AI

Systematic Review

Enhancing IoT Security in Vehicles: A Comprehensive Review of AI-Driven Solutions for Cyber-Threat Detection

Rafael Abreu [1], Emanuel Simão [1], Carlos Serôdio [1,2], Frederico Branco [1,3] and António Valente [1,3,*]

[1] Department of Engineering, School of Sciences and Technology, Universidade de Trás-os-Montes e Alto Douro, 5000-801 Vila Real, Portugal; rafaabreu03@hotmail.com (R.A.); emasimao@icloud.com (E.S.); cserodio@utad.pt (C.S.); fbranco@utad.pt (F.B.)
[2] Algoritmi Center, University of Minho, 4710-057 Braga, Portugal
[3] INESC TEC—Institute for Systems and Computer Engineering, Technology and Science, Rua Dr. Roberto Frias, 4200-465 Porto, Portugal
[*] Correspondence: avalente@utad.pt; Tel.: +351-917885934

Abstract: Background: The Internet of Things (IoT) has improved many aspects that have impacted the industry and the people's daily lives. To begin with, the IoT allows communication to be made across a wide range of devices, from household appliances to industrial machinery. This connectivity allows for a better integration of the pervasive computing, making devices "smart" and capable of interacting with each other and with the corresponding users in a sublime way. However, the widespread adoption of IoT devices has introduced some security challenges, because these devices usually run in environments that have limited resources. As IoT technology becomes more integrated into critical infrastructure and daily life, the need for stronger security measures will increase. These devices are exposed to a variety of cyber-attacks. This literature review synthesizes the current research of artificial intelligence (AI) technologies to improve IoT security. This review addresses key research questions, including: (1) What are the primary challenges and threats that IoT devices face?; (2) How can AI be used to improve IoT security?; (3) What AI techniques are currently being used for this purpose?; and (4) How does applying AI to IoT security differ from traditional methods? Methods: We included a total of 33 peer-reviewed studies published between 2020 and 2024, specifically in journal and conference papers written in English. Studies irrelevant to the use of AI for IoT security, duplicate studies, and articles without full-text access were excluded. The literature search was conducted using scientific databases, including MDPI, ScienceDirect, IEEE Xplore, and SpringerLink. Results were synthesized through a narrative synthesis approach, with the help of the Parsifal tool to organize and visualize key themes and trends. Results: We focus on the use of machine learning, deep learning, and federated learning, which are used for anomaly detection to identify and mitigate the security threats inherent to these devices. AI-driven technologies offer promising solutions for attack detection and predictive analysis, reducing the need for human intervention more significantly. This review acknowledges limitations such as the rapidly evolving nature of IoT technologies, the early-stage development or proprietary nature of many AI techniques, the variable performance of AI models in real-world applications, and potential biases in the search and selection of articles. The risk of bias in this systematic review is moderate. While the study selection and data collection processes are robust, the reliance on narrative synthesis and the limited exploration of potential biases in the selection process introduce some risk. Transparency in funding and conflict of interest reporting reduces bias in those areas. Discussion: The effectiveness of these AI-based approaches can vary depending on the performance of the model and the computational efficiency. In this article, we provide a comprehensive overview of existing AI models applied to IoT security, including machine learning (ML), deep learning (DL), and hybrid approaches. We also examine their role in enhancing the detection accuracy. Despite all the advances, challenges still remain in terms of data privacy and the scalability of AI solutions in IoT security. Conclusion: This review provides a comprehensive overview of ML applications to enhance IoT security. We also discuss and outline future directions, emphasizing the need for collaboration between interested parties and ongoing innovation to address the evolving threat landscape in IoT security.

check for updates

Citation: Abreu, R.; Simão, E.; Serôdio, C.; Branco, F.; Valente, A. Enhancing IoT Security in Vehicles: A Comprehensive Review of AI-Driven Solutions for Cyber-Threat Detection. *AI* **2024**, *5*, 2279–2299. https://doi.org/10.3390/ai5040112

Academic Editors: Sheikh Tahir Bakhsh, Sabeen Tahir and Basit Shahzad

Received: 30 September 2024
Revised: 25 October 2024
Accepted: 31 October 2024
Published: 6 November 2024

Keywords: IoT security; artificial intelligence; machine learning; deep learning; cybersecurity

1. Introduction

The Internet of Things (IoT) has become an important part of modern technological innovation, with applications ranging from smart cities and industrial automation to healthcare and connected vehicles, all capable of functioning without human intervention. Advancements in technologies such as sensors, tracking, wireless communications, and embedded computing have increased the possibility of integrating advanced capabilities into our daily activities over the Internet [1].

In recent years, the integration of intelligent vehicles into the broader Internet of Things (IoT) ecosystem has introduced significant cybersecurity challenges for manufacturers. Vehicles are now susceptible to both internal and external attacks, particularly due to the vulnerabilities inherent in the controller area network (CAN). The lack of authentication and encryption within CAN messages allows attackers to exploit these weaknesses, potentially taking control of critical vehicle functions such as brakes, steering, and gears. While CAN remains widely used for its robustness and cost-effectiveness, its cybersecurity limitations pose serious physical risks, making vehicles vulnerable to remote attacks that could jeopardize human safety. Additionally, in-vehicle networks (IVN) face increasing risks from remote exploitation, emphasizing the urgent need for enhanced security mechanisms [2–4].

In response to these challenges, artificial intelligence encompasses machine learning and has emerged as a promising solution for enhancing IoT security. AI offers sophisticated techniques for anomaly detection, real-time threat analysis, and automated response systems, allowing for more efficient and scalable security architectures. Machine-learning models can be trained to identify patterns in network traffic and detect abnormal behaviors that can indicate the presence of malicious activities. Consequently, AI-driven solutions, such as deep learning, further enhance detection capabilities by analyzing larger datasets and predicting cyber-threats with greater precision [5]. Recent research has focused on developing lightweight AI models tailored to the resource limitations of IoT devices and employing federated-learning techniques to ensure privacy while maintaining security [6].

This review seeks to explore critical areas in the intersection of IoT security and artificial intelligence (AI). It aims to uncover the key challenges and threats facing IoT devices and investigates the potential of AI in strengthening their defenses. Furthermore, the review will examine which AI techniques are being applied to enhance security and analyze how AI-based approaches differ from traditional cybersecurity methods. Through this comprehensive exploration, the review seeks to provide insights into the evolving role of AI in securing IoT ecosystems.

1.1. Motivation

Our participation in this review is based on our participation in the A-MoVeR Project, which aims to build an all-electric motorbike in partnership with some companies, equipping it with various state-of-the-art electronic devices to improve the interaction between the bike and the user, with the network being easier and more intuitive to use.

Given the importance of the electronic integration project, it is urgent that we address the security of IoT devices in the automotive sector. Since the bike will heavily rely on interconnected systems, it is crucial to ensure robust security measures to protect it from potential threats.

This review article is motivated by the need to evaluate AI-driven security solutions specifically designed for IoT devices, with an emphasis on the automotive sector. By focusing on this sector, we aim to provide valuable insights for securing emerging technologies not only in our project but similar ones that rely on the use of IoT devices. This will contribute to the success of the A-MoVeR Project, as well as the broader field of IoT security.

1.2. Organization of the Paper

The rest of the paper is organized as follows. Section 2 describes the methodology used to conduct this review, following the PRISMA guidelines. Section 3 provides a narrative synthesis of the selected articles. In Section 4, we analyze the findings and discuss the effectiveness of the different models proposed in the articles. Finally, Section 5 concludes the paper and suggests directions for future research.

2. Materials and Methods

This section describes the approach used to carry out this systematic review, which follows the PRISMA 2020 guidelines [7] to ensure a comprehensive review process. The review protocol was designed based on the PRISMA recommendations, and this article meets all the relevant items on the PRISMA 2020 checklist.

We followed a structured framework that includes formulating the research objective with the research questions, conducting the search strategy with the proper eligibility criteria, selecting the appropriate studies, extracting and analyzing the relevant data, conducting the quality assessment of the selected studies, and synthesizing the results. In addition, we used the Parsifal tool to maintain the proper rigor throughout the review process.

This approach provides a clear understanding, ensuring that our methods are reproducible and providing clear guidelines for researchers who wish to replicate our study.

2.1. Research Objective

The main objective of this review is to perform a systematic analysis of existing studies on the security of IoT devices with artificial intelligence (AI). We aim to identify the most common threats that IoT devices face, and we will also explore how AI can be used to improve their security.

Through this literature review, we hope to find the most common areas where AI is applied for IoT security, as well as identify the areas that require further investigation. Specifically, we intend to explore AI-driven security solutions for IoT devices in the automotive sector, providing guidance to future researchers in addressing cybersecurity challenges.

The research questions of this systematic review of the literature are based on the definition of PICO elements, a framework commonly used in literature reviews. Although PICO can be a useful tool, it is important to be flexible in selecting its most relevant elements to better focus the collection rate, thus reducing studies that are not as relevant to our field of study. Current recommendations suggest that the appropriate elements of the PICO should be included in the search strategy [8], as presented in Table 1. The research questions are presented in Table 2 below.

Table 1. PICO Elements of the included studies.

Components	Description
Population	Researchers that create methods to increase the cybersecurity of IoT devices using AI
Intervention	Articles in specific scientific repositories documenting techniques and technologies to improve the security related to IoT devices
Comparison	Typical security techniques (e.g., encryption, firewalls) without AI integration
Outcome	Improvement in security measures, reduced vulnerabilities, and enhanced detection

Table 2. Research questions for the literature review.

Question Number	Research Questions
RQ1	What are the primary challenges and threats that IoT devices face?
RQ2	How can artificial intelligence be used to enhance the security of IoT devices?
RQ3	What AI techniques are currently being used to enhance the security of IoT devices?
RQ4	How does applying AI to secure IoT devices differ from traditional security methods?

2.2. Search Strategy

For this review, we conducted a comprehensive search across four major repositories: https://www.mdpi.com (accessed on 1 September 2024) MDPI; https://ieeexplore.ieee.org/Xplore/home.jsp (accessed on 1 September 2024) IEEE Xplore; https://www.sciencedirect.com (accessed on 1 September 2024) ScienceDirect; https://link.springer.com/ (accessed on 1 September 2024) SpringerLink.

We used a combination of relevant keywords, such as: IoT Security; Artificial Intelligence; Machine Learning; Anomaly Detection; Cybersecurity. We also used the following search string:

("IoT" OR "Internet of Things") AND ("Machine Learning" OR "Deep Learning" OR "AI") AND ("security" OR "cybersecurity" OR "attacks") AND PUBYEAR > 2020 AND NOT DOCTYPE (sh) AND OA(publisherhybridgold) AND LANGUAGE (ENGLISH)

2.3. Eligibility Criteria

In this review, we apply the following inclusion and exclusion criteria for study selection:

Inclusion Criteria

- Peer-reviewed articles: studies (journal and conference papers) published in peer-reviewed journals focusing on AI applications in IoT security.
- Language: articles written in English.
- Publication date: we included the papers that were published in the last 4 years (2020–2024) to ensure the most up-to-date research.
- Scope of the study: articles that focused on security in IoT devices, particularly using AI for security.

Exclusion Criteria

- Duplicate studies: repeated studies found in more than one repository.
- Full-text option: articles which are not available as open access or without institutional access (UTAD).
- Irrelevancy of the study: papers that did not focus on the application of artificial intelligence to secure IoT devices were excluded.

2.4. Selection Process

In this review, the Parsifal tool, designed to organize the review process and synthesize the results, was used to assist in the selection of studies. The selection process involved two phases:

1. In the first phase, the relevance of the studies was assessed based on their titles and abstracts;
2. In the second phase, the articles that were selected in the first phase were subjected to a full-text analysis for further evaluation.

To reduce the bias risk and ensure rigor, the selection process was peer-reviewed. Both reviewers worked independently during each phase, and any discrepancies were resolved through discussion among all the authors. Parsifal helped optimize the workflow, ensuring consistency throughout the study selection process.

We identified 136 studies with potential for inclusion in the review. After removing 8 duplicate articles, we excluded 58 studies that were considered review articles, and we marked 37 studies as irrelevant to the scope of our study. This gives us a final set of 33 articles marked as eligible to be included in the review.

2.5. Data Extraction

In this phase, we collected relevant information from the selected studies using a structured approach, which included the following as key data points:

- Study objectives: The primary goal addressed by each study.
- AI techniques: Specific AI methods used for IoT security.

- IoT applications: The context that the IoT security measures were applied.
- Security challenges addressed: The cybersecurity vulnerabilities that the authors aimed to mitigate.
- Outcomes and performance: The main conclusions of each study, such as the effectiveness of AI in improving IoT security, the metrics that were used for evaluation, and comparison with traditional methods.

The extracted data were then organized to provide support for analysis and synthesis in the subsequent phases of the review.

2.6. Quality Assessment

In this section, we evaluated the rigor and validity of our selected studies using the following quality criteria:

1. Are the objectives of the study clearly stated?
2. Is the research design comprehensive enough to cover all necessary aspects of IoT security (security protocols, threat models) and AI (algorithms, models, performance evaluations)?
3. Are the methods used in the research detailed enough to allow for the reproducibility of the study?
4. Are the benchmark sources credible and representative to be relevant to the research objectives?

2.7. Data Synthesis and Reporting

In the data synthesis and reporting phase, we analyzed the information extracted to draw conclusions from the selected studies. This synthesis involved identifying patterns and similarities in the studies in order to answer our research questions and summarize the effectiveness of AI techniques in improving IoT security.

To facilitate this process, we used the Parsifal tool, as mentioned above, which helped organize the data. The Parsifal capabilities allowed us to generate detailed reports. The results were compiled into a narrative synthesis that describes the current state of AI and ML applications in IoT security, on which metrics were used to evaluate the proposed algorithms, and identify some gaps in the research.

2.8. Selection of Studies

In this section, we present the results of our study selection process, including the number of articles identified and selected from each repository.

The initial search yielded us a total of 136 articles, distributed in the following repositories:

- MDPI: 17;
- ScienceDirect: 40;
- IEEE XPlore: 39;
- SpringerLink: 40.

The selected and accepted articles can be seen in the bar chart illustrated in the Figure 1 below:

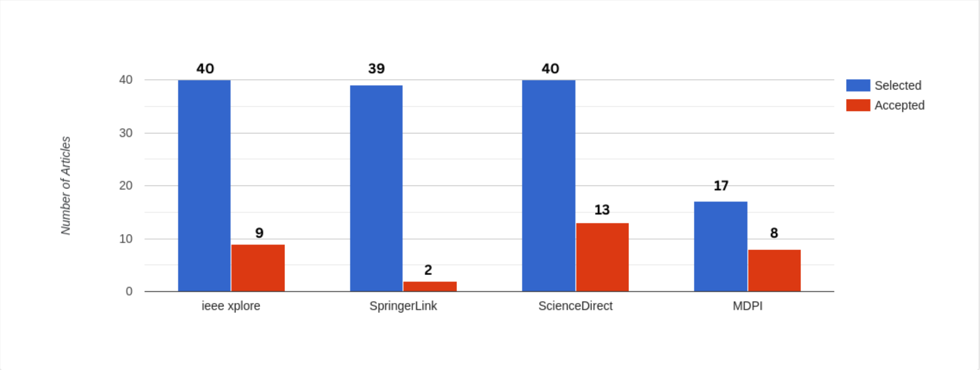

Figure 1. Bar chart of selected vs. accepted articles.

After applying the eligibility criteria and conducting the screening process, the final set of selected studies are shown in the Figure 2:

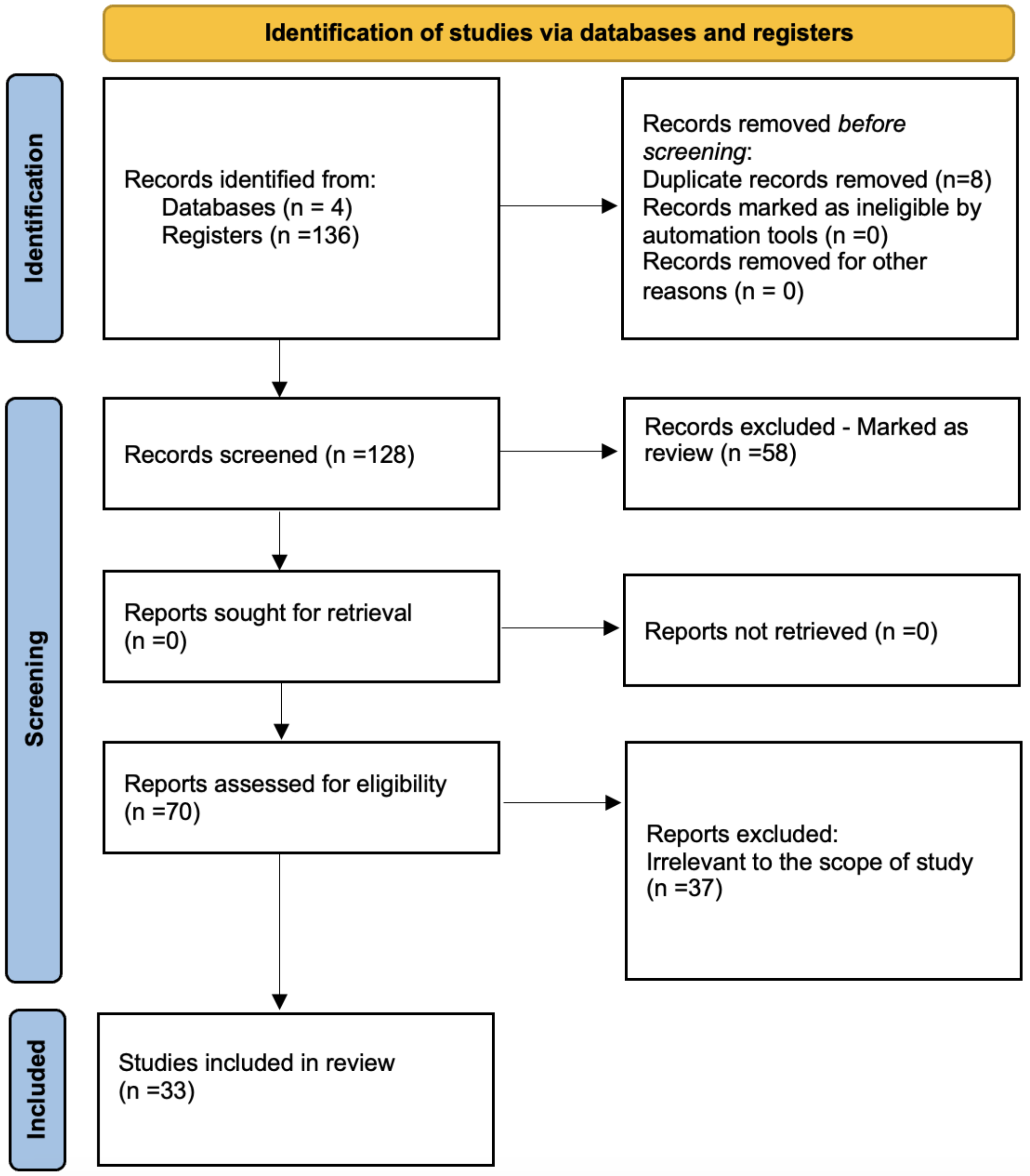
Identification of studies via databases and registers
Identification
Records identified from:
Databases (n = 4)
Registers (n =136)
Records removed *before screening*:
Duplicate records removed (n=8)
Records marked as ineligible by automation tools (n =0)
Records removed for other reasons (n = 0)
Screening
Records screened (n =128)
Records excluded - Marked as review (n =58)
Reports sought for retrieval (n =0)
Reports not retrieved (n =0)
Reports assessed for eligibility (n =70)
Reports excluded:
Irrelevant to the scope of study (n =37)
Included
Studies included in review (n =33)

Figure 2. PRISMA 2020 diagram.

2.9. Risk of Bias

To assess the risk of bias in this systematic review, we used the ROBUST (Risk of Bias in Systematic Reviews) tool [9]. We evaluated the following five domains:

2.9.1. Risk of Bias in Study Identification and Inclusion

Low risk: Our search strategy and inclusion criteria are transparent and comprehensive, covering both journal and conference papers, minimizing the likelihood of selection bias.

2.9.2. Risk of Bias in Data Collection Methods

Low risk: The use of independent reviewers and a systematic tool (Parsifal) indicates a rigorous data collection process.

2.9.3. Risk of Bias in Data Analysis Methods

Moderate risk: Narrative synthesis can introduce bias due to the subjectivity of the authors in interpreting results.

2.9.4. Risk of Bias in Presentation and Interpretation of Results

Moderate risk: While we acknowledged the limitations, the potential for bias in study selection and data synthesis is not exhaustively addressed, leaving room for overestimation of the results.

2.9.5. Risk of Bias in Funding and Conflict of Interest

Low risk: There is transparency regarding the funding, and no conflicts of interest are declared.

3. Results

The studies resulting from the final selection were categorized according to their focus areas. After a rigorous selection process, as detailed in the previous section, 33 studies were identified as relevant and included in this review. These studies mainly focus on AI techniques used to mitigate vulnerabilities in IoT systems, with an emphasis on the detection category. The articles were grouped based on three key themes:

1. Securing IoT devices with AI—general approaches, Section 3.1: This theme encompasses the studies that explored AI techniques that are applicable to securing IoT devices across different industries;
2. Securing IoT devices with AI—automotive sector, Section 3.2: This theme highlights research targeting the integration of AI in securing IoT devices within the automotive industry;
3. Security mechanisms for automotive Sector with potential AI enhancements, Section 3.3: This theme evaluates existing security mechanisms within the automotive sector and discusses how can AI enhance these mechanisms, focusing on methods that could be improved with the use of AI.

3.1. Securing IoT Devices with AI—General Approaches

Starting with the article by Alsaedi et al., where they introduced the TON-IoT dataset for intrusion detection systems (IDS) in IoT and Industrial IoT (IIoT) environments [5]. The dataset was created using a three-layer architecture (Edge, Fog, Cloud) connected via SDN and NFV on the NSX-VMware platform. Includes telemetry data, operating system logs, and network traffic from various IoT/IIoT sensors. The dataset features nine types of cyberattacks, including DoS, DDoS, and ransomware, and is organized for training and testing ML models.

Seven ML methods (LR, LDA, k-NN, CART, RF, NB, SVM) and an LSTM model were tested. LSTM and k-NN performed best on the Fridge dataset, RF and CART excelled in Modbus, and CART was the top performer for combined and multiclass datasets, while NB and SVM underperformed.

Tendikov et al. advanced cybersecurity by integrating ML techniques into SIEM systems, using k-means clustering for data grouping [10]. Their approach, which analyzed data from virtual machines and the CICIDS2017 dataset, demonstrated that the random forest model showed the best performance, particularly after key features were refined using a decision tree classifier and hyper-parameter tuning. This resulted in improved accuracy and a reduction in false negatives. Clustering of k-means provided separation of useful and irrelevant data, contributing to cybersecurity insights.

Building on the integration of machine learning for security, Akshaya et al. similarly employed advanced techniques, but their focus was on improving IoT security [11]. They trained an IDS using the NSL-KDD dataset, where k-means clustering played a role in data preprocessing. In contrast to Tendikov's use of RF, Akshaya's model leveraged a hierarchical convolutional neural network (HCNN) coupled with optimized AES encryption.

The inclusion of the entropy-hummingbird optimization algorithm for feature selection contributed to the system's superior performance, surpassing existing techniques like PSO and APSO-CNN, achieving higher accuracy, precision, recall, and F-measure, thus improving attack detection and classification.

While these studies used ML to mitigate threats, Hassan et al. took a different approach with LETM-IoT to address Sybil attacks in IoT networks [12]. Their approach, although lacking direct ML integration, laid the foundations for future improvements in this area. Using a trust-based system, LETM-IoT achieved good results in packet delivery rate and true positive rate for detecting malicious nodes, showing potential for future integration of ML techniques to enhance adaptability and effectiveness against new threats.

Sudharsanan et al. explored this potential, applying ML to enhance IoT communication through the Xception-based feedforward encapsulation algorithm (XBFE), which uses machine learning to enhance IoT communication security [13]. Unlike the trust-based approach in LETM-IoT, Sudharsanan's model classifies network characteristics and detects attacks, addressing issues such as communication failures and data loss. Using the UNSW-NB15 dataset, the results indicated that the XBFE algorithm outperformed existing methods in monitoring IoT devices and analyzing cyberattacks, showing improved performance in both the training and testing phases.

Similarly, Nawshin et al. addressed malware detection on Android IoT devices using ML techniques, focusing on feature selection, differential privacy (DP), and a zero-trust security framework [14]. Although their model used a TensorFlow/Keras neural network, like Sudharsanan's use of advanced neural network architecture, they also integrated a zero-trust approach to limit application access based on security status. This proved strong accuracy and efficiency gains outperforming LSTM, CNN, and CapsNet in malware detection accuracy. The zero-trust approach includes static and dynamic analyses to classify APKs and ensure minimal access while preserving privacy. Future research will explore diverse datasets and integrate additional privacy techniques such as federated learning.

Continuing the exploration of advanced AI techniques, Alkhonaini et al. proposed a novel model for IoT security that combined the Sine-Cosine Chimp Optimization (HSCCO) algorithm with deep learning [15]. Their model, which uses a stacked autoencoder (SAE) for classification, was tested on the WSN-DS dataset. It showed superior accuracy, sensitivity, specificity, F-score, and AUC in all classes, outperforming models such as KNN-PSO and AdaBoost in classification and efficiency.

Following Alkhonaini et al.'s combination of optimization algorithms with deep learning, Samy et al. took a step further by introducing a fog-based architecture for attack detection on IoT devices using deep learning [16]. Their framework, leveraging LSTM models, are trained in the cloud but deployed on fog nodes to classify traffic as normal or attack. The architecture not only demonstrated high accuracy using datasets such as UNSW-NB15 and CICIDS-2017, but also reduced latency compared to cloud-based systems. The inclusion of various DL models (LSTM, GRU, CNN, CNN-LSTM, DNN) highlighted LSTM's superior performance in accuracy and detection, showing lower latency compared to the cloud-based alternatives.

In contrast, Nallakaruppan et al. focused on an integrated security framework combining machine learning (ML), intrusion detection (IDS), and prevention (IPS) in IoT systems [17]. Their simulations, based on the CTU-13 dataset, evaluated eight ML algorithms, with decision trees showing the best performance. Challenges include dataset quality, real-time detection, and computational complexity. Future research will focus on improving authentication methods and adapting complex algorithms for IoT devices.

Taking a wider perspective, Ferrag et al. developed a new IoT/IIoT dataset to improve security by creating a seven-layer testbed architecture (cloud computing, NFV, blockchain, fog computing, SDN, edge computing, and IoT/IIoT perception) [18]. The Edge-IIoT dataset was created by configuring various network layers, modeling 14 attack types, and collecting normal and attack traffic data, using tools such as Wireshark and Zeek to capture and extract relevant features from protocols like IP, TCP, UDP, and MQTT. The dataset was evaluated using centralized and federated deep learning, with DNNs achieving high accuracy, and federated learning performing similarly well, even with non-IID data.

Similarly, Ullah and Mahmoud explored deep-learning models by applying CNN1D, CNN2D, and CNN3D architectures for anomaly detection in IoT networks [3]. Their study introduced the use of CNN1D for handling time-series data, while CNN2D and CNN3D managed 2D and 3D image-like data. Transfer learning further improved their model's efficiency, achieving high accuracy, precision, recall, and F1 scores in various datasets like BoT-IoT, MQTT-IoT-IDS2020, and IoT-23, which was later combined into IoT-DS-1 and IoT-DS-2 for various attack scenarios. CNN1D and CNN2D outperformed CNN3D in various datasets, offering a balance between performance and computational complexity, particularly when transfer learning was applied to reduce training times.

Habib et al. used deep convolutional neural networks (DCNN) for malware detection on IoT devices, focusing on the the Malimg dataset [19]. Their model outperformed well-known architectures such as ResNet50 and MobileNet, achieving higher accuracy with fewer epochs and lower loss. By evaluating performance through metrics such as F1 score, precision, recall, and accuracy, they concluded that DCNN could effectively identify malware while reducing computational overhead, making it a valuable addition to IoT security.

Continuing from Habib et al.'s success in malware detection using DCNN, Negabi et al. explored the vulnerabilities in IoT devices using a deep-learning-based power analysis attack using CNNs to extract AES keys from a microcontroller which is commonly used in IoT devices [20]. By analyzing power traces during encryption, the CNN model, trained with 100 k traces and tested on 2 k, successfully recovered the AES key with an average of 1200 traces and perfect accuracy. While the CNN outperformed other methods, some overfitting was observed during validation, suggesting a need for model complexity reduction.

Soliman et al. similarly integrated deep-learning techniques into IDS for Industrial IoT (IIoT), focusing on integrating these techniques into IDS [21]. Their approach employed both DL and ML algorithms to process a large-scale dataset, with preprocessing that included normalization and dimensionality reduction via single value decomposition (SVD). While DL models like LSTM and GRU processed sequential data, ML models such as bagging trees, decision trees, and K-NN aggregated predictions for faster processing times. Despite their higher training times, DL models outperformed ML methods in accuracy and error rate, demonstrating their robustness in detecting specific attacks.

Ajay et al. built upon these advancements by incorporating deep belief networks (DBNs) for intrusion detection and prevention in IoT environments [22]. Their DBN model, trained on 60% of data, tested on 30%, and validated on 10%, classifies inputs as secure or threatening and checks user behavior before granting network access. Performance is evaluated using precision, recall, and the F1 score. While the DBN shows high F1 scores, expanding the training data could further enhance its effectiveness.

In parallel, Bhayo et al. developed a machine-learning framework to improve security in software-defined IoT (SD-IoT) networks, focusing on detection of DDoS attacks [23]. Their framework utilizes SDNWISE and IoT controllers for traffic management and applies ML algorithms like Naive Bayes, decision trees (DT), and SVM for early detection of attacks. Experiments showed that the DT classifier outperformed others in speed and accuracy, with the best average classification time and an accuracy of 98.1%. The ML module processed 48 packets per second with only a 3% increase in CPU and memory usage, proving to be efficient and effective compared to traditional methods. Overall, the framework demonstrated superior performance in detecting DDoS attacks.

Manickam et al. took a unique approach for anomaly detection in IoT systems with their BBODL-ADC algorithm, combining feature selection via BPEO, anomaly detection with ERNN, and hyper-parameter tuning using BBO [24]. The results of Manickam et al. showed significant improvements in accuracy, precision, recall, F-score, and AUC in the UNSW NB-15 and UCI SECOM datasets, with improved performance over epochs and reduced losses. It surpasses traditional methods such as LR, K-NN, and SVM.

In a different way, Abbas et al. leveraged federated learning to detect cyberattacks in IoT environments, by enabling devices to train a model without sharing raw data, addressing privacy concerns while improving security [25]. Using the CIC-IoT2023 dataset, their deep neural network (DNN), optimized with binary cross-entropy loss and the Adam optimizer, demonstrated high accuracy across multiple rounds. This FL approach proved to be effective for IoT attack detection, showing potential for broader application in privacy-preserving cybersecurity.

Ali et al. introduced a hybrid deep-learning model for botnet detection in IoT systems, combining LSTM Autoencoders for sequence learning and MLP for classification [26]. The model was evaluated in on n-BAIoT 2018 and UNSW-NB15 datasets, showing that the LAE-MLP model demonstrated strong generalizability and achieved high precision, making a significant improvement over traditional IoT cybersecurity approaches.

Continuing from Ali et al.'s hybrid deep-learning approach for botnet detection, Kayode Saheed et al. proposed an ML-based IDS tailored for IoT network attacks [1]. Data were subjected to PCA for dimensionality reduction for the UNSW-NB15 dataset and models such as XGBoost, CatBoost, K-NN, SVM, and QDA were used for classification. The dataset was divided into 75% for training and 25% for testing. Evaluation metrics included precision, F1 score, and MCC. The PCA-XGBoost model showed the highest accuracy, outperforming other models. Saheed et al. also discussed the use of outdated datasets in earlier IDS studies, such as NSL-KDD, highlighting that their IDS addresses more effectively the IoT security challenges.

Ganapathy et al. then introduced a blockchain-based federated deep-learning model to secure data transmission in healthcare IoT networks, integrating blockchain and federated learning to ensure privacy during deep-learning training [27]. By ensuring that data remain decentralized and protected during training, it allows clients to contribute to a global model without revealing local parameters. Using a BLSTM network for classification, it captures data sequence dependencies, including data encryption, decentralized storage, along with access control through smart contracts. The model was evaluated using accuracy, precision, sensitivity, specificity, and F1 score, achieving 97% accuracy for normal behavior and 88% for ransomware detection. BFL-hIoT outperformed other models, particularly in normal behavior detection, and demonstrated the lowest contract deployment execution time, offering scalability and efficient feature learning compared to models like BDSDT.

3.2. Securing IoT Devices with AI—Automotive Sector

The AI applications aimed at the automotive industry that we have included are presented in this section.

Starting with Adly et al., their work focuses on applying machine-learning and deep-learning-based intrusion detection systems to prevent CAN bus attacks in electric autonomous vehicles [28]. They proposed an ECU-level mitigation strategy to detect malicious code, which is a key cause of many CAN bus attacks. Adly et al. tested a secure boot process on AURIX TC399 microcontroller (Infineon Technologies AG, Neubiberg, Germany) using six data integrity algorithms, including a novel CMAC-based ECDSA variant, and showed that the CMAC variant was the fastest due to the optimized AES hardware accelerator. The scheme effectively detected all malicious code injections but did not detect malicious ECUs added to the network. Future work aims to address this limitation by integrating ECU detection systems.

In the following, Baldini's article introduced a novel IDS that uses CNNs to detect cyberattack anomalies in CAN bus traffic by processing CANID values [29]. Their approach, tested on the Car Hacking and ROAD datasets, uses a CNN with three convolutional layers. Through hyperparameter optimization, the authors found diferent optimal settings for the two datasets, with Car Hacking showing better performance (WS = 120, PD = 80), while ROAD performed best with WS = 300 and PD = 70. The multiscale CNN approach outperformed the single scale methods. While competitive, the method has advantages like reduced input space and reliance on legitimate traffic, but also faces challenges such as large dictionary sizes and the need for precise hyperparameter tuning.

Taking the concept of machine-learning-based intrusion detection, Bhavsar et al. applied federated learning (FL) in the context of the automotive sector, developing a federated-learning-based IDS (FL-IDS) to secure connected and autonomous vehicles (CAVs) [30]. Using the Flower framework, they incorporated logistic regression (LR) and CNN methods to train local models on Raspberry Pi testbeds and aggregate them into a global model. Their evaluation, conducted with NSL-KDD and Car-Hacking datasets, and using Python-based Keras, Pytorch, and TensorFlow showed that the LR model achieved high accuracy with NSL-KDD but lower accuracy with Car-Hacking. The PCC-CNN model, which combines Pearson correlation with CNN, optimized performance on resource-constrained devices. The PCC-CNN model performed better overall, although it had longer training times, particularly with Car Hacking, indicating a need for efficiency improvements.

Similarly advancing towards real-time detection, Dini and Saponara developed an anomaly-detection algorithm for CAN networks, leveraging a feed-forward neural network optimized with TensorFlow Lite on an NXP S32K microcontroller to classify and detect intrusions [31]. Their focus on real-time performance, particularly against replay, injection, and impersonation attacks, highlighted the importance of maintaining system accuracy. The network effectively classified known units but misclassified unknown "Intruder" units, leading to the introduction of a fourth "Unknown" class for better detection. Future work includes real-world testing, integration with other techniques, protocol expansion, comparison with deterministic algorithms, and further resilience testing to improve automotive and industrial cybersecurity.

In a different approach to vehicle network security, Pascale et al. developed an IDS using ML techniques to detect vehicle network security threats. They proposed an embedded intrusion control system (EIDS) connected to the OBDII port, which uses a two-step algorithm [32]. First, the pre-processing step analyzes ten state frames of vehicle data for anomalies through temporal and spatial analysis. Then, in the Bayesian network step, a trained Bayesian network was applied to assess the likelihood of an attack based on averaged parameter values. This Bayesian network is organized into three layers (data, information, and knowledge) to classify the vehicle's status as either normal or under attack.

Four attack types were tested—DoS, Fuzzy, Impersonation, and Attack-Free State—using the CARLA simulator with 1000 malicious messages in 24 h. The evaluation involved implementing the algorithm and Bayesian network with Weka and TensorFlow, creating datasets with 8158 frames per attack type, and measuring performance with precision, recall, and F1 score. The system showed high performance, especially with real data, and future tests on actual vehicles are planned.

Addressing the intersection of IoT and smart vehicles, Alshdadi discussed the integration of IoT technologies in smart vehicles with a focus on cybersecurity [33]. They highlighted the development of IDS using machine learning to protect IoT devices from cyber-attacks. The Advanced Electronic Cyber-Physical System (AE-CPS) was introduced, which integrates 5G, IoT, and UAVs for real-time data collection and load balancing. AE-CPS uses a layered security approach to detect attacks and ensure data integrity. The system was evaluated for its efficiency and low error rates, outperforming existing methods such as PDCRT, ABAC, and IDS. With high performance and security, AE-CPS proves to be highly effective.

Gad et al. developed an IDS for VANETs by leveraging the ToN-IoT dataset, which includes network and system data [34]. They tested various ML methods: logistic regression, naive Bayes, k-NN, decision tree, random forest, SVM, AdaBoost, and XGBoost—evaluating them on accuracy, precision, recall, F1 score, and false positives. Their approach included pre-processing for missing values, categorical data, and class imbalance, with data divided into training, validation, and test sets, and cross-validation for tuning. XGBoost consistently outperformed others, showing high accuracy and recall, particularly with Chi2 feature selection and SMOTE. k-NN also performed well and XGBoost excelled in binary and multiclass classification tasks.

Further exploring the security of in-vehicle networks, Khan et al. focused on improving in-vehicle networks, specifically the CAN bus [35]. They introduced an IDS for in-vehicle networks, using a sliding-window approach to detect anomalies by comparing mean and standard deviation values. Performance metrics, such as accuracy, precision, recall, and error rates were used to evaluate its effectiveness against attacks. The experimental results were obtained using two main datasets: the car hacking dataset and the survival analysis dataset. First, the CAN bus traffic data used were collected from Hyundai, Kia, and Chevrolet vehicles while simulating DoS and fuzzy attacks.

The IDS performed well in both standalone and merged attack scenarios, with larger windows reducing the misclassification rate (MR) for fuzzy attacks. It outperformed existing methods in accuracy and F1 scores, achieving perfect accuracy on real vehicle data across various car models. The IDS has limitations, particularly in cases where an attacker ECU is active before normality values are established.

Building on the detection strategies for vehicles, Santonicola et al. proposed CARDIAN, a context-aware cybersecurity system using Bayesian networks for real-time intrusion prevention in vehicles [36]. The IDS monitors CAN bus messages for anomalies, using real data from a heavy vehicle for training, including both normal and attack data.

The system operates in three phases: data are collected and averaged, driving scenarios are identified using the Jaccard index, and a Bayesian network calculates attack probabilities. Built from 300 h of CAN data, the network detects four types of attacks—DoS, fuzzy, gear, and RPM—with 99% accuracy.

Evaluating using real and attack datasets, the system achieved high precision and recall. It benefits from domain ontologies and an FPGA accelerator for efficient, low-energy, real-time performance. Future enhancements will involve real-world testing and contextual datasets for better adaptability and defense strategies.

3.3. Security Mechanisms for Automotive Sector with Potential AI Enhancements

In this final section, we present the articles that do not use AI, but were considered important because of their relevance. These studies highlight areas where AI can enhance security measures in the Internet of Vehicles, demonstrating potential opportunities for AI improvements in automotive IoT security.

For instance, Toker and Alsweiss developed a radar sensor for autonomous vehicles designed to resist cyberattacks at the physical layer of the radar [37]. They focused on integrating a digital signal processing (DSP) algorithm into the radar's firmware to detect adversarial signals, particularly those that could bias speed estimates. Their system combined a random signature generator with a standard frequency modulated continuous wave (FMCW) radar setup. The generator alternates chirp slopes between positive and negative frequencies, while the detection algorithm analyzes these patterns to identify potential attacks. The test involved two 77 GHz radars, with measurements that captured system noise, real data, and attack signal effects. The noise was confirmed to be white Gaussian, allowing for the generation of synthetic noise data. The study's results showed that the DSP can effectively detect attacks, with a stronger attack signal needed to trigger an alarm. This study reveals the potential for AI to further enhance such systems by refining real-time detection and response mechanisms through more advanced pattern recognition and anomaly detection techniques.

In parallel, Tany et al. examined the security implications of various automotive system architectures, focusing on the vulnerabilities inherent in different electrical/electronic (E/E) vehicle setups [6]. They described four vehicle architectures: traditional (multiple ECUs, inefficient due to wiring), one-brain (centralized HPC, risks total failure), two-brain (split functions, adds redundancy and cost) and three-brain (improves scalability but increases complexity). Using the STRIDE framework, they identified threats to components such as telematics, ECUs, sensors, actuators, and data flows, with risk increasing along with architectural complexity. Key vulnerabilities include spoofing and data manipulation in sensors and actuators, and threats to telematics and HPCs. To mitigate these risks, they recommend using firewalls, identity management, IDS/IPS, secure wireless interfaces, secure boot, virtualization, and authentication for sensors. The authors found that HPC-based automotive architectures (one-brain, two-brain, and three-brain) improve the performance, scalability, and simplicity of the wiring, but also increase costs and vulnerability. Effective security measures can address these risks. In addition, HPC systems make troubleshooting, repair, memory management, and software updates easier, although they add complexity and expense. Tany et al.'s work outlines the importance of layered security measures like firewalls, secure wireless interfaces, and IDS/IPS systems. This study emphasizes a crucial area where AI could play an innovative role, by improving the adaptability of security protocols in real-time, particularly within the more complex and vulnerable HPC-based architectures.

Latif et al. took a different approach by proposing a cluster-based authentication and communication protocol to secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [38].

Their proposed protocol involves several phases. In registration, vehicles provide an e-mail, password, and registration number, which are used to encrypt passwords. The CA then creates and sends session keys. For authentication, vehicles log in with an email, password, or authentication code, while the CA verifies credentials and updates logs. Vehicles are grouped into clusters with a cluster head (CH), selected based on a weighted score. Simulations of congested, sparse, and intermediate traffic clusters tested two resource allocation algorithms in MATLAB, showing the protocol's superior performance in authentication delay, detection accuracy, and packet delivery. The baseline and greedy resource allocation algorithms optimized V2V communication, and Postman testing showed efficient API responses and improved performance with RESTful APIs in a 5G VANET. While their model demonstrated improvements in authentication delay and packet delivery, it could be enhanced with AI. More specifically, ML could be employed to analyze traffic patterns, optimize resource allocation, and improve decision-making processes. These AI-driven improvements could enhance both the security and efficiency of IoT and IoV systems, making Latif et al.'s work a prime candidate for further exploration in AI applications.

By examining these studies, it becomes clear that although AI has not yet been fully integrated into these solutions, its potential for improving security measures in the context of the automotive IoT could be vast. The opportunities that AI has to improve real-time threat detection, resource management, and the dynamic change in the system in order to increase its adaptability, offer a promising path for future developments in this automotive field.

4. Discussion

The discussion section presented below focuses on the performance and efficiency of different AI models to mitigate the cyber-threats coming from IoT devices. By examining machine-learning techniques—such as random forest, support vector machines (SVM), and naive Bayes—as well as more advanced deep-learning techniques—including convolutional neural networks (CNNs) and long short-term memory (LSTM) networks—we highlight their strengths, limitations, and suitability for more specific types of attacks, such as DdoS, ransomware, and data theft. This section also considers the importance of these algorithms in real-time detection and predictive analysis. By understanding the comparative performance analysis of these techniques, we can identify the best approaches to ensure security in IoT environments with limited resources, such as vehicular networks, where efficiency, low utilization of computational resources and the problem of scalability are important considerations. In addition, the discussion will also cover the types of attacks, the most widely adopted artificial intelligence techniques and the role of choosing the best dataset for validating AI models.

4.1. AI Techniques and Their Efficacy

Inside the traditional machine-learning (ML) models, we found that the most adopted model is the support vector machine (SVM) [1,5,17,18,23,30], primarily due to to its robust generalization capabilities and its effectiveness in handling classification with high-dimensional data, followed by the naive Bayes model [1,5,18,23,30], which is known for its simplicity and computational efficiency. Despite its simplicity, this model offers significant computational efficiency, making it a suitable choice when IoT resources may be limited. Among these models, random forest was the model that demonstrated superior accuracy in most cases [5,10,17,30] due to its approach, which mitigates overfitting through the use of ensemble learning.

Moving to the deep-learning models, which typically outperform traditional ML models like SVM, naive Bayes, and K-Nearest Neighbors (KNN) [18] in tasks involving more complex data patterns, we observed a widespread preference for convolutional neural networks (CNNs) [3,11,16,19,20,28,29]. These models are known for their ability to automatically extract and learn feature representations. The long short-term memory, another widely adopted DL model [3,11,16,26], emerged as the best option regarding real-time attack detection. Its ability to adapt to evolving patterns of cyberattacks makes LSTM a highly valued tool in environments where the IoT devices are constantly generating temporal data, making it the best in terms of attack detection and accuracy [16].

While traditional ML models provide strong baselines, the adaptability and superior detection capabilities of deep-learning models, particularly CNNs and LSTM, are making them the preferred choice for detecting and securing IoT devices against cyberattacks.

4.2. AI in Real-Time and Predictive Threat Detection

AI can excel in real-time threat detection through the continuous monitoring of network traffic and device behavior in order to identify and mitigate malicious activities. This capability is crucial for defending against various attacks. Many authors cite DoS/DDoS attacks as the most prominent threats to IoT devices [3,5,11,13,18,21,23,25,29,30,32,35], followed by brute force attacks [10,22,30] and ransomware attacks [3,5,32], the latter of which is often considered a form of DoS attack. AI systems, by leveraging techniques such as anomaly detection and pattern recognition, can detect deviations from normal behavior and flag potential malicious traffic, enabling proper mitigation actions.

One of the most crucial challenges in IoT security is the appearance of zero-day attacks, which exploit vulnerabilities previously unknown. AI systems with adaptive-learning capabilities can evolve and update their threat detection algorithms in response to new threats. This adaptive-learning process, which continuously feeds new data into the AI model, can allow it to refine its detection capacity and recognize new attack types. As noted by Ali et al. [26], this dynamic approach ensures that AI systems can provide protection against novel zero-day vulnerabilities, where traditional security mechanisms might miss. Predictive analysis is another area where AI can enhance IoT security. Predictive analysis involves AI models to predict vulnerabilities before they can be exploited, allowing for early detection and reducing reaction time.

4.3. AI Role in Improving IoT Security

AI facilitates automated responses to detect threats by employing real-time data processing, enabling it to identify malicious activities and initiate automated response actions without human intervention. This automation is valuable in scenarios that require immediate action, such as stopping a potential attack or isolating the compromised devices. The integration of AI enables improved anomaly detection [10] and automated threat response mechanisms.

Behavioral analysis, powered by AI, is essential for establishing and maintaining a baseline of normal device activity. AI systems can learn and adapt to the typical behavior of IoT devices over time, creating a profile of the expected interactions between them. and when deviations from this pattern occur, AI can flag these anomalies. This approach has proven effective, for example, in Android malware detection, as demonstrated by Nawshin et al. [14]. By analyzing patterns, the application of AI to detect and mitigate the suspicious activity can enhance the overall security of IoT systems.

4.4. Datasets and Their Impact on Model Performance

The quality and relevance of datasets are fundamental to the success of AI models. The choice of the dataset can have a significant impact on the performance of the security frameworks, influencing their ability to detect the threats. Several key datasets that are frequently used in the evaluation are highlighted below:

4.4.1. TON_IoT Dataset

The ToN-IoT dataset, created by UNSW Canberra IoT Labs and the Cyber Range, serves as a comprehensive resource for evaluating cybersecurity applications based on ML. Proposed by Alsaedi et al. [5], it is available in CSV format and contains labeled data for normal and attack behaviors, encompassing various attack types such as ransomware, password attacks, scanning, DoS, DDoS, data injection, backdoor, XSS, and MITM. It features 44 attributes and distinguishes between normal and attack data points [34]. The TON_IoT dataset is used for training and testing AI algorithms designed to detect cyberthreats in IoT devices, making it suitable for evaluating various aspects of IoT security [5].

The dataset is organized into five directories: raw datasets (including log and CSV files), processed datasets (filtered for standard features), train/test datasets (for evaluating machine-learning algorithms), descriptive statistics (offering feature descriptions and record counts), and ground truth datasets (containing security event timestamps linked to hacking incidents). Research conducted by [21,27] effectively used the TON_IoT dataset, demonstrating its significance in the field.

4.4.2. UNSW-NB15 Dataset

The UNSW-NB15 dataset, developed by Moustafa and Slay [39], was seen as the most widely adopted dataset for evaluating anomaly detection models [1,13,16,26]. Created by the Cyber Range lab at the University of New South Wales (UNSW), it was generated using a testbed configuration with the IXIA PerfectStorm traffic generator to simulate both normal and malicious network traffic across multiple servers. Network traffic was captured in pcap format using the tcpdump tool, with attack behaviors modeled from real-world threats. Traffic analysis includes flow numbers, packet sizes, and protocol types, which are categorized into normal and attack records. Specifically, the UNSW-NB15 dataset comprises nine types of attacks. Fuzzers (crashing a network with random data), analysis (port scans, spam, HTML penetrations), backdoors (bypassing security mechanisms stealthily), DoS (disrupting network availability), exploits (leveraging known security vulnerabilities), generic (techniques applied to all block ciphers based on key size), reconnaissance (information-gathering attacks), shellcode (payloads exploiting software vulnerabilities), and worms (self-replicating malware exploiting security flaws), providing a comprehensive framework for studying network security.

4.4.3. NSL-KDD Dataset

The NSL-KDD dataset is an updated version of the original KDD Cup 99 dataset, introduced by Tavallaee et al. [40] in order to address some of the issues of its predecessor. The original KDD dataset contained many duplicate records, which could lead to biased-learning algorithms that prioritize frequent records. To address this, the authors removed all repeated records from both the training and test sets. Additionally, the original dataset has been questioned for its ease of classification that resulted in false higher accuracy rates. The NSL-KDD dataset provides a more balanced and representative selection of data points. It consists of four types of attacks: DoS (which aim to overload system resources), probe (gathering information about the network, such as port scanning), remote-to-local (R2L) attacks (where an attacker exploits vulnerabilities to gain user-level access), and user-to-root (U2R) attacks (where a local user gains root access). This dataset provides a benchmark for evaluating the effectiveness of detection models, making it a reliable choice for training and testing intrusion detection systems [11,16,30].

4.4.4. CICIDS2017 Dataset

This dataset is another important resource for evaluating AI models, as it includes various types of attacks and normal traffic. Sharafaldin et al. and the Canadian Institute for Cybersecurity (CIC) created the CICIDS2017 dataset [41], which simulates realistic benign and malicious network traffic over five days. It includes various attack profiles, such as DoS, DDoS, brute force, heartbleed, botnet, web attacks (SQL Injection, XSS), and infiltration, using tools like Patator, LOIC, and Metasploit. The dataset features 80 extracted attributes using CICFlowMeter, making it ideal for evaluating intrusion detection systems (IDSs). The attacks are characterized as follows:

- Brute force—attempts all password combinations;
- Heartbleed—exploits a bug to retrieve sensitive data;
- Botnet—compromised devices controlled to steal data;
- DoS—overwhelms a resource with excessive requests;
- DDoS—multiple systems generate massive traffic;
- Web attacks—includes SQL injection and XSS;
- Infiltration—exploits software vulnerabilities for internal access.

The CICIDS2017 is part of a series of datasets developed to support the study of network security. It is recognized and adopted by several authors [10,15,16].

4.4.5. Datasets Summary

For a clearer understanding of the datasets used, Table 3 provides an overview of how each dataset was partitioned by its respective creators. Most datasets, including TON_IoT, UNSW-NB15, and NSL-KDD, were divided into training and testing sets. However, the CICIDS2017 dataset is different, since it is not split in this manner. Instead, the CICIDS2017 dataset is organized into two categories: benign traffic (2,359,087 records) and attack records, allowing for a detailed analysis of malicious activities and normal network behavior.

Table 3. Table of the datasets.

Datasets	Training	Testing	Total
TON_IoT	21,877,978	461,043	22,339,021
UNSW-NB15	175,341	82,332	257,673
NSL-KDD	1,074,992	77,289	1,152,281
CICIDS2017	Attack Records: 720,928		3,080,015

In addition to these widely used datasets, several authors used their own dataset, with some also proposing their IoT-specific tailored dataset. For example, the EDGE-IoTset, proposed by [18] or Malimg, is an established dataset used in the field of detecting metamorphic malware, used in the research by Habib et al. [19].

4.5. Challenges and Future Directions

Although the integration of AI into IoT security has progressed, there is still a number of challenges that remain, which should be addressed to improve the effectiveness of these technologies. One major issue is overfitting, where AI models perform well during training but struggle to handle new and unseen data. Overfitting is a concern in IoT security due to the unpredictable nature of new threats. Some methods, such as the use of wide deep long short-term memory (WDLSTM) networks [3], have been proposed to mitigate the overfitting problem, assisted by CNNs to allow for automatic feature extraction. However, it is necessary to create additional strategies, such as cross-validation techniques, in order to increase the robustness of AI models.

Scalability is another worrying challenge. As the proliferation of IoT networks grows, AI models must be able to adapt to the increase in data volume and also to the growing number of devices, in order not to become an obsolete model. Studies such as those by Ajay et al. [22] highlight the importance of a strong AI capability to scale the network effectively. Techniques such as recursive feature elimination and dimensionality reduction, as suggested by Samy et al. [16] and Akshaya et al. [11], are crucial to ensuring that AI models remain efficient without compromising performance.

AI can also improve radar detection of cyberattacks, especially in IoT and the automotive sector. ML and DL algorithms can integrate radar data with data from other sensors, such as cameras or GPS, providing a more comprehensive view of the environment and improving the accuracy of object tracking [37].

Another concern is environments with typically limited resources, which are easily found in IoT networks. These types of devices usually have low computing power, limited memory, and poor battery life, which is a challenge for implementing AI models that require a lot of computational resources. Future research should focus on developing lighter AI algorithms that can work effectively in these types of environments. In addition, integrating AI into threat modeling can improve risk management by being able to analyze large datasets of vehicle components to automatically identify potential threats. AI can prioritize threats dynamically, since it has the ability to assess the probability and the impact of the threats by using historical data, directing resources to the most critical risks [6].

Looking at future directions, the most critical area for future research is adapting AI to keep the pace with the rapidly growing scale of IoT devices. It would be interesting to see the integration of AI with upcoming technologies, such as 5G, 6G, and the blockchain, which could improve the security of IoT systems.

4.6. Limitations of Our Study

Although this review provides a general approach to the intersection of AI and IoT security, we should note some of the limitations. First, the rapidly evolving nature of IoT devices poses a challenge, as we may find it difficult to cover the latest technologies. Many of the techniques may be in the early stages of development, or there may be some limitations on proprietary solutions that have not been published.

Second, although we have analyzed various datasets and AI models, their performance varies based on many factors. We recognize that the effectiveness of these models can vary substantially when applied to real-world scenarios, which was outside the context of this article to evaluate.

Finally, although we have tried to follow a recognized and widely adopted methodology in reviews to the letter, we must acknowledge the limitations inherent in our possible bias, both in the search strategy and in the screening and selection of the articles included, which may not fully represent the best ones to include in the scope of this review. Additionally, the choice of the mentioned scientific repositories used on our literature review may also be acknowledged as a limitation of our study, potentially overlooking other research published in other repositories. This includes technical reports, industry publications, Master's dissertations, or PhD theses that could provide additional valuable resources to be included in this review.

5. Conclusions

With this review, we aim to highlight the growing role of artificial intelligence techniques, particularly machine learning and deep learning, in enhancing the security in IoT devices. These models are essential for automating the detection of malicious activities and improve real-time attack mitigation. Despite the widespread adoption of machine-learning methods, challenges related to scalability and real-time processing, especially in resource-limited environments such as IoT networks and the automotive sector, still remain.

Our analysis reveals that the choice of datasets, such as UNSW-NB15 and CICIDS2017, can significantly affect the performance of these models. While standard metrics like precision, recall, and F1 score are commonly used for evaluating the performance, they cannot respond to the specific challenges of IoT, such as latency, resource consumption, computational overhead, and robustness to adversarial attacks. Future research must focus on developing a more comprehensive evaluation framework that reflects the unique characteristics of IoT environments.

The integration of machine learning into IoT security is still in its early stages. While progress has been made, many models remain too computationally intensive for practical deployment in environments with limited processing power. Addressing this issue through the development of lightweight and scalable models is important for the continued advancement of this field.

Looking ahead, it is clear that the collaboration between academia and industry will be critical to overcome these challenges. Emerging approaches such as federated learning, which can distribute computation across devices while preserving data privacy, and adaptive algorithms, offer potential for the future of IoT and vehicular security. Only through these continued advancements we will be able to realize the full potential of AI in protecting IoT ecosystems and ensure resilience against increasingly sophisticated cyber-threats.

In conclusion, while AI provides promising solutions for detecting and mitigating cyber-threats in IoT devices, its full potential is yet to be fulfilled. The critical challenges of scalability and real-time detection is essential for creating more resilient and adaptable systems capable of defending against sophisticated cyberattacks. Continuous innovation, by researchers and industry professionals, will be key to developing efficient algorithms that meet the demands of IoT ecosystems and the automotive sector.

Author Contributions: Conceptualization, R.A., E.S., C.S., F.B. and A.V.; methodology, R.A. and E.S.; validation, C.S., F.B. and A.V.; formal analysis, C.S., F.B. and A.V.; investigation, R.A. and E.S.; writing—original draft preparation, R.A. and E.S.; writing—review and editing, C.S., F.B. and A.V.; supervision, C.S., F.B. and A.V. All authors have read and agreed to the published version of the manuscript.

Funding: The study was developed under the project A-MoVeR—"Mobilizing Agenda for the Development of Products & Systems towards an Intelligent and Green Mobility", operation n.º 02/C05-i01.01/2022.PC646908627-00000069, approved under the terms of the call n.º 02/C05-i01/2022—Mobilizing Agendas for Business Innovation, financed by European funds provided to Portugal by the Recovery and Resilience Plan (RRP), in the scope of the European Recovery and Resilience Facility (RRF), framed in the Next Generation UE, for the period from 2021–2026.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AES	*Advanced Encryption Standard*
AI	*Artificial Intelligence*
APK	*Android Application Pack*
BPEO	*Binary Pigeon Optimization Algorithm*
CAN	*Controller Area Network*
CARLA	*Car Learning to Act*
CART	*Classification and Regression Trees*
CAV	*Connected and Autonomous Vehicles*
CH	*Cluster Head*
CMAC	*Cipher-Based Message Authentication Code*
CNN	*Convolutional Neural Network*
CPS	*Cyber-Physical System*
DBN	*Deep Belief Network*
DCNN	*Deep Convolutional Neural Network*
DDoS	*Distributed Denial of Service*
DL	*Deep Learning*

DNN	*Deep Neural Network*
DT	*Decision Trees*
DoS	*Denial of Service*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ECU	*Electronic Control Unit*
ERNN	*Elman Recurrent Neural Network*
FL	*Federated Learning*
FMCW	*Frequency Modulated Continuous Wave*
FNR	*False Negative Rate*
FPGA	*Field-Programmable Gate Array*
GRU	*Gated Recurrent Unit*
ID	*Identifier*
IDS	*Intrusion Detection System*
IIoT	*Industrial Internet of Things*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
IoT	*Internet of Things*
K-NN	*K-Nearest Neighbors*
LDA	*Linear Discriminant Analysis*
LR	*Logistic Regression*
LSTM	*Long Short-Term Memory*
MDPI	*Multidisciplinary Digital Publishing Institute*
ML	*Machine Learning*
MLP	*Multi-Layer Perceptron*
MR	*Misclassification Rate*
NB	*Naive Bayes*
NFV	*Network Functions Virtualization*
OBDII	*On-Board Diagnostics II*
PCA	*Principal Component Analysis*
PDR	*Packet Delivery Ratio*
PICO	*Population, Intervention, Comparison, Outcome*
PRISMA	*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*
PSO	*Particle Swarm Optimization*
QDA	*Quadratic Discriminant Analysis*
RF	*Random Forest*
SDN	*Software-Defined Networking*
SIEM	*Security Information and Event Management*
SMOTE	*Synthetic Minority Over-Sampling Technique*
SNR	*Signal-to-Noise Ratio*
STRIDE	*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*
SVD	*Singular Value Decomposition*
SVM	*Support Vector Machine*
TCP	*Transmission Control Protocol*
TPR	*True Positive Rate*
UDP	*User Datagram Protocol*
V2I	*Vehicle-to-Infrastructure*
V2V	*Vehicle-to-Vehicle*
VANET	*Vehicular Ad-hoc Network*
XBFE	*eXtreme Balanced Feature Engineering*
XGBoost	*eXtreme Gradient Boosting*

References

1. Saheed, Y.K.; Abiodun, A.I.; Misra, S.; Holone, M.K.; Colomo-Palacios, R. A machine learning-based intrusion detection for detecting internet of things network attacks. *Alex. Eng. J.* **2022**, *61*, 9395–9409. [CrossRef]
2. Korium, M.S.; Saber, M.; Beattie, A.; Narayanan, A.; Sahoo, S.; Nardelli, P.H. Intrusion detection system for cyberattacks in the Internet of Vehicles environment. *Hoc. Netw.* **2024**, *153*, 103330. [CrossRef]

3. Ullah, I.; Mahmoud, Q.H. Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEE Access* **2021**, *9*, 103906–103926. [CrossRef]
4. Aliwa, E.; Rana, O.; Perera, C.; Burnap, P. Cyberattacks and countermeasures for in-vehicle networks. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–37. [CrossRef]
5. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access* **2020**, *8*, 165130–165150. [CrossRef]
6. Tany, N.S.; Suresh, S.; Sinha, D.N.; Shinde, C.; Stolojescu-Crisan, C.; Khondoker, R. Cybersecurity comparison of brain-based automotive electrical and electronic architectures. *Information* **2022**, *13*, 518. [CrossRef]
7. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, 89. [CrossRef]
8. Frandsen, T.F.; Nielsen, M.F.B.; Lindhardt, C.L.; Eriksen, M.B. Using the full PICO model as a search tool for systematic reviews resulted in lower recall for some PICO elements. *J. Clin. Epidemiol.* **2020**, *127*, 69–75. [CrossRef]
9. Nudelman, G.; Otto, K. The Development of a New Generic Risk-of-Bias Measure for Systematic Reviews of Surveys. *Methodology* **2020**, *16*, 278–298. [CrossRef]
10. Tendikov, N.; Rzayeva, L.; Saoud, B.; Shayea, I.; Azmi, M.H.; Myrzatay, A.; Alnakhli, M. Security Information Event Management data acquisition and analysis methods with machine learning principles. *Results Eng.* **2024**, *22*, 102254. [CrossRef]
11. Akshaya, V.; Mandala, V.; Anilkumar, C.; VishnuRaja, P.; Aarthi, R. Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over Internet of Things. *Meas. Sens.* **2023**, *30*, 100917.
12. Hassan, J.; Sohail, A.; Awad, A.I.; Zaka, M.A. LETM-IoT: A lightweight and efficient trust mechanism for Sybil attacks in Internet of Things networks. *Hoc. Netw.* **2024**, *163*, 103576. [CrossRef]
13. Sudharsanan, R.; Rekha, M.; Pritha, N.; Ganapathy, G.; Rasoni, G.A.N.; Uthayakumar, G. Intruder identification using feed forward encasement-based parameters for cybersecurity along with IoT devices. *Meas. Sens.* **2024**, *32*, 101035. [CrossRef]
14. Nawshin, F.; Unal, D.; Hammoudeh, M.; Suganthan, P.N. AI-powered malware detection with Differential Privacy for zero trust security in Internet of Things networks. *Hoc. Netw.* **2024**, *161*, 103523. [CrossRef]
15. Alkhonaini, M.A.; Al Mazroa, A.; Aljebreen, M.; Hassine, S.B.H.; Allafi, R.; Dutta, A.K.; Alsubai, S.; Khamparia, A. Hybrid Sine-Cosine Chimp optimization based feature selection with deep learning model for threat detection in IoT sensor networks. *Alex. Eng. J.* **2024**, *102*, 169–178. [CrossRef]
16. Samy, A.; Yu, H.; Zhang, H. Fog-based attack detection framework for internet of things using deep learning. *IEEE Access* **2020**, *8*, 74571–74585. [CrossRef]
17. Nallakaruppan, M.; Somayaji, S.R.K.; Fuladi, S.; Benedetto, F.; Ulaganathan, S.K.; Yenduri, G. Enhancing Security of Host-based Intrusion Detection Systems for the Internet of Things. *IEEE Access* **2024**, *12*, 31788–31797 [CrossRef]
18. Ferrag, M.A.; Friha, O.; Hamouda, D.; Maglaras, L.; Janicke, H. Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. *IEEE Access* **2022**, *10*, 40281–40306. [CrossRef]
19. Habib, F.; Shirazi, S.H.; Aurangzeb, K.; Khan, A.; Bhushan, B.; Alhussein, M. Deep Neural Networks for Enhanced Security: Detecting Metamorphic Malware in IoT Devices. *IEEE Access* **2024**, *12*, 48570–48582. [CrossRef]
20. Negabi, I.; Ait El Asri, S.; El Adib, S.; Raissouni, N. Deep Learning-Based Power Analysis Attack for Extracting AES Keys on ATmega328P Microcontroller. *Arab. J. Sci. Eng.* **2024**, *49*, 4197–4208. [CrossRef]
21. Soliman, S.; Oudah, W.; Aljuhani, A. Deep learning-based intrusion detection approach for securing industrial Internet of Things. *Alex. Eng. J.* **2023**, *81*, 371–383. [CrossRef]
22. Ajay, P.; Nagaraj, B.; Kumar, R.A.; Suthana, V.; Keziah, M.R. DBN-protected material Enhanced intrusion prevention sensor system defends against cyber attacks in the IoT devices. *Meas. Sens.* **2024**, *34*, 101263. [CrossRef]
23. Bhayo, J.; Shah, S.A.; Hameed, S.; Ahmed, A.; Nasir, J.; Draheim, D. Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Eng. Appl. Artif. Intell.* **2023**, *123*, 106432. [CrossRef]
24. Manickam, P.; Girija, M.; Sathish, S.; Dudekula, K.V.; Dutta, A.K.; Eltahir, Y.A.; Zakari, N.M.; Gilkaramenthi, R. Billiard based optimization with deep learning driven anomaly detection in internet of things assisted sustainable smart cities. *Alex. Eng. J.* **2023**, *83*, 102–112. [CrossRef]
25. Abbas, S.; Al Hejaili, A.; Sampedro, G.A.; Abisado, M.; Almadhor, A.; Shahzad, T.; Ouahada, K. A novel federated edge learning approach for detecting cyberattacks in IoT infrastructures. *IEEE Access* **2023**, *11*, 112189–112198. [CrossRef]
26. Ali, S.; Ghazal, R.; Qadeer, N.; Saidani, O.; Alhayan, F.; Masood, A.; Saleem, R.; Khan, M.A.; Gupta, D. A novel approach of botnet detection using hybrid deep learning for enhancing security in IoT networks. *Alex. Eng. J.* **2024**, *103*, 88–97. [CrossRef]
27. Ganapathy, G.; Anand, S.J.; Jayaprakash, M.; Lakshmi, S.; Priya, V.B.; Pandi, S. A blockchain based federated deep learning model for secured data transmission in healthcare Iot networks. *Meas. Sens.* **2024**, *33*, 101176. [CrossRef]
28. Adly, S.; Moro, A.; Hammad, S.; Maged, S.A. Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles. *Appl. Sci.* **2023**, *13*, 9374. [CrossRef]
29. Baldini, G. In-Vehicle Network Intrusion Detection System Using Convolutional Neural Network and Multi-Scale Histograms. *Information* **2023**, *14*, 605. [CrossRef]
30. Bhavsar, M.; Bekele, Y.; Roy, K.; Kelly, J.; Limbrick, D. FL-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices for Transportation IoT. *IEEE Access* **2024**, *12*, 52215–52226. [CrossRef]

31. Dini, P.; Saponara, S. Design and Experimental Assessment of Real-Time Anomaly Detection Techniques for Automotive Cybersecurity. *Sensors* **2023**, *23*, 9231. [CrossRef] [PubMed]
32. Pascale, F.; Adinolfi, E.A.; Coppola, S.; Santonicola, E. Cybersecurity in automotive: An intrusion detection system in connected vehicles. *Electronics* **2021**, *10*, 1765. [CrossRef]
33. Alshdadi, A.A. Cyber-physical system with IoT-based smart vehicles. *Soft Comput.* **2021**, *25*, 12261–12273. [CrossRef]
34. Gad, A.R.; Nashat, A.A.; Barkat, T.M. Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset. *IEEE Access* **2021**, *9*, 142206–142217. [CrossRef]
35. Khan, J.; Lim, D.W.; Kim, Y.S. Intrusion detection system can-bus in-vehicle networks based on the statistical characteristics of attacks. *Sensors* **2023**, *23*, 3554. [CrossRef]
36. Santonicola, E.; Adinolfi, E.A.; Coppola, S.; Pascale, F. Automotive Cybersecurity Application Based on CARDIAN. *Future Internet* **2023**, *16*, 10. [CrossRef]
37. Toker, O.; Alsweiss, S. Design of a cyberattack resilient 77 GHz automotive radar sensor. *Electronics* **2020**, *9*, 573. [CrossRef]
38. Latif, R.M.A.; Jamil, M.; He, J.; Farhan, M. A Novel Authentication and Communication Protocol for Urban Traffic Monitoring in VANETs Based on Cluster Management. *Systems* **2023**, *11*, 322. [CrossRef]
39. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; IEEE: Piscataway, NJ, USA, 2015, pp. 1–6. [CrossRef]
40. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, Canada, 8–10 July 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 1–6. [CrossRef]
41. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp* **2018**, *1*, 108–116. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.