IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 January 2024, accepted 21 February 2024, date of publication 26 February 2024, date of current version 1 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3369915

SURVEY

Review on Approaches of Federated Modeling in Anomaly-Based Intrusion Detection for IoT Devices

UMAR AUDI ISMA'ILA[1], KAMALUDDEEN USMAN DANYARO[1], (Member, IEEE), AMINU AMINU MUAZU[1,2], AND UMAR DANJUMA MAIWADA[1,2]

[1]Department of Computer and Information Sciences, Faculty of Science and Information Technology, Universiti Teknologi PETRONAS, Seri Iskandar, Perak 32610, Malaysia
[2]Department of Computer Science, Faculty of Natural and Applied Sciences, Umaru Musa Yar'adua University, Katsina 820102, Nigeria

Corresponding author: Umar Audi Isma'ila (umar_22005104@utp.edu.my)

This work was supported in part by Universiti Teknologi PETRONAS (UTP) and the Yayasan Universiti Teknologi PETRONAS-Fundamental Research Grant (YUTP-FRG) through the project "Digital Twin Model for Structural Asset Monitoring Solution and Decision Making for Onshore Facilities" under Grant 015LC0-312.

ABSTRACT The novelty of Federated Learning (FL) has emerged as a promising alternative to centralized machine learning systems in the context of anomaly-based intrusion detection systems (AIDS) deployed on Internet of Things (IoT) devices. Unlike traditional centralized models, FL allows on-device model training and updates, reducing privacy concerns and issues such as single points of failure and high false alarm rates (FAR). This approach, termed 'Fed-AIDS,' offers a more secure and efficient solution. However, the development of Fed-AIDS models faces challenges related to limited training data and the diverse nature of IoT datasets. Additionally, FL's decentralized nature introduces weight divergence issues arising from non-Independently and Identically Distributed (non-IID) clients. To address these challenges and optimize Fed-AIDS modeling, interdisciplinary research efforts are vital. The primary objective of this study is to conduct an up-to-date review by adopting a Systematic Literature Review (SLR) approach to analyze existing studies of Fed-AIDS modeling procedures for IoT devices. Data from the published studies were retrieved from Scopus database, which covered major publishers such as IEEE, Elsevier and others. Specifically, our review conducted from the following Fed-AIDS perspectives: workflow and tools, training dataset, complexities of non-IID data in Fed-AIDS models, classification tasks, aggregation tasks, and model validation metrics. Based on the research findings, the study highlights a series of challenges and proposes potential solutions to stand in future research in Fed-AIDS modeling, aiming to advance the field of IoT device security.

INDEX TERMS Federated learning modeling, IoT devices, anomaly-based intrusion detection, aggregation function, non-IDD data.

I. INTRODUCTION

The rapid data production at the Internet of Things (IoT) network edge is growing exponentially owing to the increased demand for IoT devices by industries and individuals [1]. Notably, corporations such as Clarivate Analytics, Azure Data Lake, and Oracle, which rely on data evaluation for industry intelligence and market modeling interpretation to expand their services [2], give utmost priority to information provided by IoT. Consequently, the continuous advancement and adoption of IoT devices have expanded the attack surface, and the lack of security measures on many of these devices makes them easy targets for attackers. Thus, the continuous advancement and adoption of IoT devices has created a larger attack surface, and the lack of security measures on many of these devices makes them easy targets for attackers [3]. As a result, the number of attacks on IoT devices has potentially increased [4], [5], [6]. This exacerbate by the fact that many

The associate editor coordinating the review of this manuscript and approving it for publication was Claudia Raibulet.

IoT devices are designed to be always-on and connected to the internet, constantly transmitting data and potentially exposing themselves to attacks. Meanwhile, Machine Learning (ML) has been well known in IoT cybersecurity. Many researchers have become interested in Anomaly-based Intrusion Detection Systems (AIDS) [7], [8], [9], [10], [11], [12], which uses classification ML that forecasts a certain discrete value, such as anomalous or normal outcomes [8], [13]. This employs the centralized approach to train the model, that needing the concentration of training data in a single server [14], [15]. However, given the volume and severity of the data shared by smart devices in centralized IoT scenarios, thus, the impact of attack such of DoS and DDoS on a single device can have unpredictable consequences for other devices [16], [17].

Consequently, Federated Learning (FL) has been introduced to tackle such issues of centralized technique [18], [19]. FL creates initial model, allows on-device training and further updating the initial model based on the local on-device model training [20]. For instance, an AIDS scenario for IoT devices. The AIDS application collects IoT network data of the connected devices, each with its own network features. This data is then used to train an AIDS model that can improve the accuracy of detecting attacks. Since the data is distributed across thousands of devices with varying data volumes and patterns [20], FL provides a way to aggregate this data without compromising the privacy of the users, thus will strongly increase the attacks detection on IoT devices. Hence, we term this approach of using FL and AIDS approach as *Fed-AIDS*. Meanwhile, the development of Fed-AIDS models faces challenges related to limited training data while networks have a wide variety of features and with the diverse nature of IoT device [21], [22]. Additionally, FL's decentralized nature introduces weight divergence issues arising from non-Independently and Identically Distributed (non-IID) clients [23], [24]. Tackling these issues and optimizing the performance of Fed-AIDS modeling to achieve near optimal accuracy necessitates this research.

Considering the research challenges, a systematic review of literature can significantly contribute to the advancement of the Fed-AIDS model for IoT devices. Employing the systematic literature review (SLR) methodology, we examine existing Fed-AIDS models for IoT devices from various angles. Firstly, we scrutinize modeling tools and frameworks, aiming to identify those well suited for Fed-AIDS modeling, particularly those compatible with IoT device scenarios. Secondly, we analyze prevalent datasets used in Fed-AIDS modeling, considering factors such as publication year, inclusion of IoT network traces, instance availability, and coverage of unknown attacks, offering insights into suitable datasets for Fed-AIDS modeling. Thirdly, we explore the complexities associated with handling non-iid data in Fed-AIDS models, dissecting the underlying principles of the employed methods. Fourthly, we investigate the classification models utilized, with the goal of standardizing them. Fifthly, we examine Federated Learning (FL) aggregation functions in Fed-AIDS modeling for IoT devices. Lastly, a systematic survey of evaluation metrics is conducted to improve our understanding of the result integrity.

A. MOTIVATION AND RELATED WORKS

Recently, the intersection of IoT technology with various facets of our lives, both in academic research and industrial applications, has garnered substantial attention. The potential of IoT to enhance the quality of life is evident, as illustrated by devices such as those that smartwatches equipped with sensors for health monitoring. The widespread availability of cost-effective sensors, remote storage services, and big data has fueled the proliferation of IoT technologies. This rapid expansion, however, has introduced a pressing security concern. As IoT devices with varying capabilities interconnect, the need for robust security measures becomes paramount. Ensuring effective modeling, guiding ethical tools usage, and ultimately contributing to a secure and beneficial future for this transformative technology are critical motivations driving our research. Meanwhile, numerous studies have already conducted review in the field of ML/FL under the hypothesis that there is a requirement for effective AIDS modeling to protect IoT devices against internet threats. This assumption is derived from the state-of-the-art reviews of ML systems employed in AIDS for IoT. For this, Costa et al. [25] focused on recent research on IDS and intelligent techniques used in conjunction with IoT. This is to protect IoT devices data. They note that the issue of FAR remains a challenge that needs to be addressed in all surveys. While in the review of Chatterjee and Ahmed, [26] presents a detailed outline of the current detection methods and their applications in the topic of IoT anomaly detection. Whereas Agrawal et al. [27] investigates the difficulties and weaknesses of FL implementations related to false alarms, poisoning attacks, and high latency, among other issues in IDS. Additionally, Belenguer et al. [29] assesses the absence of consistency in model evaluation, provides the development of a road map for quality standards to deal with advancement of IDS models. Meanwhile, Mohanta et al. [30] investigate the applications of ML, AI, and Blockchain in resolving these security challenges in IoT.

Another sensational work [31] that outlined the criteria for assessing deep transfer learning applications in IDS for industrial control network. Table 1 shows the summary of the related works. However, none of these studies addressed the difficulties that would come up when Fed-AIDS modeling for IoT devices for the best practice. Instead, they primarily focused on specific domain ensuring security to IoT devices from assaults. For examples, Kheddar et. al [31] specifically focused on industrial control IoT devices network for deep transfer learning through IDS. In this context, our research stands out as it purposely goes beyond the confines of specific domains within the field of IoT device security. Unlike these previous studies that often confined their findings to specific domain within the field of IoT device security, our research goes beyond these limitations. We purposely designed our paper to provide insights and methodologies

TABLE 1. Evaluation of the related works. (Symbol (✓) shows the paper is limited the topic, and (x) shows papers that do not cover the topic).

Ref	Brief contribution	Year	Limitations				
			IoT device	Anomaly-based IDS	IDS training dataset	FL modelling	SLR
[25]	A survey on intelligent techniques and IDS architectures in computer networks, with a specific emphasis on IoT and ML.	2019	×	✓	×	×	×
[26]	An overview of detection techniques and applications, on the classification of anomaly detection algorithms in the perspective of IoT.	2022	✓	✓	×	×	×
[27]	A comprehensive review of the utilization of FL in intrusion detection systems.	2022	✓	✓	×	×	×
[28]	Review into FL and it is implementations in advancing the Industrial IoT	2021	✓	×	×	✓	×
[29]	This paper examines the application of FL in IDS and provides a comprehensive description of both technologies.	2022	×	✓	✓	×	×
[30]	An investigation on integration of related technologies of ML, artificial intelligence, and Blockchain with IoT security.	2020	✓	×	×	×	×
[31]	A Review on Deep Transfer Learning Applications in IDS for industrial control network	2023	×	✓	✓	×	×
Our work	**A Review on information that will help researchers towards Fed-AIDS modeling for IoT devices security**	**2024**	✓	✓	✓	✓	✓

that are universally applicable. This approach is particularly relevant in the context of Fed-AIDS modeling for securing IoT devices, where security concerns extend across diverse industries, encompassing healthcare, transportation, smart cities, and more.

By fixing our work in IoT device security, we inherently tackle challenges and propose solutions that reach beyond the confines of any single industry. The goal of this review is to provide comprehensive information to assist researchers in developing Fed-AIDS models for IoT devices. Specifically, the article makes the following primary contributions.

- An overview study on the FL system and its role in AIDS modeling for IoT devices has been presented.
- We use the SLR methodology to survey and study Fed-AIDS modeling taxonomies, specifically for securing IoT devices.
- We present a systematic technical examination of the Fed-AIDS modeling for IoT devices, encompasses a focus on utilized tools/frameworks, training datasets, complexity in handling non-IDD data, classification model, aggregation functions, and model validation metrics.
- We examine the challenges and research directions for Fed-AIDS modeling in IoT devices.

Meanwhile, the article is structured as follows: Section I serves as the introduction. In Section II, the article delves into methodology. Moving on to Section III, it presents the review findings and discussion. In Section IV, the article discusses the challenges and research directions. Finally, Section V contains the concluding remarks.

B. BACKGROUND OF STUDY

The use of the Fed-AIDS approach for IoT-edge devices plays a critical role in ensuring the security and privacy of these devices, which operate at the edge of a network, helping to prevent cyber-attacks and protect sensitive data. Therefore, this section provides a background for the comprehensive study, including a brief definition of IoT-edge devices, AIDS, and its existing models for IoT-edge devices. Additionally, it will delve into the definition of FL, the FL process and protocol, and FL aggregation roles.

1) IOT DEVICES

The IoT ecosystem's core elements is IoT-edge devices [32]. Moreover, IoT-edge devices refers to Internet-connected devices that are deployed at the edge of a network [33], often nearer the data source. In real time, data from sensors and actuators are often collected, processed, and transmitted using these devices. They are often lightweight, low-power devices that can be quickly placed in a variety of settings. IoT-edge device's key role is to gather and process data from sensors and other devices. Also, they are capable of carrying out activities [34] including data analysis, storage,

and interaction with some other devices. Hence, this permits the devices to form decisions and actions on the data they collect [32], [35], [36]. However, IoT-edge devices come in a wide range of examples such as smart thermostats, smart homes devices, industrial control systems, smart agriculture devices, and smart transportation devices.

IoT-edge devices continue to create more data, as these devices are increasing in our daily life, becoming more essentials [37]. According to Jaidka [38] the majority of businesses nowadays seek to collaborate with IoT development firms to integrate this technology into their activities. Therefore, IoT-edge devices must be secured since they frequently handle sensitive data and handle significant systems [39]. Nevertheless, these devices are vulnerable to numerous cyber threats, the vulnerabilities not only have the potential to compromise the data collected by the devices, but also to destroy the physical systems, causing economic loss, harm to individuals, and even environmental degradation. This is to say there is lack contributions of absence to built-in security towards the devices design, as most of them are fairly similar, they make use of same connection and network protocols and share some exceptional characteristics which contain sensing, self-configuring, connectivity, heterogeneity [40] leaving them open to attacks. Additionally, IoT-edge device have limited communications standards [41], making it challenging to interact with security management systems. However, to address these challenges, the strong protection key that is particularly made for IoT-edge devices, is keeping track of the data produced by the devices while consistently checking them for unusual activity, in which is widely accomplished by AIDS.

2) AIDS DEFINITION

Intrusion Detection System (IDS) is a security instrument that keeps an eye out for malicious activity or rules breaking on a network or system. A type of IDS known as an Anomaly-based IDS (AIDS) employs ML techniques to spot unusual activity on the network or system. Whereas signature-based IDS, which is constrained to a particular set of signatures. Therefore, AIDS may identify both known and unknown attacks. Further, AIDS method collects legitimate users' behavior datasets [42], and then applies statistical tests to determine whether the behavior is acceptable or not. The main benefit of this strategy is that it can find attacks that were not discovered before. Moreover, the rules for the AIDS model must be created in an approach that can reduce the FAR for all types of known and unidentified threats in order for it to operate effectively [8]. Meanwhile, there are numerous ways [12], [42], [43], [44], [45], [46], [47] that AIDS models can operate. Initially when identifying patterns of network behavior that differ from what is seen as normal, some models employ unsupervised learning approaches, whilst other models employ supervised learning techniques to identify well-known attack patterns. To learn from data and recognize patterns of network behavior that are difficult to specify through rules, other models employ machine learning techniques such as neural networks or clustering. As a result, both techniques have limitations when it comes to evaluating model performance and its applications. However, while AIDS remains a challenge for both industries and academia, the number of deployed IoT devices is increasing, thereby increasing the potential for attacks on IoT environments simultaneously.

3) AIDS MODELS FOR IOT DEVICES

The effectiveness of the AIDS model has been deployed and validated by researchers using a variety of methods. In the training phase of AIDS modeling, the training mode can be classified as centralized, federated. While the use of theoretical, empirical, and simulation methods are tools for validation the AIDS model [45]. Additionally, the evaluation datasets stand essential to the validation of any AIDS model because they let us measure how effectively the proposed model can identify normal or attack outcome in IoT-edge devices. Lastly, the modeling algorithm also plays a vital role in validating the proposed AIDS models. Accordingly, many related works have been found in literature, each with different motivations. Their concepts are described in Table 2 and are summed up as follows. The proposed models in [10], [48], [49], [50], [51], [52], [53], [54], and [55] focus on federated setting towards modeling the IDS model. While models in [8], [9], [56], [57], and [58] modelled in centralized training mode. In addition to availability of various IDS-based dataset, [56], [58] used Bot-IoT dataset in evaluation of their model. NID dataset has been utilized in [57]. Meanwhile, the model proposed by [48] get to use of IoT-23. Moreover, NSL-KDD dataset has been found in the modeling of IDS models offered by [8], [9], [10], and [49]. In the proposed model of [52], UNSW-NB15 dataset has been used, while [55] have used ToN-IoT dataset.

Another very recent studies in the field of IoT security, efforts to enhance the effectiveness of AIDS for IoT are increased. One such effort is demonstrated in a study [57], which focuses on UNSW-NB15, BOT-IoT and ToN-IoT datasets and employs various ML techniques. The study introduces a novel framework that incorporates specific techniques designed to ensure the quality of both data and models. In another study [58], researchers investigate the critical issue of energy consumption in on-device ML models used for IDS applications in IoT. The research conducted in a centralized manner, seeks to quantify and compare the energy usage during the training process across cloud, at the edge, and ML directly on IoT devices settings. Moreover, a study [59], centered on a particular dataset (UNSW-NB15). Notably integrates a distinctive hybrid feature selection method, which combines elements of different feature selection techniques.

However, AIDS modeling for IoT-edge devices is an essential area that comprised many works that achieves successes with different approaches. Thus, makes it a very interesting research area with many open issues, that currently require an up-to-date, comprehensive taxonomy and survey

TABLE 2. Analysis of AIDS models for IoT devices.

Ref	Training Mode	Dataset	Modeling Algorithm	Contributions
[56]	Centralized	Bot-IoT	One-class SVM	Proposed a stacking ensemble learning to improve detection accuracy
[57]	Centralized	NID	CNN	Presented a CNN-based model that evaluated at IoT traffic to predict any potential intrusions and unusual traffic patterns
[48]	Federated	IoT23	CNN	A decentralized system with non-full peer-to-peer communication and version control has been designed, which enhances the system's performance
[58]	Centralized	Bot-IoT	NN	Suggested a model for binary and multi-class classification that employs a feed-forward neural network and cognitive principles.
[49]	Federated	NSL-KDD	LR	Proposes a pragmatic framework that can be used by IoT devices to identify potential risks by leveraging FL with the presence of three distinct use cases.
[50]	Federated	Virus-MNIST	CNN	Proposed a lightweight network called AMNET, which is trained directly on low-resource IoT devices within the Fed-Mal framework to detect malware attacks.
[51]	Federated	N-BaIoT	MLP	Presented a framework designed to be deployed on network nodes, enabling IoT devices to access Wi-Fi, 5G networks while offloading computational tasks from the IoT devices themselves for IDS.
[52]	Federated	UNSW-NB15	DNN	Proposed an effective IDS model using GAN network with a distributed FL mode.
[53]	Federated	CICDDoS2019	LSTM	Examine the DDoS attack significant features and add new features to indicate the relationships between anomalous behavior and data flow.
[54]	Federated	SEA	LSTM	Proposed an effective approach based on FL and LSTM networks to achieve high detection accuracy while protecting users' privacy.
[8]	Centralized	NSL-KDD	K-NN and DT	The Hybrid ML approach is used to obtain the highest accuracy using the least possible number of dataset features.
[10]	Federated	NSL-KDD	CNN	Proposed an intelligent intrusion detection mechanism, named FedACNN, specifically designed IoT systems. FedACNN utilizes a combination of FL and CNN to improve the IDS capabilities.
[55]	Federated	ToN_IoT	LR	Presented an evaluation of differential privacy methods utilized in the model training process of IoT-enabled IDS within FL.
[9]	Centralized	NSL-KDD	SDPN	Conducted a broad evaluation that demonstrates the superior performance of the proposed DL-IDS in terms of accuracy, precision, recall, and F-score measures.
[59]	Centralized	UNSW-NB15, BOT-IoT and ToN-IoT	DT, RF, KNN, SVM, NB, and MLP	The study aims to boost the effectiveness of supervised ML methods when used with IoT devices. It introduces a framework to enhance IDS performance within an IoT context by applying specific techniques to ensure the quality of data and models.
[60]	Centralized	Distributed Smart Space Orchestration System (DS2OS)	LR, k-NN, DT, RF, NB, and ANN	The study explores how much energy is consumed by ML models running on IoT devices for IDS. More specifically, they make a comparison regarding energy usage during the training process in the cloud, at the edge, and ML directly on IoT devices.
[61]	Centralized	UNSW-NB15	MLP	Introduced an IDS based on MLP, which integrates a unique hybrid feature selection technique named IGRF-RFE. The method combines both filter feature selection and wrapper feature selection approaches.

of these recent works because ML has been used to enhance intrusion detection over the past few decades [62]. While security challenges in IoT environment are becoming broader and becoming challenges to our physical and financial well-being.

4) FL DEFINITION

The federated learning (FL) [18] is a productive approach for utilizing distributed resources to actively train a ML model. In which FL allows numerous IoT-edge devices to work collectively to train a model without sharing the raw data on the central server [63], [64]. Moreover, FL promises to protect the decentralized raw data's privacy [65].

Further, in a standard practical approach [66], [67], FL makes the assumption that each of the k users (k_1, $k_2 \ldots k_n$) has their own database d (d_1, $d_2 \ldots$ d_n) and that they are all prohibited from directly accessing one another's data to increase their own database. Then, the user K_i can locally train its own model W_i with the local data d_i. The server creates a global model W_g from the aggregated local models (w_1, $w_2 \ldots w_n$) and updates the global model to replace each user local model.

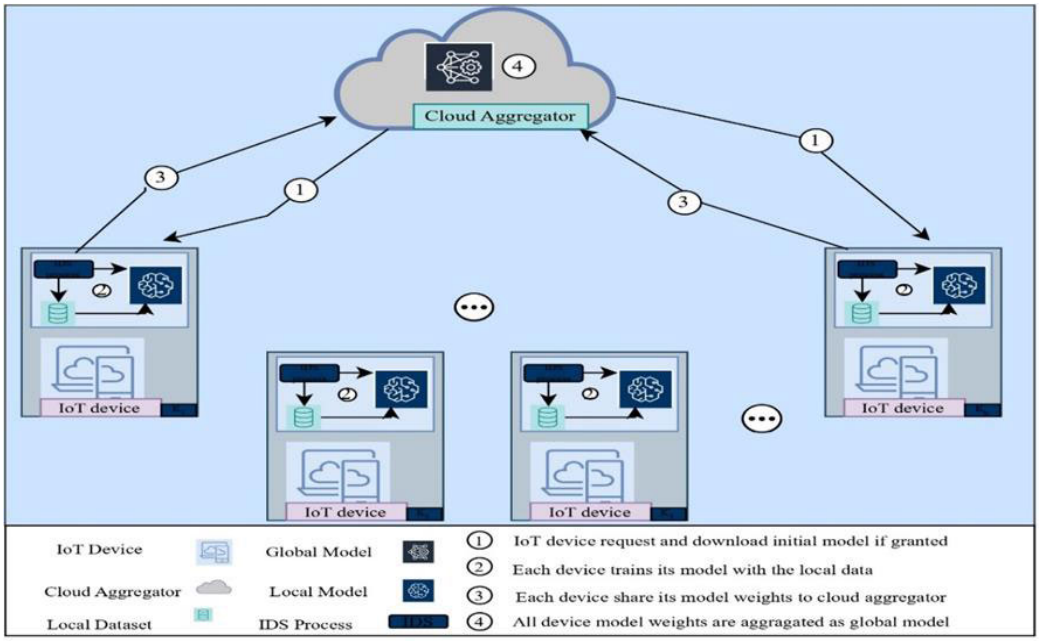

FIGURE 1. FL process in terms of AIDS model for IoT devices.

5) FL PROCESS AND PROTOCOL

The network protocol is the ideal practice, when trying to comprehend the conceptual context of FL [19]. The FL protocol's primary participants are devices, which are referred to as IoT-edge devices in this article. The FL server is also referred to as a FL aggregator, on-device storage, FL task, and FL population. Eventually, based on the kind of FL system you want, the FL process consists of these four steps as Figure 1 depicts in terms of AIDS model for IoT. Devices first notify the server that they are prepared to execute a FL task for a certain FL population and server will share the initial model with them. Secondly, each participating IoT-edge device computes locally using its local dataset. Thirdly, the participating IoT-edge devices will report back the trained model to the FL aggregator. Finally, the aggregator updates its global state with the adjustments, and the process persists.

6) FL AGGREGATION FUNCTIONS

FL aggregation functions, also known as weighted averaging, are employed to aggregate model updates across various FL participating devices. Meanwhile, these procedures are often used to aggregate the device's model updates. FedAvg [18] is one of the popular aggregation functions, in which combines individual global models into one. Conversely, FedAvg performs better, in which gradient descent compute rounds to speed the learning and convergence. Additionally, FedSGD [18] is a common FL aggregation function based on Stochastic Gradient Descent (SGD), where IoT-edge devices conduct one iteration of gradient descent for each training process while the aggregator computes a simple weighted average of all trained models to create a single shared model. The function performs this by weighing each task differently and then aggregating the set of parameters as a result.

7) NEEDS FED-AIDS MODELS FOR IOT DEVICES

In order to execute distributed learning for IoT networks, FL has emerged as a potent option that can identify a variety of cyberattacks and help network security measures [39]. Federated intrusion detection and prevention solutions can be implemented with the help of FL's privacy-enhancing characteristics, where each IoT edge device collaborate to run an AI model such as DNN in order to retrain the threat model to fight intruders [39]. FL also makes it easier to find corrupted IoT devices in federated IoT networks [39]. In fact, given the sophistication of attacks and threats, it is difficult to identify those using current centralized systems, which frequently identify attacks by deviating from user behavior profiles and suffer from a high false alarm rate and a lengthy detection delay. When performing intrusion detection for distributed IoT networks, FL appears as a rational solution. Moreover, a vast number of IoT networks with a wide variety of features and gigantic datasets are involved, which improves learning accuracy and intrusion detection effectiveness. A scalable FL technique has recently been presented [39], [68] to enhance the detectability of intrusions such as infiltration on a larger scale. While maintaining the privacy of network traces, each IoT device runs a neural network for packet classification at the line speed of neighboring switches.

II. REVIEW METHOD

This SLR study follows the phases of planning, conducting, and reporting, utilizing the methods outlined in [69]. In addition, it includes practices from the methods presented in [70]. The initial emphasis is on thoroughly analyzing the latest developments in Fed-IDS model for IoT devices as identified research. Subsequently, identifies research questions, research contents with the sources. The subsequent stage involves identifying the establishment of inclusion and exclusion criteria. The creation of a data extraction process, aimed at consolidating necessary data and addressing research questions, is then outlined. Finally, a systematic approach to analyzing data and reporting the findings of the review is developed.

A. RESEARCH QUESTIONS

Concrete Research Questions (RQ) are defined, as outlined in Table 3, providing directions for the analysis. These questions span various fields, including process flow and tools, datasets in AIDS models, classification models, aggregation functions, and evaluation metrics.

B. RESEARCH CONTENTS

Considering that certain articles on ''anomaly-based intrusion detection models'' fall under the broader category of ''intrusion detection,'' we used both the specific term ''anomaly-based intrusion detection models'' and the broader term ''intrusion detection'' in our search. Similarly, for articles related to ''IoT devices,'' which may be categorized as ''IoT-edge devices,'' we included both terms in the search. Additionally, for articles on ''federated learning'' as a methodology, we expanded the search terms to include both ''federated learning'' and the standalone term ''federated.'' This approach ensures that articles using federated learning techniques are captured in the search results. By using both general and specific search terms, we aimed to conduct a targeted and inclusive search, encompassing both broad categories and relevant subcategories to ensure comprehensive coverage of the literature.

To ensure a high-quality and relevant literature search, we evaluated three prominent databases: Scopus, Google Scholar, and Web of Science. While Scopus, covering major publishers such as ACM, Springer, and IEEE, boasts greater comprehensiveness than Web of Science, it doesn't reach the exhaustive scope of Google Scholar, which may include non-peer-reviewed materials such as technical reports. Considering this trade-off, we chose Scopus. It offered a balanced approach, providing access to a substantial pool of relevant sources while prioritizing peer-reviewed content.

Since FL has been introduced in 2017, we restricted our search to the years 2018 to as recently as 2023. This timeframe aligns with the emergence of FL as a methodology. We then applied the inclusion and exclusion criteria listed in Table 4 for further evaluation in the subsequent phase.

TABLE 3. Research questions.

Question	Motivation
RQ1: What are the key frameworks/tools commonly used in Fed-AIDS modeling for IoT devices?	To improve the effectiveness of future research and implementations, it is imperative to investigate the current methodologies and tools utilized, thereby identifying gaps, strengths, and potential areas for improvement.
RQ2: How do they contribute to the overall workflow in development of Fed-AIDS models for IoT devices?	
RQ3: What datasets are widely recognized in Fed-AIDS modeling for IoT devices?	Investigating the popularity and characteristics of datasets in this context is essential for ensuring the robustness of models. Meanwhile, by exploring how FL copes with non-IID data in the AIDS modeling paradigm, this research seeks to improve the adaptability and robustness of FL-based approaches
RQ4: How does FL handle non-IID data in the context of Fed-AIDS modeling for IoT devices?	
RQ5: What classification models are commonly employed in Fed-AIDS modeling for IoT devices?	Investigating classification models in AIDS through FL for IoT devices is vital for advancing the understanding of model architectures tailored to the unique characteristics of these devices. This exploration aims to identify effective classification approaches.
RQ6: What aggregation functions are commonly employed in Fed-AIDS modeling on IoT devices?	Understanding the nuances of aggregation functions is crucial for optimizing the collaborative learning process in decentralized environments. This research aims to uncover the characteristics and effectiveness of various aggregation functions in the context of AIDS modeling.
RQ7: What evaluation metrics are commonly utilized in assessing the performance of Fed-AIDS models developed for IoT devices?	Effective evaluation tasks are essential for assessing the performance and reliability of AIDS models developed through Federated Learning on IoT devices.

C. STUDY SELECTION

Recognizing the importance of consistent and objective evaluation in research, we adhered to established principles in our study. Table 4 clearly defines the criteria for inclusion and exclusion, emphasizing research specifically focused on AIDS models for IoT devices and those employing federated learning methodologies. To justify the exclusion criteria for article publications not in the form of journal articles, journals are authoritative in academia. Publications in reputable journals contribute significantly to scholarly discourse. Other forms, such as conference papers, may lack the same credibility and scholarly standing [71]. This approach minimizes subjectivity and ensures the selection of relevant studies for analysis.

D. DATA EXTRACTION

To streamline the analysis, we implemented a systematic filtering process guided by specific criteria, depicted in

TABLE 4. Inclusion and exclusion criteria.

Criteria	Criteria's definition
Inclusion	• Articles that are published between 2018 and 2023. • Articles on AIDS model for IoT device based on FL.
Exclusion	• Article publications not in the form of journal articles. • Non-peer-reviewed articles and articles not published in English. • FL articles unrelated to AIDS models for IoT devices. • AIDS model for IoT device articles unrelated to FL.

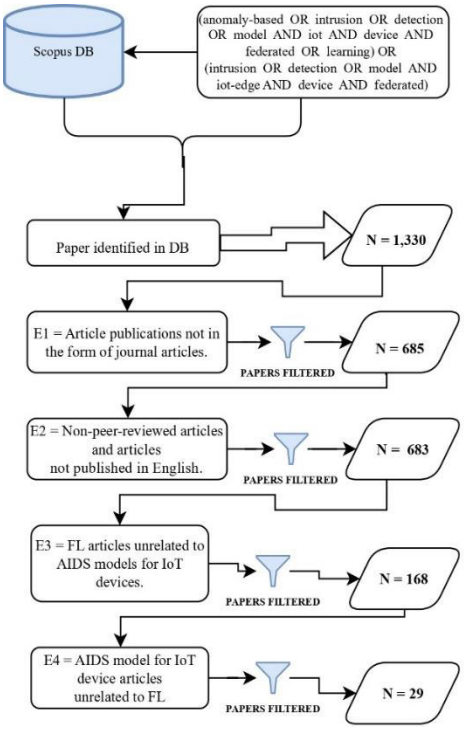

FIGURE 2. Papers extraction process.

Figure 2, resulting in a focused collection of 29 papers directly relevant to the Fed-AIDS model for IoT devices.

However, these 29 articles highlight that FL is still new to AIDS for securing IoT devices. Subsequently, we then extracted key information from each paper based on the defined research question in Table 3. This structured approach enabled us to efficiently extract essential information without requiring a review of every paper's full text. Instead, we primarily focused on the title, abstract, and introduction, and methodology, consulting the remaining body text only when necessary to clarify specific details.

E. DATA SYNTHESIS

To analyze the extracted data from chosen articles and answer our research questions (RQs), we employed different synthesis methods below, that we gained a nuanced understanding of the extracted data and addressed our research objectives effectively.

- For RQs 2, 3, 4 and 7, seeking qualitative insights: We used narrative synthesis, tabulating and visualizing results using charts to enhance understanding. This helped us identify common themes and patterns across studies.
- For RQs 1, 5 and 6, requiring quantitative analysis and conceptual comparison: We employed the binary outcome method, and reciprocal translation. This enabled us to assess the effectiveness of specific techniques across different studies related to specific Fed-AIDS modeling taxonomy for securing IoT devices.

III. REVIEW FINDINGS AND DISCUSSION

This section dives deep into the research and practical aspects of Fed-AIDS modeling for IoT devices. We explore key elements such as the workflow and tools involved in building such models, the data used to train them, the challenges of dealing with non-IDD data in FL, the choice of classification models, the methods used to combine model weights from different devices (aggregation functions), and how we measured the performance of Fed-AIDS models (evaluation metrics). In simpler terms, it answers the defined research question in Table 3, offering valuable insights for anyone working in this field. However, the data extracted implies that FL are at early use in AIDS for securing IoT devices. Figure 3 depicts the number of documents per year of published articles.

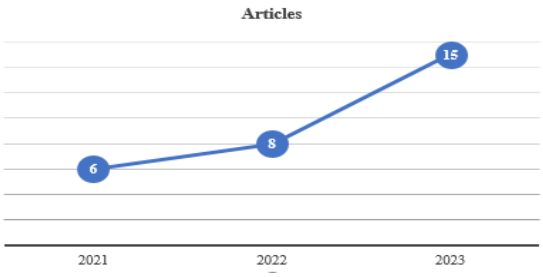

FIGURE 3. Number of articles per year.

A. PROCESS FLOW AND TOOLS

To make sure the Fed-AIDS modeling functions well and adheres to the specifications of the AIDS model for IoT devices, the FL model engineer must simulate and test the model in a controlled environment [72], [73]. Therefore, assessing the model's performance and robustness in such various FL settings, may be necessary to use simulation tools as TensorFlow Federated (TFF), FedML and PySyft.

From **RQ1,** that to find what are the key frameworks/tools commonly used? Table 4 provides a list and count of key frameworks and tools relevant to developing Fed-AIDS model specifically for IoT devices. Among the tools found, TFF has the highest count with seven instances. Followed by FedML/PyTorch, PySyft and TensorFlow/Raspberry-Pi with three mentions. Other notable tools include Flower and FL&DP with two mentions. While tools such as Pycharm focused ones including IBMFL. Each of this tools/framework contributes to the overall Fed-AIDS modeling for IoT devices. Additionally, a set of Python interfaces [19] were predominantly used in the implementation of these FL models for the stated simulation tools.

These diverse tools have emerged to streamline shared and privacy-preserving model training across decentralized devices. For example, the flower [74] is an open-source Python framework, simplifies model development by providing essential components for communication between cloud server and clients. IBMFL [75], developed by IBM, focuses on secure FL modeling, emphasizing collaboration among multiple parties while keeping data localized. While PySyft [76] extends popular DL libraries, such as PyTorch and TF, facilitating privacy-preserving computations on decentralized data. On the other side is TFF [18], which is a Google framework, seamlessly integrates with TF, enabling the creation of models trained across distributed devices. The mention of FedML [77] in the context of Fed-AIDS model indicates the implementation of FL model within these widely used DL frameworks. Sherpa.AI has developed an open-source FL&DP [78]. The objective is to encourage the advancement of research and development in edge AI services while prioritizing the protection of data privacy. Additionally, the reference to running TF on Raspberry Pi devices suggests exploration of FL modeling in edge computing [79]. While PyCharm [80] isn't explicitly designed for FL, but it remains a popular choice among developers for managing Python code, including tasks related to FL. In summary, these tools collectively contribute to Fed-ADIS modeling for IoT devices, each playing a unique role in advancing collaborative and privacy-preserving practices for IoT devices.

TABLE 5. Identified FL simulation tools.

Key frameworks/tools	Count	Open source	Ref
FL&DP	2	✓	[78]
Flower	2	✓	[81, 82]
IBMFL	1	--	[83]
Pycharm	1	✓	[80]
PySyft	3	✓	[84, 85]
FedMl/PyTorch	3	×	[77, 86, 87]
TensorFlow/Raspberry-Pi	3	✓	[79, 88, 89]
TFF	7	✓	[90-96]

Meanwhile, on how these tools contribute to the overall workflow development of Fed-AIDS models for IoT devices from **RQ2**. For this we categorize the tools functional features as presented in Table 6. Frameworks such as FL&DP and PySyft can act as 'Privacy Guardians' by securing data during collaborative training. 'Resourceful Scouts' such as Flower and TensorFlow/Raspberry Pi excel in quick deployments on limited devices. As deployments grow, 'Scalability Sergeants' such as IBMFL and TFF step up, handling complex updates and management. For intricate tasks, 'Deep Learning Dragons' such as PyTorch and TensorFlow unleash their extensive libraries and GPU support, even on resource-constrained devices. Finally, 'Customization Champions' such as Python/scikit-learn and PyTorch/TensorFlow offer flexibility to tailor models to specific device capabilities. This diverse toolbox empowers developers to navigate Fed-AIDS modeling for IoT devices, unlocking the full potential of this technology through robust, efficient, and scalable models. For example, modeling with TFF, the simulation phases serve as a bridge between the development and real-world deployment of the Fed-AIDS model. By employing TFF as a simulation tool, this phase enables the emulation of FL tasks using proxy data that closely replicates the characteristics of real IoT device data. Leveraging TFF's capabilities, researchers can rigorously assess the performance of the Fed-AIDS model in a controlled environment without exposing real-world data. Subsequently, the FL Plan Generation tasks leverage TFF to facilitate the creation of detailed FL plans, ensuring the smooth execution of the Fed-AIDS model. Specifically, TFF enables the specification of intricate plans for individual IoT devices. These plans encompass elements such as TensorFlow graph specifications, the development of local AIDS models on each IoT device using ML algorithms tailored to the task, and the management of operations such as loading and saving model weights. On the server side, the FL plan includes the aggregation task, detailing how model updates from diverse devices should be aggregated. Consequently, FL tasks equipped with FL plans are deployed to a simulated FL server and a set of emulated IoT devices. This simulated FL environment faithfully replicates the expected behavior of the Fed-AIDS model in a real-world IoT network. At the conclusion of each FL round, the FL task and plan are evaluated by the simulator to assess the performance metrics of the simulated Fed-AIDS model before its deployment in a real-world context. Hence, Figure 4 depicts hypothetical simulation process flow for Fed-AIDS considering TFF-based for IoT-edge devices. Therefore, these findings demonstrate the diverse selection of work tools by the authors, each offering its own unique strengths and weakness in the domain of FL for IoT devices.

B. DATASETS ON MODELING Fed-AIDS FOR IOT DEVICE

One of the objectives that Fed-AIDS models aim for is to create models that are generalizable and efficient of accurately detecting attacks behavior. Therefore, for the model to be trained and tested on accurate data, it is crucial that we fully comprehend the data and its attributes. In this regards, to answer **RQ3** on what are datasets are widely recognized in Fed-AIDS modeling for IoT devices, we iden-

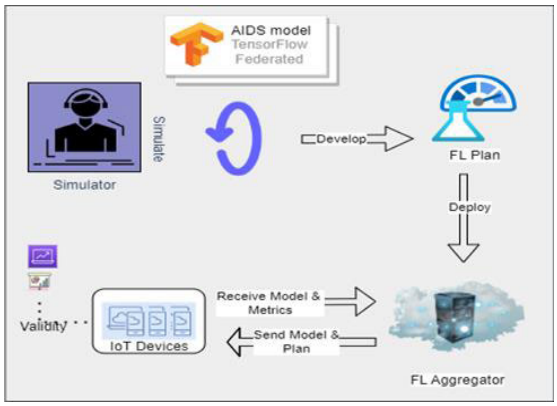

FIGURE 4. Modeling process flow for FL-AIDS model for IoT devices.

TABLE 6. FL simulation tools effectiveness.

Category	Tool(s)	Primary Contribution
Privacy Guardians	FL&DP, PySyft	Secure aggregation, encrypted communication
Resourceful Scouts	Flower, TensorFlow/Raspberry Pi	Lightweight frameworks, minimal footprint
Scalability Sergeants	IBMFL, TFF	Robust infrastructure, large-scale management
Deep Learning Dragons	PyTorch, TensorFlow	Extensive libraries, GPU support, model complexity
Customization Champions	Python/scikit-learn, PyTorch/TensorFlow	Flexibility in architecture, model tuning

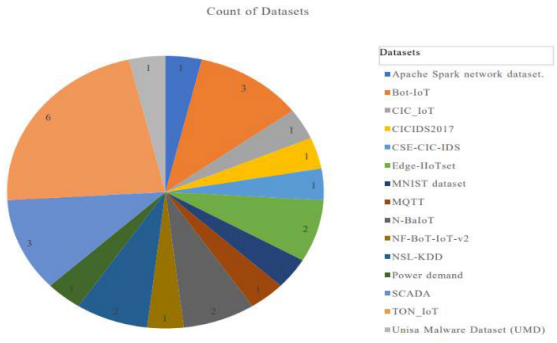

FIGURE 5. Identified datasets for Fed-AIDS models.

tified and collected 15 datasets as depict in Figure 5 with number of appearances in the studies related to Fed-AIDS models for IoT device. Based on the information on each dataset, we extracted the year of which it has been published, availability of IoT network trace, instances count, feature counts, and availability of unknown attacks as presented in Table 7, these give our suggestion in terms of potential methods to select the dataset for FL-AIDS modeling of IoT devices.

Subsequently, the synthetic ecosystem at the UNSW 's cybersecurity center is used to build UNSWNB15 [97]. While the NSL-KDD [98] dataset has been built from the initial KDD cup99 dataset. It is sufficient to enable practical application of the entire NSL-KDD dataset without the need for sampling selection. In CICIDS2017 [99] collection contains data about both known malware assaults and benign behavior, and it is identified according to the timestamp, source and destination IP addresses, source and destination ports, protocols, and attacks.

The dataset ISCX 2012 [100] is built on labelled, realistic network traffic that includes a range of attack scenarios. Furthermore, N-BaIoT [101] has been created by preprocessing the traffic from 9 commercial IoT devices of diverse categories that were either unaffected or affected by two botnet malware assaults i.e. Mirai or Bashlite. Additionally, Bot-IoT [102] has been created as an updated and accurate dataset for evaluating models to detect botnet assaults in the IoT, in which it is developed on a testbed made up of several virtual computers running different operating systems. Subsequently, the TON_IoT [103] comprises diverse data sources such of sensor interpretations, operating system (OS) logs on a network that contains a number of IoT devices. Another most sensational dataset designed for cyber security researchers to assess their ML-based IDS model i.e. the Edge-IIoTset dataset [104]. It encompasses fourteen attacks linked to IoT and IIoT connectivity protocols, which are classify into five threats including the DoS/DDoS attacks, Information gathering, Man in the Middle Attacks, Injection attacks, and Malware attacks. These datasets include a variety of features derived from various sources such as alerts, system resources, logs, and network traffic. Notably, they introduce 61 novel features with strong correlations among the 1176 features identified. It's noteworthy that the MNIST dataset [105], dating back to 1998, is not an IoT dataset but is widely recognized in ML for anomaly detection [91]. On the other hand, the MQTT dataset [106] from 2020 is associated with IoT, offering over 22 million instances with 29 features and no information about unknown attacks.

The NF-BoT-IoT-v2 dataset from 2020 [107], the Power demand dataset from 2016 [108], and the SCADA dataset from 2017 [109] are also IoT-related datasets with varying characteristics. However, it is important to highlight the unique case of the Apache Spark network dataset, where no information about its generation has been provided by the author [82]. This lack of transparency can affect the dataset's reliability and raises concerns about its suitability analyses. The UMD Dataset from 2021 [110], though not IoT-related, includes instances of unknown attacks and comprises over 30,000 instances with six features.

TABLE 7. Analysis of most popular dataset for AIDS modeling.

Dataset	Year	IoT Touch	Instances Counts	Feature Counts	Unknown Attacks
UNSW-NB15 [97]	2015	No	2,540,044	49	No
NSL-KDD [98]	2009	No	148,517	42	No
CICIDS2017 [99]	2017	No	2,830,743	80	Yes
ISCX 2012 [100]	2012	No	1,526,148	19	No
N-BaIoT [101]	2018	Yes	7,062,606	23	Yes
Bot-IoT [102]	2018	Yes	73,000,000	46	Yes
TON_IoT [103]	2019	Yes	22,339,021	46	Yes
Edge-IIoTset [104]	2022	Yes	20,952,648	61	Yes
MNIST dataset [105]	1998	No	70,000	784	No
MQTT [106]	2020	Yes	22,076,997	29	No
NF-BoT-IoT-v2 [107]	2020	Yes	1,379,274	12	No
Power demand [108]	2016	Yes	518,400	Nil	No
SCADA [109]	2017	No	101,400	Nil	No
UMD Dataset [110]	2021	No	30,113	6	Yes

There are some important datasets that are used AIDS model evaluation for IoT devices. The Unisa Malware Dataset (UMD) has been utilized by [110], while the CICIDS2017 dataset found attention from [81] and [111]. Multiple authors were involved in studying the TON_IoT dataset [55], [83], [84], [90], [93], [94], [112], while on N-BaIoT dataset [112], MNIST dataset [91], Edge-IIoTset dataset [77], [92], CIC_IoT dataset [80], CSE-CIC-IDS dataset [113]. The SCADA dataset [88], [89], NF-BoT-IoT-v2 dataset [114], while BoT-IoT dataset [79], [86], [95], MQTT dataset [115], and the Power Demand dataset [85]. This collaborative and diverse engagement with datasets underscores the multidimensional nature of research in Fed-AIDS modeling for IoT devices. Each dataset serves a specific objective in enabling the development and evaluation of Fed-AIDS models. Moreover, these datasets contribute to advancing research in AIDS by providing real-world data and standardized evaluation outlines. Consequently, the datasets exhibit variations in several aspects. Firstly, they were created in different years, ranging from 1998 to 2022, representing different times and indicating probable changes in IoT network traffic patterns over time. Secondly, some datasets focus on IoT network traffic specifically, while others encompass a broader range of network traffic. This distinction is significant as it allows researchers to investigate IoT-specific security problems or study a wider network. Additionally, the datasets differ in terms of the number of instances and features they contain, spanning from thousands to tens of millions of instances and featuring 6 to 784 attributes. These distinctions in dataset size provide researchers with options to analyze different scales of IoT network traffic. Lastly, some datasets include instances of unknown attacks, posing an additional challenge for AIDS, as they need to be capable of identifying and responding to previously unseen attack patterns. Thus, the diverse datasets offer researchers opportunities to explore and develop effective Fed-AIDS methods in the context of IoT security.

C. NON-IDD DATA IN Fed-AIDS MODELING

Data in Fed-AIDS modeling for IoT devices is diapers among numerous devices rather than being kept in central server. Besides, each device uses it is local device data train a local model, sending updates to a centralized server. However, in Fed-AIDS modeling, there are a few technical factors to consider about training dataset, such as non-iid data (data heterogeneity) that is limited amount of data, or due with network constraints [116]. In FL, non-iid data refers to data that is not distributed independently and identically across participating devices in a data heterogeneous environment. Thus, the model might not be able to generalize to new data well because of the different data distributions [117], [118], which might affect model convergence and accuracy. We identified three strategies to answer **RQ4**. Each appeared once in the existing reviewed studies as shown Figure 6, while 26 studies have lack of responding to handling complexity of non-IDD data in Fed-AIDS Modeling for IoT device. Meanwhile, classifying IoT network traffic for AIDS is a complex task due to the numerous attributes involved [5]. While FL offers advantages due to its data richness, but it introduces complexity by handling non-IID data with variations in size, type, and complexity across IoT devices [67]. This leads to unfairly trained local models, resulting in inadequate global model fitting when aggregated. Moreover, issues such as redundant or compromised data in local clients can lead to model failures, which are significant concerns in real-time AIDS scenarios. However, the data augmentation [119] strategy employs artificially produced data to equalize the distribution of data among IoT devices to overcome this problem. Single Model Convergence [83] approach prioritizes the creation of a global model by aggregating knowledge from local models on individual devices through an iterative process. While the iterative aggregation gradually converges with the global model, providing a unified understanding that accommodates the diverse data distributions present on different devices. On the other hand,

Differential Privacy [55] addresses privacy concerns and non-IID data challenges by deliberately introducing noise to local updates during training. The noise protects individual contributions' privacy and acts as a regularization technique, making the learning process less sensitive to the specifics of each device's data distribution. The aggregated noisy updates contribute to a global model, enhancing robustness and generalization in the federated learning framework for IoT devices. Subsequently, it is imperative to meticulously assess these technical strategies to guarantee the effectiveness of Fed-AIDS modeling, given the lack of existing strategies and complexity of the task and the challenges posed by non-IID data.

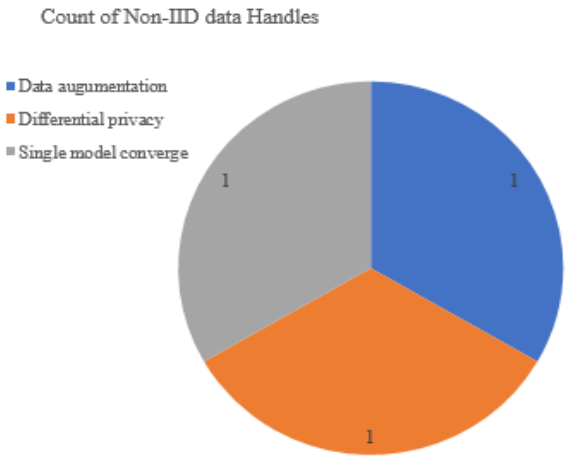

FIGURE 6. Identified strategies for handling non-iid data complexity.

D. CLASSIFICATION MODELS

The classification task of AIDS is designed to predict one of many (more than two) or one of two potential outcomes. Thus, can be used to categorize network traffic of IoT-edge devices in the context of AIDS into several categories of security concerns [120], such as denial of service (DoS) assaults, malware infections, and unauthorized access attempts. At the same time, the model is trained on labelled data and makes predictions based on attributes including network protocols, source and destination IP addresses, and payload content. Moreover, the model's output is a class label that identifies the internet threat type.

To answer **RQ5**, the question of which classification models are commonly employed in Fed-AIDS modeling for IoT devices, we categorize the identified proposed classification model into conventional ML models and DL models. For conventional ML models, we identified five models each proposed once as presented in Table 8. This includes Random Forest (RF), Stochastic Gradient Decent (SGD), Multinomial Logistic Regression (MLR), toy classifier and One-class SVM. From the second category in Table 9, DL models are the mainstream methods with eight models with multiple appearance in some models compared to conventional ML models. This is due to acceptability to implement with existing tools/frameworks; some tools/frameworks are very limited to accept the conventional ML model, more specifically the boosting algorithms. However, these DL models are CNN, RNN, NN, DNN, MLP, ANN, LSTM, Auto Encoder and lastly AE-LSTM which is an ensemble method.

To explore the principles and attributes of these models, we introduce them in the subsequent analyses. Utilization of RF [115] in Fed-AIDS model for IoT device emerges as ensembles of decision trees, each traversing a distinct path through the labyrinthine depths of the data. By aggregating the wisdom of these diverse perspectives, **RF** achieves robust predictions, mitigating the pitfalls of overfitting inherent to individual trees. On the other hand, **SGD** [94], functioning as a nimble navigator, traverses the vast expanse of datasets. It iteratively refines model parameters through judiciously chosen data samples. Its efficient steps minimize the discrepancy between predictions and reality, paving the way for accurate modeling. In the **MLR** [55], [83], extends the reach of its binary counterpart, ventures into the realm of multi-class classification. It deftly translates data into a tapestry of probabilities, assigning each class a likelihood based on the equation: $\log(P(Y=k|X))/(1-P(Y=k|X)) = \beta_0 + \beta_1 X1 + \ldots + \beta_p X_p$, where $P(Y=k|X)$ embodies the probability of reaching outcome k given data X and βs represent the nuanced weights assigned to each feature's influence. **Toy classifiers** [90], serving as training controls in this classification models, offer rudimentary decision rules, laying the groundwork for comprehending more algorithms that are intricate. Finally, in **one-class SVMs** stand as unsupervised approach [111], vigilantly guarding the borders of normalcy within the data. This unshackled from the constraints of labeled anomalies, they excel at identifying outliers that deviate from the established patterns, serving as invaluable tools for anomaly detection.

An **ANN** refers to a computational model inspired by the structure and functioning of the biological neural networks found in the human brain. ANNs can have diverse architectures and may include various types of layers, such as input layers, hidden layers, and output layers. They are designed for information processing and learning from data. A basic neural network comprises three layers: the initial layer, referred to as the input layer of neurons, followed by the middle layer, and concluding with outputs from the final layer of neurons. ANNs have the capability to learn rapidly from experiences and effectively address complex nonlinear problems [121]. In the realm of IoT security, ANNs excel in Fed-AIDS modeling for securing IoT device [81], [115]. They demonstrate proficiency in analyzing extensive sensor data from smart devices, identifying subtle deviations from normal behavior, and signaling potential threats such as malware or unauthorized access. An **MLPs** is a type of ANN with a feedforward structure that uses backpropagation to refine its parameters during the training phase. When data is fed into the input layer, it travels through

TABLE 8. Proposed conventional ML models.

Learning Type	Model	Counts
Supervised	Toy classifier	1
	MLR	2
	SGD	1
	RF	1
Unsupervised	One-class SVM	1

TABLE 9. Proposed DL models.

Learning Type	Model	Counts
Supervised	CNN	2
	RNN	1
	DNN	5
	MLP	2
	ANN	3
	LSTM	3
Unsupervised	Auto Encoder	4
	AE-LSTM	1

interconnected nodes, each equipped with weights and biases, undergoing computations using activation functions. These computations propagate through successive layers until the output nodes generate the results [122]. In essence, while ANNs encompass a wide range of neural network architectures, MLPs specifically refer to a type of ANN with a layered structure that includes multiple layers for learning and processing information. For this, MLP has been considered in Fed-AIDS modeling for securing IoT device [51], [91].

The **DNN** is a type of ANN characterized by multiple layers situated between the input and output layers. In a more specific context, it can be described as a fully connected neural network that closely resembles the structure of an MLP. The lower-layer neurons within a fully connected DNN have the capability to establish connections with all neurons in the upper layers [123]. To accomplish supervised learning tasks with nonlinear activation functions, a DNN employs the backpropagation technique, due to this property; DNN has received attention at Fed-AIDS modeling for IoT device [80], [86], [95], [96], [112]. In **CNN**, as meticulous detectives examining fingerprints, CNNs scrutinize network data for spatial anomalies. Their equation, $y = f(\sum w_i x_i + b)$, where y represents the output captures their core strength: extracting intricate patterns from inputs (x_i) using weighted filters (w_i). Convolutional layers within CNNs employ kernels that are systematically applied across the input data, reducing the number of parameters required compared to traditional neural networks. The CNN has received attentions in Fed-AIDS modeling for IoT devices [82], [124], due to their excellent performance at handling IoT network flow. Compared to DNN, where it has a fully connected structure, with each neuron in one layer connected to every neuron in the next layer, CNN has a layered structure. This structure includes specialized layers such as convolutional layers and pooling layers designed for processing grid-like data, such as images.

The **RNN** belongs to a category of ANN capable of demonstrating temporal memory behavior. This dynamic characteristic is achieved through connections between nodes, forming a directed graph over a time sequence [125]. The internal state of the RNN enables it to effectively process input sequences of varying lengths. The introduction of RNN aimed to address the challenge faced by DNN in effectively accommodating temporally changing data [126]. RNNs are now being utilized more frequently in Fed-AIDS model for IoT device [92], which often involve continuous streams of temporal data. However, a notable drawback of RNNs lies in their lack of specific treatment for the activation function, potentially resulting in the continuous product of their partial derivatives causing gradient disappearance or even gradient explosion, particularly when the network has a high number of layers [126].

LSTM tackles the gradient vanishing problem present in classical RNNs by incorporating additional storage states [127]. This innovative approach effectively controls gradient vanishing using a gate function as an activation function, selectively allowing relevant information to pass through. This introduced forgetting gates to the original LSTM architecture, simulating memory forgetting [127]. Recognized for its outstanding performance, LSTM has become a classical architecture. LSTMs are utilized in Fed-AIDS modeling studies [84], [85], [93], due to their effectiveness in classifying and predicting based on time-series data. **AE**s adopt an unsupervised approach. Their encoding equation, $h = f(Wx + b)$, reflects their ability to compress data into a "normal" representation, and then reconstruct it, flagging anomalies as distortions [128]. They excel in identifying novel attacks without prior knowledge of attack patterns and learning efficient representations of network traffic [78], [87], [88], [113].

Subsequently, most common activation functions used in by these models for Fed-AIDS on IoT devices include activation function (SoftMax) [129], loss function (Cross-entropy) [130], regularization functions [131]. In typical setting, activation function used to convert a vector of scores into a probability distribution over classes in Eq. 1, where z is the vector of scores for each class, n is the number of classes, and p is the resulting probability distribution.

$$p_i = e^{z_i} \sum \left(e^{z_j}\right) \quad \forall i \in j = 1, 2, \ldots, n \tag{1}$$

In Cross-entropy loss it is used to measure the difference between predicted and actual class probabilities [130] in Eq. 2. In which y is a one-hot vector indicating the true class label, p is the predicted probability distribution, and log is the natural logarithm.

$$L = -\sum (y * log\,(p)) \tag{2}$$

Regularization function used to prevent overfitting and improve the generalization performance of models [131].

L1 and L2 regularization are two common forms of regularization. Eq. 3 describes lambda as hyperparameter that controls the strength of regularization, w is the weight vector donated as absolute value, meaning that it shrinks some of the weights to zero, effectively selecting only the most important features. Where in Eq. 4 w is the weight vector denotes it is squaring, which penalizes large weights and encourages the model to use smaller weights, effectively reducing overfitting.

$$L1 = \lambda * \sum |(w)| \tag{3}$$

$$L2 = \lambda * \sum \left(w^2\right) \tag{4}$$

However, these functions vary depending on the specific algorithm being used, but they are essential for learning complex relationships between the input data and output classes, measuring the difference between predicted and true class labels, preventing overfitting, measuring the similarity between input and training data, and predicting the class label based on the input data and learned model.

E. AGGREGATION FUNCTIONS

Aggregation functions are used in Fed-AIDS to aggregate the output from various distributed devices into a single overall model. Also, they are made to enable the training of a global model while also preserving the privacy of data from individual devices [132]. Notably, Federated Averaging (FedAvg) [77], [81], [84], [87], [90], [95], [112], [114], Federated+ (Fed+) [55], and Federated Stochastic Gradient Decent (FedSGD) [78], [79], [91] are the answer for **RQ6,** specifically identified three aggregation functions that are commonly employed in Fed-AIDS modeling on IoT devices. Figure 7 depicts these aggregation functions as appeared in the reviewed studies.

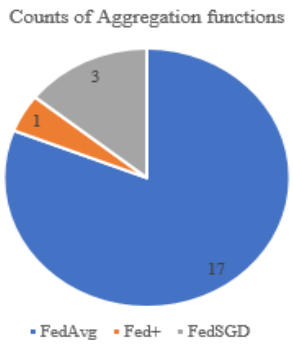

FIGURE 7. Most proposed aggregation functions in Fed-AIDS modeling.

In **FedSGD**, each device calculates the gradient of the global model on its local data, and the server averages these gradients to update the global model. This leads to frequent communication. This method is computationally efficient, but entails huge numbers of epochs of training to produce good models [18]. Therefore, in **FedAvg** [18], each device k computes the gradient of its local model parameters with respect to its local data using Eq. 5.

$$g_k = {}^1\!/_B * \sum_B^i \nabla\theta l\left(y_i, f_k, (x_i, \theta)\right) \forall k \in i = 1, 2, 3, , n \tag{5}$$

where **B** is the batch size, l is the loss function, y_i and x_i are the label and feature vector of the i-th data point, f_k is the local model on device k, and θ is the model parameters. Then, each device k sends its gradient to the central server. Where the central server aggregates the gradients from all devices k and computes the average gradient g_w using Eq. 6.

$$g_w = {}^1\!/_k * \sum_k^{k=1} g_k \tag{6}$$

The above instructions will be repeated for multiple rounds until the model has converged. The key idea behind FedAvg is to use the gradient information from each devices to update the global model in a collaborative way, while ensuring that the private data on each device remains private [18]. **Fed+** builds upon FedAvg by adapting learning rates for each device, further boosting convergence and handling data diversity better. All three algorithms involve minimizing a $l\theta$), with respect to model parameters, θ, using iterative updates based on accumulated weights. However, FedAvg is the popular method with 17 adoptions in the proposed Fed-AIDS modeling compared to FedSGD with three adoptions and Fed+ with one adoption. Compared to FedSGD and Fed+, FedAvg's balance of communication efficiency, convergence speed, and relative simplicity is presented in Table 10. It works well across various data sizes and learning tasks, making it a versatile tool for developing Fed-AIDS models for IoT devices.

TABLE 10. Trade-up between aggregation function.

Function	Communication Efficiency	Convergence Speed	Heterogeneity Handling	Privacy Considerations
FedSGD	Low	Can be slow	Limited	Potential privacy risks
FedAvg	Improved	Faster	Better	Still requires privacy measures
Fed+	Further improved	Faster	Best	Same as FedAvg

F. EVALUATION METRICS

Any ML model, including FL models, must undergo evaluation before being considered successful. A model's performance can be measured [133] or compared to other models and in which the areas for improvement can be found. Additionally, an evaluation of the model's reliability, which is necessary for making well-informed decisions on any Fed-AIDS for IoT devices [49]. In this research, we focus on the metrics used to evaluate Fed-AIDS models for IoT

devices in reviewed studies. Specifically, Figure 8 provides insights into the most frequently employed evaluation metrics, addressing our **RQ7** about their popularity in published studies. Although most of the metrics contributed detection/classification performance of the Fed-AIDS models, this include confusion matrix [80], [81], [112], [114], Matthews Correlation Coefficient (MCC) [78], Area Under Curve (AUC) [90], [134], Pearson Correlation Coefficient (PCC) [55], and also combined of Accuracy, Precision (Detection rate), Recall also known as True Positive Rate (TPR) and F-score [79], [86], [93], [115]. Lastly, False Alarm Rate (FAR) also known as False Positive Rate (FPR) [51]. While only AvgTime contributed computational performance [82], [91], [94].

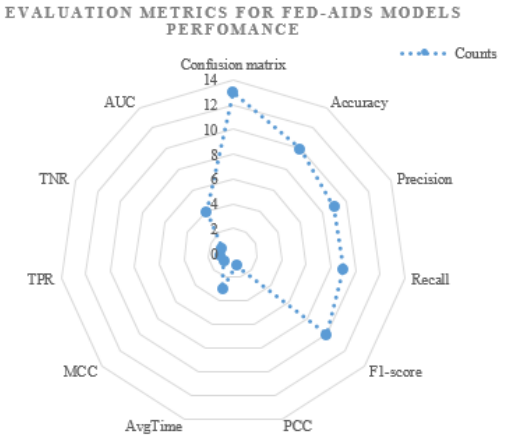

FIGURE 8. Proposed evaluation metrics.

These validation metrics represent the amount of True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN) predictions (occurrences) built by the classifier as presented in Table 11. While some refer to the performance of the classifier through the AUC, the ROC curve shows the TPR versus the FPR for various threshold values [135]. However, both metrics are crucial for improving classifiers and computational performance, in terms of Fed-AIDS modeling for securing IoT device.

IV. OPEN ISSUES AND FUTURE DIRECTIONS

This article explored Fed-AIDS modeling taxonomies in the context of securing IoT device, covering utilized tools/frameworks, most utilized datasets, non-IDD data handling complexities, the utilized aggregations functions and evaluation metrics. It emphasized conduction efficient Fed-AIDS modeling. Now, the focus shifts to identifying areas for further research in FL-AIDS modeling for IoT devices. These research gaps were pinpointed through a systematic analysis of existing taxonomies in Fed-AIDS modeling for IoT devices.

1) **Tools/Framework:** Despite the effectiveness of Fed-AIDS tools for implementing such of TFF, IBMFL, or PySyft, it is observed that it requires a deep understanding of the underlying concepts. As an example, the learning curve can be steep, especially for developers who are new to FL. Therefore, there is need for the availability of comprehensive documentation and resources for these specific tools in both academic and industry fields. Although individual documentation for these tools was provided and instantly updated accordingly. For example Flower has it is own respiratory documentation [74], likewise IBMFL [75], and PySyft [76]. Nevertheless, providing documentations of application of all these tools in application of Fed-AIDS can bridge the gap between academic research and practical industry solutions. This can help beginners and professionals in the IoT cybersecurity domain connect these technologies to enhance security measures while respecting data privacy. Additionally, this documentation could also tackle the issues that may arise when integrating FL frameworks with existing ML libraries. As this could be challenging issue when trying to combine FL tools with different technology such AIDS and IoT computing.
2) **Utilized Datasets:** Another interesting observation in the mostly utilized datasets for Fed-AIDS modeling for securing IoT device, it reveals certain limitations. These obstacles include small dataset size, imbalanced class distribution, and lack of diversity, non-representative features and privacy concerns. For example, N-BaIoT [101] could be a diverse dataset with IoT network trace, but considering the training instances and count of network traffic features could be less for training IoT cybersecurity model. Moreover, CICIDS2017 [99] could be effective in terms of feature representatives but ineffective in terms of diverse to IoT network trace. However, to overcome these limitations, several measures could be tackled. Initially, efforts could be made to gather larger and more diverse datasets to ensure better coverage of real-world IoT scenes. Secondly, steps could be taken to balance the class distribution within the datasets, ensuring that each class is balanced. Additionally, diversity could be enhanced by incorporating a wider range of IoT devices, network configurations, and attack scenarios. It is also important to ensure that the collected data is representative of the actual IoT network. However, by implementing these measures, it is possible to overcome the limitations and enhance the effectiveness of Fed-AIDS model for IoT devices. Hence, we strongly recommend the of Edge-IIoTset [104]. This dataset addresses the above limitations of the existing datasets and is correct for the vital requirements of IoT devices in Fed-AIDS modeling.
3) **Non-IDD Data Complexity:** Data augmentation, differential privacy and single model convergence are valuable techniques in addressing non-IID data issues in FL. However, they also have limitations, this include

TABLE 11. Evaluation metrics by confusion matrix.

Metrics	Formula	Description
Confusion matrix	--	Provides clear summary of TP, TN, FN and FP predictions made by classification model.
Accuracy	$(TP + TN)/(TP + TN + FP + FN)$	Successfully predicted occurrences to all expected occurrences proportion
Precision (Detection rate)	$TP/(TP + FP)$	Precision means the proportion of TP predictions among all positive predictions made by a classification model. It shows the accuracy of the model in accurately predicting positive instances.
Recall also known as TPR	$TP/(TP + FN)$	Proportion of accurately predicted positive instances to the entire number of actual positive instances in the dataset.
F-score	$2 \times (Precision \times Recall)/Precision + Recall$	A measure that combines precision and recall into a single metric, providing a balanced summary of the model's performance in terms of both precision and recall.
False Alarm Rate (FAR) also known as FPR	$FP/(FP + TN)$	Refers to metric used in classification models that calculates the proportion of negative instances that are incorrectly classified as positive by the model.
Matthews Correlation Coefficient (MCC)	$MCC = \frac{(TP \cdot \times TN) - (FP \times \cdot FN)}{\sqrt{(TP + FP) \cdot (TP + FN) \cdot (TN + FP) \cdot (TN + FN)}}$	Measures the correlation between the forecasted outcomes and the actual data. The MCC ranges from -1 to 1. A MCC value of +1 signifies 100% accuracy in the prediction, while a value of -1 indicates a completely incorrect prediction.
AUC	$\int_0^1 TP/P \; d \; FP/N$	AUC is measured by computing the area under the empirical ROC curve using numerical integration see Eq. 7, with higher AUC values indicating better performance.
Pearson Correlation Coefficient (PCC)	$PCC = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}}$	Measures the ratio of the covariance (joint variability) to the individual variability (standard deviations) of the two variables.
AvgTime	$AvgTime = \sum_{k=1}^{T} average \times time^k$	This metric refers to the average computational time in seconds. When the algorithm is run T-th iteration, it is average computational time is calculated using Equation 4. Where $average \times time^k$ is average computational time spent at run k device.

the effectiveness of data augmentation heavily relies on the available augmentation strategies and the diversity of data transformations [119], [136]. In cases where the data is highly diverse, predefined augmentations may not capture the full range of variations. Additionally, data augmentation can significantly increase the computational overhead, especially when dealing with a large volume of data and numerous clients in FL [136]. This can lead to slower training and model convergence. While some limitations of transfer learning include lack of source data. In some FL scenarios, finding a suitable source domain with ample labeled data can be challenging. While transfer learning relies on a well-labeled source dataset, and the absence of such data can limit its applicability [137]. Aiming at this problem, our future work in addressing non-IID data in FL could explore the use of genetic algorithms. Genetic algorithms are optimization techniques inspired by the process of natural selection and evolution [138], [139]. Through genetic operations, individuals with higher fitness (better solutions) are favored, and over multiple peers, this algorithm converges toward an optimal or near-optimal solution for the given problem. However, this could be applied in Fed-AIDS for IoT devices, which can potentially address some of the limitations of data augmentation and transfer learning in the context of non-IDD challenges. Firstly, adapting data augmentation to each client's needs, genetic algorithms can ensure that augmented data remains relevant and meaningful, addressing the limitation related to capturing diverse data transformations. Additionally, by reducing unnecessary augmentation operations,

genetic algorithms can mitigate the computational burden associated with data augmentation, making FL training more efficient. To sum it up, genetic algorithms can act as optimization tools to tailor data augmentation processes to the specific requirements and challenges of non-IDD of FL modeling. They can potentially address the limitations by optimizing data augmentation strategies, reducing computational overhead and enhancing privacy preservation in FL scenarios with non-IID data.

4) **Aggregation Functions:** Existing aggregation functions in Fed-AIDS modeling for IoT devices, such as FedAvg [90], FedSGD [78], and Fed+ [55], warrant exploration of more sophisticated alternatives such as FedProx and Q-FedAvg. These advanced functions address limitations inherent in FedAvg, FedSGD, and Fed+ by alleviating assumptions about every IoT device completing all epochs for the selected classifier to achieve convergence, in which some devices take longer than other does and each device has different network data. For this, future research should delve into these nuanced methods, offering potential enhancements in efficiency for aggregation mechanisms within Fed-AIDS model for IoT devices. For example, FedProx allows variable devices to variable amount of work [140].
5) **Evaluation Metrics:** During employing Fed-AIDS on IoT devices, challenges may also rise due to the limited computational resources and network connectivity constraints for IoT devices. These challenges need to be tackled. Meanwhile, only limited studies utilized computational performance of AvgTime [91], [94]. However, to guarantee the accuracy of the evaluation result, it is important to consider CPU utilization and energy consumption. This is to the evaluate percentage of the CPU load taken by a certain Fed-AIDS job and capacity vital for added energy to perform a certain Fed-AIDS job. These could affect the model's performance and make sure that the evaluation process preserves the integrity of the Fed-AIDS model of IoT devices.

V. CONCLUSION

The increasing data output from IoT devices is vital for industries such as healthcare, transportation, and smart cities. However, widespread IoT adoption raises security concerns, challenging centralized systems. Privacy violations, a single point of failure, and difficulty in identifying intruders underscore the need for enhanced security in IoT data evaluation. Our research addresses these challenges by exploring Federated Learning (FL), an ML technique enabling model training without sharing data. This approach enhances detection accuracy and efficiency, surpassing domain limitations in IoT device security. In contrast to previous studies that often focused primarily on investigating security assaults on IoT devices, our research systematically delves into the Fed-AIDS modeling process for IoT devices. We cover taxonomies that encompass workflow, tools, training datasets, technical complexities, classifier roles, aggregation tasks, and model validation metrics. Data from published studies were retrieved from the Scopus database, covering major publishers such as IEEE, Elsevier, and others. This comprehensive exploration not only emphasizes the significance of our work but also provides a practical roadmap for researchers and practitioners aiming to implement effective IoT device security solutions. This has the potential to achieve optimal or near-optimal accuracy for the Fed-AIDS model. Finally, we strongly believe that this proposed review on Fed-AIDS modeling for IoT devices can significantly enhance understanding of the field's progression and identify potential avenues for further studies.

REFERENCES

[1] T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and A. S. Avestimehr, "Federated learning for the Internet of Things: Applications, challenges, and opportunities," *IEEE Internet Things Mag.*, vol. 5, no. 1, pp. 24–29, Mar. 2022.

[2] K.-D. Thoben, S. Wiesner, and T. Wuest, "'Industrie 4.0' and smart manufacturing—A review of research issues and application examples," *Int. J. Autom. Technol.*, vol. 11, no. 1, pp. 4–16, Jan. 2017, doi: 10.20965/ijat.2017.p0004.

[3] A. Zohourian, S. Dadkhah, E. C. P. Neto, H. Mahdikhani, P. K. Danso, H. Molyneaux, and A. A. Ghorbani, "IoT Zigbee device security: A comprehensive review," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100791.

[4] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019, doi: 10.1109/COMST.2019.2910750.

[5] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review," *Sensors*, vol. 23, no. 8, p. 4117, Apr. 2023.

[6] A. A. Muazu and I. U. Audi, "Network configuration by utilizing cisco technologies with proper segmentation of broadcast domain in FNAS-UMYUK Nigeria," *J. Netw. Secur. Data Mining*, vol. 4, no. 1, pp. 1–13, 2021.

[7] E. Ashraf, N. F. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, "FIDChain: Federated intrusion detection system for blockchain-enabled IoT healthcare applications," *Healthcare*, vol. 10, no. 6, p. 1110, Jun. 2022.

[8] S. Saif, P. Das, S. Biswas, M. Khari, and V. Shanmuganathan, "HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare," *Microprocessors Microsyst.*, Aug. 2022, Art. no. 104622, doi: 10.1016/j.micpro.2022.104622.

[9] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: A deep learning-based intrusion detection framework for securing IoT," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, pp. 1–16, Mar. 2022, doi: 10.1002/ett.3803.

[10] D. Man, F. Zeng, W. Yang, M. Yu, J. Lv, and Y. Wang, "Intelligent intrusion detection based on federated learning for edge-assisted Internet of Things," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Oct. 2021.

[11] E. Rodríguez, P. Valls, B. Otero, J. J. Costa, J. Verdú, M. A. Pajuelo, and R. Canal, "Transfer-learning-based intrusion detection framework in IoT networks," *Sensors*, vol. 22, no. 15, p. 5621, Jul. 2022.

[12] M. Alanazi and A. Aljuhani, "Anomaly detection for Internet of Things cyberattacks," *Comput., Mater. Continua*, vol. 72, no. 1, pp. 261–279, 2022.

[13] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 296–312, Feb. 2023.

[14] S. Jamil and M. Rahman, "A comprehensive survey of digital twins and federated learning for industrial Internet of Things (IIoT), Internet of Vehicles (IoV) and Internet of Drones (IoD)," *Appl. Syst. Innov.*, vol. 5, no. 3, p. 56, Jun. 2022.

[15] A. Sultan, M. A. Mushtaq, and M. Abubakar, "IoT security issues via blockchain: A review paper," in *Proc. Int. Conf. Blockchain Technol.*, Mar. 2019, pp. 60–65.

[16] H. J. Hadi, Y. Cao, K. U. Nisa, A. M. Jamil, and Q. Ni, "A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs," *J. Netw. Comput. Appl.*, vol. 213, Apr. 2023, Art. no. 103607.

[17] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, "Survey of machine learning based intrusion detection methods for Internet of Medical Things," *Appl. Soft Comput.*, vol. 140, Jun. 2023, Art. no. 110227.

[18] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th Int. Conf. Artif. Intell. Statist.*, 2017, pp. 1273–1282.

[19] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konecný, S. Mazzocchi, B. McMahan, and T. van Overveldt, "Towards federated learning at scale: System design," in *Proc. Mach. Learn. Syst.*, vol. 1, 2019, pp. 374–388.

[20] M. F. Criado, F. E. Casado, R. Iglesias, C. V. Regueiro, and S. Barro, "Non-IID data and continual learning processes in federated learning: A long road ahead," *Inf. Fusion*, vol. 88, pp. 263–280, Dec. 2022.

[21] H. Tan, "An efficient IoT group association and data sharing mechanism in edge computing paradigm," *Cyber Secur. Appl.*, vol. 1, Dec. 2023, Art. no. 100003.

[22] M. R. Shahid, G. Blanc, Z. Zhang, and H. Debar, "IoT devices recognition through network traffic analysis," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 5187–5192.

[23] M. Arafeh, H. Ould-Slimane, H. Otrok, A. Mourad, C. Talhi, and E. Damiani, "Data independent warmup scheme for non-IID federated learning," *Inf. Sci.*, vol. 623, pp. 342–360, Apr. 2023.

[24] H. Wang, Z. Kaplan, D. Niu, and B. Li, "Optimizing federated learning on non-IID data with reinforcement learning," in *Proc. IEEE Conf. Comput. Commun.*, Jul. 2020, pp. 1698–1707, doi: 10.1109/INFOCOM41043.2020.9155494.

[25] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Netw.*, vol. 151, pp. 147–157, Mar. 2019.

[26] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100568, doi: 10.1016/j.iot.2022.100568.

[27] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, S. Bhattacharya, P. K. R. Maddikunta, and T. R. Gadekallu, "Federated learning for intrusion detection system: Concepts, challenges and future directions," *Comput. Commun.*, vol. 195, pp. 346–361, Nov. 2022.

[28] J. Zhou, S. Zhang, Q. Lu, W. Dai, M. Chen, X. Liu, S. Pirttikangas, Y. Shi, W. Zhang, and E. Herrera-Viedma, "A survey on federated learning and its applications for accelerating industrial Internet of Things," 2021, *arXiv:2104.10501*.

[29] A. Belenguer, J. Navaridas, and J. A. Pascual, "A review of federated learning in intrusion detection systems for IoT," 2022, *arXiv:2204.12443*.

[30] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100227, doi: 10.1016/j.iot.2020.100227.

[31] H. Kheddar, Y. Himeur, and A. I. Awad, "Deep transfer learning applications in intrusion detection systems: A comprehensive review," 2023, *arXiv:2304.10550*.

[32] S. Bansal and D. Kumar, "IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication," *Int. J. Wireless Inf. Netw.*, vol. 27, no. 3, pp. 340–364, Sep. 2020.

[33] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "When edge meets learning: Adaptive control for resource-constrained distributed machine learning," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2018, pp. 63–71.

[34] H. G. Abreha, M. Hayajneh, and M. A. Serhani, "Federated learning in edge computing: A systematic survey," *Sensors*, vol. 22, no. 2, p. 450, Jan. 2022.

[35] P. P. Ray, D. Dash, and D. De, "Edge computing for Internet of Things: A survey, e-healthcare case study and future direction," *J. Netw. Comput. Appl.*, vol. 140, pp. 1–22, Aug. 2019.

[36] J. Yuan and X. Li, "A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion," *IEEE Access*, vol. 6, pp. 23626–23638, 2018.

[37] S. Shahab, P. Agarwal, T. Mufti, and A. J. Obaid, "SIoT (social Internet of Things): A review," in *ICT Analysis and Applications*. Singapore: Springer, 2022, pp. 289–297.

[38] H. Jaidka, N. Sharma, and R. Singh, "Evolution of IoT to IIoT: Applications & challenges," in *Proc. Int. Conf. Innov. Comput. Commun. (ICICC)*, 2020. [Online]. Available: https://dx.doi.org/10.2139/ssrn.3603739

[39] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1622–1658, 3rd Quart., 2021.

[40] K. K. Patel, S. M. Patel, and P. Scholar, "Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies, application & future challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 6122–6131, 2016.

[41] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT services through software defined networking and edge computing: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1761–1804, 3rd Quart., 2020.

[42] A. Thakkar and R. Lohiya, "A review of the advancement in intrusion detection datasets," *Proc. Comput. Sci.*, vol. 167, pp. 636–645, Jan. 2020.

[43] S. V. Amanoul and A. M. Abdulazeez, "Intrusion detection system based on machine learning algorithms: A review," in *Proc. IEEE 18th Int. Colloq. Signal Process. Appl. (CSPA)*, May 2022, pp. 79–84.

[44] D. N. P. Suthishni and K. S. S. Kumar, "A review on machine learning based security approaches in intrusion detection system," in *Proc. 9th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2022, pp. 341–348.

[45] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, no. 1, pp. 1–27, Mar. 2021.

[46] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, and M. Nasser, "Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review," *Appl. Sci.*, vol. 11, no. 18, p. 8383, Sep. 2021.

[47] U. A. Isma'ila, K. U. Danyaro, M. F. Hassan, M. S. Liew, U. D. Maiwada, and A. A. Muazu, "Evaluation on bot-IoT dataset enabled reducing false alarm rate for IoT threats," *Kepes*, vol. 21, no. 3, pp. 490–504, 2023, doi: 10.5281/zenodo.7936583.

[48] Z. Lian and C. Su, "Decentralized federated learning for Internet of Things anomaly detection," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, May 2022, pp. 1249–1251.

[49] O. Shahid, V. Mothukuri, S. Pouriyeh, R. M. Parizi, and H. Shahriar, "Detecting network attacks using federated learning for IoT devices," in *Proc. IEEE 29th Int. Conf. Netw. Protocols (ICNP)*, Nov. 2021, pp. 1–6.

[50] M. Abdel-Basset, H. Hawash, K. M. Sallam, I. Elgendi, K. Munasinghe, and A. Jamalipour, "Efficient and lightweight convolutional networks for IoT malware detection: A federated learning approach," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 7164–7173, Apr. 2023.

[51] V. Rey, P. M. S. Sánchez, A. H. Celdrán, and G. Bovet, "Federated learning for malware detection in IoT devices," *Comput. Netw.*, vol. 204, Feb. 2022, Art. no. 108693.

[52] A. Tabassum, A. Erbad, W. Lebda, A. Mohamed, and M. Guizani, "FEDGAN-IDS: Privacy-preserving IDS using GAN and federated learning," *Comput. Commun.*, vol. 192, pp. 299–310, Aug. 2022.

[53] J. Li, Z. Zhang, Y. Li, X. Guo, and H. Li, "FIDS: Detecting DDoS through federated learning based method," in *Proc. IEEE 20th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Oct. 2021, pp. 856–862.

[54] R. Zhao, Y. Yin, Y. Shi, and Z. Xue, "Intelligent intrusion detection based on federated learning aided long short-term memory," *Phys. Commun.*, vol. 42, Oct. 2020, Art. no. 101157.

[55] P. Ruzafa-Alcázar, P. Fernández-Saura, E. Mármol-Campos, A. González-Vidal, J. L. Hernández-Ramos, J. Bernal-Bernabe, and A. F. Skarmeta, "Intrusion detection based on privacy-preserving federated learning for the industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 1145–1154, Feb. 2023.

[56] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting Internet of Things attacks," *Electronics*, vol. 8, no. 11, p. 1210, Oct. 2019.

[57] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107810.

[58] M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep learning-based intrusion detection for IoT networks," in *Proc. IEEE 24th Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Dec. 2019, p. 25609.

[59] S. Alkadi, S. Al-Ahmadi, and M. M. Ben Ismail, "Toward improved machine learning-based intrusion detection for Internet of Things traffic," *Computers*, vol. 12, no. 8, p. 148, Jul. 2023.

[60] N. Tekin, A. Acar, A. Aris, A. S. Uluagac, and V. C. Gungor, "Energy consumption of on-device machine learning models for IoT intrusion detection," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100670.

[61] Y. Yin, J. Jang-Jaccard, W. Xu, A. Singh, J. Zhu, F. Sabrina, and J. Kwak, "IGRF-RFE: A hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset," *J. Big Data*, vol. 10, no. 1, p. 15, Feb. 2023, doi: 10.1186/s40537-023-00694-8.

[62] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, Dec. 2019.

[63] J. Liu, J. Huang, Y. Zhou, X. Li, S. Ji, H. Xiong, and D. Dou, "From distributed machine learning to federated learning: A survey," *Knowl. Inf. Syst.*, vol. 64, no. 4, pp. 885–917, Apr. 2022.

[64] P. Kairouz et al., "Advances and open problems in federated learning," *Found. Trends Mach. Learn.*, vol. 14, nos. 1–2, pp. 1–210, Jun. 2021.

[65] A. Z. Tan, H. Yu, L. Cui, and Q. Yang, "Towards personalized federated learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 12, pp. 9587–9603, Dec. 2023.

[66] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowl.-Based Syst.*, vol. 216, Mar. 2021, Art. no. 106775.

[67] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1175–1191.

[68] R. Gálvez, V. Moonsamy, and C. Diaz, "Less is more: A privacy-respecting Android malware classifier using federated learning," 2020, *arXiv:2007.08319*.

[69] F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: A systematic literature review," *IEEE Access*, vol. 6, pp. 56046–56058, 2018, doi: 10.1109/ACCESS.2018.2872784.

[70] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," Software Eng. Group, Univ. Durham, Durham, U.K., Tech. Rep. EBSE-2007-01, 2007.

[71] R. Murray, *Writing for Academic Journals*. New York, NY, USA: McGraw-Hill, 2013.

[72] A. Qammar, J. Ding, and H. Ning, "Federated learning attack surface: Taxonomy, cyber defences, challenges, and future directions," *Artif. Intell. Rev.*, vol. 55, no. 5, pp. 3569–3606, Jun. 2022.

[73] P. Foley, M. J. Sheller, B. Edwards, S. Pati, W. Riviera, M. Sharma, P. N. Moorthy, S.-H. Wang, J. Martin, P. Mirhaji, P. Shah, and S. Bakas, "OpenFL: The open federated learning library," *Phys. Med. Biol.*, vol. 67, no. 21, Nov. 2022, Art. no. 214001.

[74] D. J. Beutel, T. Topal, A. Mathur, X. Qiu, J. Fernandez-Marques, Y. Gao, L. Sani, K. H. Li, T. Parcollet, P. P. B. de Gusmão, and N. D. Lane, "Flower: A friendly federated learning research framework," 2020, *arXiv:2007.14390*.

[75] H. Ludwig et al., "IBM federated learning: An enterprise framework white paper V0.1," 2020, *arXiv:2007.10987*.

[76] A. Ziller, A. Trask, A. Lopardo, B. Szymkow, B. Wagner, E. Bluemke, J. M. Nounahon, J. Passerat-Palmbach, K. Prakash, N. Rose, T. Ryffel, Z. N. Reza, and G. Kaissis, "PySyft: A library for easy federated learning," in *Federated Learning Systems: Towards Next-Generation AI*. Cham, Switzerland: Springer, 2021.

[77] O. Aouedi and K. Piamrat, "F-BIDS: Federated-blending based intrusion detection system," *Pervas. Mobile Comput.*, vol. 89, Feb. 2023, Art. no. 101750, doi: 10.1016/j.pmcj.2023.101750.

[78] X. Sáez-de-Cámara, J. L. Flores, C. Arellano, A. Urbieta, and U. Zurutuza, "Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks," *Comput. Secur.*, vol. 131, Aug. 2023, Art. no. 103299, doi: 10.1016/j.cose.2023.103299.

[79] T. T. Huong, T. P. Bac, D. M. Long, B. D. Thang, N. T. Binh, T. D. Luong, and T. K. Phuc, "LocKedge: Low-complexity cyberattack detection in IoT edge computing," *IEEE Access*, vol. 9, pp. 29696–29710, 2021.

[80] S. Abbas, A. A. Hejaili, G. A. Sampedro, M. Abisado, A. S. Almadhor, T. Shahzad, and K. Ouahada, "A novel federated edge learning approach for detecting cyberattacks in IoT infrastructures," *IEEE Access*, vol. 11, pp. 112189–112198, 2023, doi: 10.1109/ACCESS.2023.3318866.

[81] R. Lazzarini, H. Tianfield, and V. Charissis, "Federated learning for IoT intrusion detection," *AI*, vol. 4, no. 3, pp. 509–530, Jul. 2023, doi: 10.3390/ai4030028.

[82] F. L. de Caldas Filho, S. C. M. Soares, E. Oroski, R. de Oliveira Albuquerque, R. Z. A. da Mata, F. L. L. de Mendonça, and R. T. de Sousa Júnior, "Botnet detection and mitigation model for IoT networks using federated learning," *Sensors*, vol. 23, no. 14, p. 6305, Jul. 2023, doi: 10.3390/s23146305.

[83] E. M. Campos, P. F. Saura, A. González-Vidal, J. L. Hernández-Ramos, J. B. Bernabé, G. Baldini, and A. Skarmeta, "Evaluating federated learning for intrusion detection in Internet of Things: Review and challenges," *Comput. Netw.*, vol. 203, Feb. 2022, Art. no. 108661.

[84] T. A. Ahanger, A. Aldaej, M. Atiquzzaman, I. Ullah, and M. Yousufudin, "Federated learning-inspired technique for attack classification in IoT networks," *Mathematics*, vol. 10, no. 12, p. 2141, Jun. 2022, doi: 10.3390/math10122141.

[85] Y. Liu, S. Garg, J. Nie, Y. Zhang, Z. Xiong, J. Kang, and M. S. Hossain, "Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6348–6358, Apr. 2021.

[86] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021.

[87] O. Aouedi, K. Piamrat, G. Müller, and K. Singh, "Federated semisupervised learning for attack detection in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 286–295, Jan. 2023, doi: 10.1109/TII.2022.3156642.

[88] T. T. Huong, T. P. Bac, K. N. Ha, N. V. Hoang, N. X. Hoang, N. T. Hung, and K. P. Tran, "Federated learning-based explainable anomaly detection for industrial control systems," *IEEE Access*, vol. 10, pp. 53854–53872, 2022, doi: 10.1109/ACCESS.2022.3173288.

[89] T. T. Huong, T. P. Bac, D. M. Long, T. D. Luong, N. M. Dan, L. A. Quang, L. T. Cong, B. D. Thang, and K. P. Tran, "Detecting cyberattacks using anomaly detection in industrial control systems: A federated learning approach," *Comput. Ind.*, vol. 132, Nov. 2021, Art. no. 103509, doi: 10.1016/j.compind.2021.103509.

[90] A. Belenguer, J. A. Pascual, and J. Navaridas, "GöwFed: A novel federated network intrusion detection system," *J. Netw. Comput. Appl.*, vol. 217, Aug. 2023, Art. no. 103653, doi: 10.1016/j.jnca.2023.103653.

[91] A. Alotaibi and A. Barnawi, "IDSoft: A federated and softwarized intrusion detection framework for massive Internet of Things in 6G network," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 6, Jun. 2023, Art. no. 101575, doi: 10.1016/j.jksuci.2023.101575.

[92] M. M. Rashid, S. U. Khan, F. Eusufzai, M. A. Redwan, S. R. Sabuj, and M. Elsharief, "A federated learning-based approach for improving intrusion detection in industrial Internet of Things networks," *Network*, vol. 3, no. 1, pp. 158–179, Jan. 2023.

[93] P. Singh, G. S. Gaba, A. Kaur, M. Hedabou, and A. Gurtov, "Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 722–731, Feb. 2023, doi: 10.1109/JBHI.2022.3186250.

[94] B. Weinger, J. Kim, A. Sim, M. Nakashima, N. Moustafa, and K. J. Wu, "Enhancing IoT anomaly detection performance for federated learning," *Digit. Commun. Netw.*, vol. 8, no. 3, pp. 314–323, Jun. 2022, doi: 10.1016/j.dcan.2022.02.007.

[95] S. I. Popoola, R. Ande, B. Adebisi, G. Gui, M. Hammoudeh, and O. Jogunola, "Federated deep learning for zero-day botnet attack detection in IoT-edge devices," *IEEE Internet Things J.*, vol. 9, no. 5, pp. 3930–3944, Mar. 2022, doi: 10.1109/JIOT.2021.3100755.

[96] S. Agrawal, A. Chowdhuri, S. Sarkar, R. Selvanambi, and T. R. Gadekallu, "Temporal weighted averaging for asynchronous federated intrusion detection systems," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–10, Dec. 2021, doi: 10.1155/2021/5844728.

[97] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Nov. 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.

[98] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6.

[99] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, 2018, pp. 108–116.
[100] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput. Secur.*, vol. 31, no. 3, pp. 357–374, May 2012, doi: 10.1016/j.cose.2011.12.012.
[101] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: 10.1109/MPRV.2018.03367731.
[102] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, pp. 779–796, Nov. 2019.
[103] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustain. Cities Soc.*, vol. 72, Sep. 2021, Art. no. 102994, doi: 10.1016/j.scs.2021.102994.
[104] 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," *IEEE Access*, vol. 10, pp. 40281–40306, 2022.
[105] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.
[106] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, "Machine learning based IoT intrusion detection system: An MQTT case study (MQTT-IoT-IDS2020 dataset)," in *Proc. 12th Int. Netw. Conf.*, B. Ghita and S. Shiaeles, Eds. Cham, Switzerland: Springer, 2021, pp. 73–84.
[107] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "NetFlow datasets for machine learning-based network intrusion detection systems," in *Big Data Technologies and Applications*. Cham, Switzerland: Springer, 2020, pp. 117–135.
[108] T. Luo and S. G. Nagarajan, "Distributed anomaly detection using autoencoder neural networks in WSN for IoT," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[109] P. M. Laso, D. Brosset, and J. Puentes, "Dataset of anomalies and malicious acts in a cyber-physical subsystem," *Data Brief*, vol. 14, pp. 186–191, Oct. 2017.
[110] G. D'Angelo, F. Palmieri, A. Robustelli, and A. Castiglione, "Effective classification of Android malware families through dynamic features and neural networks," *Connection Sci.*, vol. 33, no. 3, pp. 786–801, Jul. 2021, doi: 10.1080/09540091.2021.1889977.
[111] S. Hajj, J. Azar, J. Bou Abdo, J. Demerjian, C. Guyeux, A. Makhoul, and D. Ginhac, "Cross-layer federated learning for lightweight IoT intrusion detection systems," *Sensors*, vol. 23, no. 16, p. 7038, Aug. 2023, doi: 10.3390/s23167038.
[112] S. Fenanir and F. Semchedine, "Smart intrusion detection in IoT edge computing using federated learning," *Revue d'Intelligence Artificielle*, vol. 37, no. 5, pp. 1133–1145, Oct. 2023, doi: 10.18280/ria.370505.
[113] V. T. Truong and L. B. Le, "MetaCIDS: Privacy-preserving collaborative intrusion detection for metaverse based on blockchain and online federated learning," *IEEE Open J. Comput. Soc.*, vol. 4, pp. 253–266, 2023, doi: 10.1109/OJCS.2023.3312299.
[114] M. Sarhan, W. W. Lo, S. Layeghy, and M. Portmann, "HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection," *Comput. Electr. Eng.*, vol. 103, Oct. 2022, Art. no. 108379, doi: 10.1016/j.compeleceng.2022.108379.
[115] D. C. Attota, V. Mothukuri, R. M. Parizi, and S. Pouriyeh, "An ensemble multi-view federated learning intrusion detection for IoT," *IEEE Access*, vol. 9, pp. 117734–117745, 2021, doi: 10.1109/ACCESS.2021.3107337.
[116] Y. Zhao, M. Li, L. Lai, N. Suda, D. Civin, and V. Chandra, "Federated learning with non-IID data," 2018, *arXiv:1806.00582*.
[117] A. A. Abdellatif, N. Mhaisen, A. Mohamed, A. Erbad, M. Guizani, Z. Dawy, and W. Nasreddine, "Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced data," *Future Gener. Comput. Syst.*, vol. 128, pp. 406–419, Mar. 2022.
[118] H. Wang, L. Muñoz-González, D. Eklund, and S. Raza, "Non-IID data re-balancing at IoT edge with peer-to-peer federated learning for anomaly detection," in *Proc. 14th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2021, pp. 153–163.
[119] M. Duan, D. Liu, X. Chen, Y. Tan, J. Ren, L. Qiao, and L. Liang, "Astraea: Self-balancing federated learning for improving classification accuracy of mobile deep learning applications," in *Proc. IEEE 37th Int. Conf. Comput. Design (ICCD)*, Nov. 2019, pp. 246–254.
[120] D. Rani, N. S. Gill, P. Gulia, and J. M. Chatterjee, "An ensemble-based multiclass classifier for intrusion detection using Internet of Things," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–16, May 2022.
[121] V. Sze, Y.-H. Chen, T.-J. Yang, and J. S. Emer, "Efficient processing of deep neural networks: A tutorial and survey," *Proc. IEEE*, vol. 105, no. 12, pp. 2295–2329, Dec. 2017.
[122] M. W. Gardner and S. R. Dorling, "Artificial neural networks (the multilayer perceptron)—A review of applications in the atmospheric sciences," *Atmos. Environ.*, vol. 32, nos. 14–15, pp. 2627–2636, Aug. 1998.
[123] G. Xavier and B. Yoshua. (Mar. 31, 2010). *Understanding the Difficulty of Training Deep Feedforward Neural Networks*. [Online]. Available: https://proceedings.mlr.press/v9/glorot10a.html
[124] M. B. Alazzam, F. Alassery, and A. Almulihi, "Federated deep learning approaches for the privacy and security of IoT systems," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–7, Apr. 2022, doi: 10.1155/2022/1522179.
[125] S. Dupond, "A thorough review on the current advance of neural network structures," *Annu. Rev. Control*, vol. 14, no. 14, pp. 200–230, 2019.
[126] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997, doi: 10.1162/neco.1997.9.8.1735.
[127] F. A. Gers, J. Schmidhuber, and F. Cummins, "Learning to forget: Continual prediction with LSTM," *Neural Comput.*, vol. 12, no. 10, pp. 2451–2471, Oct. 2000, doi: 10.1162/089976600300015015.
[128] C. Zhou and R. C. Paffenroth, "Anomaly detection with robust deep autoencoders," in *Proc. 23rd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2017, pp. 665–674.
[129] K. Duan, S. S. Keerthi, W. Chu, S. K. Shevade, and A. N. Poo, "Multi-category classification by soft-max combination of binary classifiers," *Multiple Classifier Syst.*, vol. 2709, pp. 125–134, Jan. 2003.
[130] S. Mannor, D. Peleg, and R. Rubinstein, "The cross entropy method for classification," in *Proc. 22nd Int. Conf. Mach. Learn.*, 2005, pp. 561–568.
[131] X. Ying, "An overview of overfitting and its solutions," *J. Phys., Conf. Ser.*, vol. 1168, Feb. 2019, Art. no. 022022.
[132] A. N. Jahromi, H. Karimipour, and A. Dehghantanha, "An ensemble deep federated learning cyber-threat hunting model for industrial Internet of Things," *Comput. Commun.*, vol. 198, pp. 108–116, Jan. 2023.
[133] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: A review," *Proc. Comput. Sci.*, vol. 171, pp. 1251–1260, Jan. 2020.
[134] G. D'Angelo, E. Farsimadan, M. Ficco, F. Palmieri, and A. Robustelli, "Privacy-preserving malware detection in Android-based IoT devices through federated Markov chains," *Future Gener. Comput. Syst.*, vol. 148, pp. 93–105, Nov. 2023, doi: 10.1016/j.future.2023.05.021.
[135] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, Jun. 2006.
[136] J. Gu, L. Wang, H. Wang, and S. Wang, "A novel approach to intrusion detection using SVM ensemble with feature augmentation," *Comput. Secur.*, vol. 86, pp. 53–62, Sep. 2019.
[137] K. Weiss, T. M. Khoshgoftaar, and D. Wang, "A survey of transfer learning," *J. Big data*, vol. 3, no. 1, pp. 1–40, May 2016.
[138] Y. Zhang, P. Li, and X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019.
[139] O. A. Arqub and Z. Abo-Hammour, "Numerical solution of systems of second-order boundary value problems using continuous genetic algorithm," *Inf. Sci.*, vol. 279, pp. 396–415, Sep. 2014, doi: 10.1016/j.ins.2014.03.128.
[140] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," in *Proc. Mach. Learn. Syst.*, vol. 2, 2020, pp. 429–450.

UMAR AUDI ISMA'ILA received the B.Sc. degree in computer science from Umaru Musa Yar'adua University. He is currently pursuing the master's (by Research) degree in information technology with Universiti Teknologi PETRONAS. His research interests include the security of IoT devices through classification machine learning and federated learning techniques. He is dedicated to making valuable contributions to the field of information technology and IoT device security through his research pursuits.

KAMALUDDEEN USMAN DANYARO (Member, IEEE) received the bachelor's degree in mathematics from Bayero University, Kano, Nigeria, the master's degree in business information technology from Northumbria University Newcastle, U.K., and the Ph.D. degree from Universiti Teknologi PETRONAS, Malaysia.

He was a Postdoctoral Researcher and a Data Engineer with the Offshore Engineering Centre, Universiti Teknologi PETRONAS (UTP), Perak, Malaysia. He is currently a Lecturer with the Department of Computer and Information Science, UTP. He is also a Researcher and a member of the Center for Research in Data Science (CeRDaS), Institute of Autonomous Systems (AIS), UTP. He had six years of experience in industry and more than seven years of research and academic experience in the fields of data science, computer networking, and knowledge representation. His current research interests include data science, computer networking, and security. He is a MikroTik Certified Network Associate (MTCNA), MikroTik Certified Routing Engineer (MTCRE), an Association for Computing Machinery (ACM) Professional Member, and an Association for Information Systems (AIS) Academic Member. He is a reviewer for many conferences and journals.

AMINU AMINU MUAZU received the B.Sc. degree in computer science from Umaru Musa Yar'adua University, Katsina, Nigeria, in 2011, and the M.Sc. degree in software engineering from Universiti Malaysia Pahang (UMP), Malaysia, in 2017. Since 2022, he has been an Academic Staff holding the post of a Lecturer I with the Department of Computer Science, Umaru Musa Yar'adua University. He held different positions, such as the Undergraduate Project Coordinator, the Examination Officer, and the Level Advisor. His main research interests include software engineering, combinatorial t-way software testing, and optimization algorithms. He received the Award of the Best Student of Master's Final Year Project Competition from Universiti Malaysia Phang, in 2016, and the Merit Award of Recognition as a Community Volunteer (Computer Application Instructor) from EC Computer Ltd., Katsina, in 2014.

UMAR DANJUMA MAIWADA received the B.Sc. degree in computer science from Bayero University, Kano, and the M.Sc. degree in computer science from Jodhpur National University, India. He is currently a Lecturer II with Umaru Musa Yar'adua University, Katsina. He is also an Education Enthusiast who strives for excellence and precision in every circumstance to contribute his best in order to improve organizational objectives and achieve managerial goals. He was awarded a certificate in computer networks (CCNA) at HiiT, Kano, with merit. He also holds certificates in information communication technology (ICT), skills acquisition, advanced digital appreciation programs for tertiary institutions (ADAPTI), and SPSS. He is proficient in computer networks, mobile communication, application packages, and programming (C++, Web).