IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 January 2024, accepted 3 February 2024, date of publication 23 February 2024, date of current version 12 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3369181

SURVEY

SoK of Machine Learning and Deep Learning Based Anomaly Detection Methods for Automatic Dependent Surveillance-Broadcast

NURŞAH ÇEVIK[1,2] **AND SEDAT AKLEYLEK**[3,4]
[1]HAVELSAN, 06510 Ankara, Turkey
[2]Department of Computer Engineering, Ondokuz Mayıs University, 55139 Samsun, Turkey
[3]Department of Computer Engineering, Istinye University, 34010 İstanbul, Turkey
[4]Institute of Computer Science, University of Tartu, 51009 Tartu, Estonia

Corresponding author: Nurşah Çevik (nursah.kaya@bil.omu.edu.tr)

ABSTRACT This paper focuses on the vulnerabilities of ADS-B, one of the avionics systems, and the countermeasures taken against these vulnerabilities proposed in the literature. Among the proposed countermeasures against the vulnerabilities of ADS-B, anomaly detection methods based on machine learning and deep learning algorithms were analyzed in detail. The advantages and disadvantages of using an anomaly detection system on ADS-B data are investigated. Thanks to advances in machine learning and deep learning over the last decade, it has become more appropriate to use anomaly detection systems to detect anomalies in ADS-B systems. To the best of our knowledge, this is the first survey to focus on studies using machine learning and deep learning algorithms for ADS-B security. In this context, this study addresses research on this topic from different perspectives, draws a road map for future research, and searches for five research questions related to machine learning and deep learning algorithms used in anomaly detection systems.

INDEX TERMS ADS-B, anomaly based intrusion detection system, anomaly detection system, cyber security, avionics security, deep learning, IDS, intrusion detection system, machine learning.

I. INTRODUCTION

The security of critical infrastructure has been received great attention. In 2003, the security of the information systems to support critical infrastructures such as avionic systems took primacy [1]. Cyber attacks on avionic systems are known to have damaging effects on critical areas such as the safety of passengers and the national economy. That is the reason why avionic systems have been designed as closed and independent systems with strict security restrictions. However, with the NextGen (Next Generation Air Transportation System) Project started in the USA as well as the SESAR (Single European Sky ATM Research) project in Europe [2], avionics infrastructures began to be renewed. These projects aim to design high-performance, low-cost, and more secure avionics systems. In the last 15 years, most of the operations carried out in avionic systems have been automated with renewed systems. Therefore, avionic infrastructures have become more interdependent structures. Even if interdependent systems are more effective than independent ones, they cause new security vulnerabilities. In addition, it is seen that the difficulties have been encountered in some areas, such as the protection of information systems in avionic systems and the determination of cyber security roles/responsibilities. Hence studies to tighten the security, reliability, and sustainability of avionic systems have begun.

Modern aircrafts are equipped with a system known as ADS-B, which periodically broadcasts various information so that air traffic controls and other aircraft can monitor it. As part of the NextGen project, the use of the ADS-B system

The associate editor coordinating the review of this manuscript and approving it for publication was Juan A. Lara.

on civil flights has been mandatory as of January 2020 [3]. In this article, the types of attacks that can be carried out against the ADS-B system are examined in detail. In 2020, the Federal Aviation Administration stated that attackers could eavesdrop on the ADS-B system and conduct man-in-the-middle-attacks on this system [1]. However, the FAA stated that the revealed data from the broadcast of this system does not expose the current systems to a higher risk [1]. Since there has not been a successful attack against the ADS-B system, the feasibility of these attacks has been discussed by the FAA [4]. Nevertheless, recent research in the literature shows that it is possible to perform successful and low-cost attacks against ADS-B systems [4].

Unmanned aerial vehicles (UAVs) and drones are other application area for GPS and ADS-B system used. They have been used for specific missions in a limited time and at a low cost. The UAV application has been increasingly used due to its unique characteristics. The components of the UAV network, such as the UAV and Ground Control Station (GCS), are dependent on GPS and ADS-B broadcasts for navigation. Therefore, this network is open to various cyber threats such as jamming and spoofing attacks [5].

Various security solutions have been proposed in the literature to provide for the security of the ADS-B system [4]. These solutions require changes to the protocol or structure of the system. Since ADS-B systems have been used in most civil aircraft today, possible changes in the protocol or structure of the system are costly. Also, providing a security solution for ADS-B systems without interrupting or slowing down the real-time data flow is another challenge. For this reason, security solutions are not used in ADS-B systems today. Recently, it has been observed that anomaly based detection systems have been widely proposed to detect anomalies in the ADS-B system. This security solution has some advantages over others: it does not require a change in the system protocol, nor additional sensors to work. This solution analyzes the ADS-B system behavior to detect anomalies, and its increase in accuracy with advances in machine learning and deep learning. That is why anomaly-based systems have been so popular lately. This article concentrates on using anomaly-detection systems for ADS-B systems, in which machine learning and deep learning algorithms are used, and in which databases and features are selected.

A. SURVEYS ON THE SECURITY OF ADS-B

There are two comprehensive survey studies on the general security of the ADS-B system published in 2015 [6] and 2020 [4]. However, there is no survey study to provide security for the ADS-B system using machine learning and deep learning methods; therefore this section summarizes general survey studies for the ADS-B system.

In 2015, Strohmeier et al. examined and summarized possible attack scenarios and security solutions for the ADS-B system in detail [6]. Within the scope of this study, it is mentioned why cryptographic security solutions used in network systems cannot be directly adapted to the ADS-B system. According to the authors, cryptosystems are unsuitable for critical infrastructure systems where real-time data transfer is significant, such as airplanes, in terms of processing power and memory requirements. Encryption and decryption processes cause latency for flight systems; therefore aviation authorities have stated that the existing vulnerabilities of the systems have a lower risk than the risk from this latency. In addition, defining a new protocol requires changes in the system infrastructure and increases the operating and maintenance costs of the system. Strohmeier et al. compared nine different attack methods in terms of the layer where the attack occurred, exploited vulnerability, attack frequency, and complexity [6]. They identified which vulnerabilities could be exploited by attackers and examined security solutions against attack methods. Then, they stated which security solutions are appropriate to use against which attack methods.

In 2020, Jun et al. divided the possible attack scenarios against the ADS-B system into two air-to-air and ground-to-air attacks [4]. These attacks are examined for four intentions: information gathering, economic benefit, terrorism, and cyber warfare, and are evaluated in four categories: confidentiality, integrity, availability, and authentication. They refer to the requirements of information security compromised by the attack. This approach is used to classify attacks and construct attack trees in the risk assessment phase. Attackers could have five capabilities: eavesdropping, message injection, message modification, message deletion, and signal jamming. The security measures against attacks are analyzed in two categories: secure location verification and secure broadcast verification. Machine learning and deep learning methods are discussed in non cryptographic methods under the secure location verification category. ML and DL algorithms are examined in Data Fusion as well as in Traffic Modeling section, in addition to the Anomaly Detection section. Traffic modeling is not quite the same thing as anomaly detection, but it is relevant. This research emphasized the suitability and importance of anomaly detection methods in anomaly detection of the ADS-B system, thanks to the developments in ML and DL [4]. In this study, the authors examined security solutions for ADS-B systems in two categories: secure broadcast verification and secure location verification. They presented a general security solution architecture in Fig. 1 [4].

When we look at these studies, both are focused on the system's overall security. Moreover, these surveys did not follow a systematic approach. Since no survey study concentrated on machine learning and deep learning methods for the security of the ADS-B system, the most comprehensive survey studies on the general security of the ADS-B system were examined within the scope of this study.

B. CONTRIBUTION

Authors present a comprehensive overview of the current state of the field, and give key concepts, methodologies,

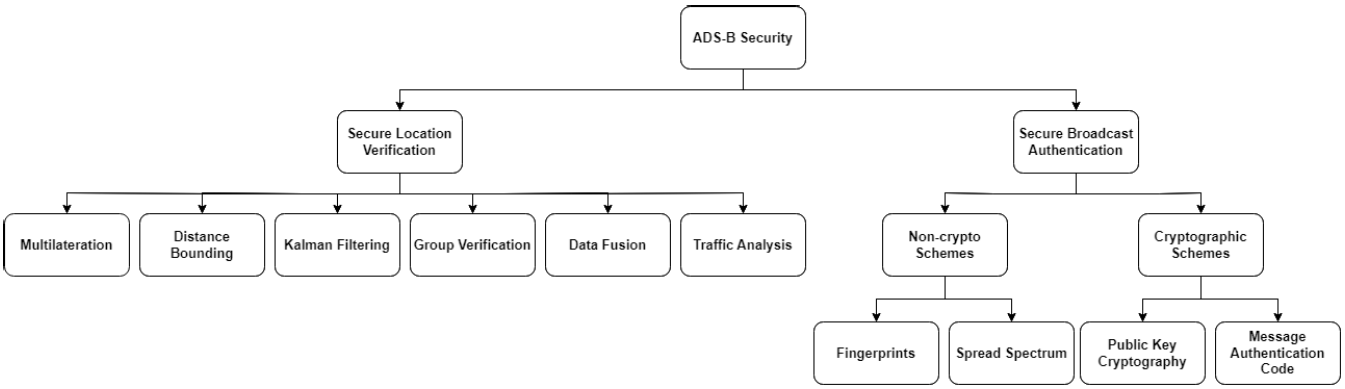

FIGURE 1. Security Solutions for ADS-B Systems [4].

and findings related to ML/DL-based intrusion detection for ADS-B devices.

1) This review evaluates the advantages and disadvantages of ML/DL models for ADS-B intrusion detection to provide insights into the performance, accuracy, and limitations of different models.
2) The literature review identifies the challenges and open research problems related to real-time implementations of ML/DL based IDS for avionic systems. Recognizing these challenges helps guide developing new methodologies.
3) The review examines existing approaches and discusses the practical implications of ML/DL based IDS for ADS-B devices in avionics cyber security.

C. MOTIVATION

The ADS-B system became mandatory for many aircraft as of 2020 [1]. Nevertheless, the security vulnerabilities of this system have not been fixed yet. The main weaknesses of this system are that it publishes flight-related information without any encryption and that the receiving party does not check the identity of incoming messages. With technological development, technologies that are difficult to reach have become accessible. This situation has made it easier for adversaries to access information and related equipment. In this way, while the cost and difficulty level of the attacks decrease, the probability of attack increases. Therefore, security constraints in critical infrastructures such as aviation systems should be reconsidered. When the security solutions offered for the security of the ADS-B system are reviewed, it is clear that machine learning and deep learning based anomaly/intrusion detection systems are more advantageous than other security solutions. Anomaly/intrusion detection systems can be quickly integrated into existing systems without requiring protocol or hardware changes. Since there is no need to work on the relevant system, it does not affect the system's complexity. Increasing accuracy rates of machine learning and deep learning methods also show that it is possible to use these systems in this field.

TABLE 1. Research questions.

	Research Questions
RQ1	Which algorithms are commonly used to detect anomalies in ADS-B data?
RQ2	Which ADS-B databases are used to train models?
RQ3	Which features are helpful for training models?
RQ4	What are common metrics used to evaluate models in the anomaly detection system of ADS-B?
RQ5	For which vulnerabilities of ADS-B can the proposed security solutions be effective?

D. ORGANIZATION

Within the scope of this study, the selection and elimination stages of the articles are defined in Section II. In Section III, the technical infrastructure, machine learning techniques, and evaluation metrics of the ADS-B system are defined. In Section IV, summaries and comparisons of the studies selected within the scope of the previous section are given. The information obtained within the scope of the research questions determined in Section V is shared. In Section VI, the limitations of the research are shared. In Section VII, the results of the research and the open problems are examined. Additionally, future research on ADS-B security are outlined.

II. METHODOLOGY

A. RESEARCH QUESTIONS

This study is a systematization of knowledge (SoK); therefore, the research questions, given in Table 1, were defined first. This section describes the research questions examined within the scope of this paper.

1) Which algorithms are commonly used to detect anomalies in ADS-B data?

   Purpose: To analyze the performance metrics and accuracy rates of algorithms frequently used for intrusion detection in ADS-B systems and to analyze their relationship with the dataset.
2) Which ADS-B databases are used to train models?

   Purpose: To identify frequently used databases in the literature and to compare the results of studies using the same database.
3) Which features are helpful for training models?

Purpose: Parameter extraction is the most crucial step in machine learning and deep learning models. To determine the parameters used in the literature and to analyze the parameters' effects on the evaluation metrics results.

4) What are common metrics used to evaluate models in the anomaly detection system of ADS-B?

Purpose: Analyzing evaluation metrics used in different fields.

5) For which vulnerabilities of ADS-B can the proposed security solutions be effective?

Purpose: The presented intrusion detection systems detect different types of attacks. Identifying which types of attacks the solutions provide security against.

B. SEARCH STRATEGY

Considering the research questions defined in Table 1, the keywords "Machine Learning," "Deep Learning," and "ADS-B" have been searched in academic databases: Scopus, IEEE Xplore, and Web of Science. Query sentences are given in Table 2.

C. SEARCH PROCESS AND FILTERING CRITERIA

Within the scope of this study, studies on the security of ADS-B data and analysis and security measures with machine learning or deep learning methods were examined. During the selection of the studies examined, academic databases were searched using the search terms defined in Table 3.

Between 2018 and 2024, a total of 34 publications, 25 of which were conference and 9 journal publications, were published in the IEEE database. On Scopus, another important database, a total of 53 publications, 30 of which were conference publications and 23 journal, were published between 2012 and 2024. 2 of the conference publications and one of the journal publications are survey studies. Finally, the Web of Science database was examined, and a total of 41 publications were published between 2018 and 2024, including 19 conference publications, 22 journal publications.

Before examining the publications obtained in the search results, studies whose language is not English and unrelated to the subject in terms of field and title were eliminated. This process is given in Fig. 2.

The summaries of these publications were examined, and their compatibility with the scope of this study was reviewed. In this way, the number of publications to be examined has been reduced from 45 to 14. In this study, 14 studies related to the security of the ADS-B system in terms of area, title, summary, and scope were examined and compared based on issues such as the method used, database, and performance rates.

III. MATERIALS AND METHODS

In this section, the general structure and technical specifications of the ADS-B system are given. In addition, machine learning and deep learning methods, which are widely used in the security mechanisms offered for the ADS-B system, and the evaluation criteria of these methods are explained.

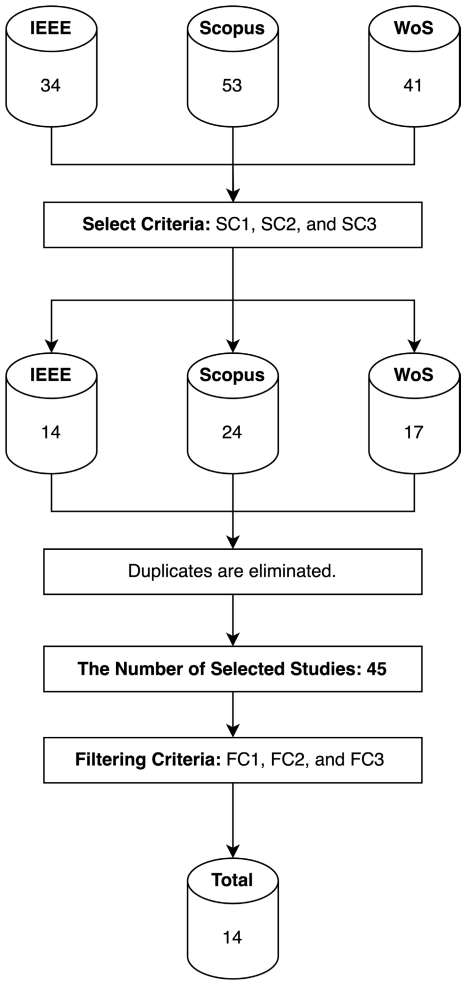

FIGURE 2. Research methodology.

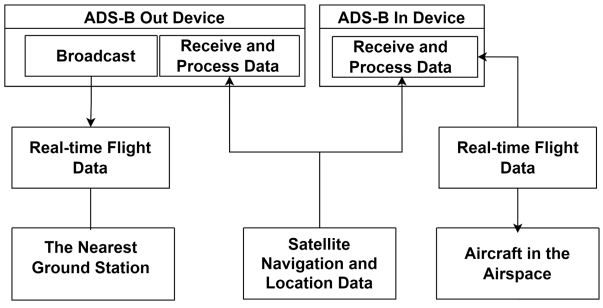

FIGURE 3. ADS-B architecture.

A. ADS-B SYSTEM

Automatic Dependent Surveillance-Broadcast (ADS–B) is an advanced surveillance technology with two different types: ADS-B Out and ADS-B In.

1) ADS–B Out is located in the aircraft and broadcasts highly accurate positional information, such as the aircraft's GPS location, altitude, and ground speed,

TABLE 2. Query clauses and fields.

Academic Database	Query Clause	Query Field
Scopus	TITLE-ABS-KEY (("Machine Learning" OR "Deep Learning" OR "Anomaly Detection")) AND (LIMIT-TO(EXACTKEYWORD, "ADS-B"))	Title, Abstract, Key Words
IEEE Xplore	(("Abstract":machine learning OR "Abstract":deep learning OR "Abstract":anomaly detection) AND "Abstract":ADS-B) AND ("Author Keywords":machine learning OR "Author Keywords":deep learning OR "Author Keywords":anomaly detection OR "Author Keywords":ADS-B) AND ("Document Title":machine learning OR "Document Title":deep learning OR "Document Title":anomaly detection OR "Document Title":ADS-B))	Title, Abstract, Key Words
WoS	TI=(ADS-B OR Anomaly Detection OR Machine learning OR deep learning) AND AB=(ADS-B AND (Anomaly Detection OR Machine learning OR deep learning)) AND AK=(ADS-B OR Anomaly Detection OR Machine learning OR deep learning)	Title, Abstract, Key Words

TABLE 3. Search and filtering criteria.

Search Criteria (SC)	
SC1	English-language studies published in a journal or conference
SC2	The journal in which the study was published should be at Q1 or Q2.
SC3	Studies focusing on intrusion detection in the ADS-B system
Filtering Criteria (FC)	
FC1	The study is a survey article
FC2	The study does not contain information about intrusion detection.
FC3	The study does not contain information about the dataset used.

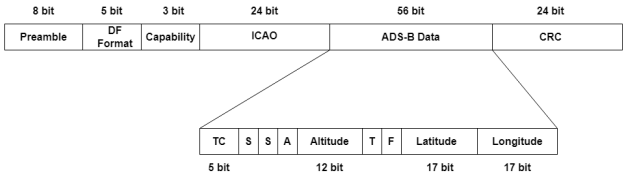

FIGURE 4. ADS-B packet format [7].

TABLE 4. ADS-B packet context [7].

Context	Definition	Bit
Preamble	A predefined sequence of bits to mark the start of a message.	8 bit
DF Format	Downlink Format, indicating the type of message.	5 bit
Capability	Aircraft capabilities and equipment codes.	3 bit
ICAO	A unique 24-bit identifier.	24 bit
CRC	Cyclic Redundancy Check, used for error detection.	24 bit
ADS-B	Position, velocity, and other information.	56 bit

to ground controllers and other aircraft. Its accuracy is greater than using conventional radar surveillance.

2) ADS-B In locates on the aircraft or at the ground station and receives data from ADS-B Out devices within range of the ADS-B In. This device, which transmits position faster than other radar systems, was initially used in ground and air traffic control systems. Today, it has started to be used in aircraft to monitor air traffic.

The general architecture of the ADS-B device is described in Fig. 3.

ADS-B In is not mandated by the ADS-B Rule; only ADS-B Out is required in order to fly in the airspace mentioned in 14 CFR 91.225. At present, the FAA does not plan to mandate ADS-B In. The ADS-B Out device periodically broadcasts the flight data such as position, altitude, and speed obtained from the satellite system to the aircraft and ground stations within its range. It thus appears on radars of other systems equipped with ADS-B In devices.

ADS-B Out message contains 112 bits of data (excluding the preamble). The bit distribution in the content of the message is shown in Fig. 4.

The definition of the parts of the ADS-B message is shown in Table 4.

The ADS-B Out broadcasts the position data in plain text form so that all ADS-B In devices within range of the ADS-B Out can obtain the data. For example, data broadcasted by ADS-B Out devices is shown on websites such as FlightRadar24, FlightAware, and OpenSky Network [8]. In civil aviation, in addition to the information such as altitude, direction, location, and speed published by the ADS-B device, much information such as flight number, start and destination point, estimated time of arrival, and aircraft model, which are published on the websites of airline companies, can be easily obtained without requiring field expertise [9]. Therefore, studies on the security of the ADS-B device have been increasing rapidly in recent years, and the scope of possible attack scenarios has expanded. ADS-B data, which the attacker can capture, and the flight information shared by the airline companies are shown in Table 5 [9].

TABLE 5. The information that attackers can obtain.

ADS-B Data	Open Data
Call Sign	Flight Number
ICAO number	Company
Country	Origin Airport
Location	Destination Airport
Altitude	Estimated Arrival Time
Direction	Airplane Model
Speed	Number of the seats
Climbing Speed	Engine Models

B. POSSIBLE ATTACK SCENARIOS

Within the scope of this section, attack scenarios that can mislead the ADS-B device are summarized for ground and air systems. Possible attack scenarios are shown in Fig. 5.

The Fig. 5 shows that the attacks on air systems are examined in two groups: active and passive [4]. In passive attacks, the attacker collects data without interfering with the system; In active attacks, the attacker intervenes in the system with different methods, such as adding/removing messages. Passive attacks are mainly aimed at collecting data about the

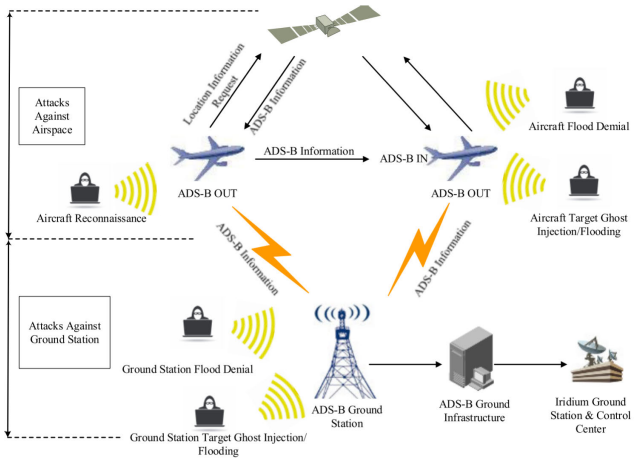

FIGURE 5. Possible attack scenarios [4].

system and analyzing it. Since there is no direct intervention in the system, it does not pose an instant danger. However, in active attacks, since the attacker can change the location information, a non-existent aircraft may appear in the system and cause a false alarm, thus threatening the safety of the flight. ADS-B attacks could have potentially catastrophic consequences [10]. Six basic attack scenarios are defined within the scope of studies in the literature. These scenarios are briefly summarized in Table 6.

C. THE PROPOSED SECURITY SOLUTIONS FOR ADS-B

Considering the possible attacks against the ADS-B system, various security solutions have been proposed to ensure the security of the systems. These solutions are examined under two main categories: secure location verification and secure broadcast verification in the study by Jun et al. [4].

1) Secure broadcast authentication methods are divided into two parts: the methods that use cryptogtaphic methods and those that do not. Cryptographic methods are among the most effective protection methods that ensure the network's security in wireless networks. Therefore, it is also considered in the security of the ADS-B network. Since, ADS-B device has broadcast nature, it is not required to encryption. Providing identification and source integrity are enough solution for ADS-B security [12], [13], [14], [15]. However, these methods have disadvantages, such as key distribution and management problems. Methods that do not use cryptographic methods are examined under the headings of fingerprint technology and spread spectrum technology. These methods, unlike encrypted methods, do not have key distribution and management problems; but they require adding new hardware components to the aircraft.
2) Secure location verification methods, unlike secure broadcast verification, verify the authenticity of the aircraft's position by cross-checking it with the location information of other participants.

The definitions of security solutions examined under these two headings are shared in Table 7.

In the literature, using anomaly detection methods is one of the effective methods for ADS-B system security. Compared with other methods, ML and DL can effectively detect and identify attack data for ADS-B systems. Since these methods do not require any modification of the existing protocol, they can be used in future practical applications on avionics cyber security.

D. THE ALGORITHMS USED IN ANOMALY/INTRUSION DETECTION SYSTEMS

This section shares basic definitions of some machine learning and deep learning algorithms frequently used in anomaly detection systems in Table 8.

According to [30], most suitable method for abnormal data detection on ADS-B device is neural networks with a recurrent architecture due to the temporal evolution of the ADS-B data. The LSTM architecture and its variants suit for the considered problem.

On the other hand, hyper-parameters are another critical factor affecting the models' performance rates. The choice of hyper-parameters depends on the specific algorithm and problem. These are used to control the models' training process and optimize model results. While machine learning/deep learning models learn parameters, hyper-parameters are external configurations for models that cannot be learned from the training data. Common hyper-parameters for machine learning/deep learning models are given below:

1) **Learning Rate (for optimization algorithms):** This parameter affects the model's learning speed by controlling the step size during optimization.
2) **The Number of Hidden Layers and Neurons (for neural networks):** It determines the neural network's architecture.
3) **Activation Function (for neural networks):** Different activation functions, such as ReLU or sigmoid, can be chosen for each layer in a neural network.
4) **Regularization Parameters (e.g., L1 or L2 regularization):** These parameters are used to prevent overfitting by controlling the amount of regularization applied.
5) **Number of Trees (for ensemble methods like Random Forest):** The number of decision trees to be used in a model.
6) **Depth of Trees (for tree-based models):** The depth of decision trees in algorithms like Decision Trees or Random Forest.
7) **Kernel Type and Parameters (for Support Vector Machines):** It refers to the kernel type of SVMs (linear, polynomial, radial basis function) and associated parameters.
8) **Batch Size and Number of Epochs (for training deep learning models):** Batch size refers to the number of training examples utilized in one iteration, and epochs refer to the number of times the entire training dataset.

TABLE 6. Attack types and definitions [11].

Attack Types	Method	Complexity	Vulnerabilities	Definition
Aircraft Reconnaissance	Eavesdropping	Low	Lack of encryption Improper design/specification	The attacker collects and analyzes publicly published flight data.
Ghost Aircraft Injection	Message Injection	Low	Lack of authentication Lack of encryption Improper design/specification	The attacker aims to misinform the air or ground system by injecting a non-existent (ghost) aircraft to the ADS-B communication channel.
Ghost Aircraft Flooding/ Ground Station Flooding	Message Injection	Low	Lack of authentication Lack of encryption Improper design/specification	The attacker aims to perform a denial of service attack on the target system by injecting multiple non-existent aircraft to the air system or the ground system ADS-B communication channel.
Virtual Trajectory Modification	Message Modification	Medium	Lack of authentication Lack of encryption Improper design/specification No Guarantees on Senders No Guarantees on Receiver	The attacker aims to modify or delete the ADS-B message and send a new modified one to the ADS-B communication channel.
Aircraft Disappearance	Message Deletion	Low	Lack of authentication Lack of encryption No Guarantees on Senders No Guarantees on Receiver Improper design/specification	The attacker aims to interrupt the transmission of data about the target aircraft by deleting all messages from the ADS-B communication channel.
Aircraft Spoofing	Message Modification	Low	Lack of authentication Lack of encryption Improper design/specification No Guarantees on Senders No Guarantees on Receiver	The attacker aims to modify the ADS-B message and send a new modified one to the ADS-B communication channel.

TABLE 7. Security solutions for ADS-B system.

Approach	Attack Type	Definition
Secure Broadcast Authentication	Fingerprint	This method is implemented in three ways: software, hardware, and channel-based. Software-based classification is difficult, as most airlines use similar structures. There may be signal distortions in hardware-based. In channel-based, it is classified according to the characteristics of the channel.
	Spread Spectrum	A random transition between channels and a randomly determined spreading code is used.
	Public Key Cryptography	In communication, the parties do not need to share the key. However, the main challenge of public key cryptography is solving the scalability and cost of public key infrastructure (PKI) for digital signatures [4].
	TESLA	TESLA (Timed Efficient Stream Loss-tolerant Authentication) is a broadcast authentication protocol which is based on loose time synchronization between the sender and the receivers. In addition, TESLA has low communication and computation costs [16].
	MAC	The MAC value is added to the standard ADS-B message to provide authentication.
Secure Location Verification	Multilateration	The system determines the aircraft's position by calculating the difference between the signal arrival times of the position information received from different (at least three) ground stations.
	Distance Bounding	Attacks can be detected according to the distance between the two aircraft and the transmission time of the data.
	Kalman Filtering	Attacks are detected using an algorithm that uses the linear system state equation to best predict the system's state and observe the system input-output.
	Group Verification	The accuracy of the incoming data is checked by comparing the data from more than one source, such as aircraft and ground stations within the range of the ADS-B device.
	Data Fusion	Different methods, such as probabilistic modeling and analysis, machine learning, and fuzzy logic, are used to combine data from different sources by considering their relationship [4].
	Traffic Modelling	By using the inverse ratio between the received signal strength and the distance, the actual position information of the aircraft can be accessed. In addition, historical position information can be checked by combining the signal arrival angle and strength. Machine learning and deep learning algorithms are used to detect abnormal behaviour of aircraft.

9) **K in k-Nearest Neighbors (k-NN):** k refers to the number of neighbors in k-NN.
10) **Distance Metrics (for k-NN):** The distance metric refers to the distance between data points.

These hyper-parameters need to be tuned carefully to achieve optimal model performance. Some techniques, such as grid search and random search, are often used to search through the hyper-parameter space.

E. EVALUATION METRICS

While evaluating machine learning and deep learning-based models, different evaluation metrics are used; different components are considered when evaluating intrusion detection systems. An intrusion detection system is considered in terms of effectiveness, efficiency, adaptability, robustness, and convenience. An efficient system can identify the attacker and the real user accurately. The computational complexity

TABLE 8. Algorithms and definitions.

Algorithm	Definition
Logistic Regression (LR) [17]	It is defined as a supervised machine learning algorithm that is frequently used in the classification of categorical or numerical data. The result is measured with a binary variable.
Decision Tree (DT) [18]	It is a supervised machine learning algorithm in which data is continuously divided according to a certain parameter. The tree can be described by two entities: decision nodes and leaves. Leaves represent decisions or final results, while decision nodes show where the data is split.
Random Forest (RF) [19]	It is one of the supervised classification algorithms that give good results even without hyperparameter estimation. It is used in both regression and classification problems. Random forest algorithm is defined as the process of choosing the highest score among many decision trees that work independently of each other. The main difference between the decision tree algorithm and the RF algorithm is that the process of finding the root node and splitting the nodes is random.
Gradient Boosting (GB) [19]	Boosting is defined as gradually transforming weak learners into strong learners with iterations. The main difference of this algorithm is how the deficiency of weak learners is defined. It can be used in regression and classification problems. In the GB, the first leaf is initially formed, and then new trees are formed by considering the estimation errors. This situation continues until the number of trees is decided or no further improvements can be made to the model [20].
eXtreme Gradient Boosting [21]	It is defined as the high-performance version of the GB algorithm optimized with various arrangements. The most important features of the algorithm are that it can achieve high predictive power, prevent over-learning, manage empty data, and do it quickly. It is shown as the best of the decision tree-based algorithms.
Support Vector Machine (SVM) [22]	It is a supervised machine-learning algorithm that can be used for classification or regression problems. The basic idea on which SVM is based is to find a hyperplane in the feature space that can optimally separate the two classes.
One Class Support Vector Machines (OC-SVM) [23]	In the one-class SVM algorithm, the data is first moved to the feature space using an appropriate kernel function and separated from the origin using a hyperplane. These hyperplane parameters are obtained by solving a quadratic problem similar to normal SVM.
Artificial Neural Network (ANN) [24]	It is defined as structures formed by connecting artificial nerve cells. Artificial neural networks are examined in three main layers; the input layer, the hidden layers, and the output layer. Information is transmitted to the network from the input layer, processed in the hidden layer, and sent to the output layer. In the hidden layer, the information is converted into output by using the weight values of the network.
Multilayer Perceptron (MP) [25]	The Perceptron Model is an artificial neural network model and it is a supervised learning algorithm. The most crucial factor in the Perceptron Model is determining the threshold value.
Recurrent Neural Networks (RNN) [20]	It is defined as a class of artificial neural networks in which the connections between nodes form a directed loop. This allows the algorithm to exhibit dynamic temporal behavior.
Convolutional Neural Network (CNN) [26]	It is a sub-branch of deep learning and is generally used to analyze visual information. Typical uses include image and video recognition, suggestive systems, image classification, medical image analysis, and natural language processing.
Long Short-Term Memory (LSTM) [27]	The long-short-term memory model is known as a repetitive RNN. LSTM is widely used in sequential or time series problems because it can learn long-term dependencies with its memory transitive mechanism.
Hidden Markov Model (HMM) [28]	In the modeling phase, some properties are kept hidden to extract the rules between the hidden states. However, it is difficult to quantify hidden states without sufficient system knowledge. The hierarchical Dirichlet Process (HDP) can be integrated to dynamically estimate the number of hidden states. sHDP-HMM is used to analyze and predict time series data.
Auto Encoder (AE) [29]	Autoencoder consists of two stages: coding and decoding. A single-layer autoencoder is a type of neural network with one hidden layer. Models are usually trained by backpropagation in an unsupervised manner. The optimization problem of the model aims to minimize the distance between the reconstructed results and the original inputs.

of the methods used in intrusion detection affects the system's efficiency. Attacks change and evolve. Therefore, the intrusion detection system must also be adaptive and detect changes. While the intrusion detection performance of the system represents the system's robustness, its usability for the user also shows its ease. A well-defined and viable intrusion detection system should be evaluated with these features in mind.

In the intrusion detection system, model evaluation metrics were used to evaluate the models. While evaluating the models, values such as the model's accuracy and error rates are calculated. These rates are used to compare models. Considering that some evaluation metrics are inversely proportional to each other, the usage area of the system determines which metric is more important. In this section, performance metrics that are frequently used in the literature are shared in detail.

Confusion Matrix: Matrices are used to evaluate the success of classification models. The matrix are represented with four values: True Negative/TN, True Positive/TP, False Negative/FN, and False Positive/FP.

- **True Negative/TN:** It represents the number of correctly classified negative samples.

- **True Positive/TP:** It represents the number of correctly classified positive samples.
- **False Negative/FN:** It refers to the number of incorrectly classified positive samples; in other words, the number of samples classified as negative while actually being positive.
- **False Positive/FP:** It refers to the number of negative samples that were misclassified; in other words, it refers to the number of samples that were classified as positive while they were actually negative.

Accuracy - ACC: It is obtained by dividing the correct answers by the total number of samples, as in (1). It is one of the most commonly used evaluation metrics.

$$ACC \equiv \frac{TN + TP}{TN + TP + FP + FN} \tag{1}$$

False Acceptance Rate - FAR: It represents the ratio of the number of misclassified negative samples to the total number of negative samples, as in (2). As the FAR value decreases, the performance rate of the system increases. In order to reduce this rate, the acceptance threshold value defined in the system should be increased.

$$FAR \equiv \frac{FP}{FP + TN} \tag{2}$$

False Rejection Rate - FRR: It represents the ratio of the number of misclassified positive samples to the total number of positive samples, calculated as in (3). As the FRR value decreases, the performance rate of the system increases. In order to reduce this rate, the acceptance threshold value defined in the system should be reduced.

$$FRR \equiv \frac{FN}{TP + FN} \tag{3}$$

Equal Error Rate - ERR: It is seen that there is an inverse relationship between FAR and FRR ratios. When comparing models, the ERR metric is used when the relationship between two ratios is desired to be defined with a single value. The ERR value represents the lowest point where the FAR and FRR values are equal.

Recall: It represents the ratio of correctly classified positive samples to the total positive samples, calculated as in (4). The higher the Recall value the higher the system's performance.

$$Recall \equiv \frac{TP}{TP + FN} \tag{4}$$

Precision: It represents the ratio of correctly classified positive samples to positively classified samples, calculated as in (5). The higher the precision value, the higher the system's performance.

$$Precision \equiv \frac{TP}{TP + FP} \tag{5}$$

F-Score: F-Score is used to compare two different models with low precision and high recall or high precision and low recall, calculated as in (6).

$$F-Score \equiv 2\frac{Precision \cdot Recall}{Precision + Recall} \tag{6}$$

ROC Curve: It is a probability curve with the FAR ratio on the X-axis and the FRR ratio on the Y-axis. It is frequently used in the comparison of models consisting of different classes. The area under this curve is called AUC-ROC and is considered a critical constraint in determining the model's performance.

F. SYSTEM ARCHITECTURE

Within the scope of this survey, anomaly-based intrusion detection systems used in the security of the ADS-B device were examined. Model development steps in these systems are presented in Fig. 6.

The review of the architecture presented in Fig. 6 is described below:

1) First, the ADS-B message is collected from the open library of websites such as Flightradar24 [31] and OpenSky [32], which are generally preferred in the literature. In addition to these, a test environment was created in some studies for model training. In both of these methods, a dataset consisting of only real flight data is obtained. Since the attack data is also needed in the model training, the attack dataset is produced by simulating the determined attack scenarios. Real flight and attack data are combined and used in testing and training stages of the models.
2) In the preprocessing step, ADS-B messages are extracted from raw data. Then, data is sorted according to the unique identifier, which is the ICAO number. In this way, different flights are separated from each other. Next, data records with missing records are cleaned or filled (by using mean values, linear interpolation or other methods). Finally, the dataset is normalized to compare features with different dimensions and measurements.
3) In the feature extraction step, many different features were used in the studies. In addition to ADS-B message content such as location and altitude, there are also studies focusing on hardware (energy statistic), software features, or signal features (pseudo range, doppler shift, bit error rate, bad packet ratio). Representative features for each flight: average path of a route and extract major geolocation points for each source and destination like takeoff, the first point of cruising, the last point of cruising, landing.
4) In the other areas, the dataset includes anomalies besides normal data. However, it is known that ADS-B messages do not include any anomaly (attack data). Therefore, after the feature extraction phase, attack data are generated, labeled, and merged with real ADS-B messages to produce the final dataset.
5) Finally, in the model training and testing phases, various machine learning and deep learning methods were used, and the success rates of the models were shared. In some studies, they prefer to use window during the training phase due to the time-dependent nature of ADS-B messages.

IV. BRIEF SUMMARIES OF STUDIES

In this section, summaries of the studies were defined, and comparisons were made. When the studies in the literature are examined in detail, it is seen that two different basic feature sets are emphasized in the ADS-B data. The most frequently used feature set consists of features related to the route information of the aircraft, such as altitude, speed, and direction. These features establish a relationship between the aircraft and the route. If the aircraft deviates from the route, this move is called an anomaly. Another feature is focused on the unique properties of electromagnetic waves emitted by ADS-B. It is known that these properties depend on different factors, such as the stability of the oscillator, phase noise, and transmitter clock. For this reason, it is stated that there are differences between manufacturers, and aircraft can be classified using these differences [33]. Electromagnetic features containing more specific information than route information were extracted and used as RF fingerprints, and aircraft were classified according to these features. In order to determine whether the aircraft are real or fake, a database that identifies unique aircraft with ICAO numbers must be created [33].

In [33], the authors stated that more than 50% of the observed planes have a specific phase order. International Civil Aviation Organization (ICAO) standards allow manufacturers to develop devices with system parameters within specific ranges. Considering the limits and parameters of these standards, the authors proposed a seven-step algorithm for pattern extraction. In the classification phase of this study, a neural network with 45 input layers, 10 hidden layers and 7 output layers was used. A neural network with 5 output layers was also tried, but it was observed that the structure with 7 output layers gave better results [33]. Another perspective is to focus on features such as error rate, bad packet ratio, and energy statistic to distinguish received jamming signals from legitimate ones, as presented in [34]. In this study, comprehensive research has been conducted emphasizing the effectiveness of machine learning-based classifiers for detecting jamming attacks. Various supervised machine learning algorithms such as support vector machine, k-nearest neighbor, artificial neural network, and decision tree are used, and their performances are compared. Within the scope of this study, different SVM types were compared, and among these methods, it was shown that the radial basis function RBF had the best performance with 67.3%. For the KNN algorithm, three different distance metrics, namely Euclid, Chebyshev, and Mahalanobis, were focused. Mahalanobis distance metric has been shown to provide the best performance with a rate of 74.6% compared to other distance metrics. Three different performance metrics were considered in the decision tree algorithm, namely accuracy, detection probability, and false alarm probability. Among all methods, the best performance was obtained by the two hidden layers neural network with accuracy, detection probability, and false alarm probability of 81%, 90.3%, and 30.9%, respectively. The lowest performance belongs to logistic regression, with an accuracy of 65.5%. However, all these techniques have a high false alarm probability exceeding 24%. Therefore, it is not suitable for use in real scenarios. In [35], the authors collected the signal data obtained from the ACARS system besides the ADS-B signals and created a large dataset. The authors used the amplitude and instantaneous phase of the raw data in systems such as ADS-B and ACARS to construct deep learning models such as CNN, RNN, and LSTM. In this study, it is stated that it outperforms methods such as SVM and logistic regression in areas such as converting signal data to images and classification using image processing. The dataset size of radio signal classification-based deep learning studies is quite limited. Therefore, a test environment is set up to create the dataset, which includes an antenna, RF receiver and sampling module, storage system, computing system, and data exchange network. According to the study's results, the signal classification accuracy of ACARS and ADS-B is 98.1% and 96.3%, respectively. When the signal-to-noise ratio exceeds 9 dB, the classification accuracy is more than 92%. The results of the transfer learning experiment show that the model trained on large-scale ADS-B datasets is more suitable for learning and training new tasks than the model trained on a small-scale dataset.

In [36], the authors focused on the features of Radio Frequency (RF) to fingerprint the system. Aircraft were identified with the extracted signatures, and an intrusion detection algorithm was developed. The system was evaluated within the scope of different attack scenarios, and the attack situation imitating the real user was also tested.The authors concluded that they presented a system with a high detection rate and a low false alarm rate. In this study, different from other literature studies, two user scenarios were considered for attack situations. First, the scenario where the part in the in-flight navigation system is replaced with a different part; the second is a scenario where an incorrect message is added to the channel by an unauthorized transmitter. Both of these attack scenarios can be detected by extracting the fingerprint of the transmitter. Some features, such as clock stability and hardware and software components, are used randomly during the production phase of the hardware. By using these features, a pattern can be extracted for the transmitter. In addition to these features, signatures based on RF signal characteristics can also be extracted. By creating an aircraft database based on these features, it can be checked whether the signature and the aircraft match. Within the scope of this study, 45 million messages from 2942 aircraft were collected over eight days in 2018. These data were obtained with the hardware infrastructure created. Since the ADS-B data contains rows related to each other, a frame size was determined, and the details of the stage of determining this frame size were shared in the study. Then, the KNN algorithm was evaluated using different frames and k values. In the best value, the frame size is 1000, and the k value is 60 with a 75% accuracy rate and a 10^{-3} false alarm rate. It is stated that the proposed method within the scope of the study has

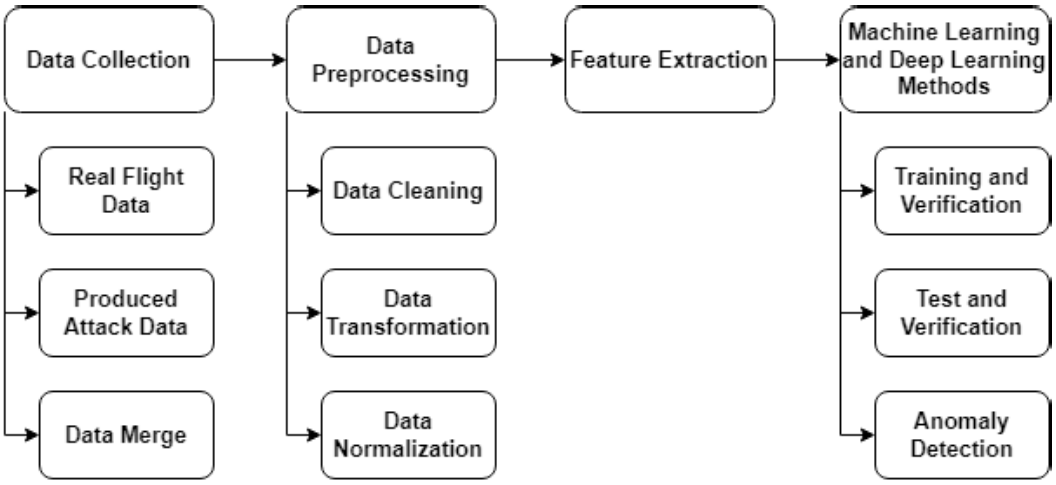

FIGURE 6. Anomaly based intrusion detection system for ADS-B security.

the features of detecting signature changes and adapting to different situations. The authors claim that even a small amount of change can be detected. But if the attacker creates a self-representing dataset without being detected, the system adapts the model according to the new data, and then the probability of the system noticing the attacker drops to zero. In addition to these studies, the study numbered [37], which focuses on GPS data with similar features to ADS-B data in the literature, is also included. The authors propose a supervised machine learning method based on an artificial neural network to detect GPS spoofing signals. Different features such as pseudo-range, doppler shift, and signal-to-noise ratio (SNR) are used to perform the classification of GPS signals. A supervised machine learning method based on artificial neural networks (NN) is proposed, in which real or fake GPS signals are fed directly into the algorithm, and the existence or absence of an attack is decided. The authors stated that this method does not require any modifications to the GPS infrastructure and can be easily applied to any GPS-guided autonomous system using microcontrollers or microcomputers. In this study, GPS data was focused, and spoofing attacks were tried to be detected with an approach similar to the ADS-B system. Therefore, it is seen that the extracted features, such as satellite vehicle number (SVN), signal-to-noise ratio (SNR), pseudo-range (PR), doppler shift (DO), and carrier phase shift (CP), are different from the ADS-B system. This study has similarities with the ADS-B system in terms of approach and is included in the review study to compare the methods used. The authors calculated accuracy rates for all combinations of five attributes to reveal the relationship between different features. As a result, it was seen that the option using all attributes had the highest accuracy rate of 98.3%. The dataset used in this study has not been shared.

In route-based anomaly detection systems, Habler et al. used an LSTM encoder-decoder algorithm to model flight routes by analyzing ADS-B message strings, and they aimed to detect aircraft deviations from the flight path [38]. The LSTM algorithm was used for the first time in the literature on ADS-B data. This study used 13 different datasets containing flight information for a selected route. While defining the flight route with these data, four main geographical location points are extracted: take off (start of route), the first point of cruise behavior, the end point of cruise behavior, and landing (end of route). This data includes standard flight data only. For this reason, different types of anomalies/attacks were produced for the dataset and added to the training/test datasets in order to be able to classify them. Afterwards, five common anomaly/attack detection algorithms, namely GMM-HMM, DBSTREAM, One Class SVM, LOF, and Isolation Forest, were applied to this dataset, and the results of the algorithms were compared. In the study, it was stated that the established models could detect produced anomalies/attacks with an average false alarm rate of 4.5%. Among the algorithms used, it has been shown that the LSTM encoder-decoder algorithm has the best performance. Moreover, in 2022, the authors presented a new study on a Stack LSTM encoder-decoder architecture harnessed for trajectory anomaly detection within the aviation domain, utilizing data from the OpenSky network [39]. The analysis spans six datasets and evaluates anomalous behavior under three attacker capabilities. The model uses self-features, such as callsign, heading, velocity, speed, and regional features, including distances measured from the center of the examined area. Furthermore, the research introduces a new approach by employing separate models for each phase of flight - climb, cruise, and descent. In addition, they use a new feature derived from AIRAC Instrumental Flight Rule (IFR) route charts that reflect real-world aviation scenarios. This multifaceted investigation aims to enhance the robustness of trajectory anomaly detection in air traffic surveillance, diversifying the data with attacker scenarios and operational phases. Since LSTM is a common algorithm used to detect anomalies in time series, Chevlot et al. focus on an LSTM contextual autoencoder (CAE) for trajectory anomaly detection using data from the OpenSky

network [11]. Various features such as altitude, consecutive delta, tracking delta, vertical rate, ground speed, and flight phases (climb, cruise, descent) are analyzed in this study. The study evaluates the model's performance using metrics including accuracy, recall, and F1 score, considering six different datasets. By leveraging LSTM-based contextual autoencoding on the OpenSky dataset, the research aims to enhance the efficacy of anomaly detection in multivariate time series associated with aircraft trajectories. Another LSTM-based study was presented by Wang et al. [40]. In this study, the authors analyzed ADS-B data and attacks against the system and proposed an LSTM-based ADS-B spoofing attack detection method. Different threshold values have been determined for the detection of anomalies/attacks. There are ten different types of attack scenarios in the dataset, containing 220000 data. The features used are the longitude, latitude, altitude, speed, heading, and rate of climb of the aircraft. An LSTM architecture has been established with 14 LSTM units and 7 fully connected layer units, which are also the vector size of ADS-B data. In the evaluation phase of the models presented in the study, different evaluation metrics such as precision, recall, and F1-score are used to evaluate the model more accurately. The proposed model has a precision of 0.85 for 10 different attack types. In this study, attack-based accuracy rates and details of attacks are not shared. In addition, the false-correct ratio, an essential factor for evaluating the models, is not given. A similar study focusing on these attack scenarios was presented by Teng Yao et al. In this study, the authors proposed a system based on the Hidden Markov Model (HMM) where temporal correlations are effectively modeled for ADS-B data to detect different attack patterns [41]. With the Sticky hierarchical Dirichlet Process (sHDP), the parameters of the HMM are obtained dynamically. The system can detect attacks dynamically. The established intrusion detection model consists of three basic steps: data preprocessing, sHDP-HMM, and intrusion detection. The data used in this study were obtained from the OpenSky database. In addition to normal data, six different attacks, namely fixed deviation attack, random deviation attack, incremental deviation attack, flight change attack, replay attack, and DoS attack, were modeled, and these attack data were produced. The database produced in the study was not shared. This study shares the accuracy rates of LSTM, HTM, and sHDP-HMM models for different attack types on the dataset. It is seen that LSTM has the highest accuracy in fixed deviation, flight change, and DoS attacks, HTM in random deviation and incremental deviation attacks, and sHDP-HMM in random deviation and incremental deviation attacks. The accuracy rates of the sHDP-HMM model are 90.8% (continuous deviation attack), 99.3% (random deviation attack), 87.9% (incremental deviation attack), 99.6% (flight change attack), 94.8% (replay attack) is given as 98.8% (DoS attack). There are also studies in which multi-layered filtering mechanisms exist in route-based studies. For example, in [42], a system called SODA, which is a DNN-based two-stage leak detector, was developed. In the first step, the message classifier examines each incoming message and labels them malicious or non-malicious. For those accepted as non-malicious, the ICAO address is estimated based on the physical layer properties. It is checked whether the specified ICAO address and the ICAO address obtained as a result of the classification match. In this way, precautions are taken against replay attacks. According to the shared results, while the SODA system has a minimal false alarm rate (0.43%) in the first stage, it can detect ground-based spoofing attacks with a probability of 99.34%. The second stage classifies a total of 238 aircraft with an accuracy rate of 96.66%. The authors state that the DNN-based method outperforms other machine learning techniques such as XGBoost, Logistic Regression, and Support Vector Machine. Instead of a malicious attack, Xavier et al. focused on anomalies that occur during the flight that a person did not design and their causes [43]. This study uses an automatic encoder-based neural network for anomaly detection on ADS-B data obtained via OpenSky. The proposed method determines air traffic flows using clustering techniques and facilitates the analysis of routes. In this study, three different datasets were used, namely city pair, airspace, and landing. The city pair dataset comprises 3536 route information of 28 ICAO numbers between two cities. The Airspace dataset contains 14461 route information obtained over seven months from aircraft cruising in the designated airspace. While the DBSCAN algorithm is used for classifying routes, automatic encoders are used for anomaly detection. The Landing dataset collected data consisting of 19489 route information that landed at a specific airport. It has been determined that most of the anomalies in these datasets are caused by the weather or the movement tactics of the ATCs. The methods used in this study are based on unsupervised learning methods, automatic encoders, and clustering algorithms. Another study using autoencoder on ADS-B data was presented by Fried et al. [44]. This study proposed a neural network model with two different architectures, an LSTM with extracted time series features and a non-repetitive autoencoder, for anomaly detection, and ADS-B data obtained from Opensky was used. While evaluating the models, FPR, TPR, AUC, and Average Detection Delay evaluation metrics were used. In the proposed method, abstract flight models are learned whose numerical and spatial values are derived from the delay difference (time series difference) in ADS-B messages. Therefore, it differs technically from previously presented studies. The authors stated that the presented model could be trained on data from more than one flight path and generalized to make inferences about routes not included in training set, such as past flight paths. As a result, the autoencoder has a higher TPR and lower detection latency over all simulated attacks; LSTM has a higher ROC AUC and a lower FPR over all simulated attacks. Unlike other studies, in [45], the authors focused on the system's ability to detect attacks by processing real-time data. A dataset was created by combining 10.000 real ADS-B messages obtained over

Opensky with 10.000 generated attack ADS-B messages. The SVM classification algorithm was used in training and testing stages, and as a result, 80% precision, 78% recall, and 79% F1-score values were obtained. The system takes 0.36 seconds for the server to preprocess the messages, 11802.38 seconds to adapt the model, and 0.36 seconds to apply the model for a prediction. The authors stated that they could process approximately 27 ADS-B messages per millisecond for intrusion detection. Considering that approximately 13 messages are generated every millisecond in the US National Airspace, It is evident that the system has real-time intrusion detection capability. In this way, appropriate measures will be taken quickly against detected attacks, and flight safety will increase.

Both approaches have some advantages and disadvantages. Aircraft classification is directly related to the route in systems that focus on route information. Therefore, a model containing the data of a previous flight in the aircraft class specified on the relevant route should be established. Although the models need to be constantly updated as flight routes may change over time, it is easy to obtain this data because the route data is published openly. Therefore, data can be collected without establishing an infrastructure for different routes, and a model can be established using the collected data. However, finding a dataset in systems that focus on the properties of electromagnetic waves is challenging. Apart from the digital data, it is necessary to know the signal information. To obtain such data, setting up a testbed is required. Since this testbed contains limited aircraft, the dataset remains small. The main goal in such studies is that all ADS-B out device manufacturers should determine the RF characteristics that define that device at the time of production, and this should be stored in a common data set and used as the identity of the relevant aircraft. In order to use this approach, aircraft equipment, software and hardware should not be changed or updated too frequently. Any change will cause a breakdown in the pattern and will require updating the database. It is foreseen that it can be used as an additional feature in attack/anomaly detection in systems where such problems do not exist [33].

V. RESULTS

In this study, using machine learning and deep learning methods to detect anomalies in ADS-B data are examined in detail. According to result of the study ML/DL models have several advantages and disadvantages. Pointing out these points are important for future studies and research [46], [47]. Advantages of using ML/DL models as a security solution for ADS-B system are given below:

1) **Automation and Scalability:** While detecting anomalies, manual inspection, and giving rapid response in real-time applications is impossible because of the amount of data, ML/DL models can automatically analyze vast amounts of ADS-B data efficiently.
2) **Adaptability:** ML/DL models can adapt to evolving threats and changing patterns in ADS-B data. They can learn from new data and adjust their detection criteria without requiring manual reprogramming. This continuous learning improves the long-term effectiveness of intrusion detection.
3) **Pattern Recognition:** Rule-based detection systems cannot detect complex patterns and anomalies. However, ML/DL models can recognize these patterns thanks to their evolving structures.
4) **Data Types:** ML/DL methods can work with diverse data types, like spatial, temporal, and multimodal data.
5) **Advanced Features:** ML/DL models can show spatial relationships, temporal trends, and complex relationships between data points.
6) **Anomaly Detection Diversity:** There are various ML/DL-based techniques for anomaly detection, including supervised, unsupervised, and reinforcement learning. This diversity allows the most appropriate method to be selected for specific use cases.
7) **Threat Detection:** ML/DL can help detect a wide range of threats, including signal spoofing, jamming, eavesdropping, and other malicious activities.

The benefits of using ML/DL for ADS-B anomaly detection make them a promising tool for improving aviation cyber security.

RQ1: Which algorithms are commonly used to detect anomalies in ADS-B data? When the studies in the literature are examined, it has been observed that algorithms such as LSTM, SVM, and ANN are frequently used in attack/anomaly detection for ADS-B, as seen in Table 11. In Section III-D, general definitions of algorithms commonly used in this area are shared.

Hyper-parameters play a crucial role defining a model result. Therefore, the best hyper-parameters of these studies are given in Table 12.

RQ2: Which ADS-B databases are used to train models?

Today, with the widespread use of the ADS-B device, it has become easier to capture flight data. ADS-B device broadcasts data openly without using any crypto mechanism. Therefore, any person with an ADS-B In device can easily obtain this data.

In the literature studies, it has been observed that there are two different basic approaches to the database. Both approaches have their advantages and disadvantages.

In the first of these approaches, a system that can capture this data is implemented at an affordable cost due to the widespread use and ease of obtaining Software-Defined Radios. It means that real-time data can be drawn directly from the system. In addition, in test environments with an ADS-B Out device, attack data can be implemented by producing and broadcasting directly from the ADS-B Out device, not by changing the real data. However, in such studies, data collected with a single device is limited to the device's coverage area. The location of the device directly affects the data that can be collected. The datasets obtained from the test environment established in the literature need

TABLE 9. Summaries of studies.

The Main Idea	Advantages	Disadvantages
[33] Some features, such as the stability of the oscillator, phase noise, and transmitter clock, which define ADS-B devices according to their hardware structures, have been used as RF fingerprints, and aircraft are divided into different classes according to these features. Later, an anomaly detection system was developed using these data.	- Additional parameters are defined for the ADS-B spatial data. - A signature database has been created for aircraft.	- A database that identifies aircraft with unique ICAO numbers needs to be established. - In order to use this approach, aircraft equipment, software and hardware should not be changed or updated too frequently. - Memory space is required for the database.
[38] It is aimed at using an LSTM encoder-decoder algorithm to analyze the ADS-B message sequences to detect the aircraft's deviation from the flight path and to model the flight paths.	- Different ML and DL algorithms are compared on the same dataset. - Since 13 different datasets were used, the performance rates of the algorithms could be observed in other datasets. - The authors also compared their proposed method with online and offline anomaly detection algorithms.	- The study's results cannot be verified because the dataset was not shared. - This study only detects anomalies on a particular aircraft's trajectory. Therefore, a different model is required for each aircraft trajectory.
[37] It proposes a supervised machine learning method based on an artificial neural network to detect GPS fraud signals. It focused on GPS data and tried to detect spoofing attacks with an approach similar to the ADS-B system. It contains similarities with the ADS-B system.	- Satellite vehicle number (SVN), signal-to-noise ratio (SNR), pseudo-range (PR), doppler shift (DO), and carrier phase shift (CP) parameters were used to establish a model from the signals.	- It does not directly map to ADS-B. - The study's results cannot be verified because the dataset was not shared.
[34] It presents a comprehensive study highlighting the effectiveness of machine learning-based classifiers for detecting jamming attacks.	- Different machine learning algorithms have been tried for jamming attacks in the ADS-B data. - Different types of SVM algorithms were compared, and the best method for the problem was analyzed. - Jamming attacks can be detected more easily than other types of attacks.	- The authors gave only the accuracy rate without a false positive rate of models. - The authors show that the network provides better accuracy as the number of hidden neurons increases. However, the computational cost also increases.
[35] Signal data obtained from both ADS-B and ACARS systems was collected, and a large dataset was created. It is aimed to classify ADS-B and ACARS data with deep learning models such as CNN, RNN, and LSTM.	- The accuracy rates of the models are high.	- The study's results cannot be verified because the dataset was not shared. - It has not different evaluation metrics shared except for accuracy.
[42] It is aimed to develop a DNN-based two-stage system to be used in anomaly detection for ADS-B data.	- An aircraft database has been created considering the physical layer features against replay attacks. - The false alarm rate is very low in the initial elimination using the aircraft database. - An attack dataset was generated by using normal data.	- The aircraft database needs to be updated. - Memory space is required for the database.
[36] To detect the difference between the real message and the message added to the system by the attacker, a fingerprint-based intrusion detection system has been proposed, and an intrusion detection algorithm has been developed.	- Different attack scenarios have been tested. - An aircraft database based on its hardware features has been created. - It has a false alarm rate of 0.003.	- The highest accuracy rate provided is 75%. - The aircraft database needs to be updated. - Memory space is required for the database.
[41] It aims to effectively model temporal relations for ADS-B data to detect different attack models.	- The results of different deep learning methods for various attack scenarios are compared. - An attack dataset was generated by using normal data.	- In the method presented in this study, the model can train offline and detect the attack behaviors online. The online training process reduces model accuracy. - The authors gave only the accuracy rate without a false positive rate of models.
[40] It is aimed to develop a detection method for ADS-B spoofing attacks.	- Ten different attack scenarios are discussed. - Different evaluation metrics were used in the evaluation of the models.	- The study's results cannot be verified because the dataset was not accessed. - The dataset volume is limited. - The attack dataset simulates only one phase of flight.
[43] The focus is on attacks or anomalies that may occur in ADS-B data, aiming to detect these deviations with automatic encoders.	- Three different dataset were used, and weather data were also taken into account.	- The study's results cannot be verified because the dataset was not shared. - This study only detects anomalies on a particular aircraft trajectory. Therefore, a different model is required for each aircraft's trajectory.
[44] It is aimed at detecting possible attacks on ADS-B data with automatic encoders. The authors evaluated two autoencoder architectures: recurrent (LSTM) and non-recurrent with time-series characteristics.	- During the model evaluation phase, four different evaluation metrics were used. - The authors show that their method enables the detection of anomalous trajectories for flights that do not have enough historical data to learn.	- The study's results cannot be verified because the dataset was not shared. - The dataset was collected during the cruising phase of the flight. Therefore, the effectiveness of the method needs to be tested at different phases.

to be shared, and sufficient information needs to be provided about the dataset. Since it is not shared, it creates a question mark about the success rates of the proposed systems.

Another approach is to collect open source data shared on websites like OpenSky Network [32] or FlightRadar24 [31]. In these sites, the movement in the airspace at any point can

TABLE 10. Summaries of studies (Continued).

The Main Idea	Advantages	Disadvantages
[45] It is focused on the system's ability to process ADS-B messages in real-time and detect possible attacks.	- The technical details required for real-time data processing are shared.	- The study's results cannot be verified because the dataset was not shared.
[11] This study focused on trajectory anomalies. It aims to develop a detection method for ADS-B spoofing attacks using the LSTM Contextual Autoencoder for 15 routes. The authors used six datasets; five included attack types, and the other included only standard data. Models give low FPR; therefore, they claim that training models for specific regions are unnecessary.	- The technical details required for real-time data processing are shared. - Codes and datasets that are created in the study are shared in Github.	- All attack types are analyzed separately. - The aircraft database needs to be updated. Because of the data size, it is not possible online.
[39] This study utilizes a stacked-LSTM encoder-decoder model to detect anomalies in flight routes. Airspace is separated into three phases: climb, cruise, and descent, and each phase has its own model. They use the Aeronautical Information Regulation and Control (AIRAC) en-route chart in the separation process. In addition, attackers are classified according to knowledge and ability level.	- The authors proposed a new approach to detect anomalies. Three different models are used for the anomaly detection phase of one route.	- The study's results cannot be verified because the dataset was not shared.

TABLE 11. Dataset and methods used in literature.

Number	Year	Method	Dataset
[33]	2017	ANN	- The data was obtained from the established test environment. - The dataset is not shared.
[38]	2018	LSTM, GMM-HMM, DB-STREAM, OC-SVM, LOF and IF	- Obtained from Flightradar24 database.
[37]	2019	ANN	- Details about the dataset have not been shared.
[34]	2019	SVM, ANN, KNN, LR, DT	- ADS-B data is simulated. - Details about the dataset have not been shared.
[35]	2019	SVM, LR, CNN, RNN, LSTM	- The data was obtained from the established test environment. - The dataset is not shared.
[42]	2019	DNN, XGBoost, LR, SVM	- The data was obtained from the established test environment. - The dataset is not shared.
[36]	2020	KNN	- The data was obtained from the established test environment. - The dataset is not shared.
[41]	2020	LSTM, sHDP-HMM	- Obtained from Opensky database.
[40]	2020	LSTM	- The link given in the study does not work.
[43]	2020	DBSCAN, AE	- Obtained from Opensky database.
[44]	2021	LSTM	- Obtained from Opensky database.
[45]	2021	SVM	- Obtained from Opensky database.
[11]	2022	LSTM CAE	- Obtained from Opensky database.
[39]	2022	Stack LSTM	- Obtained from Opensky database and AIRAC enroute charts.

be easily followed live. In addition, these sites both share data in real-time and provide access to historical databases. OpenSky Network especially provides support for academic studies in this area. Therefore, the majority of studies using open databases prefer OpenSky Network.

In 4 of the 14 studies examined within the scope of this review, a hardware test environment was established, and the data were obtained from this test environment. 8 studies' data were drawn from open databases, 6 of which were OpenSky Network and one of which was FlightRadar24. In the remaining 2, no information about the dataset was shared. Table 11 shares information about studies and preferred datasets.

RQ3: Which features are helpful for training models?

Two different feature sets were used while training machine learning models on ADS-B messages.

1) In the first approach, ADS-B message content and data that can be obtained from open sources were collected, and messages were classified using this data. ADS-B message content includes "time, ICAO24, latitude, longitude, baroaltitude, geoaltitude, heading, velocity, vertrate, callsign, on ground, alert, spi, squawk,

TABLE 12. Hyper-parameters.

Number	Year	Method	Hyper-parameters
[33]	2017	ANN	**Input:** 45 **Hidden Layer:** 10 **Output:** 5
[38]	2018	-	-
[37]	2019	ANN	**Hidden Layer:** 1, 2 **Number of Neurons:** [1, 25] **Activation Function:** tanh **Number of Folds, k:** 10 **Number of Iteration:** 200
[34]	2019	ANN	**Hidden Layer:** 2 **Number of Neurons:** 15 **DT:** 10 splits **SVM:** RBF Kernel **kNN:** 1 neighbors, Mahalanolois
[35]	2019	CNN	**Number of Blocks:** 9 **Number of Inception Modules:** 3 **Activation Function:** ReLU **Hidden Layer:** 2 **Number of Neurons:** 15
[42]	2019	DNN	**Hidden Layer:** 2 **Input Layer:** Number of Features **Output Layer:** Number of Classes **Weight Initialization:** Xavier Normal **Weight Regularizer:** L2 **Activation Function:** ReLU **Output Activation Function:** Softmax **Cost Function:** Cross entropy **Optimizer:** Adam **Epoch:** 50 **Batch Size:** 32
[36]	2020	KNN	**Window Size, M:** 1000 **Number of Folds, k:** 60
[41]	2020	sHDP-HMM	**Window Size:** 9 Other hyper-parameters are not shared.
[40]	2020	LSTM	**Loss Function:** Mean Square Error Other hyper-parameters are not shared.
[43]	2020	LSTM AE	**Window Size:** 59 **Hidden Layer:** 10
[44]	2021	LSTM AE	**Input Layer:** 150 **Output Layer:** 150 **Hidden Layer:** 64 **Activation Function:** Sigmoid **Loss Function:** Mean Square Error
[45]	2021	-	-
[11]	2022	LSTM CAE	**Window Size:** 30 **Batch Size:** 256 **Number of Units:** 32
[39]	2022	Stack LSTM AE	**Outer Layer:** 64 **Inner Layer:** 32 **Optimization:** Adam **Dropout Rate:** 0.3 **Activation Function:** ReLU

TABLE 13. Performance evaluation metrics.

Number	Year	Method	Metrics
[33]	2017	ANN	P_D: 75.6 % P_{FA}: 3.8 %
[38]	2018	GMM-HMM	P_{FA}: 4.5 % **Recall:** 98 %
[37]	2019	ANN	**Accuracy:** 98.3 % P_D: 99.2 % P_{FA}: 2.6 %
[34]	2019	ANN	**Accuracy:** 81 % P_D: 90.3 % P_{FA}: 30.9 %
[35]	2019	CNN - Transfer Learning	**Accuracy:** 96.3 %
[42]	2019	DNN	**Accuracy:** 96.6 % **Precision:** 96.6 % **Recall:** 96.6 % **F-Score:** 96.6 % P_D: 99.3 % P_{FA}: 0.43 %
[36]	2020	KNN	P_D: 75 % P_{FA}: 0.1 %
[41]	2020	sHDP-HMM	**Accuracy:** 99.3 %
[40]	2020	LSTM	**Precision:** 91.3 % **Recall:** 89 % **F-Score:** 89.3 %
[43]	2020	LSTM AE	**FPR:** 44.6 % **Recall:** 61.5 %
[44]	2021	LSTM AE	-
[45]	2021	SVM	**Precision:** 80.2 % **Recall:** 78.2 % **F-Score:** 79.2 %
[11]	2022	LSTM CAE	**Accuracy:** 85.7 % **Recall:** 54.9 % **F-Score:** 73.8 % **FPR:** 1.0 %
[39]	2022	Stack LSTM AE	**Recall:** 95 % P_D: 99.3% **FNR:** 5% **FPR:** 0.4 %

lastposupdate, lastcontact'' parameters. In addition to these parameters, additional features such as ''airline company to which the aircraft belongs, departure and arrival times, departure airport, landing airport, aircraft model'' can be obtained. ADS-B message content was generally used in the articles examined within the scope of this study. In the message content, especially ''time, ICAO24, latitude, longitude, baroaltitude, geoaltitude, heading, velocity'' parameters were taken into consideration.

2) In the second approach, attack/anomaly detection is made by considering the signal properties of the message. Satellite Vehicle Number (SVN), Signal-to-Noise Ratio (SNR), Pseudo-Range (PR), Doppler Shift (DO), and Carrier Phase Shift (CP) parameters were extracted to model the signals, and these values were used for attack/anomaly detection.

The first approach is route-based and has a high success rate in attack scenarios focusing on route changes. In this

TABLE 14. The features of the security solutions [4].

Method	Provide Security Against	Features	Applicability	Security
PKI	Eavesdropping, Message Adding/Deleting	Data and Location Integrity, Confidentiality Authentication	Hard	High
MAC	Message Adding/Deleting	Authentication	Easy	Low
TESLA	Message Adding/Deleting	Authentication	Medium	Medium
Multilateration	Message Adding/Deleting	Location Integrity	Easy	Low
Fingerprint	Message Adding/Deleting, DOS Attack	Authentication, Availability	Medium	Medium
Spread Spectrum	Eavesdropping, Jamming, DOS Attack	Confidentiality, Availability	Hard	High
Distance Bounding	Message Adding/Deleting	Location Integrity	Hard	Low
Kalman Filtering	Message Adding/Deleting	Data and Location Integrity, Authentication	Easy	Medium
Data Fusion	Message Adding/Deleting, DOS Attack	Location Integrity, Authentication, Availability	Easy	Medium
Traffic Modelling	Message Adding/Deleting	Location Integrity	Medium	Low

approach, there is no difference between attacks from the ground and a vehicle in the air. On the other hand, in the signal-based attack/anomaly detection approach, there are differences between attacks from the ground system and real aircraft in the air. The characteristics of the hardware used by the attacker gain importance in detecting this attack. It is difficult to detect fake message attacks transmitted over real aircraft. Finding a shared open dataset to train signal-based models is hard; therefore, the authors must produce their datasets. However, open datasets that share real ADS-B messages are readily available for route-based attacks.

RQ4: What are common metrics used to evaluate models in the anomaly detection system of ADS-B?

The metrics used to evaluate machine learning and deep learning methods are examined in Section III-E. This section explains the meanings and equations of evaluation metrics. Only accuracy, false positive, and false negative values have been shared in the studies. In addition to these metrics, values such as recall, precision, and F1-score can be used for the model's performance. Evaluating models with different evaluation metrics reveals the proposed approaches' performances and the models' distinctive aspects.

The Table 13 provides a detailed results of machine learning models, highlighting their performance evaluation metrics.

RQ5: For which vulnerabilities of ADS-B can the proposed security solutions be effective?

Many security solutions have been proposed with different requirements in different areas for the security of ADS-B messages. This study examines anomaly/attack detection system-based solutions in detail. These solutions focused on anomalies during flight, landing, takeoff, or route anomalies between two points. These solutions provide security for attacks such as ghost aircraft injection, ghost aircraft flood, ground station flood, virtual trajectory modification, and aircraft disappearance from the radar. Adding, removing, and changing messages can be detected at a high rate by the anomaly/attack detection system. However, it does not provide a measure against eavesdropping attacks. This attack can only be prevented by methods such as encryption of the channel. Such methods are not preferred because they increase costs and require protocol and system change.

The features of the security solutions other than the anomaly detection systems presented in the literature, the security level they provide, their applicability, and the attacks they prevent are shared in detail in Table 14.

VI. LIMITATIONS

While this literature review provides the current state of research on ML and DL-based anomaly detection methods for ADS-B systems, several limitations should be acknowledged. While this paper only includes studies published in English, non-English language publications may not have been adequately represented. Despite efforts to search relevant databases and sources comprehensively, some relevant studies may have been inadvertently excluded from this review. Additionally, while studies don't share their databases, the results of the studies couldn't be verified. The applicability of the findings from the included studies to real-world ADS-B systems may be limited by contextual factors such as airspace regulations, traffic density, weather conditions, and technological infrastructure. Despite these limitations, this literature review presents comprehensive research on ML and DL-based anomaly detection methods for ADS-B systems. It provides valuable insights into challenges and opportunities for future research.

VII. CONCLUSION AND OPEN PROBLEMS

This systematic literature review examines studies that detect attacks against the ADS-B system with anomaly/attack-based

detection systems. Machine learning and deep learning model datasets and model evaluation metrics used in these studies were investigated. Examined studies were obtained from Scopus, IEEE Xplore, and WoS academic databases with query sentences in Table 2. 15 studies obtained from the queries were selected according to the selection and elimination criteria in Table 3. This study includes the technical infrastructure of the ADS-B system, possible attack scenarios against the system, and the measures that can be taken against these scenarios. Then, algorithms and evaluation metrics used in anomaly/attack detection systems are explained. Then, after filtering within the selection and elimination criteria, 15 studies obtained from academic databases were examined in detail and summarized. The main idea, advantages, and disadvantages of these studies are shared in Table 9 and 10. Then, machine learning, deep learning methods, and datasets used within the scope of the studies are shared in Table 11. As a result, this study examines anomaly/attack detection systems for ADS-B systems and shares information about approaches consisting of machine learning and deep learning models.

According to the paper's results, it is clear that machine learning and deep learning-based ADS-B anomaly detection systems can significantly enhance aviation safety by identifying potential threats. Optimizing ML/DL models for efficient use of computational resources can reduce operational costs associated with anomaly detection in ADS-B systems. With these improvements, the real-world deployment of anomaly detection systems will increase the reliability of ADS-B messages. Considering the increasing number of UAVs, robust anomaly detection systems are essential for ensuring the safety and reliability of autonomous aircraft and UAV operations. Additionally, ML/DL-based anomaly detection systems can provide valuable insights into air traffic patterns for air traffic controllers. While ML/DL methods offer numerous advantages, it's essential to acknowledge some shortcomings and challenges of these methods. The open problems of ML/DL-based anomaly detection methods are listed below:

1) **Data Quality and Quantity:** ML/DL models often require large amounts of labeled data in the training phase. However, obtaining qualified labeled data for anomalies or intrusions can be challenging for avionic systems. Moreover, collecting a sufficiently diverse dataset is hard since real-world anomaly or intrusion events are relatively rare.
2) **Imbalanced Datasets:** Anomalies in ADS-B data are infrequent compared to normal data. Because of the imbalance class, model performance is biased. Specialized techniques like oversampling, undersampling, or generating synthetic data may be necessary to address this issue.
3) **Interpretability:** ML/DL models, particularly deep neural networks, are often considered ''black boxes.'' Understanding the model's behavior in the classification phase can be challenging. Therefore, the trust and acceptance of these models in critical applications like aviation security are complex.
4) **Computational Resources:** Using ML/DL models to detect anomalies requires considerable computational resources in the training and test phases. Due to latency and power consumption constraints, implementing ML/DL models on ADS-B devices is considered in detail.
5) **Real-time Processing:** Real-time data processing is crucial in aviation security. Developing ML/DL models suitable for real-time data processing restriction is challenging.
6) **Regulatory and Certification Issues:** The aviation industry is regulated, and using of new security solutions must meet certification standards.
7) **Cost and Resource Constraints:** ML/DL-based solutions can be costly for smaller aviation operators and organizations in terms of computational resources and expertise required for deployment and maintenance.
8) **Adversarial Attacks:** ML/DL models used for intrusion detection are vulnerable to adversarial attacks. Attacker can craft malicious data specifically designed to evade detection, leading to potential security breaches. He intentionally manipulates input data to generate incorrect predictions. These attacks are tailored to specific models and datasets, making them difficult to detect and defend against and they leads to false positives or false negatives in anomaly detection. Developing robust models that can withstand such attacks is an ongoing challenge [48].
9) **False Positive Rate:** It is critical to the usability of ML/DL models, as the results affect flight-critical decision-making mechanisms. In addition, the selected features directly affect the model results. Therefore, reducing the false positive rate and feature selection methods are significant for future research.

The real-world deployment of ADS-B anomaly detection systems faces significant challenges, particularly concerning the vulnerability of data sources like sensors or the Opensky Network to potential attacks, which could undermine the system's ability to detect anomalies accurately.

1) Trajectory fluctuations, resulting from weather conditions or congestion, pose a practical challenge for the system, given that trajectories, typically linear for the same route, may deviate under certain circumstances. A thorough evaluation is imperative to practically utilize anomaly detection systems for intrusion detection, accounting for diverse factors influencing trajectory variations.
2) Determining effective thresholds is a real-world challenge, especially in dealing with unknown attack patterns, necessitating the development of automatic adaptation capabilities to address emerging threats.
3) Periodical changes in aircraft signatures, often caused by using different or redundant transponders and two ADS-B antennas in different positions on an aircraft,

further complicate the practicality of anomaly detection systems. Detecting slow changes in aircraft signatures becomes challenging in such scenarios.

4) The sheer volume of yearly ADS-B data, estimated at 41 TiB based on FAA statistics [45], presents a practical concern, demanding scalable solutions for efficient processing and analysis in real-world applications of ADS-B anomaly detection systems.

As a result, while ML/DL based anomaly detection methods promise for enhancing the security of ADS-B devices, it is important to recognize and address these shortcomings and challenges. While this approach may not offer a definitive solution to the problem, it will increase the difficulty for attackers. Future research and development efforts aim to mitigate these issues and improve the effectiveness and robustness of intrusion detection systems in the context of aviation security. Future research in ADS-B anomaly detection systems involves comparing model results after tuning hyper-parameters and incorporating additional features.

1) Data quality and quantity are two of the critical problems in anomaly detection systems for ADS-B. Research should focus on developing techniques for augmenting labeled anomaly data, such as active learning and transfer learning. While ADS-B datasets are imbalanced, future research can focus on robust anomaly detection algorithms for class imbalance.
2) Researchers should develop efficient training algorithms and optimization techniques that minimize computational complexity and memory requirements without sacrificing detection accuracy. They investigate lightweight ML/DL architectures optimized for resource-constrained environments, such as edge devices or embedded systems.
3) Feature extraction and data processing are crucial steps for the performance of models. Including contextual features, such as the type of aircraft and sensors used, in ADS-B data for anomaly detection models will be investigated. The models can be trained for airspace states in specific geolocations besides other features to provide more contextual information and improve detection ability. Moreover, postprocessing of IQ samples will be performed to extract more stable features, and training models for different flight phases may enhance overall accuracy. Domain-specific knowledge and contextual information minimize false positive rates are decreased.
4) Minimizing data preprocessing time and feature extraction processes is crucial for the real-time application of ADS-B anomaly detection systems.
5) Addressing the demand for more effective mechanisms to dynamically optimize thresholds and overcome human factors and the limitations of static values will be crucial. Further optimization for hyper-parameters and time series feature extraction is expected to enhance empirical results, and expand the training phase to include different aircraft types, such as UAVs and rocket-powered vehicles, is proposed.
6) A reliability score is suggested as an additional enhancement for ADS-B anomaly detection systems. Additionally, it can be focused on using clustering techniques to identify aircraft with similar features and detect ADS-B attacks from different clusters (random noise, velocity attack, etc.), ultimately improving the robustness of the model.

REFERENCES

[1] *Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service—Final Rule*, Federal Aviation Admin., Washington, DC, USA, 2010.
[2] SESAR Joint Undertaking and Federal Aviation Administration, *Nextgen—Sesar State of Harmonisation Report 3 Edition*, Publications Office Eur. Union, Luxembourg, 2018.
[3] N. Çevik and S. Akleylek, "Cybersecurity and defense: Cyber security in aviation systems," in *Cyber Security and Defence*, vol. 6, Ş. Sağroğlu and S. Akleylek, Eds. Nobel Academic Publishing Education Consultancy, 2022. [Online]. Available: https://dergipark.org.tr/en/pub/ijiss/page/13335
[4] Z. Wu, T. Shang, and A. Guo, "Security issues in automatic dependent surveillance—Broadcast (ADS-B): A survey," *IEEE Access*, vol. 8, pp. 122147–122167, 2020.
[5] F. Alrefaei, A. Alzahrani, H. Song, and S. Alrefaei, "A survey on the jamming and spoofing attacks on the unmanned aerial vehicle networks," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Jun. 2022, pp. 1–7.
[6] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1066–1087, 2nd Quart., 2015.
[7] T. Kacem, D. Wijesekera, P. Costa, and A. Barreto, "An ADS-B intrusion detection system," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 544–551.
[8] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ADS-B research," in *Proc. IEEE Aerosp. Conf.*, Oct. 2006, p. 7.
[9] R. Bitton, C. Feher, Y. Elovici, A. Shabtai, G. Shugol, R. Tikochinski, and S. Kur, "A proxy-based solution for securiting remote desktop connections in mission-critical systems," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, Jan. 2017, pp. 153–156.
[10] C. Clay, M. Khan, and B. Bajracharya, "A look into the vulnerabilities of automatic dependent surveillance-broadcast," in *Proc. IEEE 13th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Mar. 2023, pp. 0933–0938.
[11] A. Chevrot, A. Vernotte, and B. Legeard, "CAE: Contextual auto-encoder for multivariate time-series anomaly detection in air transportation," *Comput. Secur.*, vol. 116, May 2022, Art. no. 102652.
[12] A. Braeken, "Holistic air protection scheme of ADS-B communication," *IEEE Access*, vol. 7, pp. 65251–65262, 2019.
[13] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, "A practical and compatible cryptographic solution to ADS-B security," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3322–3334, Apr. 2019.
[14] J. Baek, Y. Byon, E. Hableel, and M. Al-Qutayri, "Making air traffic surveillance more reliable: A new authentication framework for automatic dependent surveillance-broadcast (ADS-B) based on online/offline identity-based signature," *Secur. Commun. Netw.*, vol. 8, no. 5, pp. 740–750, Mar. 2015.
[15] J. Baek, Y. J. Byon, E. Hableel, and M. Al-Qutayri, "An authentication framework for automatic dependent surveillance-broadcast based on online/offline identity-based signature," in *Proc. 8th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput. (PGCIC)*, 2013, pp. 358–363.
[16] A. Perrig and J. D. Tygar, *TESLA Broadcast Authentication*. Boston, MA, USA: Springer, 2003, pp. 29–53.
[17] D. Hosmer and S. Lemeshow, *Introduction to the Logistic Regression Model*. Wiley, 2000, ch. 1, pp. 1–30.
[18] L. Breiman, J. Friedman, C. J. Stone, and R. A. Olshen, *Classification and Regression Trees*. New York, NY, USA: Wadsworth International Group, 1984.
[19] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, pp. 5–32, Oct. 2001.

[20] F. A. Gers, J. Schmidhuber, and F. Cummins, "Learning to forget: Continual prediction with LSTM," *Neural Comput.*, vol. 12, no. 10, pp. 2451–2471, Oct. 2000.
[21] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2016, pp. 785–794.
[22] C. J. C. Burges, "A tutorial on support vector machines for pattern recognition," *Data Mining Knowl. Discovery*, vol. 2, no. 2, pp. 121–167, Jun. 1998.
[23] K.-L. Li, H.-K. Huang, S.-F. Tian, and W. Xu, "Improving one-class SVM for anomaly detection," in *Proc. Int. Conf. Mach. Learn. Cybern.*, 2003, pp. 3077–3081.
[24] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.
[25] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," *Nature*, vol. 323, no. 6088, pp. 533–536, Oct. 1986.
[26] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.
[27] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997.
[28] L. R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proc. IEEE*, vol. 77, no. 2, pp. 257–286, Feb. 1989.
[29] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *Science*, vol. 313, no. 5786, pp. 504–507, Jul. 2006.
[30] J. Yi, L. Lin, L. Nisi, and W. Jintao, "ADS-B anomaly detection algorithm based on LSTM-ED and SVDD," in *Proc. 10th Chin. Soc. Aeronaut. Astronaut. Youth Forum*. Singapore: Springer, 2023, pp. 245–257.
[31] Flightradar24. (2006). *Flightradar24: Live Flight Tracker—Real-Time Flight Tracker Map*. [Online]. Available: https://www.flightradar24.com/22.2,-28.61/4
[32] OpenSky Network. (2015). *The OpenSky Network—Free ADS-B and Mode S Data*. [Online]. Available: https://opensky-network.org/
[33] M. Leonardi, L. Di Gregorio, and D. Di Fausto, "Air traffic security: Aircraft classification using ADS-B message's phase-pattern," *Aerospace*, vol. 4, no. 4, p. 51, Oct. 2017.
[34] M. R. Manesh, M. S. Velashani, E. Ghribi, and N. Kaabouch, "Performance comparison of machine learning algorithms in detecting jamming attacks on ADS-B devices," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, May 2019, pp. 200–206.
[35] S. Chen, S. Zheng, L. Yang, and X. Yang, "Deep learning for large-scale real-world ACARS and ADS-B radio signal classification," *IEEE Access*, vol. 7, pp. 89256–89264, 2019.
[36] M. Leonardi and F. Gerardi, "Aircraft mode S transponder fingerprinting for intrusion detection," *Aerospace*, vol. 7, no. 3, p. 30, Mar. 2020.
[37] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS spoofing attacks on unmanned aerial systems," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Oct. 2019, pp. 1–6.
[38] E. Habler and A. Shabtai, "Using LSTM encoder–decoder algorithm for detecting anomalous ADS-B messages," *Comput. Secur.*, vol. 78, pp. 155–173, Sep. 2018.
[39] E. Habler and A. Shabtai, "Analyzing sequences of airspace states to detect anomalous traffic conditions," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 3, pp. 1843–1857, Jun. 2022.
[40] J. Wang, Y. Zou, and J. Ding, "ADS-B spoofing attack detection method based on LSTM," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, pp. 1–12, Dec. 2020.
[41] T. Li, B. Wang, F. Shang, J. Tian, and K. Cao, "Dynamic temporal ADS-B data attack detection based on sHDP-HMM," *Comput. Secur.*, vol. 93, Jun. 2020, Art. no. 101789.
[42] X. Ying, J. Mazer, G. Bernieri, M. Conti, L. Bushnell, and R. Poovendran, "Detecting ADS-B spoofing attacks using deep neural networks," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 187–195.
[43] X. Olive and L. Basora, "Detection and identification of significant events in historical aircraft trajectory data," *Transp. Res. C, Emerg. Technol.*, vol. 119, Oct. 2020, Art. no. 102737.
[44] A. Fried and M. Last, "Facing airborne attacks on ADS-B data with autoencoders," *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102405.
[45] D. M. Mink, J. McDonald, S. Bagui, W. B. Glisson, J. Shropshire, R. Benton, and S. Russ, "Near-real-time IDS for the US FAA's NextGen ADS-B," *Big Data Cognit. Comput.*, vol. 5, no. 2, p. 27, Jun. 2021.
[46] F. Hoxha and A. Y. Zomaya, "A survey of machine learning for big data processing," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 32, no. 3, pp. 2865–2877, 2020.
[47] D. Kožovic, D. Durdevic, M. Dinulovic, S. Milic, and B. Rasuo, "Air traffic modernization and control: ADS-B system implementation update 2022: A review," *FME Trans.*, vol. 51, no. 1, pp. 117–130, 2023.
[48] J. Lei, R. Jiang, and Z. Wu, "Malicious ADS-B data generation based on improved GAN," in *Proc. IEEE 9th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), IEEE Int. Conf. Perform. Smart Comput. (IEEE HPSC), IEEE Int. Conf. Intell. Data Secur. (IEEE IDS)*, May 2023, pp. 72–77.

NURŞAH ÇEVIK received the B.S. degree in computer engineering from Gazi University, Ankara, in 2015, and the M.S. degree in computer engineering from Ondokuz Mayıs University, Samsun, in 2018. From 2017 to 2019, she studied as a Project Researcher in national and international TÜBİTAK projects. From 2019 to 2021, she was a Research and Development Engineer with IBSS. Until 2022, she has been an Platform Security Engineer with HAVELSAN. Her research interests include post quantum secure cryptographic protocols, cyber threats for avionic systems, and security applications on avionic systems.

SEDAT AKLEYLEK received the B.Sc. degree in mathematics majored in computer science from Ege University, İzmir, Turkey, in 2004, and the M.Sc. and Ph.D. degrees in cryptography from Middle East Technical University, Ankara, Turkey, in 2008 and 2010, respectively. He was a Postdoctoral Researcher with the Cryptography and Computer Algebra Group, TU Darmstadt, Germany, from 2014 to 2015. He was a Professor with the Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey. He has been a Professor with the Department of Computer Engineering, Istinye University, İstanbul, Turkey. He has been with the Chair of Security and Theoretical Computer Science, University of Tartu, Tartu, Estonia, since 2022. His research interests include the areas of post-quantum cryptography, algorithms and complexity, architectures for computations in finite fields, applied cryptography for cyber security, malware analysis, the IoT security, and avionics cyber security. He is a member of the Editorial Board of IEEE Access, *Turkish Journal of Electrical Engineering and Computer Sciences*, *Peerj Computer Science*, and *International Journal of Information Security Science*.