

Review

Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review

Muaadh A. Alsoufi ^{1,*}, Shukor Razak ^{1,*}, Maheyzah Md Siraj ¹, Ibtehal Nafea ², Fuad A. Ghaleb ^{1,*}, Faisal Saeed ^{2,3} and Maged Nasser ¹

- ¹ School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia (UTM), Skudai 81310, Johor, Malaysia; maheyzah@utm.my (M.M.S.); msnmaged2@live.utm.my (M.N.)
² College of Computer Science and Engineering, Taibah University, Medina 41477, Saudi Arabia; inafea@taibahu.edu.sa (I.N.); fsaeed@taibahu.edu.sa (F.S.)
³ Institute for Artificial Intelligence and Big Data, Universiti Malaysia Kelantan, City Campus, Pengkalan Chepa, Kota Bharu 16100, Kelantan, Malaysia
* Correspondence: muaadh.soufi2021@gmail.com (M.A.A.); shukorar@utm.my (S.R.); abdulgaleel@utm.my (F.A.G.)

Abstract: The Internet of Things (IoT) concept has emerged to improve people's lives by providing a wide range of smart and connected devices and applications in several domains, such as green IoT-based agriculture, smart farming, smart homes, smart transportation, smart health, smart grid, smart cities, and smart environment. However, IoT devices are at risk of cyber attacks. The use of deep learning techniques has been adequately adopted by researchers as a solution in securing the IoT environment. Deep learning has also successfully been implemented in various fields, proving its superiority in tackling intrusion detection attacks. Due to the limitation of signature-based detection for unknown attacks, the anomaly-based Intrusion Detection System (IDS) gains advantages to detect zero-day attacks. In this paper, a systematic literature review (SLR) is presented to analyze the existing published literature regarding anomaly-based intrusion detection, using deep learning techniques in securing IoT environments. Data from the published studies were retrieved from five databases (IEEE Xplore, Scopus, Web of Science, Science Direct, and MDPI). Out of 2116 identified records, 26 relevant studies were selected to answer the research questions. This review has explored seven deep learning techniques practiced in IoT security, and the results showed their effectiveness in dealing with security challenges in the IoT ecosystem. It is also found that supervised deep learning techniques offer better performance, compared to unsupervised and semi-supervised learning. This analysis provides an insight into how the use of data types and learning methods will affect the performance of deep learning techniques for further contribution to enhancing a novel model for anomaly intrusion detection and prediction.

Keywords: systematic literature review; anomaly intrusion detection; deep learning; IoT; resource constraint; IDS



Citation: Alsoufi, M.A.; Razak, S.; Siraj, M.M.; Nafea, I.; Ghaleb, F.A.; Saeed, F.; Nasser, M. Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review. *Appl. Sci.* **2021**, *11*, 8383. <https://doi.org/10.3390/app11188383>

Academic Editors: Dimitrios S. Paraforos and Anselme Muzirafuti

Received: 13 August 2021
Accepted: 7 September 2021
Published: 9 September 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Internet of Things (IoT) is the research and industrial trend in the arena of Information Communications Technology (ICT) that has become accustomed to being part of technology advancement in our everyday life [1]. The IoT term refers to a new communication paradigm in which devices have sensors and actuators that can serve as objects or 'things' to sense their surrounding environment, communicate with one another, and exchange data through the internet [2]. The IoT requires a platform in which all the applications, products, and services are associated with, used to capture, communicate, store, access, and share/transmit data from the real world [3,4]. Nowadays, there are around 50 billion IoT devices connected to the internet, and it is expected to grow to an enormous size over the next few years [5,6]. These huge numbers of devices produce a tremendous amount

of data that can be used by many applications. IoT applications scenarios are ubiquitous, and this includes, food, agriculture, smart farming, demotics, assisted living, e-health, and enhanced learning, to mention a few examples of possible IoT applications. For instance, there will be 15.3 billion IoT devices for smart agriculture by the end of 2025 [7,8]. A huge number of sensors and actuators are needed for real-time monitoring and environment of many industrial domains to provide actionable insights and make timely decisions [9]. However, many challenges hinder the full adoption of the IoT in both research and industry. These challenges include, but are not limited to, security and trust, reliability, scalability, and mobility, among many others [10].

Because IoT devices are connected to the global internet with unmaturing and vulnerable communication protocols and applications, it is exposed to many potential security threats [3,4]. Adversaries may exploit these vulnerabilities and inject anomalies that trigger the system to make wrong control decisions in IoT-based applications, causing a catastrophic impact on people's lives, properties, and economics [7,11]. The evolved threats of cyberattacks pose significant challenges to the IoT ecosystems. Moreover, IoT devices use different platforms and a combination of network connections protocols such as Ethernet, Wi-Fi, ZigBee, and wire-based technologies to increase their connectivity, which needs coordination between different standards and protocols to mitigate security risks. Besides the diverse technologies used by the IoT industry, the heterogeneity, and the distributed nature of IoT applications increase the complexity of IoT networks and thus, magnify the security risk. These shortcomings cause the IoT network to be exposed to many security issues and cyberattacks. Therefore, an accurate anomaly-detection IDS model is vital for IoT applications [12].

Many IDS solutions have been proposed to protect IoT devices from being exposed to cyber criminals [13–15]. These security solutions can be divided into either proactive or reactive measures. The proactive measures can be effective for protecting the IoT against external threats. However, due to the connectivity of the IoT to the global internet, the risk posed by intruders that can circumvent proactive measures is high. Intrusion Detection Systems (IDSs) work as a second line of defense that can impede many cyberattacks. IDS solutions have received intensive attention from researchers and industries in the IoT field, and many IDS solutions have been proposed [16–18]. Based on the detection approach, IDS solutions can be categorized into three approaches: signature, anomaly, and hybrid IDS model. In general, the signature-based approach is effective for known attacks, while the anomaly-based is effective for unknown attacks. However, due to the heterogeneity, dynamicity, and complex nature of the IoT network, the signature-based approach is inefficient and ineffective for IoT because it requires continuous human interventions and knowledge expertise to extract attack patterns and signatures to update the IDS model [19,20]. Anomaly-based IDS detection gains advantages in IoT because it detects zero-day attacks and needs fewer human interventions [20]. The hybrid approach combines both signature-based and anomaly-based approaches. However, because it is impractical to rely on pre-defined attack patterns (signature-based) intrusion detection in IoT, the utilization of the signature-based IDS is limited in IoT networks [18–20]. To this end, anomaly intrusion detection systems play a vital role in intrusion detection in IoT environments.

Most of the existing IDS use conventional machine learning techniques to develop detection models [21]. Machine learning techniques were widely adopted to construct the IDS model. However, due to the speed and volume of the IoT-generated data, conventional machine learning techniques that need well-crafted features engineering need intensive research efforts to extract the representative features from big and unstructured data generated by IoT devices. Thus, conventional machine learning-based solutions still encounter many challenges. Recently, deep learning techniques (DL) have been widely adopted for intrusion detection systems. DL expedites the analysis between fast and real data streams in extracting relevant information to predict the future of the IoT domain. DL is known to be more reliable than traditional learning because it can easily extract

information, and hence, provides better accuracy [22]. Due to this, several studies have been focused on using deep learning techniques to provide new solutions tackling two different perspectives of both technical and regulatory, such as anomaly and malware detection; however, the results are still unconvincing. Furthermore, most IDS solutions have been adopted from existing computer networks, wireless sensors networks, and mobile ad hoc networks. Yet, the unique characteristics of IoT-based networks, such as connectivity to the global internet and lightweight resources, make the IDS proposed for these networks not suitable to IoT applications [13,14]. There are only a few surveys that have been found that focus specifically on DL techniques in the IoT domain [23]. To the best of the authors' knowledge, there is no review that is dedicated to investigating the effectiveness of the deep learning-based IDS solutions in the IoT security domain. Therefore, this paper was conducted to bridge this gap and investigate the most effective and efficient use of DL approaches in securing the IoT environment. This review provides an in-depth, focused, and high-quality analysis to orient future research toward finding robust anomaly-based IDS using DL techniques.

The paper is organized as follows. The contributions introduced by this study are briefed in Section 2. Related work is presented in Section 3. The review method, which includes the review protocol, planning, research questions, is described in Section 4. Section 5 presents the search strategies, which include the primary records selection, secondary records selection, inclusion criteria, exclusion criteria, quality assessment (QA), data extraction, and synthesis. Section 6 presents the results, studies selection and quality assessment results, and overview of publication sources. Section 7 presents the outcomes, which include the answers to the research questions, taxonomy, analysis and discussion, and the open issues. Section 8 presents the discussion. Section 9 presents the future direction. Limitations of the study are illustrated in Section 10, and the study is concluded in Section 11.

2. Contributions

1. This study systemically explores the existing techniques on an anomaly-based intrusion detection system that uses the DL techniques in IoT.
2. A general taxonomy is proposed for the different deep learning techniques used for constructing the anomaly-based IDS in IoT.
3. An analysis of the state-of-art DL-based techniques of anomaly-based intrusion detection systems in IoT, which use DL, is introduced in this survey.
4. This study discusses the challenges and future direction of DL-based anomaly detection in the IoT domain.

3. Background and Related Works

Existing deep learning studies related to IoT security focus primarily on experimental aspects rather than the adopted techniques, leaving a gap for a comprehensive review of different anomaly intrusion detection. For such reason, the goals are to identify what is the most prominently used techniques and how to ensure better performances for each technique. Due to the rapid growth of advancement in this area, the relevant studies should be reviewed and appraised in parallel.

Hajiheidari et al. [19] conducted comprehensive work on intrusion detection systems in the IoT that focuses on four different types of IDS (anomaly-based, signature-based, specification-based, and hybrid-based). However, the scope of work was broad and unspecific on the anomaly intrusion detection system, which used DL techniques. On the other hand, Sharma et al. [23] surveyed studies that use DL for anomaly detection in IoT. Likewise, Fahim and Sillitti [20] conducted a general study on anomaly detection, analysis, and prediction techniques in an IoT environment. However, this study was not specific to the IDS. Alsoufi and Razak [24] in our previous work, surveyed the anomaly intrusion detection system in IoT, which used DL techniques. The finding of our work inspired us to propose this work, which is an in-depth systematic literature review following the

guideline based on proposed work by Kitchenham to provide researchers and developers in-depth information and obtain details about an up-to-date technique and methodology in anomaly intrusion detection in IoT, using deep learning [25].

Table 1 shows a detailed comparison with the similar reviewed articles in the area. Consequently, there is an urgent need to conduct a systemic review and appraise the specific studies in the field of IDS in IoT that used DL techniques. Thus, this systemic review provides an in-depth and focused analysis on orienting future research toward finding robust anomaly-based IDS using DL techniques.

Table 1. Comparison with other similar review articles in the area: (√: Yes, x: No).

Paper Name	Year	IoT	Systematic Study	Anomaly-Based	Deep Learning
Fahim et al. [20]	2019	√	√	√	x
Hajiheidari et al. [19]	2019	√	√	x	x
Sharma et al. [23]	2019	√	x	√	√
Alsoufi, Razak [24]	2021	√	x	√	√
This work		√	√	√	√

4. Review Method

4.1. Development of the Protocol

This review follows the guidelines of performing systematic reviews in the software engineering domain, according to [25,26] as well as other methods from several works [19,27,28].

4.2. Planning the Review

In the planning step, the need for SLR was determined, the research questions were identified, and the review protocol was established.

4.3. The Need for a Systematic Review

There are many approaches applied in detecting intrusion attacks in IoT, using deep learning. However, there is a lack of an in-depth and systematic analysis of those studies. Such an analysis is crucial for the research community, especially for those who are new to the area, to gain a holistic idea of the state of the art of anomaly detection in IoT, using deep learning techniques. Hence, this study focuses on literature reviews of various methods adopted for anomaly-based intrusion detection and inclusive of those researchers that have conducted overview literature on different techniques, taxonomies, and comparisons. This survey presents an in-depth discussion from different perspectives in adherence to the highlighted research questions.

4.4. Research Questions

- Q1 What is the comprehensive taxonomy of anomaly-based intrusion detection in IoT using deep learning techniques?
- Q2 What is the performance of anomaly-based intrusion detection in IoT using deep learning techniques?
- Q3 What are the challenges in the existing anomaly intrusion detection deep learning techniques in IoT?

4.5. The Review Protocol

The review protocol is known as one of the most crucial steps in establishing systematic literature reviews (SLRs). It provides an extensive guideline to determine the suitable and formal methods to be discussed in the SLR. The goal of adapting review protocols is to ensure that there is no bias and to distinguish SLR from any other traditional methods of the literature review [23]. This review protocol defines the review background, search strategy, development of RQs, extraction of data, criteria for study selection, and data syntheses. The research questions and background were discussed in previous sections.

The next sections provide insights on different components. All stages of conducting this systemic review are described in Figure 1.

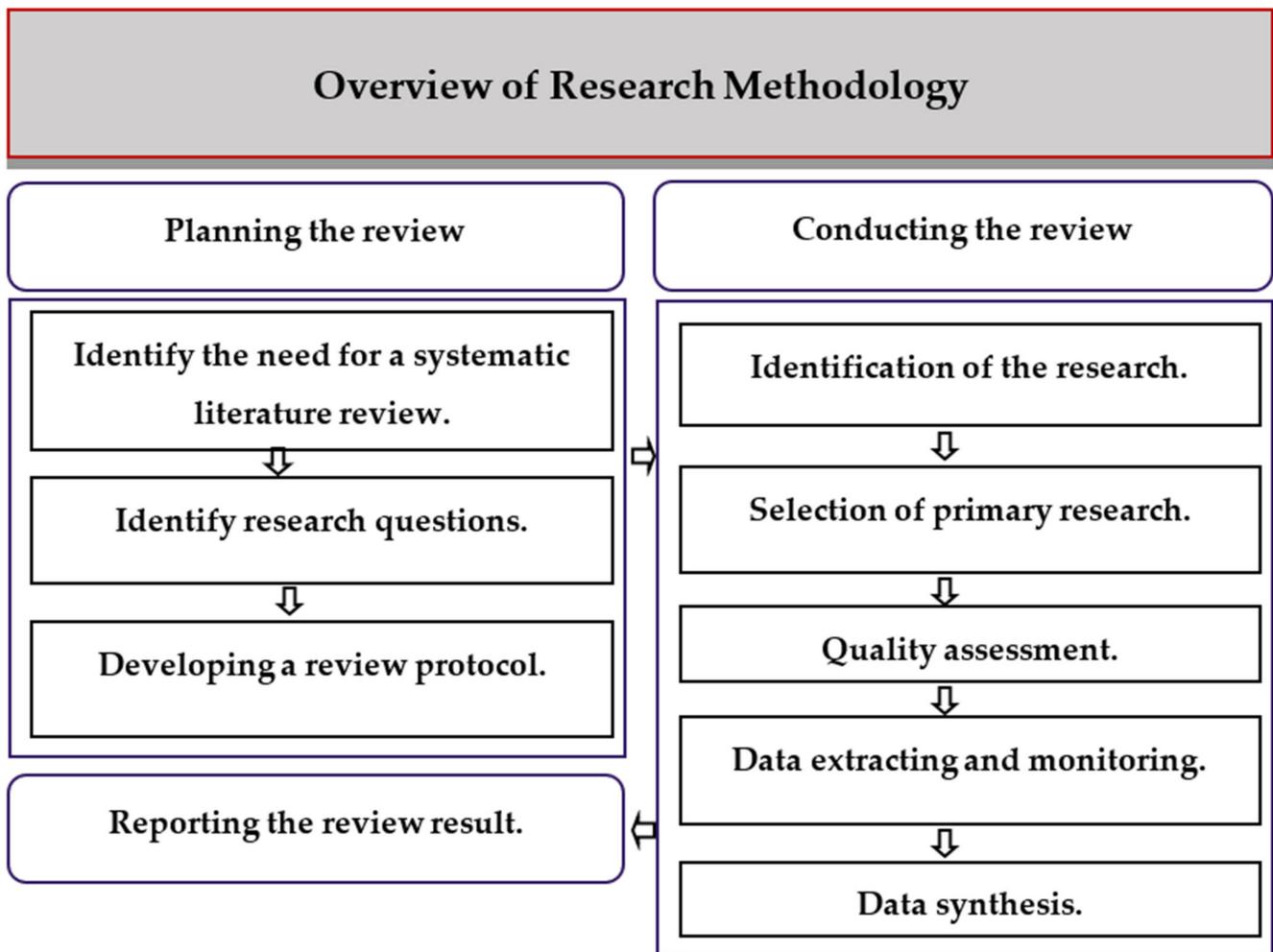


Figure 1. Literature review methodology.

5. Search Strategy

This SLR used automatic search to explore and retrieve the related scholarly publications from online databases (IEEE Explorer, Web of Science, Scopus, Science Direct, and MDPI), using specific keywords that were constructed in response to the research questions. “Anomaly intrusion detection” AND “Internet of things”, “Anomaly intrusion detection” AND “Deep learning”, “Anomaly intrusion detection system” AND “Internet of things”, “Anomaly intrusion detection system” AND “Deep learning”, “Anomaly-based” AND “Internet of things”, “Anomaly-based” AND “Deep learning”. The time frame was from any time up to 2020, while no filters were applied for countries, type of publications, or language during the retrieval of primary records from the online databases. The retrieval of primary records from the pre-specified online databases involved two independent investigators. If discrepancies occurred, a third investigator was consulted. For manual search, reference lists of published reviews and surveys were looked through, while the Google Scholar search engine was used to distinguish all studies that were cited by the chosen primary studies. The manual search was managed to ensure a comprehensive search of the pertinent studies. Any overlapping and redundancies in these publications were removed permanently.

5.1. Primary Records Selection

After the removal of duplicates, the remaining primary records were screened by titles and abstracts to exclude books, conferences, reports, lecture notes, and miscellany. This restricts selection to the original articles published in good-quality journals. The primary selection involved two independent investigators. If discrepancies occurred, a third investigator was consulted.

5.2. Secondary Records Selection

All the primary selected articles underwent secondary selection by applying eligibility criteria (exclusion and inclusion criteria), which were constructed in response to the research questions. Exclusion and inclusion criteria were employed to ensure the inclusion of only pertinent studies for data analysis regarding anomaly intrusion detection in IoT using deep learning.

5.3. Inclusion Criteria

1. Publication of articles in peer-reviewed journals.
2. Accessible research articles.
3. Relevant content to anomaly intrusion detection system in IoT, using deep learning.

5.4. Exclusion Criteria

1. Research articles published in predatory journals according to Beals' list.
2. Inaccessible articles.
3. Irrelevant to anomaly intrusion detection system in IoT using deep learning.

5.5. Quality Assessment (QA) of the Eligible Included Records

For pooling reliable data from the eligible studies, secondary selected records underwent assessment for their quality. Based on [25], a necessary step to be followed through to evaluate the quality of assorted studies was carried out by applying a quality assessment (QA). For evaluation purposes, a set of four research questions (RQs) were taken into consideration, including the following QA criteria:

1. QA1: Is the topic related to anomaly intrusion detection in IoT using deep learning techniques?
2. QA2: Is the research methodology adequately interpreted in the manuscript?
3. QA3: Is there an adequate clarification on the background review in which the study was conducted?
4. QA4: Is there a comprehensible declaration regarding the research objectives?

The reliability of each 42 research articles was assessed, according to each criterion mentioned in the four QA. There are three phases of QA quality schema, which are high, medium, and low [29]. The quality of each paper was assessed, based on its loading score. For a better context, papers that fulfill the criteria receive a score of two, whilst papers that only fulfill the criteria partially receive a score of one, and papers that did not fulfill any of the criteria receive a score of zero. In a scoring board, based on the four defined criteria, studies that receive a score of five or above can be categorized as high quality.

In contrast, studies that receive a score of four can be grouped as medium quality. Studies that receive a score below four will fall under the category of low quality. The studies that scored five and above after QA were then included in data extraction and synthesis. Two independent investigators reviewed the assessment of the quality of eligible studies. A discussion with a third investigator solved any discrepancies.

5.6. Data Extraction and Synthesis of the Systemic Literature Review

The data were extracted from the related studies that underwent the assessment for their quality. A form for better data extraction was created and performed thoroughly by using Endnote and Microsoft Excel spreadsheets to analyze and extract significant information from each eligible study. The extracted data included study ID, first author,

publication date, methodology, technique-based taxonomy, datasets, accuracy, precision, recall, False Alarm Rate (FAR), F1-Measure, False Positive Rate (FPR), and False Negative Rate (FNR). Extraction of the data from studies was performed by two independent investigators. Any discrepancies were solved by a discussion with a third investigator.

The data extracted were then synthesized for digressive analysis concerning issues associated with anomaly detection in IoT using deep learning, which includes strengths/weaknesses, classification, and approaches.

6. Results

6.1. Studies Selection and Quality Assessment

A total of 2116 records were extracted from the online database ($n = 2106$) and extra sources ($n = 10$); after the removal of duplicates ($n = 765$), 1351 records were subject to primary selection, out of which 714 records were excluded (books, lectures note, conferences and miscellaneous). Accordingly, 637 records were identified as journal articles, out of which 97 records were excluded (reviews, surveys, and reports). Finally, 540 records were subjected to inclusion and exclusion criteria, out of which 43 studies were eligible. However, only 26 studies met the criteria of quality assessment. The 26 studies that fulfill the assessment criteria were selected to extract the data and synthesis of the systemic literature review. Table 2 shows the number of retrieved records from online databases according to the pre-specified keywords. Figure 2 shows the fellow chart of selection studies.

Table 2. Number of retrieved records from online databases according to the pre-specified keywords.

Database Name	Keywords	Records	Total
IEEE explore	"Anomaly intrusion detection" AND "Internet of things"	113	1263
	"Anomaly intrusion detection" AND "Deep learning"	109	
	"Anomaly intrusion detection system" AND "Internet of things"	96	
	"Anomaly intrusion detection system" AND "Deep learning"	96	
	"Anomaly-based" AND "Internet of things"	411	
	"Anomaly-based" AND "Deep learning"	442	
Science direct	"Anomaly intrusion detection" AND "Internet of things"	6	344
	"Anomaly intrusion detection" AND "Deep learning"	4	
	"Anomaly intrusion detection system" AND "Deep learning"	1	
	"Anomaly-based" AND "Internet of things"	188	
	"Anomaly-based" AND "Deep learning."	144	
Scopus	"Anomaly intrusion detection" AND "Internet of things"	4	138
	"Anomaly intrusion detection" AND "Deep learning"	12	
	"Anomaly intrusion detection system" AND "Deep learning"	2	
	"Anomaly-based" AND "Internet of things"	4	
	"Anomaly-based" AND "Deep learning"	69	
		47	
Web of science	"Anomaly intrusion detection" AND "Internet of things"	3	71
	"Anomaly intrusion detection" AND "Deep learning"	6	
	"Anomaly intrusion detection system" AND "Deep learning"	2	
	"Anomaly-based" AND "Internet of things"	2	
	"Anomaly-based" AND "Deep learning"	36	
		22	
MDPI	"Anomaly intrusion detection" AND "Internet of things"	40	290
	"Anomaly intrusion detection" AND "Deep learning"	39	
	"Anomaly intrusion detection system" AND "Internet of things"	20	
	"Anomaly intrusion detection system" AND "Deep learning"	20	
	"Anomaly-based" AND "Internet of things"	90	
	"Anomaly-based" AND "Deep learning"	81	
Other sources	"Anomaly intrusion detection" AND "Internet of things"	2	10
	"Anomaly intrusion detection" AND "Deep learning"	1	
	"Anomaly intrusion detection system" AND "Internet of things"	2	
	"Anomaly intrusion detection system" AND "Deep learning"	1	
	"Anomaly-based" AND "Internet of things"	2	
	"Anomaly-based" AND "Deep learning"	2	

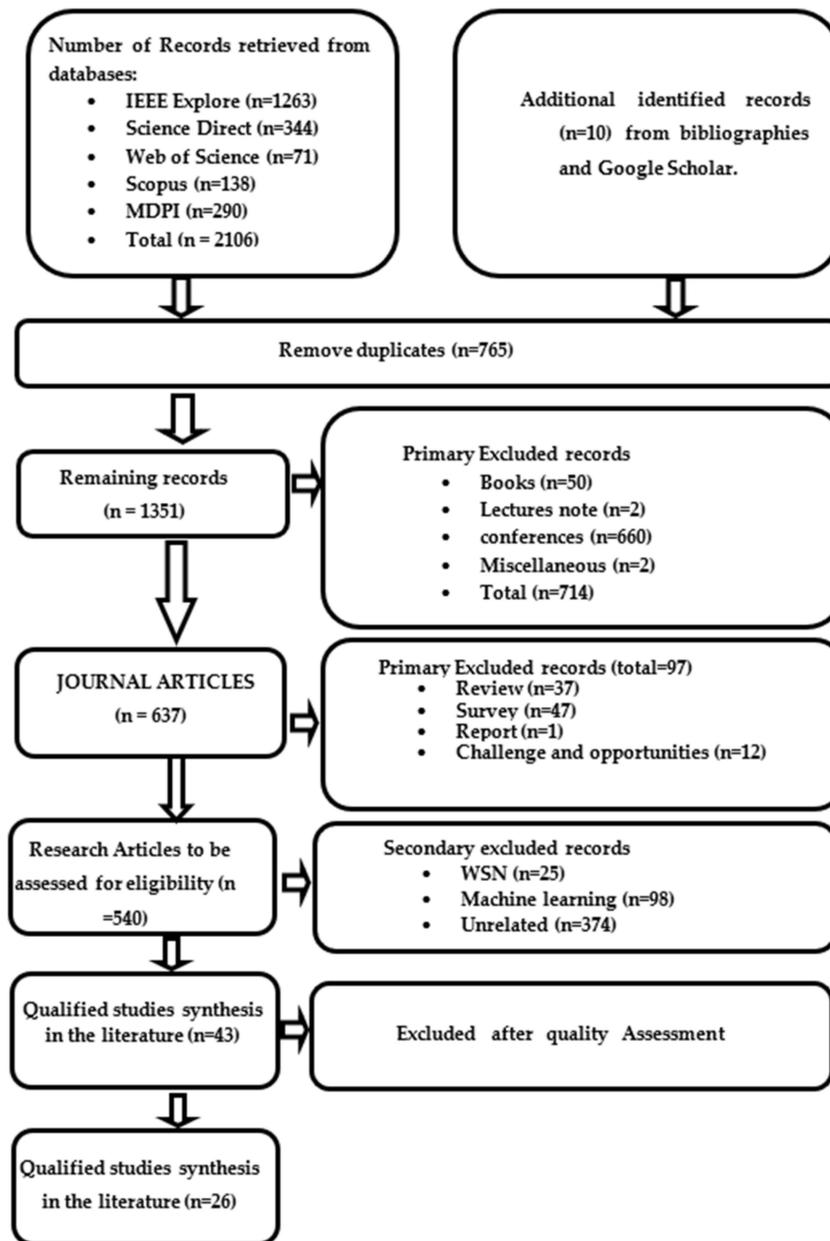


Figure 2. The fellow chart of selection studies.

6.2. Overview of Publication Sources

Figures 3 and 4 illustrate the list of selected papers published according to year and journal. Noticeably, there is a trend toward anomaly-based intrusion detection in IoT, using deep learning. This signifies a rising interest in this domain, especially after 2018. An elevated increase of nine studies in 2020 was noted, compared to only five studies in 2019. In comparison, the trend seems to start in 2017, as there was only one study published.

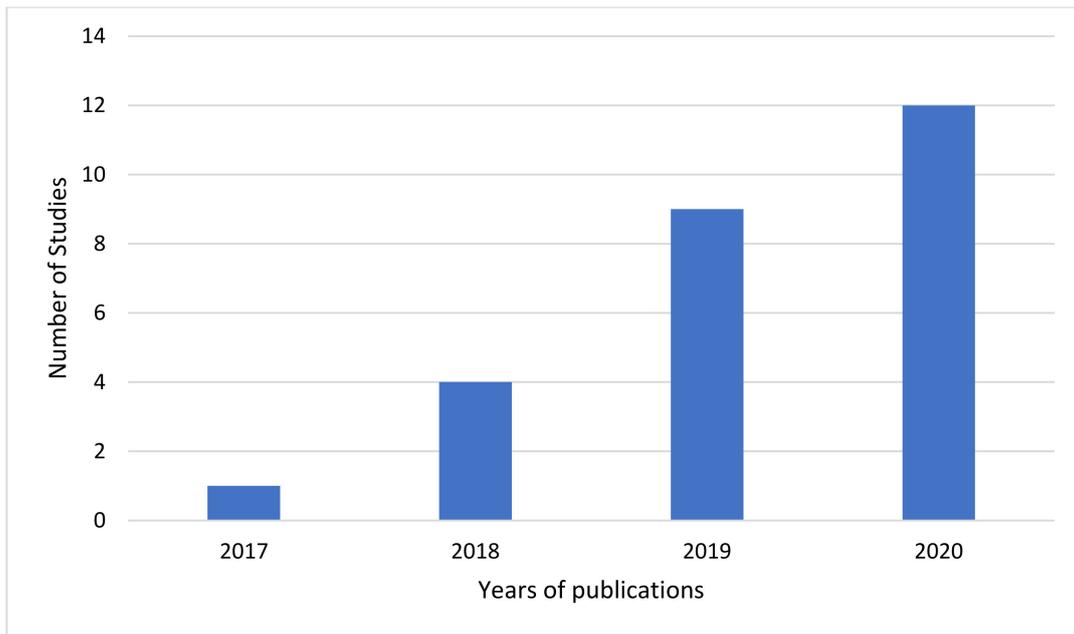


Figure 3. Selected distribution studies by years.

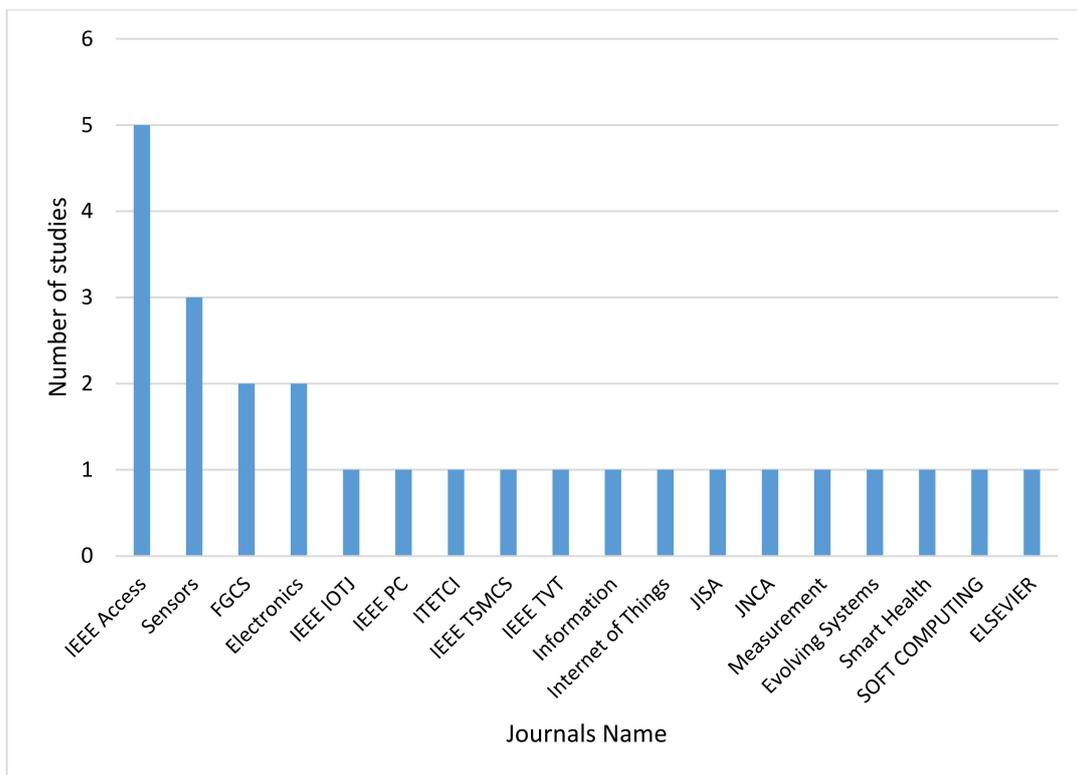


Figure 4. Selected distribution studies by journals.

7. Outcomes

7.1. RQ1: What Is the Comprehensive Taxonomy of Anomaly Intrusion Detection in IoT Using Deep Learning Techniques?

Recently, various studies have explored the application of anomaly detection in IoT using deep learning. For better insight, taxonomy is shown in Figure 5 to pinpoint all existing techniques and requirements of anomaly intrusion detection in IoT, using deep

learning techniques. The IDS are commonly categorized as supervised, unsupervised, and semi-supervised.

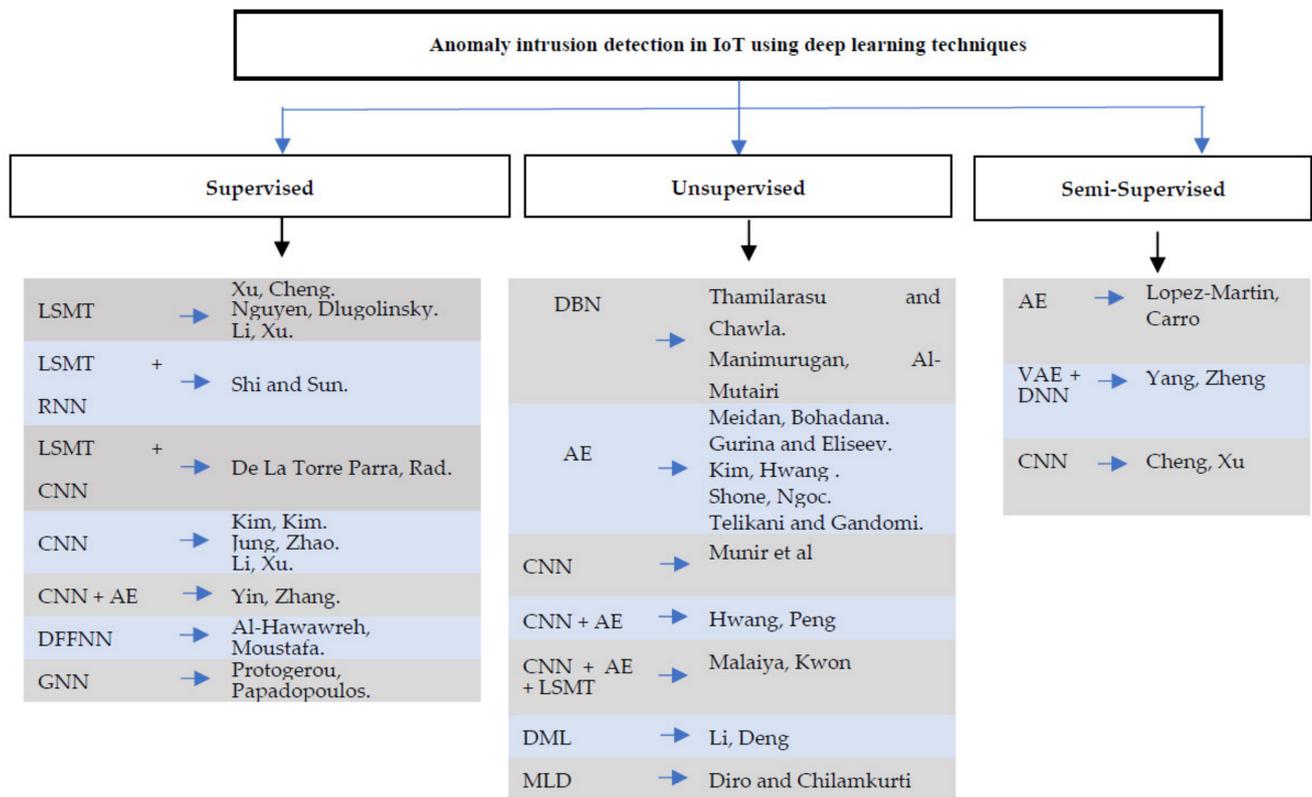


Figure 5. Taxonomy of anomaly intrusion detection in IoT using deep learning techniques [13–17,30–49].

- **Supervised:** in a supervised manner, anomalies detecting labeled datasets by constructing the network or system is normal behavior. Supervised anomaly detection techniques can leverage the measurement of distance as well as the density of clusters for the detection of intrusions.
- **Unsupervised:** in an unsupervised manner, the approach assumes a greater frequency of normal behaviors, thus leading to the establishment of the model on assumptions, wherein there is no need for any labeled data for training.
- **Semi-supervised:** in a semi-supervised manner, the algorithm is trained upon a combination of labeled and unlabeled data.

7.2. RQ2: What Is the Performance of Anomaly Intrusion Detection in IoT Using Deep Learning Techniques?

Accuracy, precision, recall, false-positive rate (FPR), false-negative rate (FNR), and f-measure are the most frequently employed model evaluation techniques based on deep learning [50–54].

As shown in Table 3, the high accuracy is nearly 100%; precision and recall are almost 100% in D-PACK [45]. They used CNN and AE techniques on the Mirai-RGU dataset. However, this model takes a long time for training and preprocessing, which is resource consuming. Additionally, it covers only a few types of attacks. Similarly, the study conducted by [37] used CNN and AE techniques on the Yahoo Webscope S5 dataset and achieved 99.62% accuracy, 98.78% precision, and 97.2% recall. This indicates that the combination of CNN and AE may improve the performance. Nevertheless, the resource-consuming aspect, network overhead, and datasets with real IoT traffic should be considered as well. D. Li et al. [47] proposed a model that achieved an accuracy of 99.78%, precision of 98.99%, recall of 91.05%, and FAR of 0.22%, using DML techniques by using

the KDDUP99 dataset. However, this model suffers from high resource consumption, and the dataset does not contain IoT traffics and modern types of attacks. Shi and Sun [16] proposed a model that achieved 99.36% accuracy, the precision of 97.97%, and recall of 98.86%, using LSTM with RNN techniques. However, they did not report the FAR, as the model is for a specific type of attack and is resource consuming. We can say that combining AE with CNN techniques could enhance the accuracy and decrease the FAR, but we should consider the resource consumption and cover the IoT attacks. Figure 6 shows the frequency of the performance measures of the studies.

Table 3. Performance of the studies models.

Study	Techniques	Accuracy	Precision	Recall	FAR	F1-Measure	FPR	FNR
Lopez et al. [48]	AE	80%	81.59%	80.1%		79.08%		
Yang et al. [15]	VAE + DNN	89.08%	86.05	95.68		90.61	19.01	
Cheng et al. [30]	LSTM	98%						
Thamilarasu et al. [14]	DBN		97%					
Shi et al. [16]	LSTM + RNN	99.36%	97.97%	98.86%		98.42		
Munir et al. [17]	CNN	99%	100%					
Gurina et al. [41]	AE				0.007			
Manimurugan et al. [40]	DBN	98.37%	97.21%	98.34%		97%		
Malaiya et al. [46]	CCN + VAE + LSTM	99%						
Kim et al. [34]	CNN	99%						
Jung et al. [35]	CNN	96.50%				85%		
Gurina et al. [42]	AE							
Diro et al. [13]	Multi-Layer deep learning	99.02%		99.27%	99.14%	0.85%		
Parra et al. [33]	CNN + LSTM	94.30%	93.48%	93.67%		93.58%	5.20%	
Cheng et al. [49]	CNN	99.88%	99.89%	97.94%		98.64%		
Moustafa et al. [38]	DFNN	98.4%, 92.5%		99%, 93%			1.8%, 8.2%	
Xie et al. [31]	LSTM							
Zhao et al. [36]	CNN	86.95% 76.67%						
Li et al. [32]	LSTM	97.58%		83.79%	2.02%			6.02%
Kim et al. [43]	AE	99.81%						
Hwang et al. [45]	CNN + AE	100%	100%	100%		100%	0%	
Yin et al. [37]	CNN + AE	99.62%	98.78%	97.2%		98.78%		
Telikani et al. [44]	AE	99.6	100%	100%	100%	0.0057		
Shone et al. [18]	AE	97.85%	100%	100%		85.42%		
Drosou et al. [39]	GNN/RNN	99%						
Deng et al. [47]	DML	99.78	98.99	91.05	0.22%			

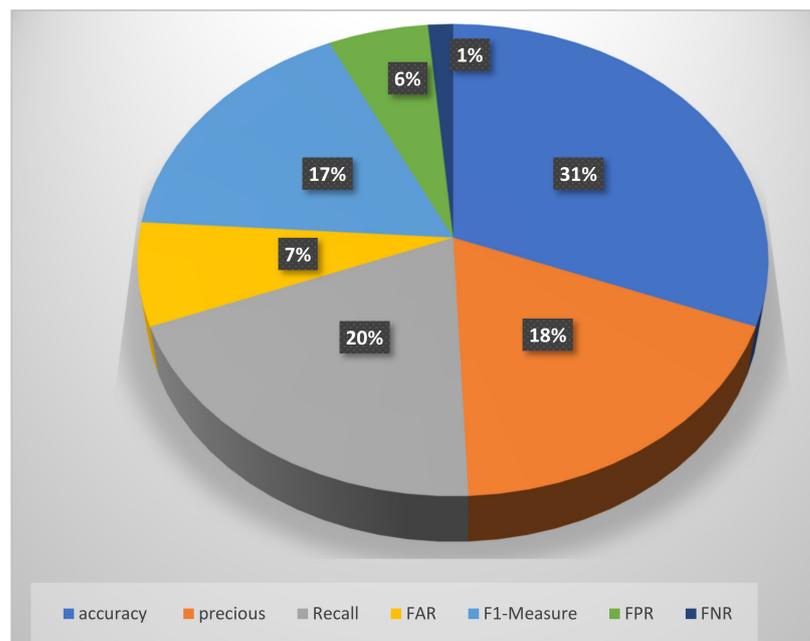


Figure 6. The frequency of performance measures of the studies.

7.2.1. Analysis of Accuracy Range

Table 4 shows the accuracy range for each deep learning technique used. The CNN has a wide range that starts from 76.76% and reaches 99.88%; this technique was tested 10 times individually and integrated with another technique. In addition, AE covers a wide range starting from 80% and reaches 99.81%, and it is similar to CNN in the detection accuracy range and the one used. LSTM was used three times and achieved an accuracy between 79.58% and 98%. DBN was used two times and gained an accuracy range from 97% to 97.21 with little enhancement. RNN and DFFNN were used once. Figure 7 shows the techniques used in the studies.

Table 4. Accuracy range for the techniques.

Study	No. of Study	Techniques Used	Accuracy Range
[17,34–36,49]	5	CNN	(76.76–99.88%)
[37,45]	2	CNN + AE	(99.62–100%)
[18,41–44,48]	6	AE	(80–99.81%)
[31,32]	3	LSTM	(79.58–98%)
[33]	1	CNN + LSTM	(94.30%)
[46]	1	CCN + VAE + LSTM	99%
[14,40]	2	DBN	(97–97.21%)
[15]	1	VAE + DNN	89.08%
[16]	1	LSTM + RNN	99.36%
[39]	1	GNN/RNN	99%
[38]	1	DFFNN	98.4%
[13]	1	Multi-Layer deep learning	99.02
[49]	1	DML	99.78

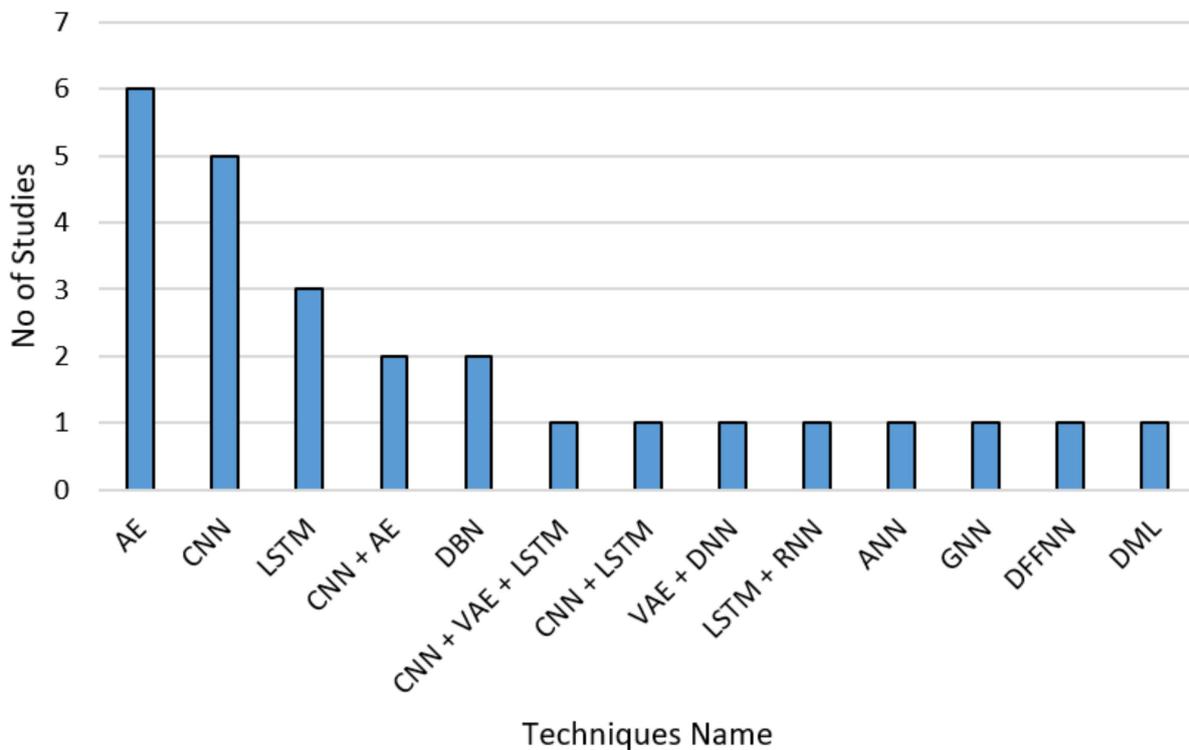


Figure 7. The frequency of the techniques used in the studies.

7.2.2. Analysis of Type of Attacks Detected

The type of attacks is the most important metric used to identify the advantage of the anomaly intrusion detection system. Some models [16,46,50] achieved high accuracy in detecting specific types of attacks. However, with only a few types of attacks included in their training datasets, their performance is questionable. Therefore, these models need more improvement to be able to detect as many attacks as possible with high accuracy. For example, in the IC_VAE model proposed by Lopez-Martin et al. [48], using the NSL-KDD dataset, the types of attacks detected by this model are Probing, Remote to Local (R2L), User to Root (U2R), and Denial of Service (DoS) Attacks. Similarly, studies proposed by [13,18,36,44,47] detected the same types of attacks, using NSL-KDD and KDD Cup 1999 datasets. Moreover, in [15,38], by adapting the NSL-KDD and UNSW-NB15, they extended the range of attack by detecting modern attacks, such as Fuzzer and worm, back door, analysis, exploits, generic, seel-code, and rectionary. In [34], by using KDD CUP 1999, CSE-CIC-IDS2018, they extended the range of attack by detecting modern attacks, such as DoS-Hulk, DoS-GoldenEye, DoS-SlowHTTPTest, DDoS-LOIC-HTTP, DoS-Slowloris, and DDoS-HOIC. The study conducted by [14] used a test-bed that contains several attacks, such as the Distributed Denial-of-Service (DDoS), sinkhole attack, Wormhole Attack, Black-hole Attack. In [40], authors used CICIDS 2017 dataset with a set of attacks, including DoS/DDoS, Botnet, Web Attack, Brute Force, Infiltration, PortScan, SQL Injection, Benign, DoS Hulk. In the study conducted by [45], the Mirai-RGU dataset with a range of attacks, including UDP Flood, SYN Flood, ACK Flood, and HTTP Flood, was used. In [41], by using N-balot databases, the authors focused on Mirai and BASHLITE. Similarly, in [33], the authors used the same dataset of N_BaIoT, but focusing on Distributed Denial of Service (DDoS) and phishing attacks. In [16], by using the MCFP dataset, they focused on Botnets, SYN flood, RST attacks. In [42], by using a test-bed, the range of attacks included flood attacks and SQL injection attacks, SYN Flood, TCP Flood, UDP Flood Detection, ICMP Flood Detection, and HTTP Flood Detection. In [35], the authors used a test-bed with a set of attacks against IoT, such as botnets attack, Mirai, Hajime, Bricker, BotIoT Reaper, Masuta, Sora. In [30], by using a test-bed, the range of the attacks included malicious scan, DoS attack, malicious control spying, malicious operation, wrong setting categories, and data probing. In [31], by using a test-bed, the range of attacks included sip, ssh, SSL, conn, DNS, and HTTP. In [39], by using a test-bed and CTU-13 datasets, the range of attacks included Infiltration attack, Propagation attack, worm infiltration, and worm propagation attack. In the study conducted by [43], the authors used the self-collection dataset and focused on interval attacks. In the studies [17,32,37,46,49], there was no report explaining what kinds of attacks they used.

The DL algorithms that were used in the previous studies prove their ability to detect a wide range of traditional types of attacks patterns, such as the attacks listed above. Moreover, DL algorithms perform better once there are huge amounts of attack data. However, more studies are needed to show the performance of the DL algorithms to detect the recent IoT attacks, such as physical attacks, privilege escalation, eavesdropping, brute-force password attacks, malicious node injection, and firmware hijacking.

7.2.3. Tools and Environments Applied by the Studied Work

Table 5 shows the categorization of the papers based on the tools and environments applied by the studied work. There are several types of development tools that have been used in such development, such as Python, MATLAB, and R language. As can be observed in Table 5, TensorFlow and Keras have been used by many researchers due to their ability to deal with large data and objects detected with high performance and provide high-level APIs for easily building and training models. Furthermore, it can run on Linux, macOS, Windows, and Android.

Table 5. Tools and environments applied by the studied work.

Study	Techniques	TensorFlow	Keras	Scikit	PyTorch	R	SoftMax	Raspberry Pi	Cooja	MATLAB	Python	Sigmoid	Hybrid Analysis Site	Entropy, K LD
Lopez et al. [48]	AE	✓		✓										
Yang et al. [15]	VAE + DNN	✓												
Cheng et al. [30]	LSTM				✓									
Thamilarasu et al. [14]	DBN		✓					✓	✓					
Shi et al. [16]	LSTM + RNN	✓	✓	✓										
Gurina et al. [41]	AE		✓											
Manimurugan et al. [40]	DBN	✓	✓							✓				
Malaiya et al. [46]	CCN + VAE + LSTM											✓		✓
Kim et al. [34]	CNN		✓									✓		
Jung et al. [35]	CNN									✓				
Gurina et al. [42]	AE									✓				
Diro et al. [13]	Multi-Layer deep learning		✓											
Parra et al. [33]	CNN + LSTM	✓												
Cheng et al. [49]	CNN				✓									
Moustafa et al. [38]	DFNN					✓								
Xie et al. [31]	LSTM	✓	✓											
Zhao et al. [36]	CNN	✓	✓											
Li et al. [32]	LSTM										✓			
Kim et al. [43]	AE												✓	
Hwang et al. [45]	CNN + AE	✓	✓											
Yin et al. [37]	CNN + AE										✓			
Telikani et al. [44]	AE						✓							
Shone et al. [18]	AE	✓												
Drosou et al. [39]	GNN/RNN				✓									
Deng et al. [47]	DML									✓				
Munir et al. [17]	CNN													

7.2.4. Analysis of the Used Datasets

Table 6 shows the datasets used by the existing research regarding deep learning in IoT security. As shown in Table 6, most of the studies used NLS_KDD and KDD CUP 1999. This is due to a lack of substitute datasets. However, these datasets are outdated and do not contain IoT traffic or modern types of attacks. Some modern datasets are now available that contain modern types of attacks—UNSW-NB15 [55] and IoT traffic BoT-IoT [56] we suggest for future researches. Table 7 shows the analysis of the most used datasets in the surveyed studies.

Table 6. The datasets used in the studies.

Study	Techniques	NSL-KDD	KDD CUP 1999	UNSW-NB15	CICIDS 2017	Mitral	CSE-CIC-IDS2018	N-BaIoT	Test-Bed	CTU-13	Gas-Water	AWID	Yahoo Webscope S5	Kyoto	MCFP	DS2OS	LOF	Synthetic
Lopez et al. [48]	AE	✓																
Yang et al. [15]	VAE + DNN	✓		✓														
Cheng et al. [30]	LSTM								✓									
Thamilarasu et al. [14]	DBN								✓									
Shi et al. [16]	LSTM + RNN								✓						✓			
Munir et al. [17]	CNN								✓									
Gurina et al. [41]	AE							✓										
Manimurugan et al. [40]	DBN				✓													
Malaiya et al. [46]	CCN + VAE + LSTM	✓												✓				

Table 6. Cont.

Study	Techniques	NSL-KDD	KDD CUP 1999	UNSW-NB15	CICIDS 2017	Mitrai	CSE-CIC-IDS2018	N-BaIoT	Test-Bed	CTU-13	Gas-Water	AWID	Yahoo Webscope S5	Kyoto	MCFP	DS2OS	LOF	Synthetic
Kim et al. [34]	CNN		✓				✓											
Jung et al. [35]	CNN								✓									
Gurina et al. [42]	AE								✓									
Diro et al. [13]	Multi-Layer deep learning	✓																
Parra et al. [33]	CNN + LSTM							✓										
Cheng et al. [49]	CNN															✓		
Moustafa et al. [38]	DFNN	✓		✓														
Xie et al. [31]	LSTM								✓									
Zhao et al. [36]	CNN	✓																
Li et al. [32]	LSTM									✓	✓	✓						
Kim et al. [43]	AE																✓	
Hwang et al. [45]	CNN + AE					✓												
Yin et al. [37]	CNN + AE												✓					
Telikani et al. [44]	AE	✓	✓															
Shone et al. [18]	AE	✓	✓															
Drosou et al. [39]	GNN/RNN									✓								✓
Deng et al. [47]	DML		✓															

Table 7. The analysis of the most used datasets in the surveyed studies.

Dataset	Published Year	IoT Specific	Features	No. of Classic	Total Normal Records	Total Attacks Records	Description
NSL-KDD	2009	NO	43	4	77,054	71,463	This dataset is an extension of the dataset “KDDCUP 99”. The duplicate records were removed and lack in modern large-scale attacks. Moreover, it is not IoT specific. It contains 22 attack types in the training dataset and 17 attack types in the test dataset, which are categorized as 4 attack classes.
KDD CUP 1999	1999	NO	43	4	1,033,372	4,176,086	This dataset does not contain modern attack data and modern large-scale attacks. Moreover, it contains unbalanced labels, and this dataset is not specific to the IoT.
UNSW-NB15	2015	NO	49	9	2,218,761	321,283	This dataset is based on a synthetic environment for generating attack activities. It contains approximately one hour of anonymized traffic traces from a DDoS attack in 2007.
CICIDS 2017	2017	NO	80	14	2,273,097	557,646	This dataset is not specific to the IoT. It contains complex features that are not present in previous datasets. However, it contains a modern large-scale attack.
CSE-CIC-IDS2018	2018	NO	80	18	N/A	N/A	This dataset is not specific to the IoT. However, it contains a modern large-scale attack.
N-BaIoT	2018	YES	115	8	17,936	831,298	This dataset contains IoT traffic, but it is unbalanced, due to the normal records being smaller than malicious records.
AWID	2015	NO	155	4	530,785	44,858	This dataset is not specific to the IoT. However, it contains modern types of attacks.
Yahoo Webscope S5/A1	2015	NO	-	-	93,197	1669	This dataset contains web traffic, which includes normal and attacks traffic. However, it is not specific to the IoT.
Kyoto	2006	NO	24	-	50,033,015	43,043,255	This dataset is not specific to the IoT. However, it contains modern types of attacks [57].

7.3. RQ 3: What Are the Challenges Faced in Current Anomaly Intrusion Detection Deep Learning Techniques in IoT?

7.3.1. Threat Detection

Because IoT supports a wide range of applications that need different resource requirements in terms of processing, storage, and communication, the network becomes more complex, due to the heterogeneity of the IoT devices that are being connected. This makes it hard to provide a secure environment in the IoT ecosystem and even harder to detect security threats. In securing an IoT environment, it is important to acknowledge the features and criteria necessary for applying security analytics in deep learning algorithms [54]. However, the existing mechanisms lack the effective and efficient methods that can perceive the hidden correlation between these features. Nevertheless, the rapid growth of deep learning algorithms is believed to have the capability of handling the hidden parameters not limited to the IoT application, but also for finding the correlation of data variation. In addition, a higher detection rate toward detecting zero-day attacks efficiently is obtainable with deep learning [58].

7.3.2. Computational and Resource Constraint

The computational complexity can be considered one of the prominent obstacles in the area of IoT security and deep learning. The usage of IoT devices requires a low battery and CPU power. Hence, the computational time in IoT devices should be quick, and the operation should be straightforward [59]. For better performance, it is more effective to mitigate the IoT computation to the edge of the cloud. There is one particular study [60] that emphasized analyzing the implementation of an algorithm that focuses on producing a lightweight computation system. The distributed computing and distributed algorithms provide better computational optimization by distributing the tasks over multiple nodes, which improves the efficiency [54,61].

7.3.3. Time Complexity

Time complexity is considered an obstacle because the current detection techniques were developed based on batch processing applications rather than real-time detection. As mentioned before, the IoT environment deals with real-data streaming. Hence, the time complexity is crucial in detecting threats in IoT applications. In addition, it can assess the impact on several attributes associated with security threats. Deep learning is highly capable of resolving time complexity issues in IoT by implementing GPU components to deal with real-time processing in an efficient manner [62].

7.3.4. Edge Computing and Security

An edge computing platform offers better extensibility in data processing and storage for resource-constrained IoT devices. Furthermore, it enables nearby devices located around the data sources to intelligently operate, even if they are far from the center node of infrastructure. The cloud infrastructure stores the IoT devices' data source regarding network computing to provide rational edge services in detecting real-time threats. Unfortunately, IoT as a standalone entity is incapable of storing and analyzing data for any potential threats, due to insufficient resources [63]. Hence, with the aid of edge computing, it will enable multiple resource distribution of data processing over the cloud for analysis [64]. It is convincible to state that the amalgamation of deep learning in IoT helps in facilitating security analytics in providing an enhanced processing system that can detect threats effectively and accurately [54].

7.3.5. Training Time

One of the major problems that existing techniques suffer from is the large and high dimensional datasets used for training [65]. Due to that, more time is needed to train the model for higher accuracy detection. In tackling these issues, deep learning algorithms are proposed because they can work on lesser training duration and dataset. This helps

to increase the efficiency during model training. The batch size may also affect the time consumed in the training phase because of the accumulation of the network onto the weight update [54,66]. To solve this, multiple layers can be used to build deep learning networks, which facilitates the weighing and recognizing of the set of significant patterns from the datasets. Furthermore, the exploits of storage and processing facilities additionally obstruct the model training time. Dealing with this issue, the adaptation of big cloud-based architecture and data technologies improve the efficiency by reducing the model training duration [63].

8. Discussion

We found that the trend goes to AE techniques. The studies [18,41–44,48] used AE techniques because of the ability of AE to take advantage of the linear and nonlinear dimensionality reduction to detect the anomalies. The AE training phase involves the reconstruction of clean input data from a partially destroyed one as well as the ability of AE to deal with heterogeneity, unstructured and high dimensional data that generated from IoT device. However, using techniques such as CNN combined with AE would be preferable for better classification, depending on the data reduction from the AE phase. Another observed five studies used CNN techniques [17,34–36,49], which can automatically detect the most important feature and learn the key feature of each class by itself without human intervention. Moreover, CNN can perform identification and prediction through the dense network. The CNN considered is a very vast technique, and this may be due to the ConvNets. Other factors that may affect the efficiency of CNN are filters, kernel size, stride, and padding. However, using techniques such as AE combined with CNN would be preferable to reduce the high dimensional data, which generate from IoT devices to minimize the exchange data between IoT nodes to avoid the energy-consuming and communication overhead.

In addition, we found that three studies used LSTM techniques [30–32] that are useful for classifying, processing, and predicting time series in long duration. Moreover, they have a memory that can store previous time step information, and this is how they learn. They also can deal with noise distributed representation and continuous value. However, LSTMs are apt for overfitting, and it is not easy to apply the dropout algorithm to restrain this problem. Combining CNN with AE [37,45] could achieve a promising result in terms of accuracy, recall, and precision. However, the researcher and developer should consider the resource consumption, training time, and the type of attacks. Notably, the AE and CNN are the most common techniques used in the literature. In addition, some studies used a single technique, and others combined multiple ones to improve the performance [16,46,47]. However, the FAR needs to be decreased when considering different types of attacks in the used dataset. Datasets that include a wide range of attacks with simulation tools are suggested above. In addition, still, some DL techniques have not been examined yet, which makes the need for more work in the area to achieve robust IDS for resource-constrained IoT devices. Combining two DL could lead to achieving high detection attacks, but it may lead to resource consumption and a high training time. The datasets used in the literature are outdated, perhaps due to a lack of substitute datasets. However, these datasets are outdated and do not contain IoT traffic or modern types of attacks. Some modern datasets are now available that contain modern types of attacks; UNSW-NB15 [55] and IoT traffic BoT-IoT [56] we suggest for future research. In addition, there is a need for new datasets that reflect the IoT traffic. Table 8 shows the domain of state-of-the-art studies, IDS architecture, the technique used, and methodology as well as the advantages and disadvantages.

Table 8. List of the state-of-the-art studies and the advantages and disadvantages.

Study	IDS Architecture	Techniques Used	Methodology	Advantages	Disadvantages
Lopez et al. [48]	Network-based	AE	proposed Model to perform feature reconstruction and detect malicious in IoT environment.	<ul style="list-style-type: none"> • Lightweight. • High accuracy in recover categorical features. 	<ul style="list-style-type: none"> • Low detection accuracy. • High training time.
Yang et al. [15]	Network-based	VAE + DNN	proposed model to perform monitoring unknown attacks using AE and DNN to learn the complex traffics and imbalanced classes.	<ul style="list-style-type: none"> • Lightweight. • Low resource consumption. 	<ul style="list-style-type: none"> • Low detection accuracy. • High training time.
Cheng et al. [30]	Network-based	LSTM	proposed model that adopts an innovative concept of the drift method to improve the accuracy of anomaly detection using LSTM.	<ul style="list-style-type: none"> • High detection accuracy. • work well for time series. • Memory effective. 	<ul style="list-style-type: none"> • Multi-classification method needs to be enhanced.
Thamilarasu et al. [14]	Network-based	DBN	Proposed an intelligent IDS to detect malicious traffic in IoT networks using DBN.	<ul style="list-style-type: none"> • Real-Time IDS. 	<ul style="list-style-type: none"> • Detection accuracy needs to be enhanced.
Shi et al. [16]	Network-based	LSTM + RNN	Proposed approach is to analyze a series of network packets to detect botnets using LSTM and RNN for better classification.	<ul style="list-style-type: none"> • Enhanced robustness. • High detection accuracy. • Lightweight. 	<ul style="list-style-type: none"> • Few types of attacks. • High false-positive rate. • Resources consuming.
Munir et al. [17]	Network-based	CNN	Proposed DeepAnTmodel to anomaly detection and time series prediction.	<ul style="list-style-type: none"> • High detection accuracy. • Detect point anomalies, contextual anomalies. • Model works well with a vast amount of data. 	<ul style="list-style-type: none"> • High computational time. • Poor data quality can corrupt the data modeling phase.
Gurina et al. [41]	Network-based	AE	Proposed N-BaIoT to extract network traffics and detect anomalies from resource constraint devices.	<ul style="list-style-type: none"> • Enhanced robustness • Efficient time to detect attacks. 	<ul style="list-style-type: none"> • Low traffic prediction. • Detection accuracy not reported.
Manimurugan et al. [40]	Centralized Host-Based	DBN	Proposed approach to detect anomaly attacks in IoT environment.	<ul style="list-style-type: none"> • High detection accuracy. • Lightweight. 	<ul style="list-style-type: none"> • Not a Real-Time IDS. • Detect few types of IoT attacks.
Malaiya et al. [46]	Network-based	CCN + VAE + LSTM	Proposed approach to detect anomaly in IoT networks by combining three deep learning techniques.	<ul style="list-style-type: none"> • High detection accuracy. • Lightweight. 	<ul style="list-style-type: none"> • Resource-consuming. • High computational complexity.
Kim et al. [34]	Network-based	CNN	Proposed approach to detect anomaly in IoT environment with focusing on DoS attacks.	<ul style="list-style-type: none"> • High detection accuracy. • Lightweight. 	<ul style="list-style-type: none"> • Detect few types of IoT attacks. • High computational complexity.
Jung et al. [35]	Host-based	CNN	Proposed approach to monitoring malicious botnet on resource constraint IoT devices using three types of IoT devices.	<ul style="list-style-type: none"> • Good classification accuracy. • Real-Time IDS. 	<ul style="list-style-type: none"> • Expensive power monitor. • Detection accuracy needs to be enhanced. • High computational complexity.
Gurina et al. [42]	Host-based	AE	Proposed approach to detect malicious in web server during users' requests processing considering the MyBB web server as a case study.	<ul style="list-style-type: none"> • Lightweight. • capable to detect zero-day attacks. • High detection accuracy for individual attacks. 	<ul style="list-style-type: none"> • High False positive rate. • High computational complexity. • No comparison with previous methods.

Table 8. Cont.

Study	IDS Architecture	Techniques Used	Methodology	Advantages	Disadvantages
Diro et al. [13]	Distributed Network-Based	Multi-Layer deep learning	Proposed a distributed approach to detect attacks in social IoT.	<ul style="list-style-type: none"> • Lightweight • High detection accuracy. • Low resource consumption. 	<ul style="list-style-type: none"> • Few types of attacks. • High training time.
Parra et al. [33]	Distributed Network-Based	CNN + LSTM	Proposed a distributed cloud-based approach to detect and mitigate phishing and Botnet attacks on client devices.	<ul style="list-style-type: none"> • Lightweight. • Low communication overhead. 	<ul style="list-style-type: none"> • Detection accuracy needs to be enhanced. • High computational complexity.
Cheng et al. [49]	Centralized Host-Based	CNN	Proposed a semi-supervised based model to detect anomalies in IoT communication.	<ul style="list-style-type: none"> • Lightweight • High detection accuracy. 	<ul style="list-style-type: none"> • High computational complexity.
Moustafa et al. [38]	Network-based	DFNN	Proposed anomaly detection to learn and validate the information collected from TCP/IP packets.	<ul style="list-style-type: none"> • Lightweight • High detection accuracy. • Model covered vast types of attacks. 	<ul style="list-style-type: none"> • Not a Real-Time IDS.
Xie et al. [31]	Network-based	LSTM	Proposed approach to monitor and detect malicious from the network traffic flow.	<ul style="list-style-type: none"> • Lightweight. • work well for time series. 	<ul style="list-style-type: none"> • Detection accuracy not reported.
Zhao et al. [36]	Network-based	CNN	Proposed approach to detect intrusion in industrial IoT.	<ul style="list-style-type: none"> • Enhanced robustness. • Lightweight. 	<ul style="list-style-type: none"> • Detection accuracy needs to be enhanced. • High computational complexity.
Li et al. [32]	Network-based	LSTM	Proposed approach to detect attack interval from historic data in industrial IoT.	<ul style="list-style-type: none"> • Enhanced robustness. • Lightweight. • High detection accuracy. 	<ul style="list-style-type: none"> • High computational complexity.
Kim et al. [43]	Host-based	AE	Proposed approach to the analysis of attack profile, detect the threats and abnormal behavior that deviates from normal behavior in IoT devices.	<ul style="list-style-type: none"> • Enhanced robustness. • Lightweight. • High detection accuracy. 	<ul style="list-style-type: none"> • High training time.
Hwang et al. [45]	Network-based	CNN + AE	Proposed D-PACK anomaly approach to detect features and profiling traffic with just a few first packets from each flow in IoT networks.	<ul style="list-style-type: none"> • High detection accuracy. • Lightweight. • Low false alarm rate. 	<ul style="list-style-type: none"> • High computational complexity. • High training time. • Focusing on few types of attacks.
Yin et al. [37]	Network-based	CNN + AE	Proposed approach to detect the anomaly and to enhance classification in time series.	<ul style="list-style-type: none"> • High detection accuracy. • Lightweight. • Low false alarm rate. 	<ul style="list-style-type: none"> • High computational complexity. • High training time.
Telikani et al. [44]	Network-based	AE	Proposed CSSAE (cost-sensitive stacked auto-encoder) to solve the class imbalance problem in IDS and detect low-frequency attacks in IoT environment.	<ul style="list-style-type: none"> • High detection accuracy. • Lightweight. • Low false alarm rate. 	<ul style="list-style-type: none"> • High training time.
Shone et al. [18]	Network-based	AE	Proposed model to dimensionality reduction for the data and detect malicious at the IoT environment.	<ul style="list-style-type: none"> • High detection accuracy. • Lightweight. 	<ul style="list-style-type: none"> • High false alarm rate. • High training time.

Table 8. Cont.

Study	IDS Architecture	Techniques Used	Methodology	Advantages	Disadvantages
Drosou et al. [39]	Distributed Network-based	GNN/ RNN	Proposed collaborative anomaly intrusion detection to detect malicious for IoT devices.	<ul style="list-style-type: none"> • High detection accuracy. • Lightweight. 	<ul style="list-style-type: none"> • High computational complexity. • Power consumption.
Deng et al. [47]	Network-based	DML	proposes an approach to detect malicious and feature extraction for smart cities.	<ul style="list-style-type: none"> • High detection accuracy. • Lightweight. • Low false alarm rate. 	<ul style="list-style-type: none"> • High computational complexity.

Table 8 also shows that there are many types of IDS architectures that have been implemented. Network-based IDS is the most applied architecture, due to the availability of labeled network traffic datasets. In the IoT networks, the architecture of the IDS depends on the application domain and the host environment [2]. The host-based approach is recommended to protect the operating system of the IoT devices from malicious attacks, while the network-based is suitable for protecting the communicated devices from malicious traffic. Most studies applied the network-based architecture, while the nature of IoT is heavily distributed. It will be more effective if the researchers and developers pay more attention to combining host-based architecture with those that are network-based in a distributed and hierarchical architectural design manner to minimize the detection time, improve the detection accuracy, and decrease the network's overhead.

9. Future Direction

Undoubtedly, improving the efficiency of deep learning detection results remains an open research direction issue. IoT security researchers and developers must always contend for 100% detection with zero false alarms while considering IoT resource constraints. Moreover, most of the studies are pertinent to the system's normal behavior. Often, most of the approaches depend on the training of normal behavior, while the deviation is pertinent to scenarios investigated as abnormal behavior. Thus, a better method in terms of precision and robustness is needed to deal with complex real scenarios. Data complexities include unexpected noise, redundancy in data, and imbalanced datasets. To extract significant knowledge and information, well-designed techniques are required to organize the datasets. In this scenario, a lightweight system can be exhaustive, due to the high computational task of dealing with complex data. The current technology of cloud computing can be utilized to obtain a productive result in real time. Most of the work done in recent years was in the detection of anomalies, as the research community did not foster much interest in anomaly prediction and prevention. This could contribute to predicting anomalies in future work. There is a need to adopt and/or develop new methods that can prevent the systems before attacks occur. Moreover, anomaly detection in multivariable time series is still an open research direction. In addition, applying anomaly intrusion detection systems, using deep learning in smart vehicles, needs to be investigated. There is an imperious need for normal and anomaly datasets that are up-to-date and integrated with IoT applications and services. These datasets could be extremely useful for testing various IDS types and methods in IoT environments. The capability to implement effective and meaningful IDS comparisons will rely on these datasets.

10. Limitation of the Study

Throughout the review study, the SLR is performed to provide extensive coverage of all relevant studies associated with the use of deep learning techniques in securing IoT environments. The main limitation of this study is in searching. There are also few limitations of the SLR that should be taken into consideration, which are listed as the following:

1. This review is limited to articles and does not include books, magazines, and conferences related to deep learning in IoT.
2. This review is limited to papers available in the English language.

11. Conclusions

In general, this study presented a systematic review of anomaly IDSs in IoT environments using deep learning. A comprehensive report was produced, regarding anomaly intrusion detection in the domain of IoT, using deep learning techniques. Upon completion of this study, a full adherence of systematic literature protocol and guidelines based on proposed work by Kitchenham is presented [25]. All the data used were gathered from primary studies published without applying any filters to differentiate between conference proceedings and journal articles. This study summarized and organized the current literature related to anomaly-based intrusion detection in IoT, using deep learning techniques according to the pre-defined keywords and RQs. A total number of 26 studies were included, according to the stated exclusion, inclusion, and quality criteria. A comprehensive taxonomy was presented based on the results of the study conducted for anomaly intrusion detection in IoT using deep learning techniques. This study provided an insight into the attributes and knowledge of existing anomaly intrusion detection in an IoT environment, using deep learning techniques. Additionally, the study presented a comparison in terms of the performance, the dataset used, attacks detection, techniques, and evaluation techniques in each study. Finally, the study discussed challenges faced in anomaly intrusion detection in IoT using deep learning. This paper can provide researchers with details about an up-to-date technique and methodology in anomaly intrusion detection in IoT, using deep learning. The limitations of current anomaly-based intrusion detection systems in IoT using deep learning techniques indicate the future direction for further improvements of the IDS systems, considering the characteristics of IoT.

Author Contributions: Conceptualization, M.A.A.; methodology, M.A.A.; resources, M.A.A., F.A.G., F.S. and M.N.; data curation, M.A.A., F.A.G. and M.N.; writing—Original draft preparation, M.A.A.; writing—Review and editing, S.R., M.M.S., F.A.G., I.N. and F.S.; supervision, S.R. and M.M.S.; project administration, S.R.; funding acquisition, S.R. and I.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by Ministry of Higher Education Malaysia under the Research Excellence Consortium in IoT Security (VOT R.J130000.7851.4L946).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Atzori, L.; Iera, A.; Morabito, G. Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Netw.* **2017**, *56*, 122–140. [\[CrossRef\]](#)
2. Elrawy, M.F.; Awad, A.I.; Hamed, H.F.A. Intrusion detection systems for IoT-based smart environments: A survey. *J. Cloud Comput.* **2018**, *7*, 21. [\[CrossRef\]](#)
3. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243.
4. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [\[CrossRef\]](#)
5. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. *Simul. Model. Pract. Theory* **2020**, *101*, 102031. [\[CrossRef\]](#)
6. Moore, S.J.; Nugent, C.D.; Zhang, S.; Cleland, I. IoT reliability: A review leading to 5 key research directions. *CCF Trans. Pervasive Comput. Interact.* **2020**, *2*, 147–163. [\[CrossRef\]](#)
7. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access* **2020**, *8*, 32031–32053. [\[CrossRef\]](#)
8. Farooq, M.S.; Riaz, S.; Abid, A.; Abid, K.; Naeem, M.A. A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access* **2019**, *7*, 156237–156271. [\[CrossRef\]](#)

9. Ruan, J.; Wang, Y.; Chan, F.T.S.; Hu, X.; Zhao, M.; Zhu, F.; Shi, B.; Shi, Y.; Lin, F. A Life Cycle Framework of Green IoT-Based Agriculture and Its Finance, Operation, and Management Issues. *IEEE Commun. Mag.* **2019**, *57*, 90–96. [[CrossRef](#)]
10. Pal, S.; Hitchens, M.; Rabehaja, T.; Mukhopadhyay, S. Security Requirements for the Internet of Things: A Systematic Approach. *Sensors* **2020**, *20*, 5897. [[CrossRef](#)]
11. Ghaleb, F.A.; Maarof, M.A.; Zainal, A.; Rassam, M.; Saeed, F.; Alsaedi, M. Context-aware data-centric misbehaviour detection scheme for vehicular ad hoc networks using sequential analysis of the temporal and spatial correlation of the consistency between the cooperative awareness messages. *Veh. Commun.* **2019**, *20*, 100186. [[CrossRef](#)]
12. Hameed, S.; Khan, F.I.; Hameed, B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *J. Comput. Netw. Commun.* **2019**, *2019*, 9629381. [[CrossRef](#)]
13. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Futur. Gener. Comput. Syst.* **2018**, *82*, 761–768. [[CrossRef](#)]
14. Thamilarasu, G.; Chawla, S. Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. *Sensors* **2019**, *19*, 1977. [[CrossRef](#)] [[PubMed](#)]
15. Yang, Y.; Zheng, K.; Wu, C.; Yang, Y. Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network. *Sensors* **2019**, *19*, 2528. [[CrossRef](#)] [[PubMed](#)]
16. Shi, W.-C.; Sun, H.-M. DeepBot: A time-based botnet detection with deep learning. *Soft Comput.* **2020**, *24*, 16605–16616. [[CrossRef](#)]
17. Munir, M.; Siddiqui, S.A.; Dengel, A.; Ahmed, S. DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series. *IEEE Access* **2018**, *7*, 1991–2005. [[CrossRef](#)]
18. Shone, N.; Ngoc, T.N.; Phai, V.D.; Shi, Q. A Deep Learning Approach to Network Intrusion Detection. *IEEE Trans. Emerg. Top. Comput. Intell.* **2018**, *2*, 41–50. [[CrossRef](#)]
19. Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion detection systems in the Internet of things: A comprehensive investigation. *Comput. Netw.* **2019**, *160*, 165–191. [[CrossRef](#)]
20. Fahim, M.; Sillitti, A. Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review. *IEEE Access* **2019**, *7*, 81664–81681. [[CrossRef](#)]
21. da Costa, K.A.; Papa, J.P.; Lisboa, C.O.; Munoz, R.; de Albuquerque, V.H.C. Internet of Things: A survey on machine learning-based intrusion detection approaches. *Comput. Netw.* **2019**, *151*, 147–157. [[CrossRef](#)]
22. Chalapathy, R.; Chawla, S. Deep learning for anomaly detection: A survey. *arXiv* **2019**, arXiv:1901.03407.
23. Sharma, B.; Sharma, L.; Lal, C. Anomaly Detection Techniques using Deep Learning in IoT: A Survey. In Proceedings of the 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 11–12 December 2019; IEEE: Piscataway, NJ, USA, 2020.
24. Alsoufi, M.A.; Razak, S.; Siraj, M.M.; Ali, A.; Nasser, M.; Abdo, S. *Anomaly Intrusion Detection Systems in IoT Using Deep Learning Techniques: A Survey*; Springer International Publishing: Cham, Switzerland, 2021.
25. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; EBSE Technical Report; Keele University: Keele, UK, 2007.
26. Kitchenham, B.; Brereton, P. A systematic review of systematic review process research in software engineering. *Inf. Softw. Technol.* **2013**, *55*, 2049–2075. [[CrossRef](#)]
27. Milani, B.A.; Navimipour, N.J. A Systematic Literature Review of the Data Replication Techniques in the Cloud Environments. *Big Data Res.* **2017**, *10*, 1–7. [[CrossRef](#)]
28. Safaei, M.; Asadi, S.; Driss, M.; Boulila, W.; Alsaedi, A.; Chizari, H.; Abdullah, R.; Safaei, M. A systematic literature review on outlier detection in wireless sensor networks. *Symmetry* **2020**, *12*, 328. [[CrossRef](#)]
29. Nidhra, S.; Yanamadala, M.; Afzal, W.; Torkar, R. Knowledge transfer challenges and mitigation strategies in global software development—A systematic literature review and industrial validation. *Int. J. Inf. Manag.* **2013**, *33*, 333–355. [[CrossRef](#)]
30. Xu, R.; Cheng, Y.; Liu, Z.; Xie, Y.; Yang, Y. Improved Long Short-Term Memory based anomaly detection with concept drift adaptive method for supporting IoT services. *Futur. Gener. Comput. Syst.* **2020**, *112*, 228–242. [[CrossRef](#)]
31. Nguyen, G.; Dlugolinsky, S.; Tran, V.; Garcia, A.L. Deep Learning for Proactive Network Monitoring and Security Protection. *IEEE Access* **2020**, *8*, 19696–19716. [[CrossRef](#)]
32. Li, X.; Xu, M.; Vijayakumar, P.; Kumar, N.; Liu, X. Detection of Low-Frequency and Multi-Stage Attacks in Industrial Internet of Things. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8820–8831. [[CrossRef](#)]
33. Parra, G.D.L.T.; Rad, P.; Choo, K.-K.R.; Beebe, N. Detecting Internet of Things attacks using distributed deep learning. *J. Netw. Comput. Appl.* **2020**, *163*, 102662. [[CrossRef](#)]
34. Kim, J.; Kim, J.; Kim, H.; Shim, M.; Choi, E. CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. *Electronics* **2020**, *9*, 916. [[CrossRef](#)]
35. Jung, W.; Zhao, H.; Sun, M.; Zhou, G. IoT botnet detection via power consumption modeling. *Smart Health* **2020**, *15*, 100103. [[CrossRef](#)]
36. Li, Y.; Xu, Y.; Liu, Z.; Hou, H.; Zheng, Y.; Xin, Y.; Zhao, Y.; Cui, L. Robust detection for network intrusion of industrial IoT based on multi-CNN fusion. *Measurement* **2020**, *154*, 107450. [[CrossRef](#)]
37. Yin, C.; Zhang, S.; Wang, J.; Xiong, N.N. Anomaly Detection Based on Convolutional Recurrent Autoencoder for IoT Time Series. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, 1–11. [[CrossRef](#)]

38. Al-Hawawreh, M.; Moustafa, N.; Sitnikova, E. Identification of malicious activities in industrial internet of things based on deep learning models. *J. Inf. Secur. Appl.* **2018**, *41*, 1–11. [[CrossRef](#)]
39. Protopogerou, A.; Papadopoulos, S.; Drosou, A.; Tzovaras, D.; Refanidis, I. A graph neural network method for distributed anomaly detection in IoT. *Evol. Syst.* **2020**, *12*, 19–36. [[CrossRef](#)]
40. Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network. *IEEE Access* **2020**, *8*, 77396–77404. [[CrossRef](#)]
41. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-BalIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Comput.* **2018**, *17*, 12–22. [[CrossRef](#)]
42. Gurina, A.; Eliseev, V. Anomaly-Based Method for Detecting Multiple Classes of Network Attacks. *Information* **2019**, *10*, 84. [[CrossRef](#)]
43. Kim, S.; Hwang, C.; Lee, T. Anomaly Based Unknown Intrusion Detection in Endpoint Environments. *Electronics* **2020**, *9*, 1022. [[CrossRef](#)]
44. Telikani, A.; Gandomi, A.H. Cost-sensitive stacked auto-encoders for intrusion detection in the Internet of Things. *Internet Things* **2019**, *14*, 100122. [[CrossRef](#)]
45. Hwang, R.-H.; Peng, M.-C.; Huang, C.-W.; Lin, P.-C.; Nguyen, V.-L. An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection. *IEEE Access* **2020**, *8*, 30387–30399. [[CrossRef](#)]
46. Malaiya, R.K.; Kwon, D.; Suh, S.C.; Kim, H.; Kim, I.; Kim, J. An Empirical Evaluation of Deep Learning for Network Anomaly Detection. *IEEE Access* **2019**, *7*, 140806–140817. [[CrossRef](#)]
47. Li, D.; Deng, L.; Lee, M.; Wang, H. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. *Int. J. Inf. Manag.* **2019**, *49*, 533–545. [[CrossRef](#)]
48. Lopez-Martin, M.; Carro, B.; Sanchez-Esguevillas, A.; Lloret, J. Conditional Variational Autoencoder for Prediction and Feature Recovery Applied to Intrusion Detection in IoT. *Sensors* **2017**, *17*, 1967. [[CrossRef](#)] [[PubMed](#)]
49. Cheng, Y.; Xu, Y.; Zhong, H.; Liu, Y. Leveraging Semi-supervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT Communication. *IEEE Internet Things J.* **2020**, *8*, 144–155. [[CrossRef](#)]
50. Sokolova, M.; Lapalme, G. A systematic analysis of performance measures for classification tasks. *Inf. Process. Manag.* **2009**, *45*, 427–437. [[CrossRef](#)]
51. Powers, D.M. Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation. *arXiv* **2011**, arXiv:2010.16061.
52. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [[CrossRef](#)]
53. Marir, N.; Wang, H.; Feng, G.; Li, B.; Jia, M. Distributed Abnormal Behavior Detection Approach Based on Deep Belief Network and Ensemble SVM Using Spark. *IEEE Access* **2018**, *6*, 59657–59671. [[CrossRef](#)]
54. Amanullah, M.A.; Habeeb, R.A.A.; Nasaruddin, F.H.; Gani, A.; Ahmed, E.; Nainar, A.S.M.; Akim, N.M.; Imran, M. Deep learning and big data technologies for IoT security. *Comput. Commun.* **2020**, *151*, 495–517. [[CrossRef](#)]
55. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; IEEE: Piscataway, NJ, USA, 2016.
56. Koroniotis, N.; Moustafa, N.; Sitnikova, E.; Turnbull, B. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Botiot dataset. *Future Gener. Comput. Syst.* **2019**, *100*, 779–796. [[CrossRef](#)]
57. Song, J.; Takakura, H.; Okabe, Y. Description of Kyoto University Benchmark Data. 2006. Available online: http://www.takakura.com/Kyoto_data/BenchmarkData-Description-v5.pdf (accessed on 15 March 2016).
58. Tang, T.A.; Mhamdi, L.; McLernon, D.; Zaidi, S.A.R.; Ghogho, M. Deep learning approach for network intrusion detection in software defined networking. In Proceedings of the 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco, 26–29 October 2016; IEEE: Piscataway, NJ, USA, 2016.
59. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In Proceedings of the 2015 IEEE World Congress on Services, New York, NY, USA, 27 June–2 July 2015; IEEE: Piscataway, NJ, USA, 2015.
60. Kotenko, I.; Saenko, I.; Branitskiy, A. Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning. *IEEE Access* **2018**, *6*, 72714–72723. [[CrossRef](#)]
61. Vinayakumar, R.; Alazab, M.; Soman, K.P.; Poornachandran, P.; Al-Nemrat, A.; Venkatraman, S. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access* **2019**, *7*, 41525–41550. [[CrossRef](#)]
62. Guo, Y.; Liu, Y.; Oerlemans, A.; Lao, S.; Wu, S.; Lew, M.S. Deep learning for visual understanding: A review. *Neurocomputing* **2016**, *187*, 27–48. [[CrossRef](#)]
63. Kozik, R.; Choraś, M.; Ficco, M.; Palmieri, F. A scalable distributed machine learning approach for attack detection in edge computing environments. *J. Parallel Distrib. Comput.* **2018**, *119*, 18–26. [[CrossRef](#)]
64. Lu, Z.; Wang, N.; Wu, J.; Qiu, M. IoTDeM: An IoT Big Data-oriented MapReduce performance prediction extended model in multiple edge clouds. *J. Parallel Distrib. Comput.* **2018**, *118*, 316–327. [[CrossRef](#)]

-
65. Zhao, Z.; Kumar, A. Accurate periocular recognition under less constrained environment using semantics-assisted convolutional neural network. *IEEE Trans. Inf. Forensics Secur.* **2016**, *12*, 1017–1030. [[CrossRef](#)]
 66. HaddadPajouh, H.; Deghantaha, A.; Khayami, R.; Choo, K.-K.R. A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting. *Futur. Gener. Comput. Syst.* **2018**, *85*, 88–96. [[CrossRef](#)]