unique approach using Deep Reinforcement Learning (DRL) optimized by the Black Widow Optimization (BWO) algorithm for intrusion detection in drone networks. Their approach employs an improved RL-oriented Deep Belief Network (DBN) and leverages BWO to optimize DRL parameters for tailored intrusion detection. Ramadan et al. (2021) advanced FANET-ID methods by introducing a practical analytics framework utilizing Recurrent Neural Networks (RNN) for Anomaly Detection (AD) in FANETs, while Tan et al. (2019) enhanced an Intrusion Detection (ID) technique based on Deep Belief Networks (DBN) using Particle Swarm Optimization (PSO) to determine optimal DBN structure. Whelan et al. (2020) proposed a novel drone intrusion detection approach employing one-class classifiers, utilizing Principal Component Analysis (PCA) for dimensionality reduction, and incorporating Local Outlier Factor, One-Class SVM, and AE-NN classifiers for each sensor. Ouiazzane et al. (2022) introduced an autonomous method using Multi-Agent systems and ML techniques to identify DoS cyber-attacks on drone networks, demonstrating high accuracy in detecting both known and unknown attacks. Unlu et al. (2019) innovatively detected and tracked UAVs using a combination of cameras, optimizing time and memory utilization through an integrated multi-frame DL detection approach.

Park et al. (2020) emphasized the significance of IDS for UAVs. While prior approaches have included rule-based and supervised ML-based IDS solutions, these methods are constrained by dataset labeling efforts and the inability to detect novel attacks. To overcome these limitations, the authors proposed an IDS based on unsupervised learning. This approach obviates extensive labeling requirements and can identify anomalous UAV behavior regardless of the attack type. The proposed model employed an autoencoder trained on benign flight data, detecting attacks by assessing the reconstruction loss during flight. Notably, the model exhibited higher reconstruction loss during attacked flights compared to benign ones, facilitating intrusion detection. The objective was to offer an efficient and pragmatic IDS solution for UAVs, striking a balance between computational demands and real-world detection effectiveness. Chohan and collaborators (Chohan et al., 2023) explored the integration of AI (AI) in smart cities characterized by AI and Internet of Things (IoT) advancements. However, security concerns prompted the deployment of Intrusion Detection Systems (IDS) for monitoring network traffic anomalies. ML-based IDS was employed to enhance threat detection, evaluating multiple ML algorithms using the UNSW-NB15 dataset. Algorithms such as ADA Boost, Linear Support Vector Machine (LSVM), Auto Encoder Classifier, Quadratic Support Vector Machine (QSVM), and Multi-Layer Perceptron were assessed. ADA Boost achieved the highest accuracy of 98.3%, demonstrating its effectiveness in this context.

Table 1 presents a concise overview of the main aspects and contributions of each study, enabling a comparative examination of the problem tackled, objectives, optimization strategy, and notable contributions, advantages, and drawbacks of the respective research papers.

4.2.2. Challenges of ML-based IDSs for EnFVs

Numerous challenges related to the implementation of ML-based IDSs for EnFVs can be gleaned from the studies mentioned above. These challenges are succinctly summarized in Table 2, accompanied by potential solutions.

These challenges underscore the complexity of developing effective and robust IDSs for various vehicular and network environments, requiring interdisciplinary research efforts to address them effectively.

4.2.3. Research gaps

A thorough and meticulous analysis of the studies presented above highlights several research gaps and potential avenues for future investigation. These areas warrant attention to further advance the field of IDSs for vehicular and network environments.

1. **UAV IDS**
   - Development of novel intrusion detection techniques tailored for UAVs.
   - Addressing emerging threats and attack scenarios specific to UAVs.
   - Comprehensive evaluation of IDS solutions in real-world UAV scenarios.
2. **Security in EV Communication Networks**
   - Development of holistic security frameworks for EV communication networks.
   - Integration of encryption and authentication techniques in EV networks.
   - Scalability and performance evaluation of IDS solutions in larger EV networks.
3. **Privacy Preservation in EVs**
   - Balancing data utility and privacy protection in EVs.
   - Integration of privacy-enhancing technologies in EV systems.
   - Applying privacy preservation techniques to various EV applications.
4. **ML-Based IDS for UAV-Assisted Networks**
   - Optimization of ML-based IDS for real-time detection in UAV-assisted networks.
   - Robustness against adversarial attacks and tailored evasion techniques.
   - Scalability and effectiveness evaluation in large-scale UAV-assisted networks.
5. **Unsupervised IDS for UAVs**
   - Adaptability and robustness assessment of unsupervised IDS for UAVs.
   - Reduction of false positives in unsupervised UAV IDS.
   - Feasibility of implementing unsupervised IDS in resource-constrained UAV environments.

Table 1
Summary of ML-based IDS studies for EnFVs.

Study	Problem & Objective	Solution approach	Key contributions	Focus areas	Pros	Cons
Da Silva et al. (2022)	IDS for UAVs	Systematic mapping of 56 studies	Identifying gaps in UAV IDS	UAV IDS, ML, standardization	Comprehensive analysis	None specified
Wu et al. (2019)	IDS design for IVNs	Survey of IDS designs	Outlining trends	IDS for IVNs, limitations	Identifies trends	Does not delve into specific solutions
Kosmanos et al. (2020)	Securing EV IVC	ML for spoofing attacks	Introducing IDS for EV IVC	Security in EV IVC, spoofing	Addresses security, high accuracy	Focus on EV IVC networks
Avatefipour et al. (2019)	EV CAN bus security	Anomaly detection model	Proposed IDS for EV CAN bus	Security in EV CAN bus	Addresses specific concern, results	Focus on EV CAN bus security
Narayanan et al. (2015)	Abnormal state detection	Hidden Markov model	HMM for abnormal state detection	Abnormal state identification	Offers specific approach	Focus on abnormal state detection
Alshammari et al. (2018)	CAN protocol security	KNN, SVM algorithms	ML for intrusion detection in VANETs	Security in CAN protocol	Focus on VANET security	Focus on VANETs security
Loukas et al. (2019)	IDS for vehicles	Survey of IDS techniques	Comprehensive survey of IDS	IDS for vehicles, challenges	Comprehensive survey	Does not propose new solutions
ElKashlan et al. (2023)	IoT-based IDS for EV charging	ML-based classifier algorithm	Proposed IDS for EV charging	IoT-based intrusion detection	Addresses cybersecurity, effective detection	Focus on IoT-based IDS for EV charging
Sani et al. (2022)	Privacy in EVs	Privacy techniques with ML/DL	Exploration of privacy in EVs	Privacy preservation, ML/DL	Highlights importance of privacy	Focus on privacy in EVs
Berger et al. (2018)	Anomaly detection in CAN bus	ML methods evaluation	Comparison of ML methods	Anomaly detection, ML methods	Compares ML methods	Focus on anomaly detection
Bangui and Buhnova (2021)	ML-based IDS in VANETs and UAVs	Exploration of ML-based IDS	Review of ML-based IDS	ML-based IDS, privacy challenges	Reviews recent advancements	Does not provide specific solutions
Hoang et al. (2019)	UAV wireless relaying security	Predictive models for attacks	Predictive models for attacks	Wireless relaying, eavesdropper attacks	Addresses specific concern, efficient models	Focus on UAV wireless relaying
Li et al. (2018)	Secure communication with UAVs	Q-learning algorithm	Secure communication with UAVs	Secure communication, Q-learning	Addresses secure communication, proposes solution	Focus on UAV communication security
Xiao et al. (2018)	Improved VANET communication	UAV relay integration	Integration of UAVs as relays	Communication in VANETs	Proposes innovative solution	Focus on VANET communication improvement
Park et al. (2020)	Unsupervised IDS for UAVs	Unsupervised IDS with autoencoder	Efficient unsupervised IDS	IDS for UAVs, unsupervised learning	Offers efficient IDS solution	Focus on unsupervised IDS for UAVs
Chohan et al. (2023)	ML-based IDS for smart cities	ML algorithms comparison	Evaluation of ML algorithms	IDS in smart cities, ML algorithms	Provides insights into ML algorithms	Does not discuss specific attacks

Table 2
Summary of challenges and solutions for ML-based IDSs in EnFVs.

Challenge	Description	Probable solution
Diverse threats	Addressing varied attack methods across EnFV systems.	Hybrid IDS systems combining multiple algorithms.
Data complexity	Obtaining realistic datasets for IDS model training.	Curate large datasets, synthetic data generation, data augmentation.
Feature extraction	Extracting meaningful patterns from diverse data.	Feature selection algorithms, domain knowledge, DL models.
Algorithm selection	Choosing appropriate ML/DL algorithms for accurate detection.	Benchmarking, parameter tuning, ensemble methods.
Real-time detection	Quickly detecting evolving attacks.	Stream processing, edge computing, parallel processing.
Model generalization	Ensuring IDS models work across environments.	Transfer learning, domain adaptation, cross-validation.
Data privacy	Balancing intrusion detection with data security.	Data anonymization, encryption, differential privacy.
Limited resources	Designing lightweight IDS for constrained devices.	Lightweight ML models, model quantization, hardware solutions.
Adversarial attacks	Resisting evasion and adversarial attacks.	Adversarial training, robust optimization, anomaly detection.
Integration	Integrating IDS into existing systems.	Modular, adaptable IDS, compatibility with standard interfaces.
Real-world testing	Validating IDS in practical scenarios.	Industry collaboration, testbeds, realistic scenario simulation.
Scalability	Scaling IDS for large dynamic vehicular networks.	Distributed computing, scalable algorithms, dynamic network modeling.

6. IDS in Smart Cities

- Scalability of ML-based IDS in large-scale smart city environments.
- Effective differentiation between anomalies and attacks in smart cities.
- IDS solutions spanning network infrastructure, IoT devices, and critical services.

These research gaps highlight areas where further investigation and development can contribute to enhancing the security and resilience of UAVs, EV communication networks, intelligent vehicular networks, and smart cities.

4.3. Anomaly detection in vehicle behavior

The utilization of ML for anomaly detection plays a pivotal role in bolstering the security of EnFV systems. As these vehicles become

increasingly intricate and interconnected, rapidly identifying unusual behaviors or deviations from anticipated norms is essential to guarantee passenger safety and safeguard infrastructure. Anomalies can emerge from diverse origins such as cyberattacks, system malfunctions, or external interventions, underscoring the significance of early detection for timely counteraction and mitigation (Shaw et al., 2022; Shaukat et al., 2021b).

4.3.1. Case studies

Numerous ML approaches have emerged recently to tackle anomaly detection challenges within EnFV systems. For instance, Pace et al. (2022) introduced BDAV, a method for detecting anomalies in battery-powered aerial vehicles. BDAV employs simple ML models to establish connections between battery measurements and operational variables, utilizing the battery as a reliable diagnostic source. An unsupervised algorithm identifies anomalies, achieving a high detection rate of up to 90.9% and a low false-positive rate of about 2.5%. Shaw et al. (2022) addressed the robustness of autonomous drones by proposing a method that detects anomalies in drone behavior using diverse sensory data streams. This approach employs an ensemble of ML models, including supervised and unsupervised techniques, achieving near-perfect accuracy in detecting anomalies, reaching almost 100%. These studies collectively demonstrate effective anomaly detection approaches for EnFV systems.

Ahn et al. (2019) presented an ML-based method to detect anomalies in swarm drone flights. Their approach involves a two-step process: the first step utilizes unsupervised learning to classify flight data as normal or abnormal based on reduced-dimensional features. In contrast, the second step employs a deep neural network classifier with convolution layers and a multi-layer perceptron to distinguish anomalies from normal conditions. The method is validated using real flight test data, demonstrating its potential for online implementation. Khan et al. (2019) explored a real-time anomaly detection solution that moves away from traditional predefined feature-based methods, investigating the isolation forest algorithm's effectiveness for efficient decision-making in engineering applications. They demonstrated its superiority over other unsupervised distance-based approaches using the Aero-Propulsion System Simulation dataset and real-time experiments on an unmanned aerial vehicle. Bell et al. (2022) addressed accurate anomaly detection in UAV operations by combining a Long Short-Term Memory (LSTM) DL Autoencoder with dynamic thresholding and a weighted loss function. They aim to enhance safety, reduce operational costs, and advance aerial technology.

Li et al. (2020b) focused on securing intelligent charging stations within modern transportation systems. While previous research primarily addressed the security of intelligent vehicles, this study aimed to safeguard charging devices, which have received less attention. They introduced a novel anomaly detection approach using a Multi-Head Attention (MHA) model that captures correlations in traffic from power-related Industrial Control Systems (ICSs), extracting meaningful features to identify anomalies. Based on the Google Transformer encoder architecture, the MHA model outperformed other detection models with an accuracy rate of 99.86%. Similarly, Savić et al. (2020) examined anomaly detection in autonomous vehicles (AVs) using principal component analysis (PCA) and kernel PCA (KPCA) to handle complex sensor relationships. They applied these techniques to detect abnormal AV behavior using a dataset from IEEE SPS Signal Processing Cup 2020, emphasizing the need for high-quality datasets for reliable algorithm performance. Sindhwani and Sidahmed proposed an unsupervised approach to detect anomalies in hybrid aerial vehicle flight data for high-speed package delivery missions. Their method trained ML models on extensive flight log data to establish typical flight behaviors and identify abnormal missions, demonstrating robust performance in recognizing diverse anomaly types.

Adil et al. (2020) introduced a novel hybrid Dynamic Wireless Charging (DWC) method for EVs in a network context. This approach leverages parameters to enable efficient DWC in EVs, employing the Enhanced-Destination Sequential Distance Vector (Enhanced-DSDV) protocol for network establishment among participating EVs. Charging between paired EVs utilizes magnetic coupling, with an unsupervised ML Charge State Estimator (CSE) employed to learn the charging status. The CSE data is shared using embedded wireless nodes via the Enhanced-DSDV routing protocol. The proposed model allows EVs to exchange power wirelessly through onboard generators' magnetic fields. Each EV features a dashboard screen providing real-time information about nearby EVs' charge status, location, and distance. Real-world scenarios demonstrate the practicality and reliability of the approach for Dynamic Wireless Charging. Tran et al. (2023) tackled anomaly detection in video surveillance using drones with cameras, focusing on unusual events in complex traffic environments, especially roundabouts. To address the lack of suitable drone-based datasets, they created the UIT-ADrone dataset, containing realistic drone-captured videos of roundabouts in Vietnam. The dataset includes 51 videos covering about 6.5 h and over 206,000 frames, showcasing various abnormal events. They evaluated existing anomaly detection algorithms using the dataset, comparing their performance. Dixit et al. (2022) investigated AI techniques for detecting anomalies in Autonomous Electric Vehicles (AEVs), offering a comprehensive survey that addresses research gaps and presents an AI-driven anomaly detection solution taxonomy. The study discussed evaluation metrics for assessing the effectiveness of such methods and highlighted challenges in the field, proposing potential solutions.

Table 3 offers a concise overview of essential aspects and contributions outlined in each paper. This enables a comparative examination of the issues tackled, goals pursued, optimization methods employed, and notable advantages and disadvantages of each study.

4.3.2. Challenges of ML-based anomaly detection for EnFVs

Numerous challenges related to the incorporation of ML-based anomaly detection in EnFVs are apparent from the mentioned research. These challenges are summarized in Table 4, and the subsequent section offers a comprehensive examination of potential solutions.

Addressing the diverse challenges associated with anomaly detection in various domains, including aerial vehicles, drone behavior, charging systems, and autonomous vehicles, was essential to improve safety, efficiency, and reliability within these contexts.

4.3.3. Research gaps

The mentioned studies provide insights into existing research gaps in the realm of ML-driven anomaly detection for EnFVs. These gaps span diverse aspects of the field and signify potential avenues for further exploration and progress. Notable among these gaps are:

1. Limited Dataset Diversity: Many studies use specific datasets, not fully representing diverse EnFV real-world scenarios. Standardized datasets encompassing various anomalies, environmental conditions, and vehicle types could improve ML model robustness.
2. Scalability and Real-Time Implementation: While some studies succeed in controlled settings, scaling ML-based anomaly detection to EnFV fleets remains unexplored. Algorithms handling real-time analysis for diverse fleet sizes and complexities are crucial.
3. Adaptability to Dynamic Environments: EnFVs operate in evolving conditions. Existing approaches often lack adaptability to changing anomalies, driving conditions, and attack vectors. Techniques enabling dynamic learning and adaptation for ML models are needed.
4. Explainability and Interpretability: Some advanced ML algorithms lack transparency, posing challenges for safety-critical EnFVs. Developing methods providing clear anomaly explanations for human decision-making is vital.

Table 3
Summary of ML-based anomaly detection systems for EnFVs.

Study	Problem	Solution approach	Key contributions	Focus areas	Pros	Cons
Pace et al. (2022)	Anomalies in aerial vehicle systems	Battery-based diagnosis, unsupervised algorithm	High anomaly detection rate, real-world application	Aerial vehicle systems, Battery-based diagnosis	High detection rate, real-world applicability	Dependency on battery measurements
Shaw et al. (2022)	Robust drone behavior	Ensemble ML models on sensory data	Near-perfect anomaly detection	Drone behavior, Ensemble models	High accuracy, robust detection	Scalability, resource requirements
Ahn et al. (2019)	Anomalies in swarm drones	Unsupervised learning, deep neural networks	Automation of anomaly detection, online implementation	Swarm drone flights, Unsupervised learning	Online implementation, effective for swarm drones	Limited scalability details
Khan et al. (2019)	Real-time anomaly detection	Isolation forest algorithm	Outperforming other approaches, real-time applicability	Unsupervised anomaly detection	Real-time applicability, out-of-the-box	Lack of direct comparisons
Bell et al. (2022)	Improved UAV anomaly detection	LSTM autoencoder, dynamic thresholding	Enhanced accuracy and speed	UAV operations, Anomaly detection	Improved accuracy, dynamic thresholding	Complexity, resource requirements
Li et al. (2020b)	Secure charging stations	Multi-Head Attention (MHA) model	High accuracy in power-related anomaly detection	Charging stations, Anomaly detection	High accuracy, DL model	Limited discussion on vulnerabilities
Savić et al. (2020)	Anomalies in autonomous vehicles	PCA, kernel PCA	Evaluation of PCA and KPCA	Autonomous vehicles, Anomaly detection	Evaluation of PCA and KPCA	Limited performance discussion
Sindhwani et al. (2020)	Anomalies in hybrid aerial vehicles	Robust regression	Robust detection of hybrid vehicle anomalies	Hybrid aerial vehicles, Anomaly detection	Robust detection, data contamination	Dependence on extensive flight logs
Adil et al. (2020)	Dynamic wireless charging for EVs	Hybrid DWC approach, Enhanced-DSDV protocol	Reliable wireless charging with magnetic coupling	Dynamic wireless charging, EVs	Reliable charging, Enhanced-DSDV protocol	Complex setup, deployment challenges
Tran et al. (2023)	Unusual events in drone surveillance	UIT-ADrone dataset, anomaly detection algorithms	New dataset for drone surveillance evaluation	Drone surveillance, Anomaly detection	New dataset, realistic evaluation	Limited algorithm comparison
Dixit et al. (2022)	AI-driven anomaly detection in AEVs	Survey, AI-based anomaly detection	Comprehensive approach, survey, case study	Autonomous EVs, AI-based detection	Comprehensive survey, AI-driven solutions	Lack of specific implementation details

5. Data Privacy and Security: Anomaly detection relies on sensitive data, requiring privacy-preserving ML methods. Balancing anomaly detection and data confidentiality through privacy-preserving techniques is important.
6. Transferability of Models: ML models trained on one fleet might not work in different contexts. Enhancing model transferability across various EnFV scenarios without extensive retraining is valuable.
7. Real-world Testing and Validation: Extensive real-world validation of ML-based anomaly detection on EnFVs is essential. Field tests with diverse fleets under varied conditions validate system effectiveness.
8. Integration with Control Systems: Seamless integration of ML-based anomaly detection with EnFV control systems is crucial. Algorithms interacting with vehicle control systems for prompt anomaly responses need exploration.
9. Human–Machine Collaboration: EnFVs involve human operators interpreting anomaly alerts. Developing interfaces aiding collaboration between ML systems and human operators is vital.
10. Long-term Performance and Adaptation: Investigate long-term ML anomaly detection performance. Ensuring accuracy over time considering model degradation, concept drift, and changing anomalies is essential.

By focusing on these areas of research, not only would the advancement of ML-driven anomaly detection for EnFVs be promoted, but also the real-world safety, dependability, and effectiveness of EnFV systems would be improved.

4.4. Cyberattack detection and mitigation

Amidst swift technological progress, the widespread adoption of EnFV systems has brought about fresh prospects for transportation innovation and ease. Nevertheless, this digitized environment has simultaneously amplified the susceptibility to cyberattacks aimed at these intricate and interlinked systems. With society's growing dependence on such technologies, safeguarding EnFV systems from cyber threats has become an utmost priority (Dey and Khanra, 2020; Guo et al., 2020; Avatefipour et al., 2019; Shaukat et al., 2017).

4.4.1. Case studies

Recently, various ML techniques have been developed to address the intricate challenge of detecting and countering cyberattacks in EnFV systems. For instance, Bera et al. (2021) introduced ACSUD-IoD, an access control scheme utilizing blockchain to enhance security in an Internet of Drones (IoD) context. This scheme ensures the reliability of transactional data by storing it in a private blockchain, allowing for practical analysis. Security validation is conducted using the Real-Or-Random (ROR) model and the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Sazdić-Jotić et al. (2022) addressed the security threats posed by drones, presenting a radio frequency drone dataset and employing DL for detection and

Table 4
Summary of anomaly detection challenges and solutions for EnFVs.

Challenge	Description	Probable solution
Increasing complexity of aerial vehicles	Complexity rises, leading to higher anomaly risks. Anomaly detection in subsystems using battery data and ML.	Use battery measurements as reliable data source to diagnose other subsystems. Link battery data with operational variables. Employ unsupervised algorithms for anomaly detection.
Robust anomaly detection for drones	Ensuring drone robustness despite faults and failures. Ensembles and sensor data for anomaly detection.	Utilize various supervised and unsupervised ML models. Train on individual and combined sensor data. Achieve high drone behavior anomaly detection accuracy.
Anomaly detection for swarm drone flights	Simultaneous monitoring of swarm drones. Two-step approach: unsupervised learning and deep neural networks.	Use unsupervised learning for labeling flight data. Apply deep neural network with convolution and MLP layers for anomaly distinction. Automate swarm drone anomaly detection.
Real-time anomaly detection for UAVs	Efficient real-time anomaly detection for unknown anomalies. Evaluate isolation forest algorithm in UAVs.	Adopt isolation forest algorithm for real-time UAV anomaly detection. Outperform distance-based methods. Employ algorithm in UAV real-time experiments.
Enhancing anomaly detection for UAVs	Enhancing UAV anomaly detection using DL autoencoders, dynamic thresholding, and weighted loss.	Combine LSTM DL Autoencoder with dynamic thresholding and weighted loss functions. Enhance fault detection accuracy and speed in UAV operations.
Security of intelligent charging stations	Securing intelligent charging stations with unique protocols. Multi-Head Attention model for anomaly detection.	Create novel anomaly detection using Multi-Head Attention. Utilize deep architecture for real power supply anomaly identification. Achieve high charging station security accuracy.
Anomaly detection in autonomous vehicles	Detecting anomalies in autonomous vehicles using PCA and unsupervised learning.	Apply PCA and kernel PCA for autonomous vehicle anomaly detection. Employ regular PCA on reduced sensors while maintaining detection. Evaluate system behavior using camera data.
Anomaly detection in hybrid aerial vehicles	Anomaly detection in hybrid aerial vehicles using ML on extensive flight logs.	Develop robust regression algorithm for flight dynamics and anomaly identification. Address data contamination and recognize normal flight patterns without manual labeling.
Dynamic wireless charging for EVs	Implementing efficient dynamic wireless charging for EVs. Enhanced-DSDV protocol and unsupervised ML for charging status.	Use Enhanced-DSDV protocol and magnetic coupling for DWC charging. Apply unsupervised ML Charge State Estimator for charging status learning.
Anomaly detection in drone surveillance	Detecting unusual events in complex traffic with drone data. Evaluating anomaly detection algorithms using new dataset.	Generate UIT-ADrone dataset with drone-captured roundabout videos. Evaluate existing anomaly detection algorithms on new dataset.
Anomaly detection in autonomous EVs	Surveying AI-driven anomaly detection for AEVs and proposing case study.	Present comprehensive survey and taxonomy of AI-driven anomaly solutions. Introduce case study with CNN-LSTM classifier for real-world data anomaly classification.

identification. Their supervised DL algorithm achieved high accuracy in detection and identification. Yazdinejad et al. (2021) tackled drone authentication in IoT through federated learning, employing RF features and a Deep Neural Network (DNN) architecture. The model is trained locally on individual drones using Stochastic Gradient Descent (SGD) and secured with techniques like Homomorphic encryption and secure aggregation, achieving accurate drone authentication with improved performance compared to other ML methods.

Guerber et al. (2021) discussed the growing importance of securing communication within drone networks, particularly in swarm operations, by identifying external intrusion and internal network misuse as key attack types. The study showcased the effectiveness of Software Defined Network (SDN) architecture against common external attacks and introduced a method using SDN flow counters to detect traffic injection. A unique approach involving the Random Forest Classifier, based on ML, was proposed to tackle insider attacks, effectively identifying abnormal behaviors and common network attacks. Baig et al. (2022) addressed cybersecurity threats faced by drones in smart cities, proposing an ML-based method to detect threats and classify drone behaviors, with the random forest algorithm performing best. Shrestha et al. (2021) highlighted security concerns related to UAVs and proposed a security model combining UAVs, satellites, and 5G networks, using ML to detect vulnerabilities and cyberattacks. They demonstrated ML algorithms' efficacy in distinguishing between benign and malicious packets in UAV networks, with the decision tree algorithm showing exceptional performance in attack detection.

Shafique et al. (2021) investigated security challenges associated with advanced technology and hacking autonomous systems like UAVs, mainly focusing on spoofing and jamming attacks. Using the SVM ML algorithm, they introduced a novel approach to protect UAVs from GPS signal spoofing attacks. The study involved evaluating different learning algorithms, selecting the most suitable one, and employing K-fold analysis to create multiple K-learning models. These models were then combined through voting techniques to enhance accuracy. The proposed model utilized specific signal features to identify counterfeit GPS signals. Performance evaluations encompassing accuracy, precision, recall, and F1-score demonstrated the proposed methodology's effectiveness compared to existing techniques. Talaei Khoei et al. (2022) addressed UAV security against cyber-attacks, particularly GPS spoofing, and introduced two dynamic selection techniques to identify the best attack detection classifier. A one-stage ensemble feature selection method was developed to improve dataset quality. Ten ML models were evaluated, and the proposed dynamic techniques showcased superior performance, achieving high accuracy, detection probability, and low false alarm and misdetection probabilities. Li et al. (2022) presented an ML approach for detecting and categorizing jamming attacks targeting OFDM receivers, particularly in UAV applications. Different jamming attacks were assessed, and radiometric features were collected using SDR before and after launching jamming attacks. Numeric features and spectrogram images were utilized to create feature-based and spectrogram-based classification models using ML and DL techniques.

The spectrogram-based model outperformed the feature-based model regarding accuracy and false alarm rate.

Guo et al. (2020) discussed the mounting concern over cyber–physical security in power electronics systems, particularly within EV powertrains connected to intelligent traffic networks. Their innovative approach combined physics-guided principles and ML to identify cyberattacks on EVs across diverse driving scenarios. Data features related to system performance and vehicle dynamics, coupled with high-fidelity physical models, were integrated into an ML classifier. This classifier, validated through hardware-in-the-loop simulations, exhibited accurate cyberattack detection in various driving situations, providing a distinctive method for tackling cybersecurity challenges in EV powertrains. Warraich and Morsi (2023) focused on fast-charging stations' role in promoting EV adoption and the "vehicle-to-grid" concept while acknowledging the cybersecurity vulnerabilities introduced by integrating communication protocols. Their study proposed an ML-based approach to detect cyberattacks on fast-charging stations, particularly denial-of-service attacks, proactively. The research evaluated the method's efficacy using varying time resolutions of metering data in a microgrid setting with renewable energy resources and EVs in vehicle-to-grid mode. Results demonstrated that higher time resolution metering data enhanced detection accuracy, with the approach achieving approximately 98% accuracy in early detecting all three attack types. He et al. (2020) addressed the burgeoning impact of Connected and Autonomous Vehicles (CAVs) and the accompanying cybersecurity challenges. The authors introduced a Unified Modeling Language (UML)-based framework aligned with UK CAV cybersecurity principles, offering a structured approach to identifying potential vulnerabilities in CAV systems. They developed the CAV-KDD dataset for communication-based CAV cyberattacks and built classification models using Decision Tree and Naive Bayes algorithms. The models' accuracy, precision, and runtime were compared, highlighting the Decision Tree model's suitability for detecting communication-based CAV attacks due to its shorter runtime and improved performance.

Dey and Khanra (2020) addressed cybersecurity challenges arising from plug-in electric vehicles (PEVs) deployment and their potential vulnerability to cyberattacks. The paper highlighted the lack of attention given to PEV cybersecurity despite its recognized benefits, leading to consequences like denial-of-charging attacks and battery damage. The focus was on control-oriented solutions that developed algorithms to detect cyberattacks impacting battery packs during charging. The paper discussed two detection algorithms: a static detector using measured variables and a dynamic detector considering system dynamics and measurements. The dynamic detector, enhanced using a filter-based design approach, demonstrated greater efficacy in attack detection. Raj et al. (2021) introduced a biometric fingerprint-based access control system for enhancing EV safety and security. They acknowledged the increasing need for improved EV safety measures due to rising road accidents, negligence, drunk driving, and vehicle theft. The authors proposed an advanced system employing fingerprint recognition technology to prevent unauthorized access and vehicle theft. Their implementation and testing on an E-Bike showcased satisfactory performance, contributing to developing secure and safe EVs amidst the growing EV market.

Biron et al. (2018) discussed challenges and potential risks related to intelligent transportation technologies, specifically connected vehicle systems. While these systems offered advantages such as improved traffic flow and reduced accidents, they were vulnerable to cyber attacks due to vehicle-to-vehicle and vehicle-to-infrastructure communication. To enhance safety, the paper proposed a real-time detection scheme to identify denial-of-service cyber attacks and estimate their impact on the connected vehicle system. The scheme employed observers designed using sliding mode and adaptive estimation theory to monitor the system for signs of cyber attacks and evaluate their effects. The mathematical stability of the observers was analyzed using Lyapunov's stability theory. Simulation results demonstrated the effectiveness and robustness of the approach against various uncertainties. Al Gizi (2023) discussed the application of UAVs for inspecting power transmission lines, emphasizing enhancing accuracy through intelligent UAV control using DL and ML techniques. They introduced a tele-powered fuzzy-controller vehicle sonar tracking checker designed for preventive maintenance of high-voltage power lines, enabling navigation around obstacles that previously hindered inspections. The utilization of deep neural networks (DNNs) was highlighted for their capacity to improve accuracy and categorize errors in various ML tasks. The study also explored the combination of DNNs and drone-captured aerial photographs for diverse applications. This integration and AI technologies streamlined power line maintenance by swiftly identifying and addressing issues.

Zahra et al. (2021) addressed the rising accidents involving UAVs by introducing a predictive maintenance strategy for UAV propulsion systems. Given that machine failure contributes significantly to accidents, especially in propulsion systems, the study proposed a solution using neural networks to predict these systems' Remaining Useful Life (RUL). The approach involved anomaly detection, calculating the propulsion system's Health Indicator (HI), and predicting its RUL. Through experimentation and modeling of the degradation process of a quadrotor UAV propulsion system, the proposed method demonstrated compelling results in predicting system health and estimating RUL, highlighting neural networks' potential to enhance UAV maintenance and safety. Brulin et al. (2022) presented a model for multirotor UAV propulsion systems that incorporated both electrical and thermal characteristics of individual components. The model aimed to simplify the creation of fault detection systems for UAV propulsion chains by generating signals representing various types of faults in different components. By employing this model, extensive datasets of interconnected and scalable components could be simulated, avoiding the need to damage real hardware components for data collection.

Table 5 presented a summarized overview of the main parameters and contributions outlined in each paper, enabling a comparative assessment of the problem scope, objectives, optimization strategies, as well as notable strengths and limitations of each research endeavor.

4.4.2. Challenges of ML-based cyberattack detection and mitigation for EnFVs

Numerous intricate challenges inherent in the incorporation of ML-based Cyberattack Detection and Mitigation in EnFVs become apparent through the studies outlined above. These challenges are succinctly synthesized in Table 6.

Addressing these challenges would require careful consideration, validation, and refinement of the proposed solutions across various real-world scenarios and environments.

4.4.3. Research gaps

The studies analyzed in the earlier assessment have highlighted notable research deficiencies in the domain of ML (Machine Learning)-based Cyberattack Detection and Mitigation for EnFVs. These gaps encompass various dimensions of the field, offering opportunities for more profound investigation and advancement. Particularly noteworthy among these research gaps are:

1. Blockchain Integration Challenges: Some studies had suggested solutions based on blockchain to enhance security; however, there existed a gap in comprehending the scalability, interoperability, and efficiency of blockchain implementations in EnFV systems. Research was required to formulate optimized blockchain frameworks tailored to EnFV requirements and evaluate their real-world suitability.
2. Diverse RF Signal Scenarios: The studies that focused on drone detection using radio frequency signals highlighted the challenge of adapting models across varying environments. Research gaps were present in devising models capable of effectively adjusting to different RF scenarios, taking into account factors such as interference, signal degradation, and the presence of other wireless devices.

Table 5
Comparative analysis of ML-based cyberattack detection and mitigation for EnFVs.

Study	Problem & Objective	Solution approach	Key contributions	Focus areas	Pros	Cons
Bera et al. (2021)	Enhanced security in an IoD environment by detecting unauthorized UAV activities.	Blockchain-based access control scheme (ACSUD-IoD).	Introduced ACSUD-IoD using blockchain for secure UAV data storage. Rigorous security evaluation using formal methods. Demonstrated robustness and efficiency.	UAV security, blockchain	Enhanced security through blockchain.	Complexity of blockchain implementation.
Sazdić-Jotić et al. (2022)	Detected, localized, and identified malicious drones using radio frequency data.	Used DL algorithms (fully connected DNN) for radio frequency drone detection and identification.	Created publicly available drone dataset. Developed DL algorithm for drone detection and identification. Achieved high detection and identification accuracy.	Drone security, DL	High detection and identification accuracy.	Focus on radio frequency data may have limited generalization.
Yazdinejad et al. (2021)	Authenticated drones in IoT using federated learning to address data security and privacy concerns.	Implemented federated learning using RF features of drones and deep neural network architecture.	Proposed federated learning-based approach for drone authentication. Ensured security using encryption and aggregation techniques. Achieved better performance compared to other methods.	Drone authentication, federated learning	High accuracy in authentication with privacy protection.	Privacy concerns in federated learning.
Guerber et al. (2021)	Ensured communication security in drone networks and detected external and internal attacks.	Utilized SDN architecture, ML (Random Forest) for attack detection.	Explored SDN architecture resilience against attacks. Proposed Random Forest for insider attack detection. Achieved effective detection of abnormal behaviors.	Drone network security, SDN architecture	Effective detection of external and internal attacks.	May not have covered all possible attack scenarios.
Baig et al. (2022)	Detected threats to drones in smart cities and classified drone behaviors using ML.	Implemented ML algorithms for attack detection and classification.	Addressed drone threat detection in smart cities. Used ML to classify drone behaviors. Highlighted importance of cybersecurity in smart city drone operations.	Drone threat detection, ML	Enhanced security in smart city drone operations.	Evaluation may have needed more diverse attack scenarios.
Shrestha et al. (2021)	Countered cyberattacks in UAV networks using ML, satellite, 5G, and UAV technologies.	Developed intrusion detection models using various ML algorithms.	Developed security model combining UAVs, satellites, and 5G networks. Used ML for intrusion detection. Distinguished between benign and malicious packets.	UAV cybersecurity, satellite technology, ML	Effective intrusion detection in UAV networks.	Limited evaluation on real-world datasets.
Shafique et al. (2021)	Safeguarded UAVs against GPS signal spoofing attacks using machine learning (SVM).	Proposed SVM-based approach using signal features to detect GPS signal spoofing.	Developed SVM-based method for GPS signal spoofing detection. Used specific signal features to identify counterfeit signals. Achieved effective detection of spoofing attacks.	UAV security, GPS signal spoofing	Effective detection of GPS signal spoofing attacks.	May have required a more comprehensive feature set for generalization.
Talaei Khoei et al. (2022)	Enhanced the classification of attack detectors for UAV systems using dynamic selection techniques.	Developed dynamic selection techniques for identifying the best classifier for attack detection.	Proposed dynamic selection techniques for improved attack detection classification. Used a one-stage ensemble feature selection method. Achieved high accuracy and performance.	Attack detection, dynamic selection techniques	Enhanced classification of attack detectors.	May have required careful tuning of dynamic selection techniques.
Li et al. (2022)	Categorized jamming attacks on UAVs using ML based on radio signals.	Used ML algorithms for classification based on radio signal features.	Developed models for categorizing jamming attacks targeting UAVs. Utilized radio signal features for classification. Achieved high accuracy and a low false alarm rate.	UAV security, jamming attacks	Effective categorization of jamming attacks.	Limited evaluation on real-world datasets.
Guo et al. (2020)	Detected cybersecurity threats in EV power electronics systems using machine learning.	Implemented ML for cybersecurity threat detection in EV power electronics systems.	Addressed cybersecurity challenges in EV power electronics systems. Evaluated different ML algorithms. Identified the random forest algorithm as the most effective.	EV cybersecurity, power electronics systems	Effective detection of cybersecurity threats in EVs.	Had the need for further validation on broader datasets.
Warraich and Morsi (2023)	Early detected cyberattacks on EV fast-charging stations using machine learning.	Implemented ML-based approach for early cyberattack detection on EV fast-charging stations.	Proposed method for early detection of cyberattacks on EV charging stations. Demonstrated high detection accuracy.	EV charging stations, early cyberattack detection	Early detection of cyberattacks in EV charging stations.	Needed evaluation on broader datasets and scenarios.

(*continued on next page*)

Table 5 (*continued*).

He et al. (2020)	Developed a UML-based framework for CAV cybersecurity to address the lack of widely accepted frameworks.	Proposed a UML-based framework for CAV cybersecurity incorporating UK principles.	Introduced UML-based framework for CAV cybersecurity. Addressed the absence of widely accepted cybersecurity frameworks.	CAV cybersecurity, UML-based framework	Provided a comprehensive framework for CAV cybersecurity.	The framework may have required adaptation for specific use cases.
Dey and Khanra (2020)	Detected cyberattacks on PEVs during charging and enhanced PEV cybersecurity.	Developed algorithms for detecting cyberattacks during PEV charging.	Proposed algorithms for detecting cyberattacks during PEV charging. Demonstrated effectiveness through theoretical analysis and simulation studies.	PEV cybersecurity, charging process	Effective detection of cyberattacks on PEVs during charging.	Focus on PEV charging process may have limited broader applicability.
Raj et al. (2021)	Enhanced safety and security of EVs using a biometric fingerprint-based access control system.	Implemented a biometric fingerprint-based access control system for EVs.	Improved safety and security of EVs through the implementation of a biometric access control system.	EV safety, biometric access control	Enhanced safety and security of EVs through biometric access control.	Limited discussion on potential limitations.
Biron et al. (2018)	Developed a real-time detection scheme for denial of service attacks in connected vehicle systems.	Implemented a real-time detection scheme using observers and adaptive estimation theory.	Proposed a real-time detection scheme for denial of service attacks in connected vehicle systems. Analyzed the mathematical stability of observers.	Connected vehicle systems, denial of service attacks	Real-time detection of denial of service attacks in connected vehicles.	May have required further validation in real-world scenarios.
Al Gizi (2023)	Intelligently controlled UAVs inspecting power transmission lines using DL and ML.	Developed intelligent UAV control using DL and ML for inspecting power transmission lines.	Enhanced UAV inspection accuracy and obstacle navigation through intelligent control using DL and ML.	UAV inspection, DL, ML	Improved accuracy and obstacle navigation in UAV inspection.	Limited focus on cybersecurity aspects.
Zahra et al. (2021)	Predictive maintenance of UAV propulsion systems using neural networks.	Utilized neural networks for predicting the Remaining Useful Life (RUL) of UAV propulsion systems.	Proposed a neural network-based approach for predicting RUL of UAV propulsion systems. Improved UAV maintenance and safety through predictive maintenance.	UAV maintenance, predictive maintenance, neural networks	Improved UAV maintenance and safety through predictive maintenance.	Limited discussion on potential drawbacks.
Brulin et al. (2022)	Developed a model for multirotor UAV propulsion systems incorporating electrical and thermal characteristics.	Created a model for fault detection in multirotor UAV propulsion systems using electrical and thermal characteristics.	Proposed a model for fault detection systems using simulated data to avoid damage to real hardware components.	UAV fault detection, multirotor UAV propulsion systems	Avoided the need for damaging real hardware components for data collection.	Focus on simulated data may have limited real-world applicability.

3. Privacy-Preserving Federated Learning: Although federated learning addressed concerns related to data privacy, gaps persisted in ensuring the robustness of privacy-preserving mechanisms. There was ongoing exploration into developing methods that could strike a balance between data privacy and model accuracy.
4. Comprehensive Attack Scenario Coverage: The continuous research was required to address the challenge of encompassing a broad range of cyberattack scenarios within EV systems. There was a research gap in developing methods that could accurately capture and classify emerging attack patterns in evolving EV architectures.
5. Evaluation on Diverse Real-World Datasets: To validate intrusion detection models, access to diverse real-world network datasets had proven essential. A gap was evident in creating standardized datasets that could cover a wide spectrum of cyber threats, necessitating collaboration with cybersecurity experts to establish practical testing environments.
6. Robustness against GPS Signal Spoofing: The development of effective models for detecting GPS signal spoofing attacks necessitated access to dependable datasets and controlled experiments. Research gaps existed in crafting comprehensive GPS signal datasets that covered various attack scenarios, alongside the formulation of techniques capable of reliably distinguishing between authentic and spoofed signals.
7. Optimal Dynamic Selection Techniques: The challenge of tuning dynamic selection techniques for classifier configuration had posed a research gap. Further research was needed to identify automated methods capable of adaptively selecting classifiers based on real-time data, thus enhancing the accuracy of early attack detection.
8. Real-World Validation of Jamming Attack Detection: The research gap stemmed from ethical and regulatory concerns surrounding the validation of jamming attack detection models in real-world scenarios. There was an ongoing exploration into constructing controlled testing environments that could faithfully replicate jamming attacks while ensuring safety.
9. Adaptation to Different EV Scenarios: The customization of early cyberattack detection methods to suit diverse EV charging station architectures and systems had revealed a research gap. The development of solutions accommodating the varied charging systems and requirements of different EV scenarios had been deemed essential.
10. Unified CAV Cybersecurity Framework: The comprehensive research into creating a unified cybersecurity framework for diverse Connected and Autonomous Vehicle (CAV) systems had been lacking. Further efforts were needed to devise adaptable frameworks capable of addressing the diverse security challenges presented by distinct CAV architectures.

Table 6
Summary of challenges and probable solutions in ML-based cyberattack detection and mitigation for EnFVs.

Challenge	Description	Probable solution
Complexity of blockchain implementation	Integrating blockchain technology into EnFV systems was complex, requiring considerations of scalability, consensus, and compatibility.	The approach involved starting with smaller pilot implementations to understand blockchain intricacies, utilizing existing blockchain frameworks, considering hybrid solutions, and collaborating with experts in blockchain development.
Generalization of radio frequency signals	RF-based drone detection models sometimes struggled with variations in signal quality and interference in diverse environments.	Strategies included augmenting RF signal datasets with diverse scenarios, improving signal processing techniques, exploring transfer learning across different environments, and validating models across various operational conditions.
Privacy concerns in federated learning	Maintaining data privacy while aggregating data from multiple sources in federated learning setups posed challenges.	Approaches included utilizing secure aggregation techniques, considering differential privacy mechanisms, and applying encryption to protect sensitive data during aggregation.
Coverage of attack scenarios	Ensuring that ML models covered a wide range of attack scenarios in EV systems was difficult.	Strategies encompassed continuously updating models with new attack data, collaborating with security experts to identify emerging threats, and implementing techniques for feature extraction that captured diverse attack patterns.
Evaluation on real-world datasets	Evaluating intrusion detection models on real-world network datasets required ensuring diversity and representation of attack types.	Approaches involved augmenting datasets with new and evolving attack patterns, engaging with cybersecurity professionals for dataset creation, and employing data augmentation techniques to mimic different attack scenarios.
Data availability for GPS signal spoofing	Developing models to detect GPS signal spoofing attacks required access to reliable and diverse GPS signal data.	Strategies included collaborating with relevant organizations to access controlled GPS signal datasets, designing controlled experiments to generate spoofed signals, and ensuring data authenticity and traceability.
Tuning dynamic selection techniques	Tuning dynamic selection techniques for optimal classifier configuration posed challenges.	Approaches encompassed experimenting with different techniques and parameter combinations, utilizing cross-validation techniques, and conducting thorough validation to select the best configuration for dynamic classifier selection.
Real-world evaluation of jamming attacks	Evaluating jamming attack detection models using real-world data involved ethical and regulatory concerns.	Strategies included collaborating with regulatory bodies to create controlled environments for testing, validating models with simulated data before real-world deployment, and ensuring compliance with safety guidelines.
Applicability to different EV scenarios	Adapting early cyberattack detection to various EV charging station architectures and systems was complex.	Customization of detection algorithms for different EV scenarios, ensuring compatibility with diverse charging systems, and validating the proposed approach in representative real-world environments were key strategies.
Applicability to different CAV systems	Developing a unified cybersecurity framework for diverse Connected and Autonomous Vehicle (CAV) systems posed challenges.	The approach included collaborating with automotive manufacturers and industry experts to create adaptable frameworks, incorporating modularity for system-specific customization, and validating the framework across different CAV architectures.
Real-world validation of PEV algorithms	Validating cyberattack detection algorithms for plug-in EVs (PEVs) in real-world scenarios faced ethical and safety concerns.	Strategies comprised a combination of real-world and simulated scenarios, collaboration with regulatory bodies to establish testing standards, and partnering with industry stakeholders to conduct controlled experiments.
Integration of access control system	Integrating biometric access control systems into EVs involved compatibility and user experience challenges.	Collaboration with vehicle manufacturers for seamless integration, consideration of user-centric design principles, ensuring biometric system reliability, and conducting user testing for optimal user experience were pursued.
Balancing simulated and real-world data	Ensuring that predictive maintenance models performed well with both simulated and real-world data was crucial.	Creating high-quality simulated datasets that closely resembled real-world conditions, continuously validating models with actual data, and adjusting model parameters to enhance alignment between simulated and real-world performance were strategies employed.
Real-world validation of fault detection model	Validating fault detection models for UAV propulsion systems with real-world data was essential.	Approaches included collaborating with UAV manufacturers for access to real-world data, conducting controlled experiments, validating the model's performance across various fault scenarios, and ensuring that the model's predictions aligned with actual hardware performance.

11. Real-World Validation of PEV Algorithms: The validation of cyberattack detection algorithms for plug-in electric vehicles (PEVs) within real-world scenarios had represented a notable research gap. Collaborative endeavors involving regulatory bodies and industry partners had been necessary to establish testing standards and gather validation data from real-world scenarios.
12. Integration of Biometric Access Control: The integration of biometric access control systems into EVs had entailed addressing concerns related to user experience and compatibility. Research gaps were evident in the formulation of seamless integration methods that could ensure user-friendliness, reliability, and security.

13. Alignment Between Simulated and Real-World Data: Ensuring the effective performance of predictive maintenance models across both simulated and real-world data had been a research gap. Further work had been necessary to fine-tune simulation parameters and adjust models to achieve better alignment between simulated and real-world performance.
14. Validation of Fault Detection Models for UAV Propulsion: The validation of fault detection models for UAV propulsion systems using real-world data had been an existing research gap. Collaborative efforts with UAV manufacturers and controlled experiments had proven essential to validate model performance across various fault scenarios.
15. Vulnerability ML-based Security Systems to Adversarial Attacks: The increasing reliance on ML-based security systems has also highlighted the potential vulnerability of these systems to adversarial attacks (Shaukat et al., 2022). Adversarial attacks involve manipulating the input data to a ML model in a way that causes the model to make incorrect predictions. In the context of EnFVs, adversarial attacks could have serious consequences, such as enabling attackers to take control of vehicles or cause them to malfunction. The potential for adversarial attacks raises serious concerns about the safety and security of EnFVs. It is important to develop robust ML-based security systems that are resistant to adversarial attacks. This will require further research into the development of adversarial training methods, as well as the development of techniques for detecting and mitigating adversarial attacks.

Addressing these research gaps mandates the synergy of interdisciplinary collaboration, the exchange of data, meticulous experimentation, and a comprehensive strategy that acknowledges the multifaceted challenges presented by cyberattacks in EnFV systems.

4.5. ML for predictive maintenance

Within the domain of transportation security, the consistent and secure functioning of EnFV systems is a critical priority. Conventional maintenance methodologies have historically taken a reactive stance, addressing breakdowns or glitches after their manifestation. Yet, the infusion of ML methods into anticipatory maintenance approaches has brought about a transformative shift in the management of transportation systems, elevating the encompassing level of safety and security (Zahra et al., 2021; Theissler et al., 2021; Hassan et al., 2019).

4.5.1. Case studies

Recently, various ML methodologies have emerged to tackle the complex task of predictive maintenance within EnFV systems. For instance,Theissler et al. (2021) delved into recent progress in maintenance modeling through data-driven techniques like ML, explicitly focusing on their application within the automotive industry. Predictive maintenance is critical in ensuring operational safety and cost-efficient upkeep throughout a product's lifecycle. Given the wealth of operational data available in modern vehicles, ML presents itself as a suitable tool for predictive maintenance. Despite prior discussions on predictive maintenance and ML in the context of automotive systems, a gap persists in the literature concerning a comprehensive survey dedicated to ML-based predictive maintenance for such systems. This paper fills this void by systematically categorizing and analyzing pertinent studies based on their applications and ML approaches. It brings attention to the need for openly accessible datasets to foster research, the prevalent use of supervised methods requiring labeled data, the potential benefits of integrating diverse data sources, and the growing adoption of DL techniques, accompanied by the need for interpretability and ample labeled data. The paper concludes by addressing challenges and proposing potential avenues for future research in this domain.

Sundaram et al. (2021) emphasized the significance of DL and its application across diverse domains, particularly in critical electrical sectors. The paper introduces AI and ML, discusses the imperative for DL, outlines prevalent DL architectures, algorithms, and frameworks, and summarizes distinct DL techniques. It proceeds to review DL's deployment in crucial electrical domains, such as detecting bearing faults, identifying PV panel hot spots, diagnosing insulator issues, inspecting power lines, and improving EV systems. The objective is to comprehensively survey DL's integration into these realms, offering insights into architectures, frameworks, and techniques suitable for real-time applications. Bronz et al. (2020) tackled real-time fault diagnosis challenges in small-scale fixed-wing unmanned aerial vehicles (UAVs), considering factors like noisy data, communication limitations, and the effects of wing structures. The study demonstrated feasibility under real flight conditions and made publicly available flight logs for further exploration. The approach employed SVMs for the binary classification of nominal and faulty flight phases. Despite data limitations leading to overfitting, basic binary classification proved viable. Geometric imperfections common in small UAVs impacted prediction accuracy, enhancing multi-class classification. The proposed SVM algorithm achieved up to 95% accuracy in detecting loss of control effectiveness faults during real flights. The dataset and software are accessible to the wider community. Trivedi et al. (2022) introduced a framework for detecting faults in EVs using DL and blockchain technology. With EVs gaining popularity in transportation, ensuring their reliability is paramount. The framework employs convolutional neural networks (CNNs) and long short-term memory (LSTM) models to predict faults such as abnormal air tire pressure, temperature irregularities, and battery malfunctions in EVs. This predictive capability enhances travel safety. Furthermore, integration with a 5G wireless network and the interplanetary file system (IPFS) protocol facilitates secure and scalable data transactions for fault detection. Incorporating blockchain technology provides the system an added layer of security and reliability. Through simulations, the framework demonstrates approximately 70% accuracy in detecting various faults and favorable performance metrics, indicating its efficacy in improving EV fault detection.

ML for predictive maintenance represents a transformative approach to enhancing transportation security. By harnessing the power of data analysis and pattern recognition, this technology contributes to the longevity, reliability, and safety of EnFV systems. As the transportation industry continues to evolve, the integration of predictive maintenance will remain an essential tool in safeguarding passengers, infrastructure, and the overall security of modern transportation.

In conclusion, ML can potentially revolutionize EnFV maintenance frameworks and surveillance and security systems. By introducing real-time threat detection, predictive maintenance capabilities, and enhanced anomaly detection, ML integration offers numerous benefits. In maintenance frameworks, predictive maintenance is achieved by analyzing historical data to predict component failures, optimizing procedures, reducing downtime, and improving EnFV availability. In surveillance and security systems, ML enhances threat detection by analyzing sensor data and user behavior patterns, detecting anomalies indicative of potential security threats. The integration of ML ensures real-time threat detection, predictive maintenance, enhanced anomaly detection, reduced downtime, and improved safety. However, challenges include data quality, model explainability, computational requirements, and ethical considerations. Addressing these challenges involves data quality management, Explainable AI (XAI) methods, hardware optimization, and ethical guidelines and framework adherence. Through responsible practices, ML can significantly contribute to the safety, security, and efficiency of EnFVs.

Table 7 offers a condensed overview of the essential aspects and achievements of each paper. This permits a comparative assessment of the tackled issue, objectives, optimization methodology, and primary contributions, as well as the strengths and weaknesses of each study.

Table 7
Comparative analysis of ML-based predictive maintenance within EnFVs.

Study	Problem & Objective	Solution Approach	Key Contributions	Focus Areas	Pros	Cons
Theissler et al. (2021)	Exploring advancements in maintenance modeling using ML in the automotive industry	Conducting a comprehensive survey of ML-based PdM for automotive systems, categorizing and analyzing relevant papers	Filling a gap in the literature, emphasizing the need for open datasets, discussing challenges and suggesting future research directions	Predictive Maintenance, Automotive Industry	Providing insights into challenges and suggesting future directions	Would benefit from additional specific case studies and more in-depth technical analysis
Sundaram et al. (2021)	Investigating the significance of DL in critical electrical areas and reviewing DL's applications in various domains	Providing an introduction to AI, ML, and DL, conducting a review of DL's application in electrical fields	Presenting a comprehensive survey of DL's integration into electrical domains, offering insights into architectures and frameworks	DL, Electrical Fields	Offering insights into multiple DL architectures and their applications	Some areas could benefit from more technical depth and detailed implementation examples
Bronz et al. (2020)	Analyzing real-time fault diagnosis challenges in small-scale fixed-wing UAVs	Utilizing SVM for binary classification of nominal and faulty flight phases, making dataset and software available	Demonstrating the feasibility of real-time fault diagnosis in small UAVs, showcasing SVM's accuracy in fault detection	UAV Fault Diagnosis, SVM Classification	Providing a practical approach and making real-flight data available	Would benefit from more extensive experimentation and validation in diverse UAV scenarios
Trivedi et al. (2022)	Examining fault detection in EVs using DL and blockchain technology	Applying CNN and LSTM models for fault prediction in EVs, integrating 5G wireless network and IPFS protocol	Proposing a framework to enhance EV fault detection, incorporating secure data transactions using blockchain technology	EV Fault Detection, Blockchain Technology	Addressing EV reliability, security, and fault prediction using innovative technologies	The performance of DL models could be further improved, and blockchain technology might introduce latency and complexity

4.5.2. Challenges of ML-based predictive maintenance for EnFVs

Numerous challenges related to the implementation of ML-based predictive maintenance within EnFVs become evident upon analyzing the studies mentioned earlier. These challenges have been comprehensively compiled in Table 8, offering a concise overview.

These challenges collectively shape the complexity and ongoing research efforts in the domain of predictive maintenance and cyberattack detection for EnFVs.

4.5.3. Research gaps

The studies examined in the preceding discussions have shed light on several notable research gaps within the domain of ML-based predictive maintenance for EnFVs. These gaps encompass a wide array of aspects within the field, presenting opportunities for further investigation and advancement. Some prominent research gaps that arise from the analysis include:

1. Standardized Datasets Absence: Numerous studies in this domain depended on limited or proprietary datasets, hindering result reproducibility and comparability. The necessity for publicly available, standardized datasets encompassing diverse operational scenarios, vehicle types, and potential attack patterns is evident. These datasets would facilitate the validation and benchmarking of novel algorithms and methods.
2. Limited Real-World Implementation: Despite several studies proposing promising solutions, practical deployment of these solutions in operational EnFV systems was often constrained. Additional research was necessary to bridge the gap between research prototypes and actual implementation, accounting for factors like integration complexities, scalability, and system constraints.
3. Interdisciplinary Collaboration: EnFV's domain integrates various fields, such as transportation, cybersecurity, and ML. Effectively connecting these domains demanded interdisciplinary collaboration, along with common frameworks, methodologies, and standards development.
4. Data Imbalance and Anomalies: The occurrence of infrequent events like cyberattacks or specific failure modes led to data imbalance, rendering accurate predictive model development challenging. Research was needed to explore techniques addressing imbalanced data, anomaly detection, and synthetic data generation to mitigate data scarcity.
5. Adversarial Robustness: Given the susceptibility of ML-based systems to adversarial attacks, creating robust models for detecting and mitigating attacks was a pivotal research gap. Designing methods capable of effectively recognizing and countering EnFV-specific adversarial attacks remained essential for system security.
6. Scalable and Real-Time Solutions: With the expansion of EnFV fleets, the issue of maintaining accuracy and real-time processing became more prominent. Research was required to develop scalable, efficient algorithms capable of handling the escalating data volume while ensuring timely predictions and detections.
7. Human–Machine Interaction: Integrating ML-based predictive maintenance and cyberattack detection solutions with human operators posed challenges involving interpretable explanations, instilling trust in automated systems, and designing user interfaces enhancing decision-making.
8. Cost-Effective Solutions: The implementation cost of ML-based solutions, encompassing infrastructure, computation, and maintenance, often acted as an adoption barrier. Research efforts were directed toward devising cost-effective approaches, striking a balance between the advantages of predictive maintenance and cyberattack detection against associated expenses.
9. Regulatory and Ethical Considerations: The integration of ML into EnFVs introduced ethical and regulatory inquiries concerning data privacy, accountability, and industry standards compliance. Addressing these considerations was crucial to ensure the responsible deployment of systems, engendering user trust.
10. Long-Term Reliability: Operating in dynamic and challenging environments, EnFVs faced the challenge of ensuring the long-term reliability of ML-based systems. Research aimed at exploring techniques for model monitoring, adaptation, and retraining to sustain accurate predictions and detections throughout a vehicle's lifecycle.
11. Legacy Systems Integration: EnFV systems encompassed a mix of modern and legacy components. Research was essential to

Table 8
Summary of ML-based predictive maintenance challenges and probable solutions for EnFVs.

Challenge	Description	Probable solution
Data availability and quality	Acquiring sufficient, high-quality data for training and validation of ML models posed a challenge.	Implemented data collection strategies, improved sensor accuracy, and considered data augmentation techniques.
Interpretable DL	Ensuring DL models were interpretable and explainable for better decision-making was essential.	Developed model interpretability techniques, used explainable AI methods, and visualized model decision-making processes.
Model generalization	Ensuring ML models generalized well to diverse operating conditions, vehicle types, and attack scenarios was a challenge.	Utilized transfer learning, data augmentation, domain adaptation, and adversarial training to improve model generalization.
Lack of labeled data	Difficulty in obtaining labeled data, especially for rare events or new attack patterns, presented a hurdle.	Employed semi-supervised learning, active learning, data labeling strategies, and synthetic data generation.
Complex System Dynamics	Vehicle systems' intricate and interconnected nature posed challenges in modeling their dynamics.	Utilized physics-based modeling, incorporated domain knowledge, and engaged in feature engineering to capture system complexities.
Integration of data sources	Efficiently integrating and processing data from various sources to enhance predictive capabilities was a challenge.	Developed data fusion methods, calibrated sensors, and integrated data from IoT and communication networks.
Security and privacy	Handling sensitive data while maintaining user privacy and system security was a concern.	Implemented privacy-preserving ML methods, ensured secure data transmission and storage, and employed encryption techniques.
Real-Time processing	Ensuring ML algorithms operated effectively in real-time, especially with limited onboard resources, posed a challenge.	Optimized algorithms for real-time processing, used lightweight models, and exploited hardware acceleration.
Scalability	Maintaining accuracy and responsiveness as EnFV fleets scaled up in number was a consideration.	Designed distributed and scalable ML architectures, leveraged cloud resources for computation and storage.
Cost considerations	Balancing the benefits of ML integration with the associated infrastructure and resource costs was important.	Evaluated cost-effectiveness, considered open-source solutions, and prioritized high-impact use cases.
Adversarial attacks	Protecting ML models from adversarial attacks that aimed to deceive or mislead the detection process was a challenge.	Implemented adversarial training, employed robust optimization techniques, and developed anomaly detection methods.
Regulatory compliance	Ensuring ML-based solutions adhered to safety, privacy, and data protection regulations and standards was a concern.	Collaborated with legal and regulatory experts, conducted thorough compliance assessments, and adopted industry standards.

develop strategies enabling the seamless integration of ML-based solutions with existing systems and legacy equipment, guaranteeing interoperability and reliability.

Working to fill these identified research gaps would result in significant progress for predictive maintenance and cyberattack detection within Electric and Networked Fleets of Vehicles (EnFVs). This progress would improve these systems' safety, reliability, and security, which are becoming progressively essential components of contemporary transportation infrastructure.

5. Future directions and emerging trends

Recently, the domain of transportation security has experienced a dynamic interaction between technological progress and the continuously changing panorama of risks and weaknesses. As we steer through the complex terrain of the future, this segment delves into the promising possibilities and emerging patterns that could influence the trajectory of security enhancement within EnFV systems.

5.1. Advancements in ML for transportation security

The swift advancements in ML methodologies have recently brought about significant transformations across diverse sectors, including transportation security. This field is no exception to the transformative impact of technology. As technology's evolution persists, the continuous progress in ML opens up thrilling avenues for fortifying the security of Electric and Networked Fleets of Vehicles (EnFV). These innovations enhance the capacity to identify and counter potential risks and lay the foundation for more effective and resilient security protocols.

1. Advanced Threat Detection: The development of more sophisticated ML algorithms enabled the identification of complex and subtle threats. These algorithms analyzed vast amounts of data from sensors, cameras, and other sources to detect anomalies and patterns indicative of potential security breaches (Marinho and Holanda, 2023). As ML models became more accurate and adaptive, they could better distinguish between normal and abnormal behavior, enhancing the effectiveness of threat detection systems (Heidari et al., 2023; Mohamed et al., 2023).
2. Real-time Decision-Making: ML algorithms were increasingly used to make real-time decisions in security-critical scenarios. Autonomous decision-making processes, guided by ML models, rapidly responded to emerging threats and mitigated risks effectively. These systems dynamically adjusted security protocols, rerouted vehicles or triggered emergency measures based on evolving situations (Xu et al., 2019; Li et al., 2020a; Althubiti et al., 2022).
3. Explainable AI for Transparency: As ML algorithms became more complex, the challenge of understanding their decision-making processes also grew. Advancements in explainable AI (XAI) aimed to provide insights into how these models arrived at their conclusions. This transparency was crucial in transportation security, where decision rationale needed to be understandable to human operators and regulators (Dixit et al., 2022; Sazdić-Jotić et al., 2022).
4. Federated Learning for Privacy: The rise of federated learning allowed multiple parties to collaboratively train ML models without sharing sensitive data. In transportation security, vehicle manufacturers, service providers, and regulatory bodies could

pool their data to improve threat detection models while maintaining data privacy (Yazdinejad et al., 2021; Ibrar et al., 2022). This approach helped address data sharing and privacy concerns in a collaborative environment.

5. Continual Learning and Adaptation: EnFV systems operating in dynamic and evolving environments. ML models capable of continual learning and adaptation updated their knowledge and behavior over time. This adaptability ensured that security measures remained effective in the face of emerging threats and changing circumstances (Ouiazzane et al., 2022; Shaukat et al., 2020a).
6. Multimodal Fusion for Enhanced Situational Awareness: Combining data from various sources, such as sensors, cameras, and communication networks, through multimodal fusion provided a more comprehensive understanding of the transportation environment. Advanced DL techniques integrated these diverse data streams to improve situational awareness, leading to more accurate threat detection and prevention (Li et al., 2020b; Sazdić-Jotić et al., 2022).
7. Human–Machine Collaboration: As autonomous and semi-autonomous vehicle systems became more prevalent, the collaboration between humans and machines in security operations became crucial. ML facilitated human decision-making by providing real-time insights, recommendations, and predictions based on complex data analysis (Maulik and Kundu, 2023; Shaukat et al., 2020b).
8. Continued Innovation in Neural Architectures: Ongoing research into novel neural network architectures could further enhance the performance of machine and DL models in transportation security. Techniques such as capsule networks, graph neural networks, and transformer-based architectures could offer improved accuracy, robustness, and efficiency in threat detection and response (Vanitha and Ganapathi, 2020; Abbaspour et al., 2016).
9. Data Augmentation: Addressing the data scarcity issue in machine learning for EnFVs through data augmentation presents a promising future direction (Alzubaidi et al., 2023). As EnFV datasets are often limited in size and diversity, leveraging advanced data augmentation techniques can enhance model performance and generalization. Future research could focus on developing tailored data augmentation strategies that account for the challenges and nuances of EnFV scenarios, such as rare events, diverse operational conditions, and potential cyber threats. By exploring innovative augmentation methods and integrating domain-specific knowledge, researchers can contribute to creating more robust and effective machine learning models for predictive maintenance, cyberattack detection, and other critical applications in EnFVs.
10. Model interpretability: Model interpretability is pivotal for ensuring expected behavior, identifying vulnerabilities, and fostering trust in real-world deployment (Renda et al., 2022). Techniques such as feature importance, model visualization, counterfactual explanations, and post-hoc interpretability methods can be explored to enhance interpretability. In deploying machine learning models for critical EnFV security, factors like accuracy, robustness, and efficiency are vital. Addressing this aspect will contribute to the practical adoption and effectiveness of the proposed ML models in securing EnFVs.
11. Quantum Computing for EnFV Security: In anticipating the future trajectory of machine learning for EnFV security, quantum computing emerges as a pivotal and transformative technology. Quantum computing's prowess in handling complex calculations and large datasets can revolutionize machine learning algorithms, particularly in identifying and predicting cyberattacks with enhanced precision and efficiency (Burkacky et al., 2020). Integrating quantum computing into EnFV security-oriented machine learning opens avenues for advanced anomaly detection, enabling real-time analysis of sensor data and network traffic to identify potential threats promptly. Furthermore, quantum-enhanced machine learning models could significantly improve predictive maintenance, offering more accurate predictions of system issues for proactive maintenance and disruption prevention. Quantum computing also holds promise in shaping advanced cybersecurity threat models, simulating intricate cyberattacks to anticipate vulnerabilities proactively (Ralegankar et al., 2021). Developing secure communication protocols backed by quantum cryptography, ensures confidentiality and resistance to eavesdropping or manipulation in EnFV systems. As quantum computing continues to mature, its synergy with machine learning stands poised to revolutionize EnFV security, effectively addressing the evolving threat landscape and ensuring the integrity, availability, and safety of these groundbreaking transportation systems (Kumar et al., 2021).
12. Edge Computing for EnFV Security: Future-oriented technologies like edge computing play a pivotal role in shaping the trajectory of ML for EnFV security advancements (Garg et al., 2019). By bringing computational capabilities closer to data sources, Edge computing facilitates swift and efficient processing of real-time information generated by EnFVs. This capability is crucial for ML algorithms to make timely and precise decisions in security-critical scenarios, reducing reliance on cloud-based infrastructure and enhancing overall responsiveness. The integration of edge computing and ML in EnFV security involves equipping edge devices with ML models for real-time sensor data analysis, enabling the timely detection of anomalies indicative of cyberattacks or system malfunctions. Additionally, edge computing facilitates the deployment of federated learning algorithms, enabling collaborative ML model training without compromising data privacy or security. This edge computing and ML convergence unlocks new possibilities for real-time threat detection, anomaly identification, and predictive maintenance, contributing to a more secure and resilient transportation ecosystem (Hua et al., 2023).

5.2. Integration of AI with autonomous vehicles

The automotive sector has recently experienced a transformative change by introducing autonomous vehicles, a groundbreaking technological development set to redefine transportation. Central to this evolution is the incorporation of AI into autonomous vehicles, a collaborative approach with significant potential to elevate safety, efficiency, and the broader landscape of transportation security.

1. The Role of AI in Autonomous Vehicles: AI-enabled autonomous vehicles to perceive, reason, and act in dynamic and complex environments. Through a combination of advanced sensors, computer vision, ML algorithms, and deep neural networks, AI-equipped these vehicles with the ability to interpret their surroundings, make real-time decisions, and navigate safely without human intervention. This integration enabled autonomous vehicles to analyze massive amounts of data, anticipate potential hazards, and adapt to changing scenarios with remarkable precision (Mohamed et al., 2023).
2. Enhancing Security through AI: One of the most compelling aspects of integrating AI with autonomous vehicles was its potential to enhance security measures significantly. AI-powered autonomous vehicles can process data from various sources, including cameras, LiDAR, radar, and GPS, to identify potential threats, avoid collisions, and respond to emergencies swiftly. By continuously analyzing their surroundings, AI-driven autonomous vehicles could detect anomalous behaviors or unauthorized access attempts, contributing to proactive threat prevention and robust security enforcement (He et al., 2020; Bera et al., 2021).

3. Challenges and Considerations: While integrating AI with autonomous vehicles offered unprecedented benefits, it also presented complex challenges and ethical considerations. Ensuring the security of AI algorithms and preventing adversarial attacks against autonomous vehicles became critical imperatives. Furthermore, the dependability of AI systems in critical situations, accountability for accidents or failures, and the potential impact of AI biases on decision-making processes warranted careful examination (Dixit et al., 2022).
4. Emerging Trends: As the field of autonomous vehicles evolved, several trends emerged at the intersection of AI and transportation security (Heidari et al., 2023; Loukas et al., 2019; Srivastava et al., 2021):
    - Multi-Sensor Fusion: Autonomous vehicles incorporate an increasing number of sensors to enhance perception accuracy. Multi-sensor fusion and AI techniques allowed vehicles to create a more comprehensive and reliable understanding of their environment.
    - Real-Time Threat Detection: AI-driven autonomous vehicles could rapidly identify potential threats, such as pedestrians, cyclists, or other vehicles, and take evasive actions in real-time to ensure the safety of passengers and the surrounding environment.
    - behavioral Analysis: AI systems learned and recognized typical behaviors of road users, enabling autonomous vehicles to predict and respond effectively to unpredictable or non-standard actions.
    - Secure Communication: AI-enabled autonomous vehicles utilized secure communication protocols to exchange critical information with infrastructure components, such as traffic lights and road signs, contributing to safer and more coordinated traffic flow.
    - Continuous Learning: AI's adaptive nature enabled autonomous vehicles to continuously learn from their experiences and improve their decision-making capabilities, enhancing their ability to handle new and complex scenarios.

5.3. Research gaps and potential areas of exploration

As the field of EnFV systems rapidly advances due to technological progress, the need to recognize and bridge research gaps while uncovering new areas of investigation becomes more crucial. This section explores existing research gaps and unexplored prospects, highlighting the importance of strengthening security within these transformative transportation technologies.

1. Adapting Security Models for Evolving Threats: While ML showed promise in bolstering security, the dynamic nature of cyber threats demanded continuous adaptation of security models. Research was needed to develop self-learning and self-evolving security systems to swiftly identify and counteract emerging threats, ensuring robust protection against evolving attack vectors (Srivastava et al., 2021; Marinho and Holanda, 2023).
2. Human-Centric Security: The integration of AI and autonomous systems in transportation raised questions about the human factor in security. How could security measures be designed to accommodate human decision-making and interventions while maintaining high protection? Exploring human-centered security models and understanding the interplay between AI-driven systems and human operators was a vital study area (Maulik and Kundu, 2023).
3. Ethical and Legal Implications: As autonomous systems became more prevalent, ethical and legal considerations became paramount. Research is needed to delve into the ethical dilemmas surrounding security decisions made by AI algorithms and address issues related to accountability, liability, and decision transparency. Establishing ethical guidelines and legal frameworks for AI-driven security measures was essential (Dixit et al., 2022; Loukas et al., 2019).
4. Secure Data Sharing and Interoperability: EnFVs generate vast amounts of data that must be shared securely for effective traffic management and coordination. Investigating secure data-sharing protocols, interoperability standards, and data privacy mechanisms was crucial for creating a seamless and secure transportation ecosystem (Heidari et al., 2023; Sani et al., 2022).
5. Resilience to Physical Attacks: While much attention was directed toward cyber threats, the vulnerability of EnFVs to physical attacks should not be overlooked. Research could explore methods to enhance the physical resilience of vehicles, infrastructure, and communication systems against sabotage and malicious activities (Loukas et al., 2017).
6. Human–Machine Interaction Security: As transportation systems became more automated and integrated with AI, ensuring the security of human–machine interactions became essential. Studying how AI interpreted and responded to human inputs and developing secure methods for human authentication and control was vital for safe and secure operation (Heidari et al., 2023; Putri et al., 2021; Mohamed et al., 2023).
7. Real-Time Threat Intelligence: The ability to anticipate and respond to threats in real time was an essential security aspect. Research should focus on developing advanced threat intelligence systems that utilize machines and DL to monitor, analyze, and predict potential security breaches continuously (Biron et al., 2018; Hsieh et al., 2021).
8. Regulatory Frameworks for Emerging Technologies: The regulatory landscape needed to keep pace with the rapid development of EnFV systems. Research could contribute to formulating comprehensive regulatory frameworks that strike a balance between innovation and security, fostering a conducive environment for adopting new technologies (Reddy et al., 2021; Marinho and Holanda, 2023).
9. Broader Security Facets: In addition to the specific focus on predictive maintenance and cyberattacks in EnFVs, it is essential to recognize the paramount importance of addressing broader security facets, particularly physical safety and privacy within the EnFV ecosystem (Zhi et al., 2020; Mekdad et al., 2023). Ensuring the physical safety of EnFVs involves robust measures to mitigate risks of accidents, collisions, and unauthorized access. Additionally, safeguarding privacy is crucial as EnFVs have various sensors and communication technologies that process sensitive data. Future research efforts should explore comprehensive security frameworks that encompass not only predictive maintenance and cyberattacks but also incorporate strategies for enhancing the physical safety and privacy of EnFVs, fostering a holistic approach to security in these advanced transportation systems.
10. DL models and their computational demands: DL methods hold immense potential for transforming the security of EnFVs, enabling applications such as cyberattack detection, maintenance prediction, and anomaly detection (Kurunathan et al., 2023). However, the computational demands associated with DL models, attributed to factors like model size, complexity, data size, and hardware, pose challenges for efficient deployment in real-time operational settings. For applications like real-time cyberattack detection, models must run swiftly on EnFVs. Overcoming these challenges involves designing smaller and simpler models using techniques like pruning and quantization, utilizing more efficient algorithms, and deploying specialized hardware like GPUs. By addressing these computational demands, DL models

can enhance the security, reliability, and safety of EnFVs, offering benefits in various aspects, from cybersecurity to predictive maintenance.

11. Ethical Considerations: The integration of ML applications in EnFV systems brings forth a range of ethical implications that warrant thorough consideration. One key aspect involves ensuring transparency and interpretability of ML algorithms to comprehend their decision-making processes, particularly in critical scenarios (Mohsan et al., 2023). Accountability mechanisms must be established to address issues related to system failures, biases, and unforeseen consequences. Additionally, data collection and utilization in EnFVs raise privacy concerns, necessitating robust data protection measures and adherence to ethical data handling practices. As EnFV systems become more autonomous, there is a need to establish clear guidelines for human intervention and control, balancing the benefits of automation with ethical principles. Moreover, addressing the potential economic and social impacts of ML-driven automation in transportation is crucial to mitigate disparities and ensure equitable access to evolving technologies. This comprehensive ethical analysis is a foundation for the responsible development and deployment of ML applications in EnFV systems. Future research directions should delve deeper into these ethical considerations, exploring specific frameworks and guidelines tailored to the unique challenges posed by EnFVs (Heidari et al., 2023).

6. Conclusion

This study comprehensively explored the pivotal role that machine learning (ML) techniques play in enhancing the security of electric and flying vehicles (EnFVs). The research spans various crucial domains, including predictive maintenance, cyberattack detection, and intelligent decision-making for EnFVs, revealing key insights and trends that will significantly influence the trajectory of EnFV technology.

Theoretical implications drawn from this research underscore the transformative potential of ML-based approaches in fortifying EnFV security. By enabling real-time threat detection, predictive maintenance capabilities, and enhanced anomaly detection, ML emerges as a cornerstone for advancing EnFV safety and efficiency. Integrating ML into existing frameworks holds promise for addressing challenges related to data quality, algorithmic complexity, ethical considerations, and interdisciplinary collaboration, marking a theoretical shift toward more robust and adaptive security solutions.

Practically, the research envisions ML-based EnFV security solutions as instrumental in preventing cyberattacks, reducing downtime, and elevating overall safety. The optimization of maintenance schedules, cost reduction, and lifespan extension for EnFVs are practical outcomes of ML applications. The study advocates for developing intelligent decision-making systems through ML, contributing to improved EnFV performance and efficiency in real-world scenarios.

The contributions of this study are multifaceted. It offers a comprehensive overview of the current state-of-the-art in ML for EnFV security, identifying key challenges and research gaps within the domain. Additionally, the study lays the foundation for future research directions, addressing critical aspects to advance the field further.

Acknowledging its focus on literature review and analysis, the study underscores the need for further research to implement and evaluate proposed ML-based security solutions in actual EnFV environments. It also highlights that ethical considerations require more attention, emphasizing the necessity of developing guidelines for the ethical use of ML in EnFV security applications.

Future research directions emerge as pivotal for advancing EnFV security. Development of Explainable AI (XAI) techniques, investigation of real-time ML algorithms for resource-constrained environments, and creating privacy-preserving ML techniques stand out as critical areas requiring exploration. These suggestions pave the way for a more transparent, efficient, and privacy-aware integration of ML in EnFV security.

CRediT authorship contribution statement

Hamed Alqahtani: Research, Writing and Revising. **Gulshan Kumar:** Conception, Design, Research, Writing and Revising.

Declaration of competing interest

Authors declare no conflict of interest.

Data availability

No data was used for the research described in the article.

Acknowledgement

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number (RGP2/ 159 /44).

References

Abbaspour, A., Yen, K.K., Noei, S., Sargolzaei, A., 2016. Detection of fault data injection attack on uav using adaptive neural network. Procedia Comput. Sci. 95, 193–200.

Abo Mosali, N., Shamsudin, S.S., Mostafa, S.A., Alfandi, O., Omar, R., Al-Fadhali, N., Mohammed, M.A., Malik, R., Jaber, M.M., Saif, A., 2022. An adaptive multi-level quantization-based reinforcement learning model for enhancing UAV landing on moving targets. Sustainability 14 (14), 8825.

Adil, M., Ali, J., Ta, Q.T.H., Attique, M., Chung, T.-S., 2020. A reliable sensor network infrastructure for electric vehicles to enable dynamic wireless charging based on machine learning technique. IEEE Access 8, 187933–187947.

Ahn, H., Choi, H.-L., Kang, M., Moon, S., 2019. Learning-based anomaly detection and monitoring for swarm drone flights. Appl. Sci. 9 (24), 5477.

Al Gizi, A.J., 2023. UAV flight fuzzy controller with deep learning network fault checker of high-voltage lines. Int. J. Intell. Syst. Appl. Eng. 11 (2), 877–891.

Al-Rubaye, S., Tsourdos, A., Namuduri, K., 2023. Advanced air mobility operation and infrastructure for sustainable connected evtol vehicle. Drones 7 (5), 319.

Alshammari, A., Zohdy, M.A., Debnath, D., Corser, G., 2018. Classification approach for intrusion detection in vehicle systems. Wirel. Eng. Technol. 9 (4), 79–94.

Althubiti, S., Escorcia-Gutierrez, J., Gamarra, M., Soto-Diaz, R., Mansour, R.F., Alenezi, F., 2022. Improved metaheuristics with machine learning enabled medical decision support system. Comput. Mater. Contin. 73 (2), 2423–2439.

Alzubaidi, L., Bai, J., Al-Sabaawi, A., Santamaría, J., Albahri, A., Al-dabbagh, B.S.N., Fadhel, M.A., Manoufali, M., Zhang, J., Al-Timemy, A.H., et al., 2023. A survey on deep learning tools dealing with data scarcity: definitions, challenges, solutions, tips, and applications. J. Big Data 10 (1), 46.

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, 127580–127592.

Baig, Z., Syed, N., Mohammad, N., 2022. Securing the smart city airspace: Drone cyber attack detection through machine learning. Future Internet 14 (7), 205.

Bangui, H., Buhnova, B., 2021. Recent advances in machine-learning driven intrusion detection in transportation: Survey. Procedia Comput. Sci. 184, 877–886.

Bell, V., Rengasamy, D., Rothwell, B., Figueredo, G.P., 2022. Anomaly detection for unmanned aerial vehicle sensor data using a stacked recurrent autoencoder method with dynamic thresholding. arXiv preprint arXiv:2203.04734.

Bera, B., Das, A.K., Sutrala, A.K., 2021. Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. Comput. Commun. 166, 91–109.

Berger, I., Rieke, R., Kolomeets, M., Chechulin, A., Kotenko, I., 2018. Comparative study of machine learning methods for in-vehicle intrusion detection. In: International Workshop on Security and Privacy Requirements Engineering. Springer, pp. 85–101.

Bharathidasan, M., Indragandhi, V., Suresh, V., Jasiński, M., Leonowicz, Z., 2022. A review on electric vehicle: Technologies, energy trading, and cyber security. Energy Rep. 8, 9662–9685.

Biron, Z.A., Dey, S., Pisu, P., 2018. Real-time detection and estimation of denial of service attack in connected vehicle systems. IEEE Trans. Intell. Transp. Syst. 19 (12), 3893–3902.

Bithas, P.S., Michailidis, E.T., Nomikos, N., Vouyioukas, D., Kanatas, A.G., 2019. A survey on machine-learning techniques for UAV-based communications. Sensors 19 (23), 5170.

Bronz, M., Baskaya, E., Delahaye, D., Puechmore, S., 2020. Real-time fault detection on small fixed-wing UAVs using machine learning. In: 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC). IEEE, pp. 1–10.

Brulin, P.-Y., Rizoug, N., Khenfri, F., 2022. Failure-prone propulsion system modelization for UAV predictive maintenance. In: 2022 IEEE Vehicle Power and Propulsion Conference (VPPC). IEEE, pp. 1–6.

Burkacky, O., Pautasso, L., Mohr, N., 2020. Will Quantum Computing Drive the Automotive Future, Vol. 1. Mckinsey & Company, pp. 33–38.

Bylykbashi, K., Qafzezi, E., Ikeda, M., Matsuo, K., Barolli, L., 2020. Fuzzy-based Driver Monitoring System (FDMS): Implementation of two intelligent FDMSs and a testbed for safe driving in VANETs. Future Gener. Comput. Syst. 105, 665–674.

Chen, X.-C., Chen, Y.-J., 2019. A machine learning based attack in UAV communication networks. In: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall). IEEE, pp. 1–2.

Chen, J., Shi, J., 2019. A multi-compartment vehicle routing problem with time windows for urban distribution–A comparison study on particle swarm optimization algorithms. Comput. Ind. Eng. 133, 95–106.

Chohan, M.N., Haider, U., Ayub, M.Y., Shoukat, H., Bhatia, T.K., Hassan, M.F.U., 2023. Detection of cyber attacks using machine learning based intrusion detection system for IoT based smart cities. EAI Endorsed Trans. Smart Cities 7 (2).

Chriki, A., Touati, H., Snoussi, H., Kamoun, F., 2021. Deep learning and handcrafted features for one-class anomaly detection in UAV video. Multimedia Tools Appl. 80, 2599–2620.

Da Silva, L.M., Ferrão, I.G., Branco, K.R., 2022. A systematic mapping study in intrusion detection system for unmanned aerial vehicles security. In: 2022 Latin American Robotics Symposium (LARS), 2022 Brazilian Symposium on Robotics (SBR), and 2022 Workshop on Robotics in Education (WRE). IEEE, pp. 43–48.

Dey, S., Khanra, M., 2020. Cybersecurity of plug-in electric vehicles: Cyberattack detection during charging. IEEE Trans. Ind. Electron. 68 (1), 478–487.

Dixit, P., Bhattacharya, P., Tanwar, S., Gupta, R., 2022. Anomaly detection in autonomous electric vehicles using AI techniques: A comprehensive survey. Expert Syst. 39 (5), e12754.

ElKashlan, M., Aslan, H., Said Elsayed, M., Jurcut, A.D., Azer, M.A., 2023. Intrusion detection for electric vehicle charging systems (evcs). Algorithms 16 (2), 75.

Escorcia-Gutierrez, J., Gamarra, M., Leal, E., Madera, N., Soto, C., Mansour, R.F., Alharbi, M., Alkhayyat, A., Gupta, D., 2023. Sea turtle foraging algorithm with hybrid deep learning-based intrusion detection for the internet of drones environment. Comput. Electr. Eng. 108, 108704.

Garg, S., Singh, A., Kaur, K., Aujla, G.S., Batra, S., Kumar, N., Obaidat, M.S., 2019. Edge computing-based security framework for big data analytics in VANETs. IEEE Netw. 33 (2), 72–81.

Gopi, A., Sharma, P., Sudhakar, K., Ngui, W.K., Kirpichnikova, I., Cuce, E., 2022. Weather impact on solar farm performance: A comparative analysis of machine learning techniques. Sustainability 15 (1), 439.

Guerber, C., Royer, M., Larrieu, N., 2021. Machine Learning and Software Defined Network to secure communications in a swarm of drones. J. Inf. Secur. Appl. 61, 102940.

Guo, L., Ye, J., Yang, B., 2020. Cyberattack detection for electric vehicles using physics-guided machine learning. IEEE Trans. Transp. Electr. 7 (3), 2010–2022.

Hassan, M.U., Shahzaib, M., Shaukat, K., Hussain, S.N., Mubashir, M., Karim, S., Shabir, M.A., 2019. DEAR-2: An energy-aware routing protocol with guaranteed delivery in wireless ad-hoc networks. In: Recent Trends and Advances in Wireless and IoT-Enabled Networks. Springer, pp. 215–224.

He, Q., Meng, X., Qu, R., Xi, R., 2020. Machine learning-based detection for cyber security attacks on connected and autonomous vehicles. Mathematics 8 (8), 1311.

Heidari, A., Jafari Navimipour, N., Unal, M., Zhang, G., 2023. Machine learning applications in internet-of-drones: systematic review, recent deployments, and open issues. ACM Comput. Surv. 55 (12), 1–45.

Hoang, T.M., Nguyen, N.M., Duong, T.Q., 2019. Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and k-means clustering. IEEE Wirel. Commun. Lett. 9 (2), 139–142.

Hsieh, Y.-T., Anjum, K., Huang, S., Kulkarni, I., Pompili, D., 2021. Hybrid analog-digital sensing approach for low-power real-time anomaly detection in drones. In: 2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS). IEEE, pp. 446–454.

Hua, H., Li, Y., Wang, T., Dong, N., Li, W., Cao, J., 2023. Edge computing with artificial intelligence: A machine learning perspective. ACM Comput. Surv. 55 (9), 1–35.

Ibrar, M., Hassan, M.A., Shaukat, K., Alam, T.M., Khurshid, K.S., Hameed, I.A., Aljuaid, H., Luo, S., 2022. A machine learning-based model for stability prediction of decentralized power grid linked with renewable energy resources. Wirel. Commun. Mob. Comput. 2022, 1–15.

IEA, 2022. Global Electric Car Stock, 2010–2022. IEA, Paris, URL https://www.iea.org/data-and-statistics/charts/global-electric-car-stock-2010-2022.

Javed, U., Shaukat, K., Hameed, I.A., Iqbal, F., Alam, T.M., Luo, S., 2021a. A review of content-based and context-based recommendation systems. Int. J. Emerg. Technol. Learn. (iJET) 16 (3), 274–306.

Javed, I., Tang, X., Shaukat, K., Sarwar, M.U., Alam, T.M., Hameed, I.A., Saleem, M.A., 2021b. V2X-based mobile localization in 3D wireless sensor network. Secur. Commun. Netw. 2021, 1–13.

Jayachandran, M., Gatla, R.K., Rao, K.P., Rao, G.S., Mohammed, S., Milyani, A.H., Azhari, A.A., Kalaiarasy, C., Geetha, S., 2022. Challenges in achieving sustainable development goal 7: Affordable and clean energy in light of nascent technologies. Sustain. Energy Technol. Assess. 53, 102692.

Kanti, P.K., Sharma, P., Sharma, K., Maiya, M., 2023. The effect of pH on stability and thermal performance of graphene oxide and copper oxide hybrid nanofluids for heat transfer applications: Application of novel machine learning technique. J. Energy Chem. 82, 359–374.

Kateb, F., Ragab, M., 2023. Archimedes optimization with deep learning based aerial image classification for cybersecurity enabled UAV networks. Comput. Syst. Sci. Eng. 47 (2).

Khan, S., Liew, C.F., Yairi, T., McWilliam, R., 2019. Unsupervised anomaly detection in unmanned aerial vehicles. Appl. Soft Comput. 83, 105650.

Kosmanos, D., Pappas, A., Maglaras, L., Moschoyiannis, S., Aparicio-Navarro, F.J., Argyriou, A., Janicke, H., 2020. A novel intrusion detection system against spoofing attacks in connected electric vehicles. Array 5, 100013.

Kulkarni, N.N., Raisi, K., Valente, N.A., Benoit, J., Yu, T., Sabato, A., 2023. Deep learning augmented infrared thermography for unmanned aerial vehicles structural health monitoring of roadways. Autom. Constr. 148, 104784.

Kumar, A., Bhatia, S., Kaushik, K., Gandhi, S.M., Devi, S.G., Diego, A.D.J., Mashat, A., 2021. Survey of promising technologies for quantum drones and networks. Ieee Access 9, 125868–125911.

Kurunathan, H., Huang, H., Li, K., Ni, W., Hossain, E., 2023. Machine learning-aided operations and communications of unmanned aerial vehicles: A contemporary survey. IEEE Commun. Surv. Tutor..

Lakhan, A., Mohammed, M.A., Abdulkareem, K.H., Jaber, M.M., Kadry, S., Nedoma, J., Martinek, R., 2023. Fuzzy decision based energy-evolutionary system for sustainable transport in ubiquitous fog network. Human-centric Comput. Inf. Sci. 13, 34.

Li, Y., Han, W., Wang, Y., 2020a. Deep reinforcement learning with application to air confrontation intelligent decision-making of manned/unmanned aerial vehicle cooperative system. IEEE Access 8, 67887–67898.

Li, Y., Pawlak, J., Price, J., Al Shamaileh, K., Niyaz, Q., Paheding, S., Devabhaktuni, V., 2022. Jamming detection and classification in OFDM-based UAVs via feature-and spectrogram-tailored machine learning. IEEE Access 10, 16859–16870.

Li, C., Xu, Y., Xia, J., Zhao, J., 2018. Protecting secure communication under UAV smart attack with imperfect channel estimation. IEEE Access 6, 76395–76401.

Li, Y., Zhang, L., Lv, Z., Wang, W., 2020b. Detecting anomalies in intelligent vehicle charging and station power supply systems with multi-head attention models. IEEE Trans. Intell. Transp. Syst. 22 (1), 555–564.

Lipu, M.S.H., Mamun, A.A., Ansari, S., Miah, M.S., Hasan, K., Meraj, S.T., Abdolrasol, M.G., Rahman, T., Maruf, M.H., Sarker, M.R., et al., 2022. Battery management, key technologies, methods, issues, and future trends of electric vehicles: A pathway toward achieving sustainable development goals. Batteries 8 (9), 119.

Loukas, G., Karapistoli, E., Panaousis, E., Sarigiannidis, P., Bezemskij, A., Vuong, T., 2019. A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. Ad Hoc Netw. 84, 124–147.

Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., Gan, D., 2017. Cloud-based cyber-physical intrusion detection for vehicles using deep learning. Ieee Access 6, 3491–3508.

Lu, X., Xiao, L., Dai, C., Dai, H., 2020. UAV-aided cellular communications with deep reinforcement learning against jamming. IEEE Wirel. Commun. 27 (4), 48–53.

Marinho, R., Holanda, R., 2023. Automated emerging cyber threat identification and profiling based on natural language processing. IEEE Access.

Maulik, U., Kundu, S., 2023. Automatic vehicle pollution detection using feedback based iterative deep learning. IEEE Trans. Intell. Transp. Syst. 24 (5), 4804–4814.

Mekdad, Y., Aris, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., Uluagac, A.S., 2023. A survey on security and privacy issues of UAVs. Comput. Netw. 224, 109626.

Meyer, M.-A., Granrath, C., Feyerl, G., Richenhagen, J., Kaths, J., Andert, J., 2021. Closed-loop platoon simulation with cooperative intelligent transportation systems based on vehicle-to-X communication. Simul. Model. Pract. Theory 106, 102173.

Miao, Y., Tang, Y., Alzahrani, B.A., Barnawi, A., Alafif, T., Hu, L., 2020. Airborne LiDAR assisted obstacle recognition and intrusion detection towards unmanned aerial vehicle: Architecture, modeling and evaluation. IEEE Trans. Intell. Transp. Syst. 22 (7), 4531–4540.

Mohamed, N., Bajaj, M., Almazrouei, S.K., Jurado, F., Oubelaid, A., Kamel, S., 2023. Artificial Intelligence (AI) and Machine Learning (ML)-based information security in electric vehicles: A review. In: 2023 5th Global Power, Energy and Communication Conference (GPECOM). IEEE, pp. 108–113.

Mohammed, M.A., Garcia-Zapirain, B., Nedoma, J., Martinek, R., Tiwari, P., Kumar, N., et al., 2022. Fully homomorphic enabled secure task offloading and scheduling system for transport applications. IEEE Trans. Veh. Technol. 71 (11), 12140–12153.

Mohammed, M.A., Lakhan, A., Abdulkareem, K.H., Zebari, D.A., Nedoma, J., Martinek, R., Kadry, S., Garcia-Zapirain, B., 2023. Homomorphic federated learning schemes enabled pedestrian and vehicle detection system. Internet Things 23, 100903.

Mohsan, S.A.H., Othman, N.Q.H., Li, Y., Alsharif, M.H., Khan, M.A., 2023. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. Intell. Serv. Robot. 16 (1), 109–137.

Narayanan, S.N., Mittal, S., Joshi, A., 2015. Using data analytics to detect anomalous states in vehicles. arXiv preprint arXiv:1512.08048.

Ouiazzane, S., Addou, M., Barramou, F., 2022. A multiagent and machine learning based denial of service intrusion detection system for drone networks. In: Geospatial Intelligence: Applications and Future Trends. Springer, pp. 51–65.

Pace, J., Rao, J.P., Williams, J., He, L., 2022. Unsupervised anomaly detection using batteries in electric aerial vehicle propulsion test-bed. In: Annual Conference of the PHM Society, Vol. 14.

Park, K.H., Park, E., Kim, H.K., 2020. Unsupervised intrusion detection system for unmanned aerial vehicle with less labeling effort. In: Information Security Applications: 21st International Conference, WISA 2020, Jeju Island, South Korea, August 26–28, 2020, Revised Selected Papers 21. Springer, pp. 45–58.

Perumalla, S., Chatterjee, S., Kumar, A.S., 2023. Modelling of oppositional Aquila Optimizer with machine learning enabled secure access control in Internet of drones environment. Theoret. Comput. Sci. 941, 39–54.

Praveena, V., Vijayaraj, A., Chinnasamy, P., Ali, I., Alroobaea, R., Alyahyan, S.Y., Raza, M.A., 2022. Optimal deep reinforcement learning for intrusion detection in UAVs. Comput. Mater. Continua 70 (2), 2639–2653.

Putri, T.D., et al., 2021. Intelligent transportation systems (ITS): A systematic review using a Natural Language Processing (NLP) approach. Heliyon 7 (12).

Qureshi, A.M., Butt, A.H., Jalal, A., 2023. Highway traffic surveillance over UAV dataset via blob detection and histogram of gradient. In: 2023 4th International Conference on Advancements in Computational Sciences (ICACS). IEEE, pp. 1–5.

Raj, M.J., Gadde, S., Jayaraman, R., 2021. Implementation of biometric access control using fingerprint for safety and security system of electric vehicle. In: 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC). IEEE, pp. 1684–1689.

Ralegankar, V.K., Bagul, J., Thakkar, B., Gupta, R., Tanwar, S., Sharma, G., Davidson, I.E., 2021. Quantum cryptography-as-a-service for secure UAV communication: applications, challenges, and case study. IEEE Access 10, 1475–1492.

Ramadan, R.A., Emara, A.-H., Al-Sarem, M., Elhamahmy, M., 2021. Internet of drones intrusion detection using deep learning. Electronics 10 (21), 2633.

Rasool, R.U., Ahmad, H.F., Rafique, W., Qayyum, A., Qadir, J., 2022. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. J. Netw. Comput. Appl. 201, 103332.

Reddy, D.K., Behera, H.S., Nayak, J., Vijayakumar, P., Naik, B., Singh, P.K., 2021. Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. Trans. Emerg. Telecommun. Technol. 32 (7), e4121.

Renda, A., Ducange, P., Marcelloni, F., Sabella, D., Filippou, M.C., Nardini, G., Stea, G., Virdis, A., Micheli, D., Rapone, D., et al., 2022. Federated learning of explainable AI models in 6G systems: Towards secure and automated vehicle networking. Information 13 (8), 395.

Said, Z., Sharma, P., Nhuong, Q.T.B., Bora, B.J., Lichtfouse, E., Khalid, H.M., Luque, R., Nguyen, X.P., Hoang, A.T., 2023. Intelligent approaches for sustainable management and valorisation of food waste. Bioresour. Technol. 128952.

Sanguesa, J.A., Torres-Sanz, V., Garrido, P., Martinez, F.J., Marquez-Barja, J.M., 2021. A review on electric vehicles: Technologies and challenges. Smart Cities 4 (1), 372–404.

Sani, A.R., Hassan, M.U., Chen, J., 2022. Privacy preserving machine learning for electric vehicles: a survey. arXiv preprint arXiv:2205.08462.

Savić, J., Perić, D., Lagundžin, S., 2020. Autonomous vehicle behavior anomaly detection based on principal component analysis.

Sazdić-Jotić, B., Pokrajac, I., Bajčetić, J., Bondžulić, B., Obradović, D., 2022. Single and multiple drones detection and identification using RF based deep learning algorithm. Expert Syst. Appl. 187, 115928.

Shafique, A., Mehmood, A., Elhadef, M., 2021. Detecting signal spoofing attack in uavs using machine learning models. IEEE Access 9, 93803–93815.

Sharma, P., Bora, B.J., 2022. A review of modern machine learning techniques in the prediction of remaining useful life of lithium-ion batteries. Batteries 9 (1), 13.

Shaukat, K., Alam, T.M., Hameed, I.A., Khan, W.A., Abbas, N., Luo, S., 2021a. A review on security challenges in internet of things (IoT). In: 2021 26th International Conference on Automation and Computing (ICAC). IEEE, pp. 1–6.

Shaukat, K., Alam, T.M., Luo, S., Shabbir, S., Hameed, I.A., Li, J., Abbas, S.K., Javed, U., 2021b. A review of time-series anomaly detection techniques: A step to future perspectives. In: Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 1. Springer, pp. 865–877.

Shaukat, K., Iqbal, F., Alam, T.M., Aujla, G.K., Devnath, L., Khan, A.G., Iqbal, R., Shahzadi, I., Rubab, A., 2020a. The impact of artificial intelligence and robotics on the future employment opportunities. Trends Comput. Sci. Inf. Technol. 5 (1), 050–054.

Shaukat, K., Iqbal, F., Hameed, I.A., Hassan, M.U., Luo, S., Hassan, R., Younas, A., Ali, S., Adeem, G., Rubab, A., et al., 2020b. MAC protocols 802.11: A comparative study of throughput analysis and improved LEACH. In: 2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). IEEE, pp. 421–426.

Shaukat, K., Luo, S., Chen, S., Liu, D., 2020c. Cyber threat detection using machine learning techniques: A performance evaluation perspective. In: 2020 International Conference on Cyber Warfare and Security (ICCWS). IEEE, pp. 1–6.

Shaukat, K., Luo, S., Varadharajan, V., 2022. A novel method for improving the robustness of deep learning-based malware detectors against adversarial attacks. Eng. Appl. Artif. Intell. 116, 105461.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., Chen, S., Liu, D., Li, J., 2020d. Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies 13 (10), 2509.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., Xu, M., 2020e. A survey on machine learning techniques for cyber security in the last decade. IEEE Access 8, 222310–222354.

Shaukat, K., Rubab, A., Shehzadi, I., Iqbal, R., 2017. A socio-technological analysis of cyber crime and cyber security in Pakistan. Transylv. Rev. 1, 84.

Shaw, S., Joshi, K., Pathak, A., Thyagarajan, A.K., Vidya, G., Hemal Shah, R., Ram Kishan, V., Alex, J.S.R., 2022. Anomaly detection in drones with machine learning algorithms. In: Futuristic Communication and Network Technologies: Select Proceedings of VICFCNT 2020. Springer, pp. 433–441.

Shrestha, R., Omidkar, A., Roudi, S.A., Abbas, R., Kim, S., 2021. Machine-learning-enabled intrusion detection system for cellular connected UAV networks. Electronics 10 (13), 1549.

Sindhwani, V., Sidahmed, H., Choromanski, K., Jones, B., 2020. Unsupervised anomaly detection for self-flying delivery drones. In: 2020 IEEE International Conference on Robotics and Automation (ICRA). IEEE, pp. 186–192.

Srivastava, S., Narayan, S., Mittal, S., 2021. A survey of deep learning techniques for vehicle detection from UAV images. J. Syst. Archit. 117, 102152.

Sundaram, K.M., Hussain, A., Sanjeevikumar, P., Holm-Nielsen, J.B., Kaliappan, V.K., Santhoshi, B.K., 2021. Deep learning for fault diagnostics in bearings, insulators, PV panels, power lines, and electric vehicle applications—the state-of-the-art approaches. IEEE Access 9, 41246–41260.

Suriya, N., Vijay Shankar, S., 2022. A novel ensembling of deep learning based intrusion detection system and scroll chaotic countermeasures for electric vehicle charging system. J. Intell. Fuzzy Systems 43 (4), 4789–4801.

Talaei Khoei, T., Ismail, S., Kaabouch, N., 2022. Dynamic selection techniques for detecting GPS spoofing attacks on UAVs. Sensors 22 (2), 662.

Tan, X., Su, S., Zuo, Z., Guo, X., Sun, X., 2019. Intrusion detection of UAVs based on the deep belief network optimized by PSO. Sensors 19 (24), 5529.

Thakur, K., Alqahtani, H., Kumar, G., 2021. An intelligent algorithmically generated domain detection system. Comput. Electr. Eng. 92, 107129.

Theissler, A., Pérez-Velázquez, J., Kettelgerdes, M., Elger, G., 2021. Predictive maintenance enabled by machine learning: Use cases and challenges in the automotive industry. Reliab. Eng. Syst. Saf. 215, 107864.

Tran, T.M., Vu, T.N., Nguyen, T.V., Nguyen, K., 2023. UIT-ADrone: A novel drone dataset for traffic anomaly detection. IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens..

Trivedi, M., Kakkar, R., Gupta, R., Agrawal, S., Tanwar, S., Niculescu, V.-C., Raboaca, M.S., Alqahtani, F., Saad, A., Tolba, A., 2022. Blockchain and deep learning-based fault detection framework for electric vehicles. Mathematics 10 (19), 3626.

Unlu, E., Zenou, E., Riviere, N., Dupouy, P.-E., 2019. Deep learning-based strategies for the detection and tracking of drones using several cameras. IPSJ Trans. Comput. Vis. Appl. 11 (1), 1–13.

Vanitha, N., Ganapathi, P., 2020. Traffic analysis of UAV networks using enhanced deep feed forward neural networks (EDFFNN). In: Handbook of Research on Machine and Deep Learning Applications for Cyber Security. IGI Global, pp. 219–244.

Warraich, Z., Morsi, W., 2023. Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids. Sustain. Energy, Grids Netw. 34, 101027.

Whelan, J., Sangarapillai, T., Minawi, O., Almehmadi, A., El-Khatib, K., 2020. Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles. In: Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks. pp. 23–28.

Wu, W., Li, R., Xie, G., An, J., Bai, Y., Zhou, J., Li, K., 2019. A survey of intrusion detection for in-vehicle networks. IEEE Trans. Intell. Transp. Syst. 21 (3), 919–933.

Xiao, L., Lu, X., Xu, D., Tang, Y., Wang, L., Zhuang, W., 2018. UAV relay in VANETs against smart jamming with reinforcement learning. IEEE Trans. Veh. Technol. 67 (5), 4087–4097.

Xiao, K., Zhao, J., He, Y., Li, C., Cheng, W., 2019. Abnormal behavior detection scheme of UAV using recurrent neural networks. IEEE Access 7, 110293–110305.

Xu, J., Guo, Q., Xiao, L., Li, Z., Zhang, G., 2019. Autonomous decision-making method for combat mission of UAV based on deep reinforcement learning. In: 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Vol. 1. IEEE, pp. 538–544.

Yassine, S., Stanulov, A., 2024. A comparative analysis of machine learning algorithms for the purpose of predicting Norwegian air passenger traffic. Int. J. Math. Stat. Comput. Sci. 2, 28–43.

Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Karimipour, H., 2021. Federated learning for drone authentication. Ad Hoc Netw. 120, 102574.

Zahra, N., Buldan, R.S., Nazaruddin, Y.Y., Widyotriatmo, A., 2021. Predictive maintenance with neural network approach for UAV propulsion systems monitoring. In: 2021 American Control Conference (ACC). IEEE, pp. 2631–2636.

Zhi, Y., Fu, Z., Sun, X., Yu, J., 2020. Security and privacy issues of UAV: a survey. Mob. Netw. Appl. 25, 95–101.