MJEN

MANAS Journal of Engineering
ISSN 1694-7398 | e-ISSN 1694-7398

Volume 12, Issue 1, (2024) Pages 1-28
https://doi.org/10.51354/mjen.1197753

A Systematic Survey of Machine Learning and Deep Learning Models Used in Industrial Internet of Things Security

Ersin Enes Eryılmaz[1],*, Sedat Akleylek[2], Yankı Ertek[3], Erdal Kılıç[4]

[1] Department of Computational Science, Samsun, Türkiye, enes.eryilmaz@bil.omu.edu.tr, ORCID: 0000-0003-1163-970X

[2] Department of Computer Engineering, Samsun, Türkiye, sedat.akleylek@bil.omu.edu.tr, ORCID: 0000-0001-7005-6489

[3] Renaissance System and Technology Solutions, Ankara, Türkiye, yanki.ertek@ronesanssistem.com, ORCID: 0000-0001-7005-6489

[4] Department of Computer Engineering, Samsun, Türkiye, erdal.kilic@bil.omu.edu.tr, ORCID: 0000-0003-1585-0991

ABSTRACT

IIoT “Industrial Internet of Things” refers to a subset of Internet of Things technology designed for industrial processes and industrial environments. IIoT aims to make manufacturing facilities, energy systems, transportation networks, and other industrial systems smarter, more efficient and connected. IIoT aims to reduce costs, increase productivity, and support more sustainable operations by making industrial processes more efficient. In this context, the use of IIoT is increasing in production, energy, healthcare, transportation, and other sectors. IoT has become one of the fastest-growing and expanding areas in the history of information technology. Billions of devices communicate with the Internet of Things with almost no human intervention. IIoT consists of sophisticated analysis and processing structures that handle data generated by internet-connected machines. IIoT devices vary from sensors to complex industrial robots. Security measures such as patch management, access control, network monitoring, authentication, service isolation, encryption, unauthorized entry detection, and application security are implemented for IIoT networks and devices. However, these methods inherently contain security vulnerabilities. As deep learning (DL) and machine learning (ML) models have significantly advanced in recent years, they have also begun to be employed in advanced security methods for IoT systems. The primary objective of this systematic survey is to address research questions by discussing the advantages and disadvantages of DL and ML algorithms used in IoT security. The purpose and details of the models, dataset characteristics, performance measures, and approaches they are compared to are covered. In the final section, the shortcomings of the reviewed manuscripts are identified, and open issues in the literature are discussed.

ARTICLE INFO

Review article

Received: 01.11.2022
Accepted: 16.02.2024
Keywords:
industrial internet of things,
IIoT security,
deep learning,
machine learning,
Industry 4.0.

**Corresponding author*

1. Introduction

The internet environment is changing at an incredible speed. The internet is not just about smartphones or laptops; it has gone beyond internet-connected devices. Physical devices communicate with each other or large systems through the Internet of Things (IoT). Users can complete their work in a short time with devices connected with IoT. As the future of IoT looks so promising, it will be an integral part of every device, from home appliances to security devices.

While the number of IoT devices worldwide was 15.14 billion in 2023, it will reach 29.42 billion devices in 2030 and will increase 2.3 times [1] because it is cheaper and more accessible. Almost 75% of devices connected to the IoT network use short-range technologies such as Bluetooth, Zigbee, and Wi-Fi. These technologies will naturally be used by default as long as these networks exist. IoT revenues will exceed $1,5 trillion by 2030. China, North America, and Europe have 73% of IoT global revenue [2]. With the expansion of the IoT ecosystem, security concerns are also increasing. Considering the IoT architecture brings together multiple pieces of sensing and communication. Integrating devices is not only a complex task but also demonstrates that IoT networks and devices are a system that requires constant attention [3], [4].

IoT can be divided into three main groups. Consumer IoT can be considered end-user applications, smartphones, smart watches, wearable devices, and internet-connected home devices. Large infrastructures for enterprises are referred to as

Commercial IoT, while controllers, actuators, sensors, industrial assets, remote telemetry, monitoring, and management systems are classified as Industrial IoT. In this survey, Industrial IoT (IIoT) will be discussed [4]. The IIoT is a new, fully connected, efficient vertical model for intelligent systems and is vulnerable to cyber threats. Malicious actors can exploit some vulnerabilities and risks due to the misapplication of security standards [6].

Automation and intelligent computing services such as industrial systems, critical infrastructure devices, embedded devices, and modern systems have come together with production engineering thanks to the internet. However, standardization with IIoT brings many new challenges, including legal and social aspects of security, and privacy. In particular, the increasing diversity of IoT network and IoT device presence requires highly scalable solutions for data communication, naming, information management, addressing and service delivery. Many IoT devices still have limited capabilities that require low-cost, low-power, fully networked architectures compatible with standard communication methods [7].

It is a well-known fact that IoT is an ecosystem where data is transmitted and requires some privileged features to manage large amounts of data. At this point, ML and DL models collect and analyze data with artificial intelligence (AI). The security of devices can be ensured by making predictions with DL and ML models from the data produced by IoT ecosystems. Using the AI concept in security ensures a regular data flow between IoT devices and proper management without human error. Thus, AI has become necessary in the growth of the IoT industry.

The communication protocol used in wearable technologies and industrial applications Bluetooth low energy: BLE has been seen in many attacks where it is vulnerable to attacks. Since the packets transmitted with BLE consist of plain text content, it has been seen to contain security vulnerabilities in user authentication and reconnection of two paired devices [4], [5].

The increasing benefits of internet-connected devices have also brought challenges related to security issues. With the widespread use of IoT devices, security problems have also increased, and anomalies have occurred in IoT networks. Anomalies in the IoT network and systems are detected by intrusion detection systems. Work on IDS has been ongoing since Anderson's network security monitoring work [8]. Since Anderson's technical report, manuscripts have continued for different intrusion detection systems based on various methods [9]-[15]. There are different approaches for detecting anomalies in IoT networks with DL and ML models [16]-[19]. The ML and DL algorithms used to detect anomalies in IIoT security recognize malicious network traffic by comparing it to benign network traffic. In the papers, support vector machine [20], Bayes networks [21], decision trees [22], k-nearest neighbors [23], random forest [24], and k-means [25], machine learning algorithms are preferred. As deep learning algorithms generally convolutional neural networks [26], recurrent neural networks [27], long short-term memory [28], gated recurrent unit [20], [29], autoencoder [30], generative adversarial network [31], restricted Boltzmann machines [32] and deep belief networks [33] are used.

1.1. Related Surveys

In this subsection, current manuscripts compiling recently published or highly cited ML and DL-based models for IIoT security are reviewed. Some of these survey manuscripts used the systematic literature survey method, and some consisted of summarizing the papers. A systematic literature survey is the distinction and examination of papers prepared to answer research questions according to predetermined selection and elimination criteria related to a selected topic. Table 1 summarizes the characteristics of the reviewed surveys.

IIoT security research activity is geographically dispersed, the most popular broadcast locations, and fog computing for IIoT security threats [34]. IIoT security requirements refer to the geographical distribution of scientific publications, popular publication areas, and distribution over the years. In addition, the future of fog computing in the industrial field is discussed and proposed four-layer IIoT security architecture [35]. Firstly, security analysis includes MAC, ucode, IP, and EPC. Analysis of the network layer is also available in capillary networks (HomePlug, BLE, Bluetooth, RFID, NFC, IrDA, INSTEON, EnOcean, ANT+, WirelessHART, UWB, ZigBee, Thread, and ISA 110.11a, etc.). Secondly, their coverage and functionality ranges are mainnet in the background (3G, LR-WAN, Ethernet, WiMax, WLAN) and backbone network (DASH7, LoRaWAN, NB-Fi, NB-IoT, SigFox, NWAVE, and RPMA). At the processing layer, security analysis resides in end-to-end data protection. Finally, application layers work on HTTP, MQTT, CoAP, SOAP, XMPP, REST, DDS, and AMQP protocols [36]. Protocol-based and data-based attacks show that traditional IoT attack prevention tools are no longer effective. Artificial intelligence methods, blockchain, and elliptic curve encryption seem to be new effective methods for securing IoT networks [37]. IoT security threats and countermeasures, common points, and differences between IoT and IIoT are defined. A literature review of different security approaches specific to IIoT [38]. Blockchain, AI algorithms, consensus mechanisms, storage and communication perspectives on smart supply chains, and Industry 4.0 are explained [39]. A comprehensive analysis of attacks against IIoT systems and solutions to these attacks, as suggested in the latest literature, is presented [40]. DL and ML methods and blockchain integration for the IoT perception, network, and application layers are discussed [41]. Reviews various DL techniques and their uses in different industries, including CNN, AE, and RNN. DL use cases for intelligent IoT technologies are summarized [42]. A systematic literature review specifically addressing DL and ML algorithms commonly used in IoT network security is proposed, but does not focus on IIoT [43]. A systematic survey of how deep learning approaches detect IoT network and system security and large-scale attacks is studied [44]. An anomaly-based systematic survey with ML and DL together; however, the datasets are not exhaustive [45] and [46]. 40 manuscripts were summarized in databases such as Google Scholar, Academia, Science Direct, and IEEE with the keywords IoT, cyber security, cyber security frameworks, and cyber security approaches. No information is provided about ML and DL-based algorithms and the databases used [115]. ML and DL-based solutions for privacy threats in IoT systems were analyzed with dataset features without a systematic survey [116]. A detailed analysis of the IDS developed in the IoT environment was performed and a new smart IDS was proposed, which was tested on the NS3 simulator using fuzzy CNN by extracting features with information gain. This manuscript can be considered as a non-systematic detailed survey that includes experiments and analysis [117]. Many manuscripts have been summarized about ML or DL-based approaches to IoT security solutions [118]. Many manuscripts have been summarized about ML or DL-based approaches to IoT security solutions on between 2017 and 2022 [119]. One hundred five manuscripts were examined through different elimination and purification steps with the research questions' queries. The use of DL has been claimed to be a permanent and reasonable approach to IoT security. M. A. Al-Garadi et al. explained DL and ML methods with dataset details, but it is not a systematic survey [41]. R. Ahmad & I. Alsmadi gave a systematic review of manuscripts conducted in the years 2019-2020 specialized in IoT security, which explains the ML and DL methods with dataset detail and is not an IIoT-specific review. Our manuscript differs from other manuscripts in that it consists of systematically conducted manuscripts with detailed datasets where IIoT-specific ML and DL approaches were experimented on between 2019 and 2023 [43], [119].

Table 1. *Deep Learning and Machine Learning Based Survey Papers for IIOT Security*

Survey	Article Title	Journal Name	Year	Systematic survey?	ML and DL together?	Anomaly based?	Dataset detail?
[34]	Towards a systematic survey of industrial IoT security requirements: research method and quantitative analysis	ACM Digital Library Proceedings of the Workshop on Fog Computing and the IoT	2019	✓	X	✓	X
[35]	A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities	IEEE Communications Surveys & Tutorials	2020	✓	X	X	X
[36]	Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey	MDPI Sensors	2021	X	X	X	X
[37]	Security trends in Internet of Things: A survey	SpringerLink SN Applied Sciences	2021	X	X	X	X
[38]	Challenges and Opportunities in Securing the Industrial Internet of Things	IEEE Transactions on Industrial Informatics	2021	X	X	X	X
[39]	Deep reinforcement learning for blockchain in industrial IoT: A survey	ScienceDirect /Elsevier Computer Networks	2021	X	✓	X	X
[40]	Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures	MDPI IoT	2021	X	✓	X	X
[41]	A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security	IEEE Communications Surveys & Tutorials	2020	X	✓	✓	✓
[42]	Deep Learning in the Industrial Internet of Things: Potentials, Challenges, and Emerging Applications	IEEE Internet of Things Journal	2021	X	X	✓	X
[43]	Machine learning approaches to IoT security: A systematic literature review	ScienceDirect /Elsevier Internet of Things	2021	✓	✓	✓	✓
[44]	A systematic review on Deep Learning approaches for IoT security	ScienceDirect/ Elsevier Computer Science Review	2021	✓	X	✓	✓

[45]	A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity	MDPI Electronics	2022	✓	✓	✓	X
[46]	State-of-the-art survey of artificial intelligent techniques for IoT security	ScienceDirect/ Elsevier Computer Networks	2022	✓	✓	✓	X
[115]	Cybersecurity Risk Analysis in the IoT: A Systematic Review	MDPI Electronics	2023	✓	X	✓	X
[116]	A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things	MDPI Sensors	2023	X	✓	X	✓
[117]	A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things	Hindawi Computational Intelligence and Neuroscience	2023	X	X	✓	✓
[118]	Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions	SpringerLink Mobile Networks and Applications	2023	X	✓	X	X
[119]	Intelligent approaches toward intrusion detection systems for Industrial Internet of Things: A systematic comprehensive review	ScienceDirect/ Elsevier Journal of Network and Computer Applications	2023	✓	✓	✓	✓
Our paper	A Systematic Survey of Machine Learning and Deep Learning Models Used in Industrial Internet of Things Security	-	-	✓	✓	✓	✓

1.2. *Motivation, Scope and Contribution of Manuscript*

In this systematic literature survey, we focused on the schemes for anomaly-based attack detection in the IIoT network. This survey differs from the other survey manuscripts in Table 1 in that it is systematic, includes ML and DL models, is based on anomalies found in IIoT networks, includes details of the datasets used, and focuses on the framework of industrial internet of things. The general content and scope of this systematic review, which is prepared with the aim of providing detailed information to researchers working in the field of IIoT security, are as follows:

- The proposed schemes in the selected approaches are examined, and the information on these schemes is briefly summarized.
- Manuscripts that propose models developed to detect anomaly-based attacks in industrial IoT networks and reduce these attacks are systematically selected and eliminated according to specific criteria.
- It is stated which ML and DL models are used in the approaches.
- Manuscripts with performance metrics have been interpreted.
- Details of the datasets presented in the training and testing phases of the proposed models are given.
- The methods compared with the performance metrics reached by the setup of the models are shown.
- In the final section, the deficiencies of the examined manuscripts are outlined. Evaluation of what situations these deficiencies may lead to is presented.

The contributions of this survey are as follows:

- Research strategies with seven different academic databases were scanned.
- Article scans were made systematically.
- Survey articles and literature were searched.
- Frequently used abbreviations and metrics in the article and in the literature are explained in detail.
- Manuscripts with machine learning and deep learning models have been researched.
- The main idea, advantages, and disadvantages of the proposed models are explained.
- The benign and malignant numbers and features of the dataset used in the models were extracted.
- The usage purposes, tasks, and performance results of the models are given.
- The models against which the proposed schemes are compared, and open research problems are discussed.

1.3. *Organization*

In this systematic survey, to make the technical information outlined in the manuscript more understandable, IoT architecture, IIoT concept, vulnerabilities in IIoT devices, some attacks against IIoT devices, and ML and DL models are briefly explained in Section 2. Section 3 explains the research questions and objectives, search strategy, search process, and filtering criteria. The approaches taken in the selected manuscripts are summarized in Section 4. Section 5 answers the research questions that a systematic review should answer, summaries of the models, advantages, and disadvantages, and details of the datasets used. In Section 6, DL and ML models, datasets, and their properties are evaluated, an overview of the models is presented, and the deficiencies encountered in the manuscripts examined are emphasized. Finally, our manuscript briefly addresses general and open issues, offering a comprehensive overview of the broader challenges. Table 2 shows the abbreviations and expansions frequently used in this survey.

Table 2. *Abbreviations and Expansions*

Abbreviation	Expansion	Abbreviation	Expansion
IDS	Intrusion Detection System	MLP	Multilayer Perceptron
DT	Decision Tree	AI	Artificial Intelligence
NB	Naive Bayes	RNN	Recurrent Neural Network
AE	Autoencoder	DAE	Denoising Autoencoder
RBM	Restricted Boltzmann Machines	SAE	Stacked Autoencoder
KNN	K-Nearest Neighbors	RF	Random Forest
FDI	False Data Injection	GAN	Generative Adversarial Networks
DoS	Denial of Service	LSTM	Long Short-Term Memory
UDP	User Datagram Protocol	CART	Classification and Regression Tree
DBN	Deep Belief Network	LR	Linear Regression
BN	Bayesian Network	RT	Random Tree
DDoS	Distributed Denial of Service	SDN	Software Defined Networking
SVM	Support Vector Machine	ICMP	Internet Control Message Protocol
NN	Neural Networks	ANN	Artificial Neural Networks
MitM	Man-in-the-middle	TCP	Transmission Control Protocol
CNN	Convolutional Neural Networks	ROC	Receiver Operating Characteristic Curve
ACC	Accuracy	DR	Detection Rate
TN	True Negative	AUC	Area Under the ROC Curve
PRE	Precision	TRT	Training Time
TP	True Positive	TET	Testing Time
REC	Recall	F1	F1-Score
FP	False Positive	LL	Log Loss
SPC	Specificity	G-mean	Geometric mean
FN	False Negative	RI	Rand Index
TPR	True Positive Rate	SR	Speedup Ratio
SNS	Sensivity	ER	Encryption Time
FPR	False Positive Rate	IMF	Intrinsic Mode Function
FAR	False Alarm Rate	GCM	Gradient Compression Mechanism
FNR	False Negative Rate	CCQ	Clustering Center Quality
PoR	Proof of Reliance	KBL	Kernel Based Learning
PoW	Proof of Work	RTU	Remote Terminal Unit
FL	Federated Learning	PSO	Particle Swarm Optimization
SSO	Swallow Swarm Optimization	CFS	Cloud Service System
RS	Random Subspace	SHOCFS	Secure High-Order Clustering with Fast Search
CEEMDAN	Complete Ensemble Empirical Mode Decomposition with Adaptive Noise	IABC	Improved Artificial Bee Colony
SCADA	Supervisory Control and Data Acquisition	SHODS3O-CFS	Safe High-Order Optimum Density Selection in a Hybrid Cloud Environment
AB	Adaboost	GXGBoost	Genetic-Based Extreme Gradient Boosting
VIF	Variance Isolation Forest	MQTT	Message Queuing Telemetry Transport

2. Preliminaries

In this section, basic definitions and background are given. At the same time, deep learning and machine learning models are briefly explained.

2.1. IoT, IIoT and Attack Types

With IoT, using other machines to talk to other machines on behalf of humans, the concepts of ubiquity apply. In the age of IoT, where people communicate with objects and objects communicate with each other, there are connectivity dimensions for everything and everyone, anytime, anywhere. Objects have identities and virtual personalities in the internet of the future [47]. IoT is a network where physical devices can communicate via the internet. IoT is to be connected to various devices that make use of different communication models from human to human, human to machine, or a machine to machine [48].

In recent years, IoT has been used in automotive, energy, health, manufacturing, water, finance, etc. It has entered a wide range of industry sectors, including IIoT. With machine learning, the IIoT will advance the fourth industrial revolution. While IIoT facilitates data collection in an industrial environment, the collected data are used for training algorithms with the help of ML and especially DL.

The industrial use of IoT technologies has emerged with the concept of Industry 4.0. IoT networks consist of structures that monitor, analyze and change data without human intervention. SCADA systems also consist of several smart devices that monitor and control machines in industries for years [49]. IIoT standardization has emerged as a technology developed on SCADA with scalability, resolution, and data analytics. Using AI methods, IIoT can create new security measures from data collected from the cloud. [50].

IIoT is considered to be a subset of IoT. IoT typically encompasses retail and lifestyle consumer devices. IoT usually consists of single device structures such as smart television, smart phone, wearable devices, home automation, and display systems. IIoT technologies, on the other hand, are potent systems formed by the combination of more and advanced IoT devices such as smart factories, smart city, smart grids, innovative vehicles, robotics. While the plans for IoT are between 2-5 years, 30-year frameworks are considered for IIoT systems. The IoT is sensitive to water, dust, and power fluctuations and is highly mobile. IIoT is also suitable for operation in extreme situations, and its mobility is low. While the IoT prioritizes critical operations, IIoT systems have to synchronize in milliseconds. Since IIoT is built on smart logistics, smart cities, and smart manufacturing processes, it has to rely on broader security measures than IoT. At the same time, security solutions that apply to the IoT also apply to the IIoT. The confidentiality, integrity, and availability (CIA) triad is an elementary information security and includes security requirements and objectives. Solutions for Industry 4.0 should be evaluated within this framework [35]. IoT consists of less scope, while IIoT consists of systems that receive data from sensors, analyze it, and transfer it to the cloud [38].

2.1.1. IoT and IIoT Layers

IoT is a 3-layer structure: application, network, and perception layer [38]. The perception layer provides the outside world communication of IoT devices. It houses the actuators and sensors that generate data. At the perception layer, attacks such as physical attacks, impersonation, and DoS are carried out. Some manuscripts explain the perception layer as the physical layer and the network layer as the communication layer [44].

IoT devices are connected to the internet environment through the network layer. The network layer forms a bridge between the perception and application layers. IoT networks reach the internet with wired and wireless communication technologies at the network layer. At the network layer, attacks such as DoS, MitM, and routing attacks are carried out.

On the other hand, the application layer consists of the perception and network layer communication data and IoT applications. Therefore, it can be difficult to ensure security due to the possibility of software changes creating different bugs. As a result, application layer attacks like malicious code injection, data leakage, and denial of service (DoS) are carried out.

In the early stages of IoT-related research, three layers were introduced. It has three layers: perception, network and application layers. Three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for IoT research. New research describes more multilayered architectures. IoT has five layers, the middleware, and the business layers, as well as the IoT detection, network, perception and application layers [87]. Middleware is a system and software that uses data collected by the perception layer and runs primarily on servers serving the upper layers. These software and services are part of training a new computationally demanding machine learning model. Application and business layers provide software for the end user [86], [87]. Middleware and network layers are vulnerable to attacks such as MitM and DoS. In addition, attacks such as SQL injection, session hijacking, and buffer overflow occur at the business and application layers. Some manuscripts have named the layers differently. These are called perception, application, business, transport and preprocessing layers [114].

2.1.2. IIoT Attacks and Countermeasures

Because IIoT is a natural evolution of IoT, there are similar security challenges and specific security concerns to protect critical industrial control systems.

There are always security vulnerabilities for devices connected to the Internet. If security vulnerabilities are not detected and fixed, devices turn into zombie and robot devices. Without security solutions, IoT devices turn into a botnet. Large-scale attacks such as TCP timeouts and keeping HTTP connections open on web servers slowly consume the server's resources and ultimately cause it to stop responding to legitimate requests. Other large-scale volume-based attacks include SNMP, DDoS, TCP SYN packet, UDP flood, ICMP flood, slowdown, ping of death, zero-day attacks, known web server exploits, scrambling attack, OpenBSD, and amplification attack [51], [52]. The first purpose is to block IoT traffic and make it inaccessible to regular users.

There are two main attack techniques, anomaly, and signature-based. Signature-based attacks can be defined as exploitation or knowledge-based attacks, and anomaly-based attacks can be defined as behavior-based attacks [53]. Signature-based techniques rely on existing threats to identify attacks. Anomaly-based systems detect attacks based on traffic patterns [54]. Systems that detect signature-based attacks work well for attacks, but updating the signature database takes time. As datasets grow, it will become harder to compare input. This method cannot detect Zero-day attacks [55]. Anomaly detection systems block malicious traffic. Anomaly-based systems can detect unknown attack types and zero-day attacks. However, too many false positives are encountered with anomaly prevention systems [56].

Physical attacks such as RF interference or jamming, tampering, fake node injection, malicious code injection, permanent denial of service (PDoS), sleep denial attacks, and side channel attacks are made in the perception layer [57]-[59]. Against these attacks, there are techniques such as PUF-based Authentication, CUTE Mote, PAuthKey, support vector machine (SVM), masking technique, and NOS middleware [60]-[65]. At the network layer, there are RFID spoofing, traffic analysis attacks, routing information attacks, unauthorized access, sinkhole attack, selective routing, wormhole attack, MitM, Sybil attacks, DoS/DDoS attacks, replay attacks [57], [58], [66]. For attacks on the network layer, have privacy-protecting traffic obfuscation framework, SRAM-based PUF, hash chain authentication, cluster-based intrusion detection system, trust-aware protocol, secure MQTT: cross-device authentication, beacon encryption, EDoS Server: SDN-based IoT framework and machine learning models [67]-[77]. At the application layer, there are malware attacks such as viruses, worms, trojans, spyware, and adware [57], [66]. The most well-known of these are the Mirai botnet and Jeep hack attacks. Lightweight framework for attacks on the application layer; high-level synthesis (HLS), and malware image classification; there are prevention methods such as the lightweight neural network framework [78]-[81]. There are also data attacks such as unauthorized access, data inconsistency, and data breaches. Chaos-based schema against data attacks; blockchain architecture, blockchain-based ABE; privacy protection ABE, two-factor authentication; measures and methods such as DPP, ISDD, and machine learning [82]-[87]. As it can be seen, many prevention methods have been proposed for IoT attack types, and many of these proposed methods include machine learning methods. Table 3 presents IIoT attack types and suggested measures.

Table 3. *IIoT Attack Types and Recommended Measures*

Attack Type	IIoT Layer/Attack Target	Recommended Measures	Papers
Side channel attack, RF interference or jamming, fake node injection, tampering, permanent denial of service (PDoS), malicious code injection, sleep denial attack.	Perception Layer	PUF-based authentication, CUTE Mote, PAuthKey, machine learning methods, masking technique, NOS middleware.	[60]-[65]
RFID spoofing, traffic analysis attack, routing information attacks unauthorized access, Sinkhole-attack, selective routing, wormhole-attack, MitM, Sybil-attack, DoS/DDoS attacks, replay-attack.	Network Layer	Privacy-protecting traffic obfuscation framework, SRAM-based PUF, hash chain authentication, clustering-based intrusion detection system, trust-aware protocol secure MQTT; cross-device authentication, digital signature, and encryption (signcryption), EDoS Server; SDN-based IoT framework, machine learning methods.	[67]-[77]
Malware attacks like viruses, worms, trojans, spyware and adware, Mirai botnet, and jeep hack.	Application and Business Layer	Lightweight framework; high-level synthesis (HLS), lightweight NN, malware image classification.	[78]-[81]
Data inconsistency, unauthorized access, and data breach.	Middleware layer and Data Attack	The chaos-based scheme, blockchain architecture, blockchain-based ABE; privacy protection ABE, two-factor authentication; DPP, ISDD, and machine learning methods.	[82]-[87]

2.2. *Machine Learning and Deep Learning Methods*

ML is a branch of AI and computer science that imitates how humans learn, focusing on using data and algorithms and increasing their accuracy. For example, SVM, BN, DT, KNN, RF, and K-Means are machine learning, CNN, RNN, LSTM, GRU, GAN, RBM, DBN, and AE are deep learning algorithms [112]. In addition to these, there are ensemble learning (EL) and transfer learning methods. At the same time, algorithms such as ABC, PSO, and SSO as machine learning methods based on biological intelligence are also used in IIoT attack detection and prevention.

3. Research Method

This section refers the method applied when selecting papers specific to ML and DL-based IIoT security and the numerical results found. At the same time, the research questions and objectives, query sentences and areas, criteria for selecting and screening from the remaining manuscripts, and the general flow of the research method are given in the tables.

3.1. Research Questions and Purposes

This systematic literature survey examines ML, and DL-based IDS approaches developed to prevent or detect attacks on IIoT devices and systems. To achieve this goal, the focus has been on which ML and DL models are used to distinguish between benign network traffic and malignant network traffic. In addition, the performance criteria used to evaluate the models and the preferred datasets for training and testing the models are reviewed. For this systematic review to reach its goal, the research questions (RQs) and the purposes of these questions are shown in Table 4.

Table 4. *Research Questions and Purposes*

Research Question Number	Research Questions	Purposes
RQ1	In IIoT security, what performance metrics or measures are evaluated in ML and DL models?	Evaluating the proposed machine learning and deep learning models in IIoT security with their performance metrics and defining the most used performance metrics.
RQ2	In terms of IIoT security, What are the malign and benign data types found in the datasets used in the ML and DL models, and what are the features of the datasets?	To reveal which datasets are preferred for training and testing of ML and DL models used in IIoT security and to learn the properties of these datasets.
RQ3	Which ML and DL approaches are used in IIoT security, and what are the application fields of the models?	To identify the tasks of the ML and DL models used in the proposed schemes to protect IIoT devices and systems from attacks and to measure the models' performances.

3.2. Research Strategy

In order to find articles that can be examined in this systematic literature survey, research is conducted in seven basic academic databases (Web of Science: WoS, Scopus, IEEE Xplore, ScienceDirect: Elsevier, Hindawi, Wiley Online Library, MDPI) accepted by the scientific community.

These academic databases are preferred because they have search engines that can be searched in detail to obtain the manuscripts to be examined. However, it has been observed that the other academic databases, SpringerLink and Google Scholar websites, have limited ability to perform detailed filtering, querying, and advanced search in search engines. These databases do not allow searching by query clauses, they only offer advanced search. Therefore, SpringerLink and Google Scholar databases were not used in this manuscript as they were not systematically searched.

The research questions shown in Table 4 were transformed into the necessary queries to conduct research in the seven databases described above, with Table 5. Table 5 indicates the query sentences used to search seven databases and in which areas they were made.

Table 5. *Query Sentences and Fields*

Database	Query Sentence	Query Area
Web of Science (WoS)	ALL=(("industrial internet of things security" or "iiot security" or "industrial iot security") and ("machine learning" or "deep learning"))	All metadata
Scopus	TITLE-ABS-KEY (("industrial internet of things security" OR "iiot security" OR "industrial iot security") AND ("machine learning" OR "deep learning"))	Title, abstract and keywords
IEEE Xplore	("All Metadata": industrial internet of things security or industrial iot security) AND ("All Metadata": deep learning or machine learning)	All metadata
ScienceDirect (Elsevier)	("industrial internet of things security” OR "IIot Security" OR "industrial iot security”) AND ("Deep Learning" OR " Machine Learning ")	Title, abstract and keywords
Hindawi	("industrial internet of things" OR "IIot Security" OR "industrial iot security") AND ("Deep Learning" OR "Machine Learning")	All metadata

Wiley Online Library	("industrial internet of things security" OR "IIot Security" OR "industrial iot security") AND ("Deep Learning" OR " Machine Learning")	All metadata
MDPI	Keywords = ("industrial internet of things security" OR "IIot Security") AND ("Deep Learning" OR "Machine Learning")	Title and keywords

3.3. Search Process and Filtering Criteria

The criteria determined for selection and elimination among the manuscripts obtained as a result of the query sentences in Table 5 are given in Table 6.

This systematic review included manuscripts published in 2019-2023 (SC2). The reason for choosing this date range is that the manuscripts published before 2019 have been performed today. Then, among the journal manuscripts written in English (SC1) in this date range, articles published in Q1 or Q2 level journals (SC3) and manuscripts using ML and DL models in IIoT security (SC4) are listed. However, publications in the conference, editorial notes, books, and preprint stages were eliminated. Replicated manuscripts (EC1), which are literature searches or reviews and are also found in other academic databases, are eliminated. In the continuation of the review, manuscripts that do not deal with anomaly detection (EC2) in IIoT network security do not disclose the datasets used (EC3) and do not cover ML and DL models for IIoT security (EC4) are discarded. 252 papers were obtained from seven different databases with the help of query clauses in Table 5 and selection criteria in Table 6. The remaining papers were analyzed using the elimination criteria in Table 6, resulting in the examination of 25 different papers for this survey. During the analysis, it was preferred that the article was new and had been cited more. At the same time, the content of the remaining articles after the elimination criteria was read and the remaining articles were selected accordingly. When all selection and elimination processes are carried out, 25 articles containing the answers to the research questions in Table 4 along with their analysis processes are examined in detail within the scope of this systematic survey research. Figure 1 shows the general flow of the research method developed to select the articles to be reviewed.

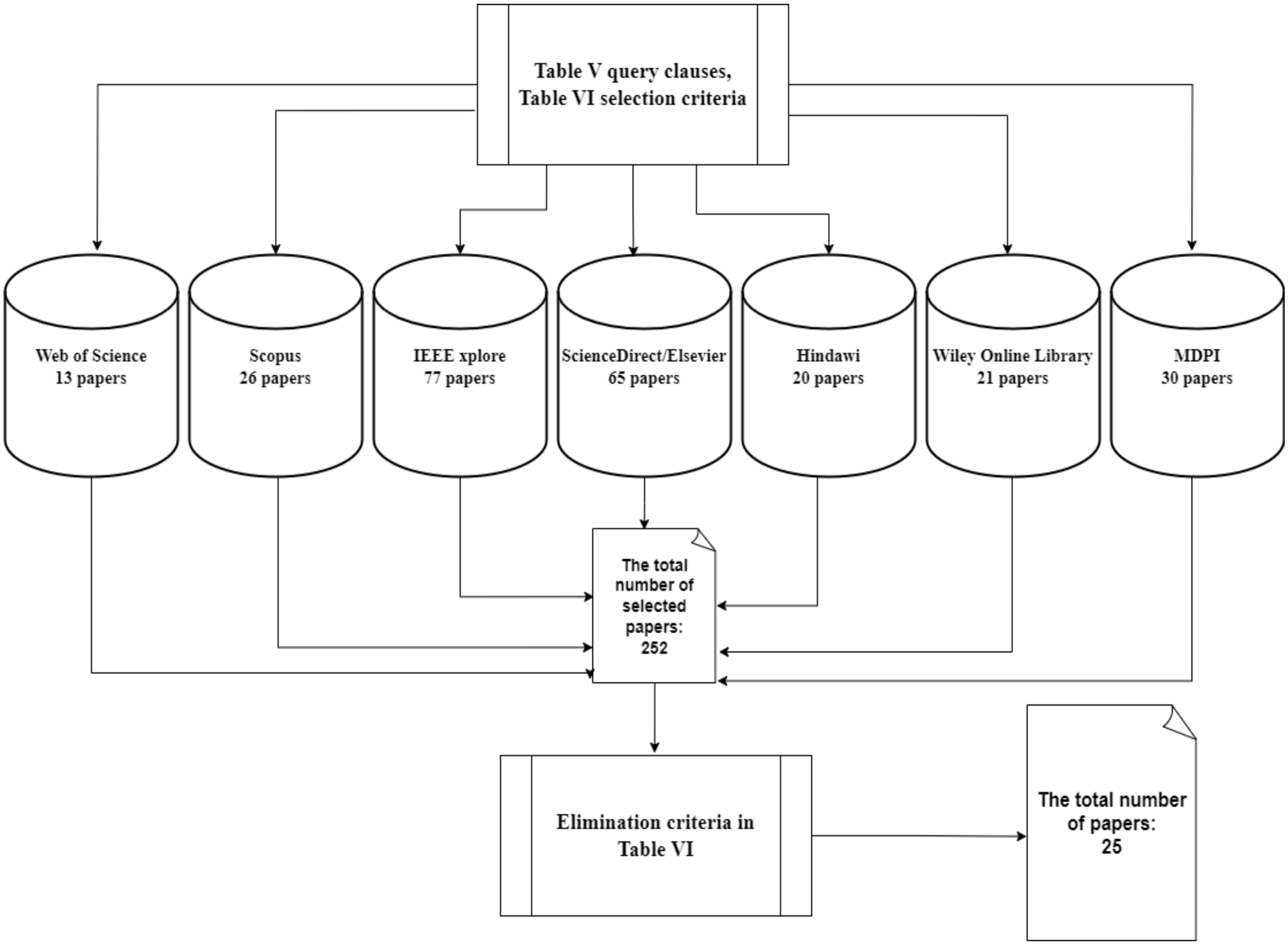

Figure 1. *General Flow of the Research Method*

Table 6. *Selection and Elimination Criteria*

Selection Criteria Number	Selection Criteria (SC)	Elimination Criteria Number	Elimination Criteria (EC)
SC1	Articles published in English in a journal.	EC1	Whether the article is a survey or a literature search.
SC2	Articles published in 2019-2023.	EC2	The focus of work on IIoT network anomaly detection.
SC3	Have an article-type manuscript published in a Q1 or Q2 level journal.	EC3	Articles lacks reference to the datasets employed in the research.
SC4	Articles using ML and DL models in IIoT security.	EC4	Articles do not include ML and DL models.

4. Descriptions of Manuscripts in the Literature

In this section, manuscripts on deep learning and machine learning used to ensure IIoT security in the literature are reviewed.

Researchers used a modified PoW algorithm PoR, which is computationally more challenging, to identify malicious IIoT devices based on blockchain-powered deep learning and verify the transactions of malicious nodes. The model has been tested with the Bot-IoT dataset [90].

The AE algorithm is used for false data injection (FDI) attack detection, and the DAE algorithm is used for noise removal of corrupted data. It also performed significantly better than the SVM model. A distributed dataset of sensor readings was used for hydraulic system monitoring [91].

A new random hybrid deep network (HDRaNN) is tested on DS2OS and UNSW-NB15 datasets. HDRaNN has classified 16 types of cyber-attacks used for DS2OS and UNSW-NB15 with 98% and 99% higher accuracy, respectively. The model achieves its best performance for the optimum learning rate and a certain number of epochs. The results were evaluated with 10-fold cross-validation for the datasets. The HDRaNN model is run for 150 epochs. The simulation is run at five learning rates; 0,005 – 0,01 – 0,75 – 1,00 and 1,50 [92].

The KDL CUP99 used in GRU and SVDD log anomaly detection model is preprocessed by PCA to remove unnecessary features and increase productivity in the high-dimensional original dataset. Then, the advanced GRU-based algorithm with the SVDD algorithm for modeling the network log shows that it is better than traditional methods in detecting the anomaly according to the analysis of many experimental results on the dataset [93].

Different security attacks like spying, wrong setup, DoS, malicious control, malicious operation, probing, and scanning are remarked. ML algorithms are applied to the DS2OS dataset against attacks. To predict attacks, a RaNN-based random neural network model is suggested. Various evaluation criteria such as F1 measurement, accuracy, recall, and precision were used for the RaNN model. RaNN approach achieved 99,2% accuracy, 99,20% F1 score, 99,13% recall, 99,11% accuracy in 34,51 seconds. The detection accuracy is 5,65% better than other algorithms compared [94].

A deep random neural (DRaNN) based model for IDS in IIoT was estimated on the UNSW-NB15 dataset. The DRaNN model has successfully classified nine different attack types with low FPR and high accuracy of 99,54%. The results are compared with other DL-based IDS models. In addition, the proposed model achieved a high intrusion detection rate with 99,41% DR [95].

IIoT attack models are updated and validated with the collaborative data generator DNN. The approach using SCADA data is compared with DNN and SVM (sigmoid) models. In terms of performance in the proposed noisy environment, it gave better results than other models available. Classification performances are also reported for the dataset with different levels of noise added, ranging from 1% to 50% noise. It was classified with 95.42% accuracy without noise and 92.91% accuracy with semi-noise. It is classified as 17.85% Log Loss without noise (binary cross entropy) and 21.59% Log Loss with semi-noise [96].

An RS learning method and an RT combination were used to detect SCADA attacks using network traffic from the SCADA IIoT platform. All 15 different datasets in SCADA consist of thousands of different attacks. Datasets are randomly sampled at a rate of 1% to reduce the impact of a small sample size. With Binary Classification, 96,71% accuracy, 0,05% false positive rate (FPR), 0,22 ms total training time for 3738 samples, and 0,1 ms total test time for 1602 samples were measured. The proposed model is compared with the RSKNN model [97].

AMCNN-LSTM with gradient compression based on Top-k selection is used to detect anomalies accurately, while the model is used to train the FL scheme in anomaly detection. AMCNN with LSTM model accuracy is 96.85% for the power demand dataset [98].

Feature selection is made by training the original dataset in the first stage. Then the previously trained data is tested. It is then combined with the original sample set with a subset of other instances of the same classifier. Finally, Kernel-Based Learning (KBL) has been proposed, which clusters the controversial samples according to their distance from the center. The proposed method on 3000 malign and 5000 benign datasets yielded 86.08% accuracy and 0.8655 (KBL) G-mean, 80.69 accuracies, and 0.7843 (random) G-mean [99].

The features were normalized with the min-max technique in a single preprocessing step. PCA was used to reduce the size and extract the best features. Training, testing times, confusion matrix of the models, and computational complexity are given. The OCSVM model has been added to the proposed framework to detect unprecedented attacks. The OCSVM algorithm showed a detection accuracy of 86,14% in attacks that were not seen before in the natural gas pipeline dataset and 94,53% in attacks that were not seen before in the SWaT dataset. The total training time for the SWaT dataset is 1200 seconds, and the model testing time is 0,03 ms for each sample, with a total of 2,98 seconds. The total training time for the Gas Pipeline dataset is 1115 seconds, and a model test time of 0,02 ms for each sample, with a total of 1,1 seconds [100].

7 ML methods and 1 DL model were evaluated with the dataset TON_IoT containing telemetry data, operating system logs, and network traffic. The ML and DL frameworks used are LR, RF, LDA, CART, KNN, NB, SVM, and LSTM algorithms, and all models have been cross-validated by four times. The TON_IoT dataset consists of 7 different datasets: refrigerator sensor, GPS tracking, remote garage door, thermostat, smart light detection, weather, and Modbus datasets. These datasets feature nine types of cyber-attacks (Ransomware, scanning, backdoor, DoS, XSS, DDoS, password cracking attack, data injection and MitM). After the preprocessing and normalization steps, the datasets are trained with AI based model. LSTM model for refrigerator sensor 100% accuracy, accuracy, all models for garage door 100% accuracy, kNN algorithm for GPS tracking 88% accuracy, CART algorithm for Modbus 98% accuracy, LSTM for smart motion detection 59% accuracy, kNN for thermostat and except for the CART algorithms, all other models achieved 66% accuracy. For the weather dataset, the CART algorithm reached 87% accuracy. A new experiment result was made by combining the entire dataset, and the CART algorithm for

binary classification gave 88% accuracy, and again for the multi-classification model, the CART algorithm gave 77% accuracy [101].

The paper proposes a new anomaly detection approach based on centralized data collection and forwarding design that can successfully cooperate in using adaptable CEEMDAN feature with a single, smart optimization for IIoT small data. The swarm intelligence algorithm is used with the IABC OCSVM classifier to detect different anomalies. The recommended IABC-OCSVM model has high performance. The dataset was collected from sensors in an oil field in China. These sensors contain engine speed, electrical parameters, and flow and pressure information. WIA-PA transmits data to Remote Terminal Unit: RTU and RTU transmit data to a higher monitoring center via ModBus and TCP. There are 109672 IIoT data, 225 data strings, and 100 abnormal data strings. OCSVM is optimized using traditional ABC and PSO algorithms under five different attack powers. The training accuracy of the ABC-OCSVM model is 95,1%, and the test classification accuracy is 89%. The IABC-OCSVM model reaches average training accuracy of 94,5% and test accuracy of 89,8% [102].

IIoT cloud computing risks privacy disclosure by outsourcing users. There is the SHOCFS technique to solve this problem. With the SHOCFS method, the most suitable density peaks are determined, and the model's speed is tried to increase. Swallow swarm optimization (SSO) enables the selection of optimal density peaks of clustering models. A clustering algorithm is proposed to find optimal density points with the hybrid cloud SHODS3O-CFS model. In the SHODS3O-CFS model, the overlapping peaks of the cluster can be reduced. Clustering center quality (CCQ), Rand index (RI), speedup-ratio (SR), and encryption time performance metrics were used. It achieved a higher mean RI of 93.4%, compared to 29.68% and 17% of the proposed manuscript. The dataset is taken from the 5567 home energy consumption data warehouse participating in the UK Power Network meeting for the low carbon London project, and the dataset is available on the Kaggle website [103].

IoT-Flock developed as an open source, a benign and malignant health dataset is created for IoT devices. Six machine learning models were used to detect cyber-attacks and protect the health system from attacks. The RF algorithm showed the best performance with 99,7% accuracy, 99,79% sensitivity, 99,51% accuracy, and 99,65% F1 score [104].

Feature selection with Fisher score and genetic-based extreme gradient boosting model was used to detect IoT attacks. GXGBoost achieved 99.96% accuracy on the N-BaIoT dataset with 10-fold cross-validation. The dataset malicious Mirai and the Bashlite class are instantiated in the Benign class dimension [105].

Job Safety Analysis (JSA) was conducted to identify factors that cause worker accidents and injuries. With smart PPE, notifications from electronic devices are transmitted to operators, and ThingsBoard, an open-source IoT platform, provides communication between active sensors for data processing and IoT management. Device connectivity is provided via industry IoT protocols (HTTP, MQTT, CoAP), supporting cloud and on-premises deployments. CNN has been realized with the ThingsBoard platform. The cross-validation CNN has an accuracy of 92,05% [106].

The dataset for IoT and IIoT applications called the open-source Edge-IIoTset was proposed, and tests have been carried out on the dataset with ML and DL-based models [107].

EDIMA, an IoT botnet detection solution, is proposed. A new two-stage Machine Learning (ML) based detector developed for IoT bot detection uses supervised ML algorithms and an Autocorrelation function for bulk traffic classification. As a result, EDIMA has a high detection rate, low bot detection delays, and low RAM consumption in detecting IoT bots [108].

LSTM, CNN, and RNN deep learning methods based on a feature selection method based on LightGBM, and DDQN and DQN Deep Reinforcement Learning models were used [109].

IIoT threat detection was performed with the Cu-LSTMGRU + Cu-BLSTM hybrid model, and high accuracy was achieved with a low false positive rate. The proposed model was compared with the Cu-DNNLSTM and Cu-DNNGRU models [110].

Ensemble models RF-PCCIF and RF-IFPCC methods were used to improve IDS performances on Bot-IoT and NF-UNSW-NB15-v2 dataset [120].

23 features were selected with a feature selection based on correlation; SVM and Decision Tree classification models and NSL-KDD dataset are used to analyze network intrusion and attack detection performance [121].

Synchronous optimization of parameters and architectures by genetic algorithms with convolutional neural networks blocks (SOPA-GA-CNN) on five intrusion detection datasets in IIoT, including secure water treatment (SWaT), water distribution (WADI), Gas Pipeline, BoT-IoT and Power System Attack Dataset for the intrusion detection has been implemented [122].

The residual neural network (P-ResNet) model was implemented by combining seven IoT sensors (e.g., fridge_sensor, GPS_tracker_sensor, motion_light_sensor, garage_door_sensor, modbus_sensor, thermostat_sensor, and weather_sensors) TON_IoT datasets [123].

The main idea and focus of the examined approaches and the advantages and disadvantages of the models proposed in these approaches are given in Table 7.

Table 7. *An Overview of Suggested Approaches in Manuscripts*

Paper	Main Idea	Advantages	Disadvantages
[90]	A new modified PoW algorithm PoR, which is computationally more difficult, to identify malicious IIoT devices based on blockchain-powered deep learning	With the improved PoW algorithm, PoR, the operations of malignant nodes are made difficult.	Not applied in a real environment. Untested in different deep learning and machine learning models.
[91]	A new method of false data injection (FDI) attack detection using automatic encoders (AE) is introduced. Also, corrupted data is cleaned using denoising AEs (DAEs). DAE is very efficient in recovering clean data	Proposed framework can detect other types of attacks without any updates It is the first manuscript to recommend using DAEs to clean up corrupted (hacked) data.	The denoising autoencoder needs to be trained for all attack types. When the Autoencoder is supervised learning, it does not need to be constantly trained.
[92]	A new hybrid and random deep learning model (HDRaNN) DS2OS and UNSW-NB15 have been tested with two different datasets.	Various performance metrics HDRaNN is compared to key detection patterns.	Not applied in a real environment. Untested in machine learning models
[93]	Gated Recurrent Unit and Support Vector Domain Definition log anomaly detection model has been proposed. The model has been tested on the KDLLCUP99 dataset.	Compared with many deep learning models.	Not applied in a real environment. No known performance measures were used.
[94]	Attacks are classified with ML models. The best model is RaNN based random NN model.	Attacks are detected, and classified with high success rates such as 99,11% accuracy, 99,13% precision and 99,20% F1 score.	Not applied in a real environment. Untested in different machine learning models.
[95]	The DRaNN-based model was estimated on the UNSW-NB15 dataset.	The attacks were detected with 99,54% accuracy and 99,41% detection rate, with a high success rate of 0,76% false positives.	Not applied in a real environment. Untested in different ML and DL models.
[96]	A downsampling encoder-based collaborative data generator trained using an adaptive algorithm is proposed.	Real IIoT dataset. The data were classified by adding noisy data to the test dataset.	Accuracy and loss rates are given only as performance criteria, and other known criteria are not used.
[97]	RS learning method and RT combination were used to detect SCADA attacks using network traffic from the SCADA IIoT platform.	Creating a detection engine based on industrial protocols and a high DR of 96,71%	If a feature exists, the best feature is limited to random selection. Excessive execution time
[98]	A deep learning-based federated learning tool to detect communication-efficient, new anomalies to detect time series data in IIoT	It uses convolutional neural network units based on the attention mechanism, thus avoiding memory loss and gradient distribution problems.	The federated learning model is vulnerable for loss of malign anomaly attacks
[99]	ML-based KBL selection method is proposed for defense against hostile attacks in an IIoT environment.	Extracted from the malware dataset as static features with the Androguard tool.	Untested in different deep learning models. Feature selection method is used, which is not used very much in the literature.
[100]	A new two-stage community deep learning model and attack correlation scheme is proposed for unstable industrial control system data using the OCSVM model to detect unprecedented attacks.	Resistant to unstable datasets where the numbers of malignant and benign datasets are not close to each other. Capable of detecting never-before-seen attacks	Complex architecture
[101]	A new dataset (TON_IoT) is proposed, which includes Telemetry data of IoT and IIoT services, traffic of IoT network, and operating systems logs. It is designed based on integrating IoT/IIoT systems with three layers of Fog, Edge, and Cloud.	Variety of benign and malign events for different IoT or IIoT devices. Contains heterogeneous data sources.	Advanced parameter optimization is required to optimize hyper parameters and obtain better results.
[102]	CEEMDAN feature and swarm intelligence algorithm ABC-based IABC-OCSVM model.	The real-world dataset in China oil IIoT system. Attacks under five different attack power have been detected.	The dataset is not public and not detailed. No evaluation was made with different performance criteria. No comparison with deep learning models.
[103]	With IIoT cloud computing, the SHODS3O-CFS algorithm, which is a new SHOCFS technique, is recommended for users outsourcing privacy disclosure risk.	A safe optimized clustering method is proposed to obtain optimal density peaks.	No evaluation has been made with other ML and DL algorithms. Not tested in a real environment.
[104]	Developing a benign and malignant IoT use case with IoT-Flock, which creates open source IoT data, and traffic generation and evaluation of IoT health dataset with ML techniques.	An open source software has been created for IoT healthcare environments that capture data in the context-aware MQTT and COAP categories.	Deep learning models are not used.

[105]	IoT botnet network attacks are detected by feature selection with Fisher score and GXGBoost algorithm and identify the most relevant features.	A high detection rate (average accuracy results in 99,96%)	Hard to verify that parameters reach the global optimum, Sensitivity and randomness of the genetic algorithm used for the initial population
[106]	A smart helmet 5.0 CNN model that monitors environmental conditions and performs real-time risk assessment	The model was evaluated with ML and DL algorithms.	Except for the accuracy performance metric, no other performance metric is used.
[107]	The dataset for IoT and IIoT applications called the open-source Edge-IIoTset has been proposed, and tests have been carried out on the dataset with ML and DL-based models.	Data was collected from more than 10 IoT devices, and 61 new features were extracted from 1176 features. Performance was evaluated with ML and DL algorithms.	Realistic but not real environment
[108]	EDIMA, an IoT botnet detection solution, is proposed. A new two-stage Machine Learning (ML) based detector developed for IoT bot detection uses supervised ML algorithms and an Autocorrelation function for bulk traffic classification.	A high detection rate, Low bot detection delays, and low RAM consumption in detecting IoT bots.	Difficulty of retraining the model, Deep learning models are not used. Not tested in a real environment.
[109]	For IIoT, LSTM, CNN, and RNN, deep learning methods based on a feature selection method based on LightGBM, DDQN, and DQN Deep Reinforcement Learning models were used.	Both deep learning methods and deep reinforcement learning models were used.	Machine learning models are not used. Not tested in a real environment.
[110]	For the IIoT environment, a hybrid DL, SDN-enabled approach is proposed to detect threats and intrusions.	The model is programmable and expandable on iiot data devices. Open flow switches are used in SDN	Not tested in a real environment, Machine learning models are not used.
[120]	Ensemble models RF-PCCIF and RF-IFPCC methods	Pearson Correlation Coefficient (PCC) Isolation Forest (IF) to reduce computational cost and prediction time	Not used deep learning models, Not tested in a real environment.
[121]	Correlation based features selection SVM and DT methods	Correlation features selection	Not tested in a real environment, Deep learning models are not used.
[122]	Synchronous optimization of parameters and architectures by genetic algorithms with convolutional neural networks blocks (SOPA-GA-CNN)	On five intrusion detection datasets in iiot, including secure water treatment (swat), water distribution (WADI), Gas Pipeline, bot-iot and Power System Attack Dataset for the intrusion detection	Not tested in a real environment, Machine learning models are not used.
[123]	Residual neural network (P-ResNet) model with seven IoT sensors dataset	Combining seven iot sensors	Not tested in a real environment.

5. Results

In the results section, the determining research questions are answered.

5.1. RQ1: In IIoT security, what performance metrics or measures are evaluated in ML and DL models?

The performance of the ML and DL models used in the proposed schemes was evaluated by means of various criteria. These criteria are given in Table 8. Table 8 summarizes the definitions of performance criteria, their mathematical equations, if any, and in which manuscripts they are used. According to Table 8, it is seen that the criteria of F-1 score, precision, accuracy, recall, FPR, DR and FAR and are widely preferred for the evaluation of the models. Since these criteria were used, TP, FP, TN and FN values were measured in each manuscript. The total time taken for training (TRT) and testing (TET) models is also frequently used in manuscripts. Other criteria are used in the evaluation of the models in accordance with the purpose of the proposed models.

Table 8. *Performance Metrics Used in the Evaluation of Machine Learning and Deep Learning Algorithms*

Performance Metrics	Performance Description	Mathematical Equation	Articles Used
TP	A correctly predicted situation is correct	-	All
TN	An incorrectly predicted situation is correct	-	All
FP	False of a positively predicted situation	-	All
FN	False of a negatively predicted situation	-	All
ACC	Percentage of correctly classified sample data out of all classified sample data.	$\frac{TP+TN}{TP+TN+FP+FN}x100$	[90], [91], [92], [94], [95], [96], [97], [98], [99], [100], [101], [102], [104], [105], [106], [107], [108], [109], [110], [120],

			[121], [122] , [123]
PRE	Percentage of how accurately we guessed from all classes	$\frac{TP}{TP+FP}x100$	[90], [92], [94], [99], [100], [101], [104], [105]], [107], [108], [109], [110], [120] , [122], [123]
REC	Percentage of how accurately we guessed from all positive classes	$\frac{TP}{TP+FN}x100$	[90], [92], [94], [99], [100], [101], [104], [105]], [107], [108], [109], [110], [120], [123]
SPC (TNR)	Ratio of true negative samples.	$\frac{TN}{TN+FP}x100$	[99], [110]
F1	Harmonic mean of precision and recall measures. Low recall or high precision (or vice versa)	$\frac{2xPRExREC}{PRE+REC}x100$	[92], [94], [99], [100], [101], [104], [105]], [107], [108], [109], [120] , [122], [123]
SNS (TPR)	Rate of positive samples correctly classified as positive.	$\frac{TP}{TP+FN}x100$	[99], [110]
FPR/FAR	Rate of negative samples falsely classified as positive.	$\frac{FP}{FP+TN}x100$	[91], [93], [95], [97], [110]
G-Mean	Geometric mean of Specificity and Sensitivity	$\sqrt{SPCxSNS}$	[99]
MCC	Matthews correlation coefficient	$\frac{TP.TN-FP.FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$	[110]
FNR	Rate of positive samples falsely classified as negative.	$\frac{FN}{TP+FN}x100$	[110]
FDR	False Discovery Rate	$\frac{FP}{TP+FP}x100$	[110]
ROC	The curve obtained by plotting FPR versus TPR, as the threshold data values vary over a range.	-	[91], [92], [104], [110], [120], [123]
MSE	Mean square error	-	[91], [92], [104]
AUC	ROC area under the curve.	-	[91], [110], [120], [123]
RMSE	Root mean square error	$\left[\frac{1}{n}\sum_{i=1}^{m}\left(\lvert y_i-\hat{y}_p\rvert\right)^2\right]^{\frac{1}{2}}$	[98]
RI	The measure of the exact clustering results versus the actual clustering results of the clustering algorithm.	$\frac{TP+TN}{TP+TN+FP+FN}x100$	[102]
DR	Rate of correctly detected positive samples among total positive samples.	$\frac{TP}{TP+FN}x100$	[91], [93], [95], [108]
ER	The rate of how often the model misclassifies.	$\frac{FP+FN}{TP+TN+FP+FN}x100$	[103]
TRT	Total time spent training the model.	-	[93], [98], [99], [102], [103], [120], [121], [123]
TET	Total time spent testing the model.	-	[96], [99], [102], [103], [107], [110], [120], [122], [123]
ATR	Average time spent training the model.	-	[105]
ATE	Average time spent testing the model.	-	[105]
ET	The encryption time of the model.	-	[105]
Log Loss: LL	The log loss is found by subtracting the performance results of the model from the expected results. Lower log loss is better performance.	$-\sum_{c=1}^{M} yo,c\, log(po,c)$	[94]
CCQ	Distance between clustering centers produced	$\sqrt{\sum_{i=1}^{C}\lVert v_{ideal}^{i}-v^{i}\ \rVert^2}$	[103]
SR	Speedup ratio	-	[103]

5.2. RQ2: In Terms of IIoT Security, what are the Malign and Benign Data Types Found in the Datasets Used in the ML and DL Models, and the Features of What are the Datasets?

There are various types and numbers of datasets used for the manuscripts reviewed. With ML and DL algorithms, models are trained and tested on data sets. The datasets used in the models are selected by the purpose of the proposed schemes to ensure IIoT security. If the developed approaches are used to detect which attack types, datasets containing examples of those attack types are recommended for train and testing the models. Table 9 shows the datasets used to train and test the models or the datasets created by the authors for use in papers. The datasets encompass various types of malignant and benign samples, and pertinent information about the statistical properties of these samples, as well as the manuscripts in which they were utilized. The number of features, classes, and dimensions of the dataset is also given. However, detailed information about the datasets used in the manuscripts are not given in the articles in which they are used [91], [103], [104]. For this reason, the details of these datasets are not available in Table 9. Data types and attack types are not given for malign and benign [96]-[98], [102], [106].

The Bot-IoT [113] dataset contains 14 features. These are the numeric expression of feature status, the minimum duration of total records, the standard deviation of total records, number of inbound connections per destination IP, the average duration of total records, highest period of total records, total bytes per destination IP, the sequence number of the Argus agent, per unit time packets from source to destination, packets from destination to source, packets from source to destination, packets from destination to source per unit of time, total bytes per source IP, incoming connections per source IP [90]. The DS2OS dataset has eight classes and 13 features [92], [94], and the UNSW-NB15 dataset] has ten classes and 49 features [92], [95. The KDD CUP99 (NSL-KDD) dataset includes DOS, R2L, U2R, and Probe attack types with 42 features [93]. Datasets containing 15 different datasets in the SCADA network were sampled at a rate of 1%. Detailed information about the features was not given [96], [97]. There are time series datasets consisting of four real-world data (Engine, Power Demand, ECG, Space Shuttle) combined from various sensors. These datasets have normal subsequences and abnormal subsequences. No detailed information was given about the features [98]. In the manuscript found [99], the Android Malware dataset recommended and the number and types of features used were not given [111]. There are 17 features in the Pipeline dataset, 51 features, and 31 scenarios in the Swat dataset [110]. There are 52 features within the attack types (ransomware, scanning, backdoor, DoS, XSS, DDoS, password cracking attack, data injection, and MitM) [101]. The articles do not have dataset details and feature information [102]-[104]. The N-BaIoT dataset has 115 features derived from malignant and benign data [105], [110]. The number of features is not specified in the dataset created for Smart Kask 5.0 [106]. Edge-IIoTset dataset is generated from various IoT devices and proposes 61 new features [107]. IoT-NSS-BPR uses IoT-23 dataset, and UNSW IoT dataset. Dataset types are malware samples, malware traffic pcap files, and aggregate IoT traffic pcap files [108]. Real dataset of the natural gas pipeline transportation network publicly released by the U.S. Department of Energy's Oak Ridge National Laboratory [109].

Table 9. *Datasets Used in Models and Properties*

Dataset	Type and Number of Malign Data	Type and Number of Benign Data	Total Data Numbers	Number of Features/ Classes/ Dimensions	Articles Using
Bot-IoT: is a dataset containing detailed network information of benign and malignant data traffic and various network attacks.	- UDP DoS and DDoS: 39624597 - Service scanning: 1463364 - HTTP DoS and DDoS: 49477 - TCP DoS and DDoS: 31863600 - OS fingerprint: 358275 - Keylogging: 1469 - Data theft: 118	- UDP: 7225 - ICMP: 9 - TCP: 1750 - RARP: 1 - ARP: 468 - IGMP: 2 - IPV6-ICMP: 88	- Malign: 73360900 - Benign: 9543 - Total: 73370443	14 features	[91], [120], [122]
DS2OS: It includes 13 features and 7 malign and 1 benign data	-Spying: 532 -DoS: 5780 -Malicious Control: 889 -Wrong setup: 122 -Scan: 1547 -Malicious Operation: 805 -Data type probing: 342	Normal: 347935	-Malign total: 10017 -Benign total: 347935 -Total: 357952	13 features and 8 classes	[92], [94]
UNSW-NB15: 9 malign, 1	-Fuzzers: 24246	Normal: 93000	-Malign total:164673	49 features and 10	[92],

benign data produced by the Australian Cyber Security Center's Cyber Range Laboratory	-Backdoor: 2329 -Analysis: 2677 -Reconnaissance: 13987 -Exploits: 44525 -Generic: 58871 -DoS: 16353 -Shellcode: 1511 -Worms: 174		-Benign total: 93000 -Total: 257673	classes	[95], [120]
KDD CUP 99 NSL-KDD	-DOS:2000 -R2L:1000 -U2R:500 -PROBE:1500	Normal: 2000	-Malign total: 4000 -Benign total: 2000 -Total: 6000	42 features	[93], [121]
SCADA	28 attack scenarios	9 normal event scenarios	28 total scenarios	-	[96], [97]
Power Demand	Abnormal substring: 6	Normal substring: 45	Normal substring: 45 Abnormal substring: 6 Total substring: 51 Original sequence:1	1 Dimension	[98]
Space Shuttle	Abnormal substring: 8	Normal substring: 20	Normal substring: 20 Abnormal substring: 8 Total substring: 28 Original sequence:3	1 Dimension	[98]
ECG	Abnormal substring: 1	Normal substring: 215	Normal substring: 215 Abnormal substring: 1 Total substring: 216 Original sequence:1	1 Dimension	[98]
Engine	Abnormal substring: 152	Normal substring: 240	Normal substring: 240 Abnormal substring: 152 Total substring: 392 Original sequence:30	12 Dimension	[98]
Android Malware dataset suggested by the authors [111]	3000 malwares	5000 benign	Total 8000	-	[99]
Pipeline	60048 (21,86%) attack examples - Malicious state command injection (MSCI) -Naive malignant response injection (NMRI) -Reconnaissance (Recon) -Complex malignant response injection (CMRI) -DoS -Malign function code injection (MFCI) - Malignant parameter command injection (MPCI)	214580 (78,14%) normal samples	274628 total samples	17 features	[100] , [122]
Swat (safe water treatment)	12,1% attacks	87,9% normal	Total: 449920 samples	51 features 31 scenario	[100] , [122]
TON_IoT	Total: 162932 - XSS - scanning - data injection - DoS, - MitM - DDoS, - ransomware - backdoor - password cracking attack	Benign 35000 for all datasets Total benign: 245000	Malicious:162932 Benign: 245000 Total: 407932	- Refrigerator sensor:7 - GPS tracking:7 - Garage door:7 - Thermostat:7 - Intelligent light detection:7 - Weather:8 - Modbus:9 Total Features: 52	[101], [123]
Oil field dataset in China [102]	100 abnormal data strings	200 normal data strings	300 data strings	-	[102]
N-BaIoT	Mirai: 3668402 Bashlite: 1032056	Benign: 555932	Malignant: 4700458 Benign: 555932 Total: 5256390	115 features	[105], [110]
Dataset created by the authors [106] for Smart Helmet 5.0	-	-	11755 samples in total	12 scenarios	[106]
Edge-IoTset	Backdoor: 24862 DDoS_HTIP: 229022	Normal: 11223940	Normal: 11223940 Attack: 9728708	New 61 features with high	[107]

	DDoS_ICMP: 2914354 DDoS_TCP: 2020120 DDoS_UDP: 3201626 Fingerprinting: 1001 MITM: 1229 Password: 1053385 Port_Scanning: 22564 Ransomware: 10925 SQL_injectioion: 51203 Uploading: 37634 Vulnerability_scanner: 145869 XSS: 15915		Total: 20952648	correlations from 1176 found features	
IoT-NSS-BPR, IoT-23 dataset, UNSW IoT dataset	IoT-NSS-BPR: 23 live IoT malware samples, UNSW IoT dataset :28 different uninfected IoT devices collected at a gateway.	-	-	Best 8 features	[108]
U.S. Department of Energy’s Oak Ridge National Laboratory natural gas pipeline transportation network	NMRI 2763 CMRI 15466 MSCI 78 MPCI 7637 MFCI 573 DoS 1837 Recon 6805	Normal: 161156	Normal: 161156 Attack: 32396 Total: 193552	26 features and one label	[109]

5.3. RQ3: which ML and Dl Approaches are Used in IIoT Security, and What are the Application Fields of the Models?

Table 10 summarizes the usage areas of the models, the datasets they are trained and tested with, the performances they show as a result of the experiments, and the information about which models they are compared with.

When Table 10 is examined, a feedforward multilayer multiclass neural network with Microsoft Azure Machine Learning Studio is used with the Bot-IoT dataset with various hyperparameters. An advanced intrusion detection method using a deep learning model together with blockchain is proposed for malignant IIoT devices. High-performance results have been achieved with this model [90].

It is aimed to detect false data injection attacks with an automatic encoder algorithm that is easy to train and learns hidden complex relationships. When SVM and AE were compared, AE gave more successful results. A DAE was used to get rid of the effects of the attack on the data [91].

HDRaNN, proposed for cyber-attack detection in IIoT uses implementations of HDRaNN and MLP. The HDRaNN includes input, hidden, and output layers. Performance measurements were made on two separate datasets such as UNSW-NB15 and DS2OS. With the HDRaNN model, attacks are classified with an accuracy of 98% and over 99% for the UNSW-NB15 and DS2OS datasets. HDRaNN model has been compared with RNN, DBN, DAE, and RBM deep learning models [90].

A log anomaly and malignancy detection model based on GRU and Support Vector Domain Definition algorithms framework is proposed. Numerous experiments and analyses of experimental results on the KDL CUP99 dataset have shown that the advanced GRU-based algorithm is better than traditional deep learning models in detecting an anomaly. The highest DR was measured at 99,6%, and the smallest FAR at 0,01%. Five types of anomalies (DoS, R2L, U2R, PROBE, and mixed) were detected with five algorithms (GRU-SVDD, BGRU-MLP, LSTM, LSTM-RNN, PCA-SVM) [93].

RaNN deep learning model evaluated accuracy, precision, precision, and F1 score performance metrics on the DS2OS dataset. The RaNN model is compared with SVM, DT, and ANN models. RaNN model accuracy is compared with the accuracy of previous intrusion detection models [94].

Intrusion detection was performed on a model UNSW-NB15 dataset based on a DRaNN model for intrusion detection in IIoT. Feature transformation and normalization were performed in the preprocessing step. With the DRaNN model intrusion detection system, the data is classified as normal or attack [95].

The down sampler-based data generator for SCADA attacks detection is alternatively updated and validated using a deepNN splitter during training. A GAN was developed to generate conflicting attack data, and this generated data was classified [96].

A reliable ensemble learning model with a combination of the SCADA network RS learning method and RT has been tested on 15 different datasets. The model, whose classification accuracy and model complexity was balanced, performed well compared to other cutting-edge approaches [97].

Firstly, the FL model is developed to collaboratively train anomaly detection on decentralized edge devices. Secondly, the attention mechanism CNN-LSTM model is proposed for the correct detection of anomalies. The AMCNN-LSTM scheme uses CNN units based on the attention mechanism to capture important detailed features, thus avoiding memory loss and gradient distribution problems. Thirdly, in order to increase communication efficiency, anomaly detection has been made in the industrial area with the model that compresses the gradients based on Top-k feature selection [98].

It has been tested with feature selection methods such as random, L1, Euclidean, and KBL. High performance was obtained with the KBL selection method SVM algorithm [99].

OCSVM was used to detect previously unseen attacks, creating a boundary around normal samples and reporting others as never-seen attacks. The proposed model is a complex deep neural network consisting of partially or fully connected layers that detect IoT attacks [100].

4-fold cross-validation of LR, RF, LDA, CART, KNN, NB, and SVM models were evaluated on the newly proposed TON_IoT dataset. 80% of the data and 20% of the data are allocated to the test dataset to train/validate ML methods. Classification results are given for the TON_IoT dataset refrigerator sensor, GPS tracking, garage door, thermostat, smart light detection, weather, and Modbus datasets with different models. As a result of the estimation made by combining the whole dataset, the CART algorithm for binary classification reached the most successful result with 88% accuracy, and again for the multi-classification model, the CART algorithm achieved the most successful result with 77% accuracy. Training and testing times for binary classification are high for LSTM, SVM, and KNN models and low for LR, LDA, RF, CART, and NB models. Training and testing times for multiclassification are high for LSTM, SVM, LR, and KNN models and low for LDA, RF, CART, and NB models [101].

A new IABC-OCSVM anomaly attacks classification scheme is proposed for the IIoT small dataset that can skillfully cooperate in CEEMDAN model feature use compatible with the smart optimizer OCSVM classifier. With CEEMDAN decomposition, energy entropies are measured with IMF components. Multi-scale analysis of the IIoT dataset is performed. The IABC-OCSVM model created with Gaussian mutation was found to have 94.5% training accuracy, 89.8% test accuracy, and 0.0081 seconds test time [102].

SHODS3O-CFS clustering algorithm and the most appropriate density selection in the hybrid cloud are suggested. The SHODS3O-CFS algorithm gave clustering center accuracy (RI) of 87.7% for 50 data objects, while PPHOCFS achieved lower RI results of 62.7% and SHOCFS 76.6%. The SHODS3O-CFS algorithm achieved 95,2% RI for 250 data objects. The PPHOCFS and SHOCFS methods, on the other hand, yielded lower clustering accuracy of 66% and 81,2% RI, respectively [103].

Benign and malignant data in pcap format with IoT-Flock software were converted into CSV format with the python program. The categorical properties of the dataset, such as the protocol type (MQTT and COAP), have been replaced with numeric values using the Label Encoder to facilitate further processing. Missing data is filled with 0. The most important ten features consist of TCP and MQTT data by feature selection with the LR algorithm. The dataset was tested with NB, KNN, RF, AB, LR, and DT algorithms. Confusion matrix, ROC-AUC, F1 score, precision, accuracy, recall, and values of each algorithm are given. The RF model showed the best performance with 99,70% accuracy, 99,79% recall, 99,51% accuracy and 99,65% F1 score [104].

Improved GXGBoost algorithm to well classify IIoT network attacks. Several trials have been conducted on the public N-BaIoT dataset of IIoT devices. GXGBoost achieved 99.96% accuracy on the N-BaIoT dataset using only three features out of 115 features [105].

An intelligent helmet prototype is presented that monitors environmental conditions and works in near real-time risk assessment. The dataset consisting of 11755 examples and 12 different attack-type scenarios is evaluated by ML and DL. The cross-validation CNN model for business risk analysis yielded 92,05% accuracy. The CNN approach is evaluated by comparing it with NB, SVM, and NN [106].

Normal centralized DT, RF, KNN, SVM, DNN model PRE, REC, and F1 have 100% and federated 2-class IID and Non-IID ACC:100% performance. Edge-IIoTset, produced by ten different IoT devices, was evaluated together with two different ML-based IDS with the centralized and federated mode in 7 different layers [107].

The EDIMA model has been proposed. EDIMA consists of a traffic parser, feature extractor, ML-based bot detector, policy engine, ML model constructor, and a malware PCAP database. RF algorithms ACC, PRE, REC, and F1 have 100% performance [108].

LightGBM feature selection method, PPO2 interface, and CNN, RNN, LSTM, DDQN, and DQN model were used. Deep Reinforcement Learning model DDQN has a 97,74 F1-score [109].

The hybrid model (Cu-LSTGRU + Cu-BLSTM), Cu-DNN-LSTM, and Cu-DNN-GRU were evaluated, and (Cu-LSTMGRU + Cu-BLSTM) gave the highest performance result with an F1-score rate of 99.47%. Model GRU-RNN has been compared with Autoencoder (EDSA) and Multi-CNN [110].

RF-PCCIF and RF-IFPCC have 99.98% and 99.99% Acc and prediction time of 6.18 sec and 6.25 sec, respectively, on Bot-IoT. The two models also achieve 99.30% and 99.18% accuracy and prediction time scores of 6.71 sec and 6.87 sec on NF-UNSW-NB15-v2, respectively [120].

Quadratic SVM has 99.7% accuracy, prediction speed is 1100 s and training time is 465.28 s. Fine Tree has 99.4% accuracy, prediction speed is 570.000 sec and training time is 11.029 seconds [121].

(SOPA-GA-CNN) has 98.1 F1 Score with gas pipeline dataset [122].

P-ResNet has a performance of 87% accuracy, 88% precision, 86% recall, 86% F1 Score, 83% ROC AUC, TRT: 24401.586s, TET: 3.014s [123].

Table 10. *An Overview of the Models*

Papers	Models/Methods Used and Their Tasks	Datasets and Uses	Performance	Compared Models or Approaches
[90]	A feedforward multilayer multiclass neural network with various hyperparameters is used with Microsoft Azure Machine Learning Studio to simulate the deep learning model.	Bot-IoT: the dataset is split 6:4 into training and test data.	- Overall ACC: 95,9% - Average ACC: 98,36% - Micro average PRE: 95,9% - Micro-average REC: 95,9% - Macro averaged REC: 58,18%	-
[91]	The Auto-encoder algorithm is used to reveal false data injection attacks. Clean corrupted data (AE) performed better with the support vector machine (SVM) algorithm in terms of ROC. Pump, coolant, valve, and accumulator values are measured.	The dataset includes a total of 15 sensor data. (volumetric flow, pressure, engine, temperature, cooling, vibration, and power).	MSE training loss: 3.99e-7 MSE validation loss: 4.37e-7 AE ACC: 97,65% SVM ACC: 85,1% AE DR: 100% SVM DR: 88,55% AE FAR: 6,42% SVM FAR: 16,3% DAE MSE: 0,0064 AE MSE: 0,1 AE TRT:1 min SVM TRT:15 min	-SVM RBF Kernel -SVM Linear Kernel -SVM Gaussian Kernel

[92]	HDRaNN model has been used for cyber-attack detection in IIoT.	DS2OS is used for training and testing. Attack distributions are given in detail. A confusion matrix was created.	ACC: %98,56 PRE: %98,25 REC: %98,36 F1: %98,3 LL: %36,24 AUC-ROC: %91,28	RNN, DBN, DAE, RBM
		UNSW-NB15 is used for training and testing. Attack distributions are given in detail. A confusion matrix was created.	ACC: 99,19% PRE: 99,07% REC: 98,98% F1: 99,02% LL: 12,23% AUC-ROC: 98,82%	
[93]	A log anomaly detection model based on GRU and Support Vector Domain Definition algorithms framework	10% of the KDL CUP 99 dataset is trained.	DR: 99,6% FAR: 0,01%	BGRU-MLP, LSTM, PCA-SVM and LSTM-RNN
[94]	Detecting attacks in DS2OS dataset with a new lightweight random neural network model	Intrusion detection was performed by dividing the DS2OS dataset 8:2 train and test data	ACC: 99,2% PRE: 99,08% REC: 99,16% F1: 99,04% TET: 34,51 ms	SVM, DT, ANN
[95]	Intrusion detection was performed on the UNSW-NB15 dataset with DRaNN based model.	UNSW-NB15 is used for 75% training and 25% testing. Attack distributions are given in detail.	ACC: 99,54% DR: 99,41% FPR: 0,76%	BLSTM RNN, Adaboost, CNN and WDLSTM, DL, FFDNN, DNN, DBN
[96]	The down sampler-based data generator for SCADA attack detection is alternatively updated and validated using a deepNN splitter during training. Developing and classifying a GAN to generate conflicting attack data	SCADA: 36000 samples, half of which benign traffic and half of malign attack traffic	Noiseless ACC: 95,42% Semi-noisy ACC: 92,91% GAN ACC: 95,55% GAN LL: 47,55% TRT: 2,58h	DNN, SVM
[97]	An improved ensemble learning model is proposed to detect SCADA cyberattacks based on the combination of RS learning method and RT.	SCADA 15 datasets and thousands different attacks. Datasets are randomly sampled at a rate of 1%.	Binary Classification ACC: 96,71% FPR: 0,05% TRT: 0,22 TET: 0,1	RSKNN
[98]	AMCNN-LSTM model based on the attention mechanism is proposed.	Engine, Space Shuttle, ECG, Power Demand	For Power Demand, AMCNN-LSTM ACC: 96,85% RMSE: <5% AMCNN-LSTM time with GCM: 25min AMCNN-LSTM time without GCM: 90min	SVM, SAE, GRU, CNN with LSTM and LSTM
[99]	In the malware literature, the KBL selection method has a 6% performance improvement over random selection.	Android Malware dataset	ACC: 86,08% G-Mean: 86,55% AUC: 95,8% SVM ACC: 98,5%	DNN, SVM, RF, Bayes
[100]	The proposed IDS consist of two unsupervised SAEs, feature extraction using PCA and a Decision Tree classification and using OCSVM to detect previously unseen attacks	Pipeline dataset created by Mississippi State University	ACC: 96,2% PRE: 96,17% REC: 96,2% F1: 96,18% TRT: 1200s TET: 2,98s	DT, SVM, K-Means, NB, AIKNN, LSTM
		Swat (safe water treatment) dataset created by Singapore Technological University	PRE: 99,99% REC: 99,99% F1: 99,98% TRT: 1115s TET: 1,1s	DT, LADS-ADS, DNN, ID CNN, MADGAN, Tabor, LSTM, ST-ED
[101]	A new dataset (TON_IoT) is proposed for the next generation IoT and IIoT dataset for data-driven IDS. On the TON_IoT dataset, LR, RF, LDA, CART, KNN, NB, and SVM models were evaluated with 4-fold cross-validation. All algorithms classification results are given on seven different datasets, TON_IoT dataset, refrigerator sensor, GPS tracking, garage door, thermostat, smart light detection, weather, and Modbus datasets. In addition, for the combined_TON_IoT dataset, which is the combination of all	Refrigerator sensor	For LSTM; ACC, PRE, REC and F1: 100% TRT:190,493 TET:3,705	LR, RF, LDA, CART, KNN, NB, SVM, LSTM
		GPS tracking	For KNN; ACC: 88% PRE: 89% REC: 88% F1: 88% TRT: 0,08 TET: 1,508	
		Garage door	For all algorithms ACC, PRE, REC and F1: 100% NB TRT: 0,01sec	

	data sets, all algorithms are evaluated with binary and multi-classification models, and attack types are classified.		TET: 0,02sec	
		Thermostat	For NB; ACC: 66% PRE: 44% REC: 66% F1: 53% TRT: 0,009 TET: 0,002	
		Intelligent light detection	For LSTM; ACC: 59% PRE: 35% REC: 59% F1: 44% TRT: 63,132 TET: 3,73	
		Weather	For CART; ACC: 87% PRE: 88% REC: 87% F1: 87% TRT: 0,258 TET: 0,03	
		Modbus	For CART; ACC: 98% PRE: 99% REC: 98% F1: 99% TRT: 0,367 TET: 0,01	
[102]	An improved ABC algorithm IABC-OCSVM, based on an arrow-variable Gaussian mutation with CEEMDAN decomposition compatible with the intelligent optimizer OCSVM classifier	Pressure, engine speed, flow and some electrical parameters	Training ACC: 94,5% Test ACC: 89,8% TET: 0,0081s	EEMD and CEEMDAN ABC-OCSVM, PSO-OCSVM
[103]	SHOCFS was used for speed improvement and detection of optimum density peaks, SSO was used to select optimum density points of the clustering model, and the SHODS3O-CFS method was suggested in a hybrid cloud. The SHODS3O-CFS model reduces overlapping peaks in the cluster and increases security in the hybrid cloud.	Incorporating daily weather changes into energy use, clustering center quality collected from data in England, Wales and Scotland is evaluated on clustering center quality, encryption time, accuracy, speed-up rate performance measures.	RI: 95,2% ER: 778,80ms SR: 36,86 CCQ: 0,401	PPHOCFS and SHOCFS
[104]	Data in MQTT and COAX categories from environment monitoring sensors and patient monitoring sensors were created with IoT-Flock software. The created dataset was evaluated with NB, KNN, RF, AB, LR, and DT algorithms. The model that gave the best results was the RF algorithm.	From environmental monitoring sensors (air-humidity, air-temperature, co, fire, smoke, barometer, solar radiation sensors) and patient monitoring sensors (remote electrocardiogram (ECG) monitoring, galvanic skin response (GSR) sensor), infusion pump pulse oximetry (SPO2), nose/mouth air flow sensor, blood pressure monitor sensor, glucose meter, electromyography (EMG) sensor, body temperature sensor	ACC: %99,51% PRE: 99,7% REC: 99,79% F1: 99,65% AUC: 100%	NB, KNN, RF, AB, LR
[105]	GXGBoost performed several experiments on the public N-BaIoT dataset for efficient classification	The N-BaIoT dataset consists of the malignant Mirai, Bashlite and Benign datasets.	ACC: 99,96% PRE: 99,95% REC: 99,95% F1: 99,95% ATR: 545,040 sec ATE: 4,208 sec	DNN, DT, KNN, DAE, SVM, VIF
[106]	CNN model ThingsBoard tool. ThingsBoard. CNN algorithm works independently with an alarm system in	It consists of a dataset of 11,755 examples and 12 different scenarios.	ACC: 92,05%	NN, NB, SVM

	simulation.			
[107]	DT, RF, SVM, KNN, DNN centralized model and 2-class (binary classification), 6-class (multi-classification), and 15-class (multi-classification) federated DL approach.	Edge-IIoTset, produced by 10 different IoT devices, was evaluated together with 2 different ML-based IDS with centralized and federated mode in 7 different layers.	Normal centralized DT, RF, KNN, SVM, DNN model PRE, REC, F1: 100% federated 2-class IID and Non-IID ACC:100%, etc. [107]	DT, RF, SVM, KNN, DNN and Federated DL models
[108]	Supervised ML algorithms (NB, SVM, RF model) and Autocorrelation Function	Top 8 features selected to train ML classifiers	RF ACC, PRE, REC, F1:100%	NB, SVM, RF
[109]	GBM's feature selection algorithm, and PPO2 interface of the Stable baseline to implement model training has been used. DRL-IDS intrusion detection agent is tested on the training and validation sets.	26 features are removed and only 3 features are used without reducing performance.	For DDQN ACC: 99,05% PRE: 98,42% REC: 97,08% F1: 97,74%	CNN, RNN, LSTM, DDQN, DQN
[110]	Hybrid model (Cu-LSTMGRU + Cu-BLSTM) 10-fold cross-validation multiclass, GPU-Enabled, Compared with hybrid algorithms, Cuda-DNNLSTM and Cuda-DNNGRU	N-BaIoT hosts malware, namely Bashlite and Mirai. It consists of 8 attacks and 115 features. 49500 normal IIoT data.	Cu-LSTMGRU + Cu-BLSTM ACC: 99,45% PRE: 99,34% REC: 98,49% F1: 99,47% FNR, FDR: 0.002 FOR: 0,004 FPR: 0,003 TPR: 99,33% TNR: 99,13% MCC: 99,13% TET: 9,79ms	Cu-DNN–LSTM and Cu-DNN–GRU, GRU-RNN, Autoencoder (EDSA) Multi-CNN
[120]	RF-PCCIF and RF-IFPCC Ensemble model	Bot-IoT with 15 selected features and with NF-UNSW-NB15-v2 with 24 features	Bot-IoT ACC: RF-PCCIF: 99,98% RF-IFPCC: 99,99% UNSW-NB15-v2 ACC: RF-PCCIF: 99,3% RF-IFPCC: 99,18% TRT: 145.24s	Information gain and gain ratio, Chi-square, CNN, ET
[121]	Linear SVM, Quadratic SVM, Fine Tree, Medium Tree	NSL-KDD	Linear SVM ACC: 99.3% Quadratic SVM ACC: 99.7% Fine Tree ACC: 99.4% , TRT: 11.029s Medium Tree ACC: 95.9%	Linear SVM, Quadratic SVM, Fine Tree, Medium Tree
[122]	synchronous optimisation of parameters and architectures by genetic algorithms with convolutional neural networks blocks (SOPA-GA-CNN)	Secure water treatment (SWaT), water distribution (WADI), Gas Pipeline, BoT-IoT and Power System Attack Dataset	Gas pipeline: ACC: 99,04% PRE: 98,14% REC: 98,07% F1: 98,1%	SVM, RNN, LSTM, NB, BiLSTM, CNN, VCDL, Deep-IFS
[123]	Residual neural network (P-ResNet)	Seven IoT sensors (e.g., fridge_sensor, GPS_tracker_sensor, motion_light_sensor, garage_door_sensor, modbus_sensor, thermostat_sensor, and weather_sensors)	P-ResNet ACC: 87% PRE: 88% REC: 86% F1: 86% ROC AUC: 83% TRT: 24401.586s TET: 3.014s	LSTM, NN, CNN, RNN, FCN, LeNet, IncepNet, MCDCNN

6. Conclusion, Discussions and Open Research Problems

In this manuscript, a systematic literature survey used in Industrial Internet of Things security was done, and studies on ML and DL models used to detect anomaly-based attacks in IIoT networks were examined. The examined approaches are obtained from the Web of Science, Scopus, IEEE Xplore, ScienceDirect, Hindawi, Wiley Online Library, and MDPI academic databases using the query sentences in Table 5. Among the papers revealed as a result of the queries, 25 of them were selected and summarized according to the selection and elimination criteria given in Table 6, with the publication years between 2019 and 2023. A systematic literature survey used in Industrial Internet of Things security was done, and manuscripts on ML and DL models used to detect anomaly-based attacks in IIoT networks were examined. The examined approaches are obtained from the Web of Science, Scopus, IEEE Xplore, ScienceDirect, Hindawi, Wiley Online Library, and MDPI academic databases using the query sentences in Table 5. Among the papers revealed as a result of the queries, 25 of them were selected and summarized according to the selection and elimination criteria given in Table 6, with the publication years between 2019 and 2023.

When the reviewed manuscripts are evaluated, it is concluded that many manuscripts have different deficiencies. These deficiencies are summarized as follows:

- There are extra security measures in the blockchain to make it harder for malicious nodes to verify transactions and connect to other devices, but it has not been compared to other DL and ML algorithms [90].
- Except for a few manuscripts, their datasets have not been publicly shared [99], [103], [105]. Therefore, the performance results of the proposed approaches are controversial. Additionally, if the datasets are shared publicly, other researchers will be able to evaluate the usability of these datasets and improve the datasets.
- Some datasets do not include detailed counts of malignant and benign data types [91], [96]-[98], [103], [104]. The lack of these details prevents obtaining sufficient information about the datasets.
- Most of the models proposed in the manuscripts have not been tested in a real-life. Therefore, the performance values of these approaches in an environment where they are actually used cannot be estimated. Manuscripts should be tested in a real environment, and their performance should be measured.
- The vulnerabilities of the proposed approaches against various types of attacks were not addressed in the reviewed manuscripts. Apart from a manuscript [100], other systems proposed to be secure against certain types of attacks can be used as schemes, frameworks, models, or parts. The status of security levels against different or unknown attack types is unknown. That is, the usability of the proposed models in the real-world environment is questioned.
- A manuscript has not been tested in other machine learning and deep learning models, except for biologically inspired intelligence-based methods, and has been evaluated with performance measures that are not often used. The results obtained in different models with known performance metrics will become important for the evaluation of the manuscript [103].
- Some studies did not provide any conclusions regarding training or testing times, such as the ML and DL models used in other reviewed manuscripts. An analysis of the resource consumption of IIoT devices with insufficient resources cannot be made. Therefore, the efficiency of approaches that include models without resource consumption and training-test time analysis in a real IIoT environment is unknown [90]-[93], [95], [99].

The source codes of the ML and DL models used in the manuscripts examined were not shared in a public environment, except for the manuscript [103]. Therefore, these models are not known to be established, as shown in manuscripts. In addition, by sharing the source codes of the approaches, other researchers examining the codes will contribute more to the literature in their future manuscripts.

In this survey, firstly, short and concise explanations about the approaches proposed in the selected articles are given. Then, the main ideas, advantages and disadvantages found in these manuscripts are summarized in Table 7. Second, the criteria used to evaluate the performance of the ML and DL models used in the approaches are shown in Table 8. Third, various information about the datasets used in the testing and training processes of the models are presented in Table 9. Fourth, the ML and DL approach used in the proposed approaches to IIoT security are given in Table 10. Table 10 summarizes the usage areas of the models, the datasets they use, the training-test result performances, and the information about which models they are compared with. In the evaluation part, the shortcomings of the manuscripts examined are given. In the conclusion part, the manuscript is summarized, and open research problems are briefly explained.

IIoT leverages a variety of existing and emerging technologies such as communication networks, sensing technologies, and high-performance processing platforms to build its entire ecosystem. As a result, IIoT security and privacy concerns don't just focus on monolithic technology issues. There is an integrated heterogeneous environment from the physical security of connected devices to the communication security of networks, from data security to IIoT application security. It covers a wide variety of IIoT ecosystems, consisting of various security protocols, defense schemes, and many standards of IIoT structure. Most models have traditional methods of protecting and defending data communications. It is debatable whether these traditional mechanisms deployed are still sufficient to protect the latest IIoT technologies; this section also discusses the overt security and privacy issues of IIoT.

- Classes with fewer datasets will give less successful results in the real environment or a new dataset, as they will cause data to be overfitting [98], [102]. The imbalance of datasets, that is, very different numbers of benign and malignant datasets will also create complexity and invalidate learning for different data and real environments [90], [92]-[95], [100].
- Except for some manuscripts, other datasets are old and outdated [93], [107]. Therefore, it is difficult to find a suitable benchmark dataset to apply ML and DL models in IIoT security. However, most of the datasets used are not publicly available or the datasets are too small, especially for deep learning models [102].
- While machine learning models are successful in some datasets, deep learning models give more successful results in others [101]. Some approaches do not make comparisons between ML and DL models. In addition, some articles do not apply preprocessing and feature selection steps for datasets [91]. Therefore, too many features are obtained. Feature selection and feature extraction are very important in terms of performance and complexity, especially for ML models. The performance of ML models can be increased by selecting the feature.
- Several authors working on the same dataset did not compare the results of the manuscripts [90], [99], [91]. Some articles do not include dataset details and feature information [96]-[99], [102]-[104], [106].
- Anomaly detection, which is mainly used, may not be applied in the same way in all areas. For example, while temperature change is very important in the field of industrial medicine, it may not be that important for a smart factory. Therefore, anomaly detection should not be applied to all areas in the same way [98], [100], [102], [106].
- Normal data may be close to the cluster containing the anomaly data, and anomaly data may be close to the cluster containing the normal data [46]. In such cases, anomaly detection becomes very difficult. Normal data may change according to time and space and appear as an anomaly. In these cases, it may be necessary to change the hyperparameters used in the ML and DL models.
- The DL and ML models used in IIoT security focus only on the accuracy performance metric in some articles [96], [102], [106]. Instead, manuscripts including precision, recall, and F1 score performance criteria should be conducted to better understand the manuscripts. In some cases, performance criteria such as log loss, speedup ratio, g-mean, rand-index, and specificity are used, which are not used much in the literature [92], [102].
- For an accurate assessment of the energy consumption and computational complexity of the proposed approaches, on which platforms the datasets are created and tested, training, testing, real-time response, and execution times are not explicitly given [90], [92], [93], [95], [99], [103], [104], [106].
- Zero-day attacks are a type of security vulnerability that is exploited the day a vulnerability is discovered or before an update is available by the developer. Dynamically changing zero-day attacks can cause unknown malicious behavior to be detected [46].
- False positives will cause economic worsening that will affect the relevant services and production areas. Whenever a false positive is found, especially medical, industrial units will have to stop production. False negatives are even more problematic. It is the appearance of a condition as negative as a result of a test when it actually is. As a result of misinterpretation of data due to unforeseen conditions, not only economic but also human losses will occur [98], [100], [102], [104], [106]. Such cases are still important problems to be solved.

As a result, in this systematic survey, detailed information about open research problems in the literature and models consisting of deep learning and machine learning algorithms to find anomalies in IIoT networks and reduce these anomalies are given.

REFERENCES

[1] L.S. Vailshery, Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ , Statista, Last accessed: October 31, 2021.

[2] M. Hatton, The IoT in 2030: Which applications account for the biggest chunk of the $1.5 trillion opportunity? TransformaInsights, https://www.kisa.link/PsHW, Last accessed: October 31, 2021..

[3] F. Meneghello, et al., *IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices*, IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182–8201, 2019.

[4] C. Xenofontos, et al. Consumer, commercial and industrial iot (in) security: attack taxonomy and case studies. IEEE Internet of Things Journal, 2021.

[5] D. Antonioli, et al., Blurtooth: Exploiting cross-transport key derivation in bluetooth classic and bluetooth low energy, arXiv preprint arXiv:2009.11776, 2020.

[6] L. L. Dhirani, E. Armstrong, and T. Newe, Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. Sensors, 21(11), 3901, 2021

[7] A. R. Sadeghi, C. Wachsmann, & M. Waidner, *Security and privacy challenges in industrial internet of things*. In 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC) (pp. 1-6). IEEE, June 2015.

[8] J. P. Anderson, *Computer security threat monitoring and surveillance,* Technical Report, James P. Anderson Company, 1980

[9] B. B. Zarpelão, et al, *A survey of intrusion detection in Internet of Things*, Journal of Network and Computer Applications, Volume 84, Pages 25-37, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2017.02.009, 2017

[10] E. Hodo, et al, *Threat analysis of IoT networks using artificial neural network intrusion detection system.* In 2016 International Symposium

on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE, May 2016.

[11] E. Anthi, et al, *A supervised intrusion detection system for smart home IoT devices*. IEEE Internet of Things Journal, 6(5), 9042-9053, 2019.

[12] S. Raza, L. Wallgren, & T. Voigt, *SVELTE: Real-time intrusion detection in the Internet of Things.* Ad hoc networks, 11(8), 2661-2674, 2013.

[13] V. Kumar, A. K. Das, & D. Sinha, *UIDS: A unified intrusion detection system for IoT environment.* Evolutionary Intelligence, 14(1), 47-59, 2021.

[14] M. Eskandari, et al, Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal, 7(8), 6882-6897, 2020.

[15] E. Aydogan, et al. *A central intrusion detection system for rpl-based industrial internet of things*. In 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS) (pp. 1-5). IEEE, May 2019.

[16] M. Zolanvari, et al., Machine learning-based network vulnerability analysis of industrial Internet of Things. IEEE Internet of Things Journal, 6(4), 6822-6834, 2019.

[17] J. B. Awotunde, C. Chakraborty, & A. E. Adeniyi, Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection. Wireless Communications and Mobile Computing, 2021.

[18] A. H. Muna, N. Moustafa & E. Sitnikova, *Identification of malicious activities in industrial internet of things based on deep learning models.* Journal of Information security and applications, 41, 1-11, 2018.

[19] G. E. I. Selim, et al. Anomaly events classification and detection system in critical industrial internet of things infrastructure using machine learning algorithms. Multimedia Tools and Applications, 80(8), 12619-12640, 2021.

[20] A. F. M. Agarap, A neural network architecture combining gated recurrent unit (GRU) and support vector machine (SVM) for intrusion detection in network traffic data. In Proceedings of the 2018 10th international conference on machine learning and computing (pp. 26-30). 2018, February.

[21] S. Aljawarneh, M. Aldwairi, & M. B. Yassein. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, 152-160. 2018.

[22] L. Breiman, et al, *Classification and regression trees.* Routledge. 2017.

[23] L. Li, H. Zhang, H. Peng, & Y. Yang, *Nearest neighbors based density peaks approach to intrusion detection.* Chaos, Solitons & Fractals, 110, 33-40. 2018.

[24] A. L. Buczak & E. Guven. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176. 2015.

[25] A. P. Muniyandi, R. Rajeswari, & R. Rajaram, Network anomaly detection by cascading k-Means clustering and C4. 5 decision tree algorithm. Procedia Engineering, 30, 174-182. 2012.

[26] R. Vinayakumar, K. P. Soman, & P. Poornachandran, *Applying convolutional neural network for network intrusion detection*. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1222-1228). IEEE. September, 2017.

[27] A. A. Diro, & N. Chilamkurti. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768. 2018.

[28] J. Kim, et al. *Long short term memory recurrent neural network classifier for intrusion detection*. In 2016 International Conference on Platform Technology and Service (PlatCon) (pp. 1-5). IEEE. (2016, February).

[29] P. Liu, X. Qiu, & X. Huang, X. Recurrent neural network for text classification with multi-task learning. arXiv preprint arXiv:1605.05101. 2016.

[30] M. Yousefi-Azar, et al. *Autoencoder-based feature learning for cyber security applications*. In 2017 International joint conference on neural networks (IJCNN) (pp. 3854-3861). IEEE. (2017, May).

[31] T. Salimans, et al. *Improved techniques for training gans*. Advances in neural information processing systems, 29, 2234-2242. 2016.

[32] U. Fiore, et al. Network anomaly detection with the restricted Boltzmann machine. Neurocomputing, 122, 13-23. 2013.

[33] Y. Zhang, P. Li, & X. Wang, Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEE Access, 7, 31711-31722. 2019.

[34] K. Tange, et al. Towards a systematic survey of industrial IoT security requirements: research method and quantitative analysis, Proceedings of the Workshop on Fog Computing and the IoT, 2019.

[35] K. Tange, et al, *A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities,* in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2489-2520, Fourthquarter 2020.

[36] T. Soo Fun, & A. Samsudin, Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey. Sensors, 21(19), 6647. 2021.

[37] S. Bhatt, & P.R. Ragiri, *Security trends in Internet of Things: A survey*. SN Applied Sciences, 3(1), 1-14. 2021.

[38] M. Serror, et al, *Challenges and Opportunities in Securing the Industrial Internet of Things*, IEEE Transactions on Industrial Informatics, vol. 17, no. 5, pp. 2985-2996, doi: 10.1109/TII.2020.3023507, May 2021.

[39] Y. Wu, et al. Deep reinforcement learning for blockchain in industrial IoT: A survey. Computer Networks, 191, 108004. 2021.

[40] K. Tsiknas, et al, Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. IoT, 2(1), 163-188, 2021.

[41] M. A. Al-Garadi, et al, *A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security*, IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, 2020.

[42] R. A. Khalil, et al. *Deep Learning in the Industrial Internet of Things: Potentials, Challenges, and Emerging Applications*, IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11016-11040, 15 July15, 2021.

[43] R. Ahmad & I. Alsmadi, Machine learning approaches to IoT security: A systematic literature review. Internet of Things, 100365. 2021.

[44] L. Aversano, et al. A systematic review on Deep Learning approaches for IoT security. Computer Science Review, 40, 100389. 2021

[45] Rudenko, R., Pires, I. M., Oliveira, P., Barroso, J., & Reis, A. (2022). A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity. Electronics, 11(11), 1742.

[46] Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. Computer Networks, 108771.

[47] L. Tan and N. Wang, *Future internet: The Internet of Things*, 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), pp. V5-376-V5-380, 2010

[48] F. A. Alaba, et al, *Internet of Things security: A survey*, J. Netw. Comput. Appl., 88, 10–28, 2017.

[49] H. Boyes, et al. The industrial internet of things (IIoT): An analysis framework. Computers in industry, 101, 1-12. 2018.

[50] J. Sengupta, S. Ruj & S. D. Bit, *A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT*. Journal of Network and Computer Applications, 149, 102481. 2020.

[51] U. Saxena, J. S Sodhi, & Y. Singh. *An Analysis of DDoS Attacks in a Smart Home Networks*. In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 272-276). IEEE. January 2020.

[52] S. Alzahrani and L. Hong, Generation of DDoS attack dataset for effective IDS development and evaluation, J. Inf. Secur. 9 (4), 225–241, 2018.

[53] Y. Gu, et al, Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm, IEEE Access 7, 64351–64365, 2019.

[54] Y.N. Soe, et al, *DDoS attack detection based on simple ANN with SMOTE for IoT environment*, in: 2019 Fourth International Conference on Informatics and Computing (ICIC), pp. 1–5, 2019.

[55] N. Chaabouni, et al, *Network intrusion detection for iot security based on learning techniques*, IEEE Commun. Surv. Tutor. 21 (3), 2671–2701, 2019.

[56] P. García-Teodoro, et al, Anomaly-based network intrusion detection: techniques, systems and challenges, Comput. Secur. 28 (1), 18–28, 2009.

[57] I. Andrea, C. Chrysostomou, G. Hadjichristofi *Internet of things: security vulnerabilities and challenges*, 2015 IEEE Symposium on Computers and Communication (ISCC),), pp. 180-187, 2015.

[58] M.M. Ahemd, M.A. Shah, A. Wahid, *Iot security: a layered approach for attacks and defenses*, 2017 International Conference on Communication Technologies (ComTech), pp. 104-110, 2017.

[59] M. R. Bartolacci, et al, Personal denial of service (PDOS) attacks: A discussion and exploration of a new category of cyber crime. Journal of Digital Forensics, Security and Law, 9(1), 2. 2014.

[60] M.N. Aman, et al, *A light-weight mutual authentication protocol for iot systems*, GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pp. 1-6, 2017.

[61] T. Gomes, et al, Cute mote, a customizable and trustable end-device for the internet of things, IEEE Sens. J., 17 (20), pp. 6816-6824, 2017.

[62] P. Porambage, et al, Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications, Int. J. Distributed Sens. Netw., 10 (7), 2014.

[63] X. Hei, et al, *Defending resource depletion attacks on implantable medical devices*, 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, pp. 1-5. 2010.

[64] J. Choi and Y. Kim, *An improved lea block encryption algorithm to prevent side-channel attack in the iot system* 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), pp. 1-4, 2016.

[65] S. Sicari, et al, Reato: reacting to denial of service attacks in the internet of things, Comput. Network., 137, pp. 37-48, 2018.

[66] P. Varga, et al, *Security threats and issues in automation iot*, 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), pp. 1-6, 2017.

[67] J. Liu, et al, Epic: a differential privacy framework to defend smart homes against internet traffic analysis, IEEE Internet Things J., 5 (2), 2018.

[68] U. Guin, et al, *A secure low-cost edge device authentication scheme for the internet of things*, 31st International Conference on VLSI Design and 17th International Conference on Embedded Systems (VLSID). 2018.

[69] G. Glissa, et al, *A secure routing protocol based on rpl for internet of things*, IEEE Global Communications Conference (GLOBECOM), 2016.

[70] C. Pu and S. Hajjar, *Mitigating forwarding misbehaviors in rpl-based low power and lossy networks*, 2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC), 2018.

[71] C. Cervantes, et al, *Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things*, 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015.

[72] P. Shukla, Ml-ids: A machine learning approach to detect wormhole attacks in internet of things, Intelligent Systems Conference (IntelliSys), 2017.

[73] D. Airehrour, J.A. Gutierrez & S.K. Ray, Sectrust-rpl: a secure trust-aware rpl routing protocol for internet of things, Future Gener. Comput. Syst., 2019.

[74] M. Singh, et al, *Secure mqtt for internet of things (iot)*, 5th International Conference on Communication Systems and Network Technologies, 2015.

[75] Y. Ashibani, Q.H. Mahmoud, *An efficient and secure scheme for smart home communication using identity-based signcryption*, 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), 2017.

[76] V. Adat, B.B. Gupta, *A ddos attack mitigation framework for internet of things*, 2017 International Conference on Communication and Signal Processing (ICCSP), 2017.

[77] D. Yin, et al, A ddos attack detection and mitigation with software-defined internet of things framework, IEEE Access, 6, 2018.

[78] C. Liu, P. Cronin, C. Yang, *A mutual auditing framework to protect iot against hardware trojans*, 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 2016.

[79] S.T.C. Konigsmark, D. Chen, M.D.F. Wong, *Information dispersion for trojan defense through high-level synthesis*, 2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2016.

[80] H. Naeem, et al, *A light-weight malware static visual analysis for iot infrastructure*, International Conference on Artificial Intelligence and Big Data (ICAIBD), 2018.

[81] J. Su, et al, *Lightweight classification of iot malware based on image recognition*, IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), vol. 02, 2018.

[82] T. Song, et al, A privacy preserving communication protocol for iot applications in smart homes, IEEE Internet Things J., 4 (6), 2017.

[83] C. Machado, A.A.M. Frhlich, *Iot data integrity verification for cyber-physical systems using blockchain*, 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC), 2018.

[84] Y. Rahulamathavan, et al, *Privacy-preserving blockchain based iot ecosystem using attribute-based encryption*, IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017.

[85] D. Zheng, et al, Efficient and privacy-preserving medical data sharing in internet of things with limited computing power, IEEE Access, 6, 2018.

[86] P. Gope, B. Sikdar, Lightweight and privacy-preserving two-factor authentication scheme for iot devices, IEEE Internet Things J., 2018.

[87] J. Sengupta, et al, *End to end secure anonymous communication for secure directed diffusion in iot*, Proceedings of the 20th International Conference on Distributed Computing and Networking, ICDCN '19, 2019.

[88] F. Li, et al, *System statistics learning-based IoT security: Feasibility and suitability*, IEEE Internet Things J., vol. 6, no. 4, pp. 6396-6403, Aug. 2019.

[89] Magaia, Naercio, et al. Industrial Internet-of-Things Security Enhanced with Deep Learning Approaches for Smart Cities. IEEE Internet of Things Journal 8.8, 2020

[90] Sharma, M., Pant, S., Kumar Sharma, D., Datta Gupta, K., Vashishth, V., & Chhabra, A. *Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions.* Transactions on Emerging Telecommunications Technologies, 32(7), e4137. 2021.

[91] M. M. N. Aboelwafa, et al, *A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT*, in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8462-8471, Sept. 2020.

[92] Z. E. Huma et al., A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things, in IEEE Access, vol. 9, pp. 55595-55605, 2021.

[93] S. Liu, et al, *Network Log Anomaly Detection Based on GRU and SVDD*, 2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), pp. 1244-1249, 2019.

[94] S. Latif, et al, A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network," in IEEE Access, vol. 8, pp. 89337-89350, 2020.

[95] S. Latif, et al, *DRaNN: A Deep Random Neural Network Model for Intrusion Detection in Industrial IoT,* 2020 International Conference on UK-China Emerging Technologies (UCET), pp. 1-4, 2020.

[96] M. M. Hassan, M. R. Hassan, S. Huda and V. H. C. de Albuquerque, *A Robust Deep-Learning-Enabled Trust-Boundary Protection for Adversarial Industrial IoT Environment,* in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9611-9621, 15 June15, 2021.

[97] M. M. Hassan, A. Gumaei, S. Huda and A. Almogren, *Increasing the Trustworthiness in the Industrial IoT Networks Through a Reliable Cyberattack Detection Model,* in IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6154-6162, Sept. 2020.

[98] Y. Liu et al., Deep Anomaly Detection for Time-Series Data in Industrial IoT: A Communication-Efficient On-Device Federated Learning Approach, in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6348-6358, 15 April15, 2021.

[99] M. Khoda, T. Imam, J. Kamruzzaman, I. Gondal and A. Rahman, *Robust Malware Defense in Industrial IoT Applications Using Machine Learning With Selective Adversarial Samples,* in IEEE

Transactions on Industry Applications, vol. 56, no. 4, pp. 4415-4424, July-Aug. 2020.

[100] A. N. Jahromi, H. Karimipour, A. Dehghantanha and K. -K. R. Choo, *Toward Detection and Attribution of Cyber-Attacks in IoT-Enabled Cyber–Physical Systems*, in IEEE Internet of Things Journal, vol. 8, no. 17, pp. 13712-13722, 1 Sept.1, 2021.

[101] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems, in IEEE Access, vol. 8, pp. 165130-165150, 2020.

[102] J. Zhao, et al, Anomaly Detection Collaborating Adaptive CEEMDAN Feature Exploitation with Intelligent Optimizing Classification for IIoT Sparse Data. Wireless Communications and Mobile Computing, 2021.

[103] T. Primya & G. Subashini, Swarm intelligence-based secure high-order optimal density selection for industrial internet-of-things (IIoT) data on cloud environment. International Journal of Communication Systems, 34(17), e4976, 2021.

[104] F. Hussain et al, A Framework for Malicious Traffic Detection in IoT Healthcare Environment. Sensors, 21(9), 3025. 2021.

[105] M. Alqahtani et al, IoT botnet attack detection based on optimized extreme gradient boosting and feature selection. Sensors, 20(21), 6336, 2020.

[106] I. Campero-Jurado et al. Smart Helmet 5.0 for industrial internet of things using artificial intelligence. Sensors, 20(21), 6241. 2020

[107] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," in IEEE Access, vol. 10, pp. 40281-40306, 2022, doi: 10.1109/ACCESS.2022.3165809.

[108] Kumar, A., Shridhar, M., Swaminathan, S., & Lim, T. J. Machine learning-based early detection of IoT botnets using network-edge traffic. Computers & Security, 117, 102693. 2022

[109] Tharewal, S., Ashfaque, M. W., Banu, S. S., Uma, P., Hassen, S. M., & Shabaz, M. Intrusion detection system for industrial Internet of Things based on deep reinforcement learning. Wireless Communications and Mobile Computing, 2022.

[110] Javeed, D., Gao, T., Khan, M. T., & Shoukat, D. A hybrid intelligent framework to combat sophisticated threats in secure industries. Sensors, 22(4), 1582. 2022.

[111] D. Arp, et al. Drebin: Effective and explainable detection of android malware in your pocket. In Ndss (Vol. 14, pp. 23-26), February 2014.

[112] H. Satilmiş & S. Akleylek, A review of machine learning and deep learning models used for IoT security. Bilişim Teknolojileri Dergisi, 14(4), 457-481. 2021.

[113] N. Koroniotis, et al. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Future Generation Computer Systems, 100, 779-796. 2019.

[114] Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of electrical and computer engineering, 2017.

[115] AlSalem, T. S., Almaiah, M. A., & Lutfi, A. (2023). Cybersecurity Risk Analysis in the IoT: A Systematic Review. Electronics, 12(18), 3958.

[116] Rodríguez, E., Otero, B., & Canal, R. (2023). A survey of machine and deep learning methods for privacy protection in the Internet of Things. Sensors, 23(3), 1252.

[117] Santhosh Kumar, S. V. N., Selvi, M., & Kannan, A. (2023). A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things. Computational Intelligence and Neuroscience, 2023.

[118] Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 28(1), 296-312.

[119] Nuaimi, M., Fourati, L. C., & Hamed, B. B. (2023). Intelligent approaches toward intrusion detection systems for Industrial Internet of Things: A systematic comprehensive review. Journal of Network and Computer Applications, 103637.

[120] Mohy-Eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., & Farhaoui, Y. (2023). An Ensemble Learning Based Intrusion Detection Model for Industrial IoT Security. Big Data Mining and Analytics, 6(3), 273-287.

[121] Alshahrani, H., Khan, A., Rizwan, M., Reshan, M. S. A., Sulaiman, A., & Shaikh, A. (2023). Intrusion Detection Framework for Industrial Internet of Things Using Software Defined Network. Sustainability, 15(11), 9001.

[122] Huang, J. C., Zeng, G. Q., Geng, G. G., Weng, J., & Lu, K. D. (2023). SOPA-GA-CNN: Synchronous optimisation of parameters and architectures by genetic algorithms with convolutional neural network blocks for securing Industrial Internet-of-Things. IET Cyber-Systems and Robotics, 5(1), e12085.

[123] Mehedi, S. T., Anwar, A., Rahman, Z., Ahmed, K., & Islam, R. (2022). Dependable intrusion detection system for IoT: A deep transfer learning based approach. IEEE Transactions on Industrial Informatics, 19(1), 1006-1017.