electronics

Review

A Comprehensive Survey on Generative AI Solutions in IoT Security

Juan Luis López Delgado [1,†] and Juan Antonio López Ramos [2,*,†]

[1] Elastacloud, Ltd., P Almería, 63, 04004 Almería, Spain; jld791@inlumine.ual.es
[2] Department of Mathematics, University of Almería, 04120 Almería, Spain
* Correspondence: jlopez@ual.es
† These authors contributed equally to this work.

Abstract: The influence of Artificial Intelligence in our society is becoming important due to the possibility of carrying out analysis of the large amount of data that the increasing number of interconnected devices capture and send as well as making autonomous and instant decisions from the information that machines are now able to extract, saving time and efforts in some determined tasks, specially in the cyberspace. One of the key issues concerns security of this cyberspace that is controlled by machines, so the system can run properly. A particular situation, given the heterogeneous and special nature of the environment, is the case of IoT. The limited resources of some components in such a network and the distributed nature of the topology make these types of environments vulnerable to many different attacks and information leakages. The capability of Generative Artificial Intelligence to generate contents and to autonomously learn and predict situations can be very useful for making decisions automatically and instantly, significantly enhancing the security of IoT systems. Our aim in this work is to provide an overview of Generative Artificial Intelligence-based existing solutions for the very diverse set of security issues in IoT environments and to try to anticipate future research lines in the field to delve deeper.

Keywords: Artificial Intelligence; Cybersecurity; Internet of Things; AIoT; cyberattack

Citation: López Delgado, J.L.; López Ramos, J.A. A Comprehensive Survey on Generative AI Solutions in IoT Security. *Electronics* **2024**, *13*, 4965. https://doi.org/10.3390/electronics13244965

Academic Editor: Flavio Canavero

Received: 6 October 2024
Revised: 4 December 2024
Accepted: 12 December 2024
Published: 17 December 2024

1. Introduction

Undoubtedly the Internet is one of the most important tools for humanity since its appearance and it has contributed to the digitalization of societies, bringing connectivity, efficiency and comfort to our lives among many other advantages, but resulting in many other challenges with respect to providing security when we make use of any online tool or communication system. The amount of data circulating through the Internet is increasing exponentially, especially since the birth of the Internet of Things (IoT), which is considered to have appeared sometime between 2008 and 2009 [1] and represents the first evolution of the Internet. IoT refers to a network of physical devices, vehicles, appliances and other physical objects that are embedded with sensors, software and network connectivity, allowing them to collect and share data [2]. The appearance of IoT played a fundamental roll in the so-called datafication of our society, i.e., we are experiencing a phenomenon that quantifies human life through digital information, very often due to economic values and with major consequences in many aspects of our lives [3]. This has led international institutions and governments to strongly consider the necessity of efficient and effective methods to protect data, not only those connected to companies and organizations, but also to individuals [4].

According to [5], in 2023, the total number of IoT connections, including wide-area IoT, cellular IoT and short-range IoT reached 15.7 billion and it is estimated to become 38.8 billion by 2029. Thus, protecting data arising and circulating from all these devices becomes a real challenge as well as a presenting opportunities to those aiming to take advantage of the information provided by these data [6]. Most of the IoT architecture models are

composed of a number of functional components ranging from 3 to 7, from the perception to application layers passing through the transport layer in a basic model architecture [7] and every functional component is susceptible to an information leakage, so security is a crucial issue. IoT is basically the interconnection of a huge heterogenous network of frameworks and systems that use different patterns of communications, including human to human or human to thing as in traditional communications, but also thing-to-thing patterns [8]. Thus, conventional security architecture does not address all security issues appearing in this paradigm given that it does not take into account patterns where machines communicate directly to machines and new approaches have to be considered [9]. Then, the first task is to determine the security challenges and attacks that such heterogenous networks face. In [10–23], it is possible to find different attack taxonomies, as well as detection methods and challenges. Among these works, the most recent, i.e., [21–23], cite Artificial Intelligence-based methods for attack detection.

The use of Artificial Intelligence (AI) helps to understand, learn, reason and interact, increasing efficiency. AI technology such as Machine Learning allows extracting knowledge from large amounts of structured and unstructured data provided by multiple sources, to make decisions and to take appropriate actions [24]. One of the application fields is IoT, which is being increasingly incorporated into organizations and is an AI-based asset-management systems that can solve many challenges that arise by feeding new levels of intelligence to a human team across use cases [25].

Generative Adversarial Networks (GANs) were first introduced by Goodfellow et al. in [26] as a model that connects supervised and unsupervised learning, becoming the most inspirational work in AI and revolutionizing the approaches to finding AI-based solutions to the increasing number of challenges in communication networks and particularly in IoT environments. GANs have promoted many emerging data-driven applications related to Big Data given that these models can help to improve and to innovate in technical applications due to their capability to learn from huge amounts of data, as well as working with multiple modal outputs obtained from a single input and where more than one of these outputs can be correct.

In Figure 1, we can observe the functioning of a Generative Adversarial Network. This consists of two neural networks, named generator and discriminator, respectively, trained simultaneously in a competitive framework. The generator learns to produce realistic data samples by transforming random noise into data, while the discriminator evaluates whether a given sample is real (from the original dataset) or fake (produced by the generator). The generator aims to fool the discriminator by creating increasingly realistic samples, while the discriminator improves its ability to distinguish real from fake. This adversarial process drives both networks to improve iteratively, resulting in the generator producing high-quality, realistic samples over time.

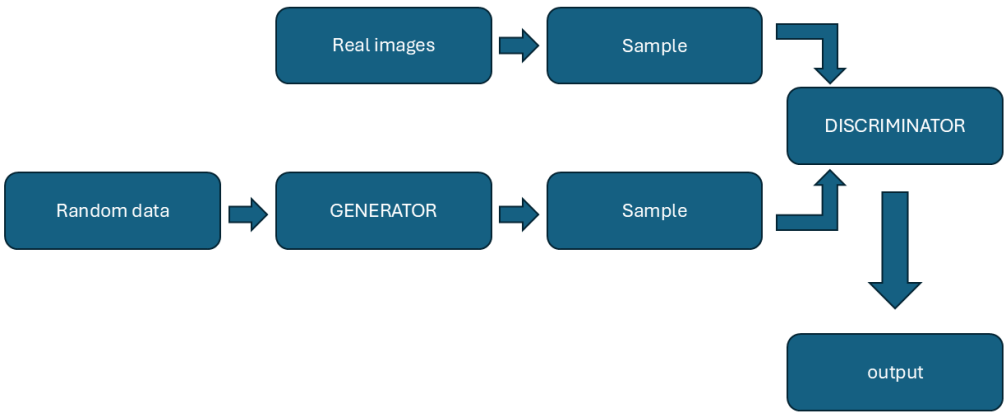

Figure 1. Flowchart of a Generative Adversarial Network model.

This inspirational idea has led to a new field in AI focused in models capable of generating original content known as Generative AI, imitating human intelligence. Figure 2 depicts a diagram flow of a Generative AI (GenAI) model. This starts with input data, which are then processed to create embeddings, a structured representation of these data. Next, the embeddings are fed into the GenAI model, which generates the desired output, completing the transformation from raw input to a meaningful result.

Figure 2. A general Generative AI model.

The other models that are currently widely spread are the Variational Autoencoder model, the Transformer-based model and the Diffusion model.

Variational Autoencoders (VAEs) (see Figure 3) are generative models that transform input data into a compressed representation within a probabilistic latent space. They use an encoder to compute two parameters, the mean and variance, which define a probabilistic distribution in the latent space, where data are represented in lower dimensions using a reparameterization technique. A decoder takes the values contained in the latent space and generates a reconstruction that approximates the original data, optimizing a loss function composed of a term measuring the difference between the encoder inputs and the information that can be retrieved from the decoder outputs and a regularization term to ensure a well-distributed latent space. This enables the VAE to learn useful data representations and generate new samples similar to the original dataset.

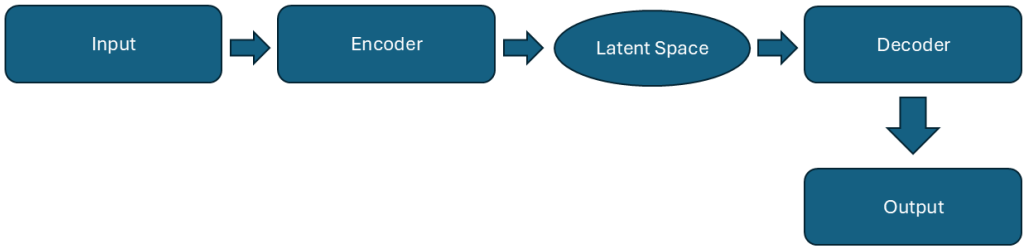

Figure 3. Flowchart of a Variational Autoencoder.

On the other hand, Transformer-based models (see Figure 4) are highly versatile architectures designed to handle sequential and contextual data, such as text, code or temporal sequences. They leverage attention mechanisms to model relationships between sequence elements. The process begins with discrete input data (e.g., words or tokens) that are converted into dense vectors through embeddings, incorporating positional information. A Transformer layer uses multihead attention to capture relationships between elements regardless of their relative position, followed by a feedforward network to refine the representations. The output provides contextualized representations of each sequence element, which are then used for tasks like classification, translation or token-by-token generation. Transformers underpin models like GPT (for text generation) and BERT (for contextual representation), revolutionizing fields such as NLP, computer vision and bioinformatics by effectively handling long dependencies and learning complex patterns.

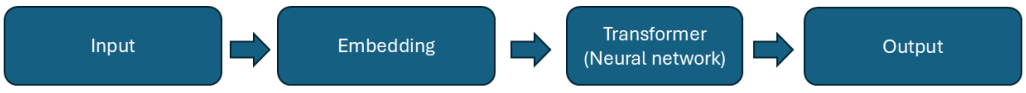

Figure 4. Flowchart of a Transformer-based model.

Finally, Diffusion models (see Figure 5) are a type of generative model that transform structured data into Gaussian noise and then learn to reverse this process to generate new data. This approach involves two main steps: a forward process, where progressive noise is added to the original data over several iterations until it becomes a completely random representation, typically a standard normal distribution; and a reverse process, where the model learns to step-by-step denoise the random representation (noised data) using a trained network (commonly a denoising model) to reconstruct the original data or generate new, similar samples. At the end of this process, the generated data mimic the statistical properties of the original dataset. Diffusion models are particularly effective for image-generation tasks, excelling at producing highly detailed and realistic samples.

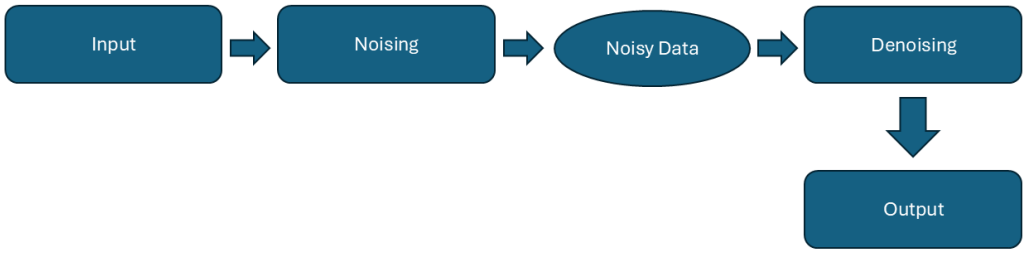

Figure 5. Flowchart of a Diffusion model.

The aim of this work is to study how Generative AI is motivating nowadays the development of solutions to the great amount of IoT security challenges. We provide a review of recent works on Generative AI and classify them with respect to their application in several areas of IoT security, discerning the way they are improving the security of the huge amount of managed and transmitted data, as well as the devices, networks and users that compose an IoT environment.

The main contributions of this work are the following:

- We provide a study of previous review works on Generative AI applied on IoT Cybersecurity;
- We study the use of different Generative AI models in different areas of IoT Cybersecurity;
- We classify recent works in Generative AI by their application field in IoT Cybersecurity and identify those less explored.

Thus, we can summarize the content of this review work in the following way. In Section 2, we cite some works collecting applications of AI in Cybersecurity. In some cases, the survey collects applications of Machine Learning or Deep Learning in specific fields of Cybersecurity such as anomalous traffic detection, intrusion detection or specific attacks, whereas some others are focused in IoT environments. Here, we review the most recent trends in AI that are applied in Cybersecurity of IoT networks. Section 3 is devoted to enumerating the fields of IoT Cybersecurity and for each one we cite novel approaches and applications based on Generative Artificial Intelligence that are having an impact. We divided this section into subsections to categorize the works concerning these application fields. The first subsection concerns Access Control models, an essential part of Cybersecurity to preserve privacy and availability of the IoT network data and resources. Authentication, a process that plays a central role in any Access Control model, and proposals in this direction are collected at the end of this subsection. A very recent technique that allows authentication of the information is Blockchain, which is the objective of the second subsection of Section 3. Blockchain turns out to be very convenient in distributed environments and with a deep Generative AI model impact. Another research field directly related to this is discussed in the next subsection and this is Cyber Threat Detection, a crucial issue in environments with an absence of central trust authorities and where detection methods have received a considerable boost with the use of Generative AI. The development of techniques that allow an efficient use of a network drive applications of generative models in IoT software security tools. This field is treated in Section 3.4. Privacy is directly related by definition with encryption algorithms, so we dedicate Section 3.5 to

reviewing how generative AI models can help to reinforce encryption. In the section, we observe that every generative model needs datasets for training and thus Section 3.6 is devoted to applications in IoT data traffic generation. Concerning the application fields, we end the discussion of them by addressing applications to Penetration Testing, dealt with in Section 3.7. Penetration Testing is a group of techniques that allow one to audit a network system. We will see how we can automate these processes using generative models. Finally, Section 3.8 is devoted to the very recent application of Large Language Models (LLM) in some of the aforementioned Cybersecurity methods. The reason for this is to emphasize the novelty of the application of LLM, included in the Transformer-based model mentioned above. In Section 4, we include a discussion of the impact of Generative AI models in IoT Cybersecurity, identifying those fields that are less explored and that could represent promising research lines. The paper ends with the conclusions that we can extract from our wide collection of works and that show that generative models are already established as a main research trend in some Cybersecurity applications and the huge possibilities that these offer with respect to enhancing the Cybersecurity and Quality of Service of IoT networks.

2. Materials and Methods

In the recent years, much attention has been paid to recent developments and new applications of AI in IoT as shown by the explosive growth of publications in the field. A good proof of this is the existence of many surveys that collect this huge number of papers appearing in multiple journals and conference proceedings, some of them focused in specialized technologies such as Deep Learning (DL) or more generally Machine Learning (ML), some others gathering publications related to some specific type of attacks. In this section, we would like to list some of them that motivated us to make our own collection with a specific purpose.

2.1. Some Non-Generative ML/DL Review Works

One of the main characteristics of IoT environments is the open nature of the communication channel given that the vast majority of the communications used to be wireless. Therefore, conventional methods to monitor the traffic and appearing anomalies cannot be applied. These anomalies can be the result of illegal access or intrusions and some ML methods can be very useful for detecting them. In [27], the authors provide a comprehensive survey of outlier-detection approaches based on ML for IoT, analyzing the corresponding advantages and drawbacks, providing some open issues to be solved and motivating future research.

The purpose of [28] is twofold: on the one hand, the authors select and classify some security issues depending on the different IoT layers they consider, which correspond to an IoT architecture given by the perception, the network, the middleware and the application layers and then they provide a study of papers based on ML and DL techniques that can address these issues.

In other cases, the survey papers also collect ML techniques applied to specific attacks such as Denial of Service (DoS) or Distributed Denial of Service (DDoS), as in the case of [29]. In this work, the authors compile different approaches to detect DDoS attacks in IoT-based networks using ML models as well as to study their limitations and thus try to derive appropriate research directions for improving this type of attack detection in IoT networks using these models.

This is also the case of [30], where the authors study the layered architecture of IoT networks and an array of security challenges, heightening the vulnerability of IoT devices to potential DDoS attacks as well as the life cycle and the launch mechanism of IoT Botnet and the corresponding variants responsible for much of this malicious activity. Then, they provide a collection of papers on AI techniques that can detect these attacks, both ML- and DL-based.

In a more general context, other review works try to assess AI algorithms for classifying or/and detecting intrusions and attacks as in [31], which appears as a work with a very general purpose, given that it gives a relationship between Cybersecurity in IoT and AI, by introducing different cyberattacks against IoT devices, and it recommends some existing AI based methods for their protection.

In [32], the author develops work similar to the previous one and describes the security requirements and challenges encountered in Industrial Internet of Things (IIoT) environments. Then, there is an exploration of solutions based on AI to these security challenges, introducing a study of appropriate AI-based alternatives to prevent or detect different attacks. To do so, the author classifies the attacks concerning the corresponding layer where the attack takes place: perception, network or application layers and then solutions based on different technologies studied in the literature are provided.

2.2. Surveys on Access Control

Anomaly detection is one of the first application fields that researchers identify to have benefited from the use of ML techniques, which constitutes the aim of [33]. In this work, the authors describe the state-of-the-art on ML techniques that detect anomalies in a system that could be the result of an intrusion or an attack based on a zero-day vulnerability. They also analyze the use of ML techniques for IoT anomaly detection and specially focus on the Federated Learning technique that could help in a collaboratively effective training of ML models to this end by making use of Blockchain. Some of the cited works make use of the VAE model.

Deep Learning (DL) techniques are particularly useful with large amounts of data, such as those provided by IoT systems. Thus, the use of this special case of ML techiques is also widely studied by many researchers and this is reflected as well in some existing surveys on this AI technique applied in IoT Cybersecurity. The survey presented in [34] offers a collection of papers where ML and DL techniques are used again for intrusion detection. They examine some of the IoT challenges and analyze the feasibility of technologies such as multi-access edge computing with respect to designing security applications for the IoT, revising the placement strategies used in multi-access edge computing to develop Intrusion-Detection Systems for the IoT. They also review various datasets and metrics used to develop these Intrusion-Detection Systems, some of them based on GANs and VAEs, and propose a security framework for the resource-constrained IoT systems by utilizing multi-access edge computing.

In [35], the authors try to obtain an answer to the problem of performing data transformation/preprocessing analysis of IoT datasets to perform anomaly detection. They conduct a literature review on papers that use DL to detect anomalies that could be the result of an intrusion in the IoT system. Generative AI methods used in some of these works include the GAN model.

The author of [36] classifies and characterizes the intrusion-detection methodologies that use ML applied to IoT security, focusing specially on recent advancements in intrusion detection across several IoT domains such as medical, industrial, farming IoT, etc. The Generative AI models cited include GANs, VAEs and Diffusion-based models. The author provides a classification of the Intrusion-Detection Systems concerning certain attacks. He also addresses the requirement for new datasets to assess ML models for this intrusion-detection task.

Another significant work that gathers ML and DL techniques applied to intrusion detection in IoT systems, including GAN-based models, is [37]. Here, the authors pick out those works that use bio-inspired methodologies integrated with ML and DL techniques. They classify the algorithms with respect to three different categories: evolutionary, swarm-based and ecology. They name evolutionary those algorithms that treat dataset features as chromosomes, gauging feature importance through fitness evaluation. The chosen features are subsequently integrated into the classification module, where diverse attack patterns drive effective classification. In the case of the swarm-based category, the algorithms start

with a phase that configures parameter values and persistently operates until specified termination conditions are met or a stop criterion is triggered. The fitness function is evaluated for each solution, leading to mathematical adjustments guided by the results. Assessing fitness functions for individual solutions or search agents in the swarm aids in proposing a taxonomy and identifying the most suitable solution for the problem. Finally, they consider ecology-based systems that can be presented in homogeneous or heterogeneous forms. In the first case, all populations evolve using the same optimization strategy and identical parameters, whereas in the heterogeneous model, strategies or parameters may vary among populations.

On a more practical side, the work presented in [38] provides again a collection of ML and DL algorithms, including case studies with GAN and VAE models. They implemented some of these algorithms with various adjustments to detect botnet attacks on several IoT devices, showing the great utility of some of them.

The objective of [39] goes further than the preceding works. This review paper compares the performance assessment of AI algorithms, including GAN-based schemes, for classifying or/and detecting intrusions and attacks in order to improve security in the IoT domain. The attacks are classified with respect to four layers: physical, the one where perception is developed; network, which is the one in charge of transmitting these from the sensors; middleware, in charge of processing and analyzing IoT data, decision making and removing anomalies; and finally, the application layer. The authors aim to give a general vision of the classification methods.

Another detachable work is [40], where the authors make a comparative analysis of state-of-the-art ML-based Intrusion-Detection Systems (IDSs) in the landscape of IoT security. This work does not include more references than the previous works, but they discern some unresolved issues and challenges within this field and provide a future vision with Generative AI and Large Language Models to enhance IoT security.

In [41], the authors review the Federated Learning-based security and privacy systems for several types of IoT applications, including application to the construction of an Intrusion-Detection System (IDS). They also list some vulnerabilities that can be exploited in Federated Learning and show how GANs can help not only to enhance efficiency in the training process, but also to avoid such vulnerabilities.

2.3. Surveys on Cyber Threat Detection

Privacy is a major concern in Cybersecurity and particularly in IoT environments given the limited capabilities of the devices and the increasingly sophisticated attacks. This has lead researchers to consider the use of ML techniques for a better detection of novel cyberattacks and their accuracy. In [42], the authors identify the challenges for successful application of ML to privacy protection in these environments and provide a complete review of research work that applies ML techniques for privacy protection in IoT. AboulEla et al's review ([43]) is a more recent work in the same direction, but focusing on privacy protection focused in healthcare environments. Both studies include works that make use of the GAN model.

In this context, ref. [44] addresses several approaches including cryptographic technologies, perturbation schemes and adversarial training that help to solve challenges, such as security attacks and privacy-leakage problems of Federated Learning in the edge IoT. The authors enumerate a series of security attacks based on GAN training that can affect the system producing a privacy leakage of the transmitted data.

The review paper [45] provides a revision of adversarial attacks against ML-based Intrusion-Detection Systems, Malware-Detection Systems and Device-Detection Systems. providing classifications for both adversarial attack-generation methods and adversarial defense mechanisms, including generative methods.

The very recent survey [46] analyzes methods, some of them based on GAN and/or VAE models, to detect cyber threats, including different types of attacks and compare them.

They focus on and compare works based on DL and ML approaches, evaluate the available IoT datasets and provide a detailed analysis, including their issues and advantages.

2.4. Surveys on IoT Traffic Data Generation

The use of data training sets for enhancing the behavior of different applications for Cybersecurity is essential. Thus, the larger the datasets are, the more effective the training will be, and therefore generation of traffic data that simulate real situations that include malicious traffic data turns out to be very important. In this sense, the papers [47–49] contain reviews on applications of GANs in Cybersecurity, citing some works related to IoT that concern, respectively, the use of GANs to generate adversarial data which can then serve as training data for other Machine Learning models in order to detect attacks or data that can fool a security system, privacy preserving speech of voice assistant or space-temporal data in IoT systems and applications of synthetic data for privacy preserving.

Table 1 summarizes the aforementioned review papers citing, among their references, works that make use of Generative AI models to be applied for some IoT Cybersecurity applications. As can be observed, despite the fact of the big number of existing surveys, there are no review papers that collect the works that make use of the distinct Generative AI models and list all possible applications for IoT Cybersecurity.

Table 1. AI Cybersecurity surveys citing generative models .

Reference	Application	GenAI Model
[33]	Access Control	VAE
[34]	Access Control	GAN, VAE
[35]	Access Control	GAN
[36]	Access Control	GAN, VAE, Diffusion
[37]	Access Control	GAN
[38]	Access Control	GAN, VAE
[39]	Access Control	GAN
[40]	Access Control, Software Security	LLM
[41]	Access Control	GAN
[42]	Cyber Threat Detection	GAN, VAE, Diffusion
[43]	Cyber Threat Detection	GAN
[44]	Cyber Threat Detection	GAN
[45]	Cyber Threat Detection	GAN
[46]	Cyber Threat Detection	GAN, VAE
[47]	IoT Data Traffic Generation	GAN
[48]	IoT Data Traffic Generation	GAN
[49]	IoT Data Traffic Generation	GAN

Thus, our aim in this paper is to conduct systematic research on Generative Artificial Intelligence methods specifically used in different areas of IoT in order to improve security as has been done in more traditional communication networks. To this end, we conducted intensive research on several databases, including Scopus, IEEE Xplore and Google Scholar. The works that were selected to appear in this review are basically those appearing in scientific journals and proceedings of international conferences referenced in Scopus and IEEE Xplore. We also included some works that are not cited in these scientific databases, but that are publicly available in renowned repositories such as arXiV and that have a considerable number of citations.

3. Results

In this section, we present the review resulting from our research on the different situations where we find applications of Generative Artificial Intelligence concerning privacy and security issues. We classified the works according to use case although some of them could appear in more than a single item in this classification.

In Figure 6, we can observe a graphical representation of the distinct subsections we have considered in order to classify the collected works that use Generative AI models in different AI Cybersecurity fields. At this point, we point out that we have considered an extra subsection devoted to the application of Large Language Models in IoT Cybersecurity that is not included in the figure. This is due to the fact that its use is diverse and not very extended yet, although the possibilities are promising.

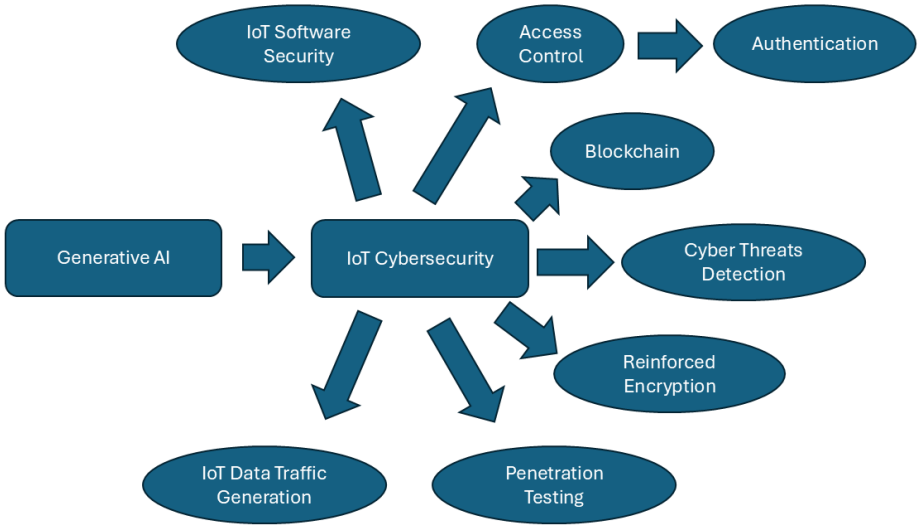

Figure 6. Generative AI applied in IoT Cybersecurity.

3.1. Access Control

Access Control is a data security process that enables organizations authorization for accessing corporate data and resources. Unauthorized access to the system could result not only in corresponding information leakage and subsequent loss of privacy, but also in the possibility that a malicious party could inject false information that might cause a potential risk for the system itself. Thus, a highly recommended option is to include an Intrusion-Detection System (IDS) that could detect suspicious network connections or data traffic. This is the case of [50], where the authors implement a GAN given by a deep neural network that defines the discriminator and a generator consisting of a convolutional neural network (CNN), which are used to generate the images in order to train the system to detect possible fake information submitted to the Controller Area Network in charge of providing information on a vehicle network.

Another example of the use of GANs in vehicles is [51]. Here, the authors introduce a Risk-Prediction-Based Access Control model, which assigns the access rights to a node by predicting the risk level of vehicles. Data are used to predict vehicle behavior, trying to improve traffic safety. The GAN increases the items of training sets to train the neural network, which is used to predict the risk level. They use the Wasserstein distance to deal with the pattern collapse and gradient disappearance. They show how the datasets generated with this GAN converge faster and have a higher similarity with real datasets and how the neural network that is trained with real datasets and those produced by the GAN has a higher prediction accuracy and the training is performed faster.

In a heterogenous IoT network with different types of IoT devices, it is vital to identify the type before applying fine-graded security policies. This can enable global management for security purposes at a large-scale level in order to permit or prohibit IoT devices' specific behavior. However, due to the security breaches existing in these environments, it is important to avoid sending information that identifies the devices and usually, alternative methods based, for instance, on the network traffic are used to this end. In this way, Machine Learning-based methods turn out to be very successful, but there exist attacks

that can undermine Machine Learning-based IoT device identification. In [52], the authors introduce an attack based on GAN that allows an IoT device to manipulate its traffic to camouflage itself and avoid being identified. They add a manipulative model to the usual architecture of GANs formed by a discriminative and a generative model. The manipulative model works as the generative model in GAN to manipulate the traffic of IoT devices by adding perturbations.

The authors in [53] develop a multi- stage multi-class classifier based on semi-supervised GAN that performs automatic feature extraction with minimal labeled data. The classifier identifies ID and type devices and uses an approach where data are preprocessed and treated as image matrices.

A novel training method for GANs is introduced in [54], where a Federated Learning framework is used following different federation strategies. This approach is later applied by other researchers to introduce different IDSs. For instance, [55] introduces a Federated Learning architecture for intrusion detection in medical cyber-physical system networks using a GAN. The models are trained on two distinct data categories, namely, patient medical data and network traffic data, using publicly available datasets, to simulate a medical cyber-physical system data ecosystem.

In [56], the authors propose a parallel learning and detection model for routing attack detection in IIoT. They reduce the training time by means of a parallel GAN classifier model to detect attacks and classify them into the corresponding classes involved in the routing protocol in Low-Power and Lossy Networks and that affect the network communication performance. Motivated by the fact that detecting attacks near the source and point of effect can reduce loss and latency, they distribute the processing tasks across the edge nodes, leading to a distributed Cybersecurity architecture.

Ref. [57] provides a strategy based on the use of conditional GANs for anomaly detection in IoT. The authors define what they call a one-class conditional GAN model. This model works with one data class and generates the synthetic instances of the class in the binary class dataset. In typical conditions, the dataset is unbalanced since most network traffic is normal, while malicious data are always in the minority. Thus, this model is used to create synthetic data of the minority class to balance the dataset. The data part corresponding to the minority class is used to train the GAN and later synthetic data of this class are created by using a second GAN.

Another case of use of Federated Learning using GANs is [58], where a GAN network in a federated setting is introduced. Here, local generators and discriminators are synchronized periodically by a central generator and discriminator with continuous improvement by exchanging gradients and model upgrades. Each device trains its single model on its own data and synthetic local data generated by the local GAN. Then, it transfers the model parameters to the global model and the local data and generated data of each device are not shared. Thus, the IDS model is trained individually although every smart device contributes to a global detection model. The aim of [59] is analogous. Here, the authors introduce a distributed IDS using Federated Learning. The IDS has two layers: an IDS at the gateway and a second IDS located at the edge layer. They also develop two GAN-based poisoning attacks using Federated Learning based IoT sensor data aggregation and implement an attribute GAN-based defense mechanism at the gateway using GANs to mitigate these attacks.

An autoencoder (AE) is a neural network that learns to reconstruct its input as output by compressing input data to lower dimensions and then uses these to recreate the original input. In [60], the authors use an AE combined with a GAN model in the Message Queuing Telemetry Transport (MQTT) protocol. This is a protocol that has become a standard for IoT data transmission due to among other reasons its efficiency, light weight and scalability. Most of the existing IDS models in MQTT networks are supervised, which make them vulnerable to attacks they are not trained for. In this paper, the authors propose a GAN-based AE architecture, combining the power of the AE and the adversarial training used in GANs to build an unsupervised intrusion-detection model called GAN-AE to detect

anomalous traffic in MQTT networks. In the AE-based method, parameters are updated not only based on the reconstruction loss, but also including GAN-based adversarial loss. Training of GAN-AE involves two phases. During the first one, the model parameters of the AE are updated by back-propagating on only reconstruction loss. Then, in the second one, the AE is made to compete with another model that acts as a discriminator; i.e., the AE acts as a generator. The objective of the discriminator model is to successfully differentiate between input traffic flows and samples reconstructed by the AE. The objective of the AE (generator) is to fool the discriminator by reconstructing the input traffic flows similar to the actual input. The proposed GAN-AE model trained with the generated dataset can be used to extract malicious (anomalous) traffic and in that case, the captured packet data in the current interval are saved to the database as evidence of the attack and further analysis.

The work presented in [61] studies the problem of intrusion detection for IoT based on edge computing. The authors propose an IDS implemented by big data mining based on a fuzzy rough set, a GAN and a CNN. They first propose a fuzzy rough set-based algorithm to perform feature selection for big data via IoT. Then, based on selected features, they use the CNN to implement an intrusion-detection method and finally, the combination of the CNN with the GAN allows them to implement an intrusion-detection model adequate for different types of cyber attacks.

In Table 2, we list the datasets used in every reference and the corresponding accuracy obtained for the proposed model. In some of the accuracy values, we have given an average value, which is denoted by (avg) and this is due to the fact that the authors provide different accuracy values corresponding to different classes of the used datasets.

Table 2. Access control accuracies.

Ref.	Datasets	Accuracy (%)
[50]	Own dataset	97.5% (avg)
[51]	Own dataset	87%
[52]	UNSW IoT Trace Data	90%
[53]	Not provided	92%
[54]	MNIST, CIFAR-10 (IID data)	MNIST: 99.5% (avg), CIFAR-10: 42.9% (avg)
[54]	CIFAR-10 $p = 0.7$, CIFAR-10 $p = 0.9$ (Non-IID data)	CIFAR-10 $p = 0.7$: 99.5% (avg), CIFAR-10 $p = 0.9$: 42.9% (avg)
[55]	CHARIS, UNSW-NB	CHARIS: 91.51%, FL CHARIS: 92.98%, UNSW-NB: 76.74%, FL UNSW-NB: 78.37%
[56]	IRAD	93%
[57]	KDD99, NSlKDD, BoT-IoT, IoT-NI, IoT-23, MQTT, MQTTset	Check reference [1]
[58]	KDD99, NSL-KDD, UNSW-NB15	KDD99: 99.1%, NSL-KDD: 99.29%, UNSW-NB15 99.56%
[59]	CICIDS 2017, IoT-23, NBAIoT	Check reference [1]
[60]	Own dataset, MQTT-IOT-IDS2020	Own dataset: 89.8% (avg), MQTT-IOT-IDS2020): 71.55%(avg)
[61]	CSE-CIC-IDS2018, CIC-DDoS2019	Check reference [1]

[1] In these cases, the reference includes several results obtained for different datasets, models and attack types.

Authentication

Access Control relies on two basic processes, identification and authorization, and authentication plays a central role in both of them. The articles [62–64] are examples of

works of how GANs can generate biometrical data that can fool a biometrical authentication system. The same idea can be also applied to technology. For instance, some approaches to physical layer wireless security are able to authenticate the device wireless transmitters through specific imperfections that appear in their transmitted signals. In [65], the authors show how a GAN can be trained to produce signals with the same data content, but with imperfections so classifiers trained only on datasets corresponding to transmissions of real devices are vulnerable and training the classifier with the outputs of a different GAN can contribute to strengthening security by enhancing the classifier action.

The authors of [66] use the same fingerprint of an IoT device for identification. The work proposes starting with a differential constellation trace figure generation process to transform radio frequency fingerprint features from time-domain waveforms to two-dimensional figures and then, by means of a GAN model, it is possible to discriminate rogue devices without any prior information. An analogous approach led the authors of [67] to introduce an authentication method. Their method is based on GAN and CNN, which provide spoofing detection and authentication, respectively.

Another example of a malicious application of Generative AI in IoT authentication is password guessing. Based on [68], a tool that uses a GAN to autonomously learn the distribution of real passwords from actual password leaks and to generate high-quality password guesses, in [69] the authors modify the structure of the original model to obtain new models of password guessing that are applied for IoT password guessing.

In [70], the authors show how to use generative AI to obtain a new version of a well-known active attack in Cryptography. This paper presents a Man-in-the-Middle attack on IoT devices that utilize the MQTT protocol for communications. The attack basically consists of an MQTT Parser that dissects and alters MQTT messages and an adversarial model based on a GAN that produces malicious messages.

The authors of [71] propose a secure message multi-factor authentication scheme based on steganographic secret sharing for building trust in IoT systems, where messages are protected through personal keys, source images and morphing parameters.They introduce a method that splits messages into two participants that receive a share in the form of a human face image via a GAN. A CNN is trained at the side of each participant in order to extract the corresponding received share from the shadow image that is generated with the participant's key. To avoid cheating, each participant's shadow image is morphed with that for the other and then morphed further with the given source image.

The aim of [72] is face recognition in IoT systems. The authors propose a GAN framework where constraint of local consistency is added in order to force the encoder to mine consistent features. The GAN provides a method with the robust encoding ability for defending against adversarial attacks. The GAN also has a refinement stage with the expert network that allows one to extract clear features on non-salient areas, enhancing the identity preservation.

In [73], the authors make use of physical layer authentication and ML for authentication. They use a generative model that makes use of an AE and a variational AE. The architecture can extract features of high-dimensional Channel Impulse Response that are used for authentication without prior channel information on attackers. The loss function that they propose depends on both the reconstruction error and the quality of representation of the Channel Impulse Response, which allows one to improve the authentication performance. Wireless physical layer authentication is the aim of [74] as well. The authors use the channel impulse response data for classification. The GAN model is used to augment the channel impulse response data that will allow one to later train the classifier model given by a CNN.

Another application of GANs in biometrical identification is given in [75]. Here, the authors propose a mobile continuous authentication system, i.e., authenticating users based on the level of risk and contextual information about the user, which includes role, location or device type, They use a Transformer-based GAN for data augmentation, leveraging the accelerometer, gyroscope and magnetometer sensors on smartphones. In the same

line, we find [76], where the authors introduce an autoencoder GAN model for continuous authentication in mobile devices that uses a conditional variational autoencoder GAN for data augmentation. Sensors like the accelerometer and the gyroscope in the mobile are used during the enrollment stage to collect behavioral patterns. Then, these are used jointly with user's data selected by the first autoencoder GAN to train the conditional variational autoencoder GAN for data augmentation and so train again the autoencoder GAN for user data reconstruction. Authentication is carried out taking into account a reconstruction error from the data reconstruction at the moment a user operates the mobile and a predetermined authentication threshold for user authentication.

The GAN proposal included in [77] refers to a system that allows communication between an autonomous vehicle and its digital representative in the system. The GAN provides augmentation of raw data captured by vehicle sensors. The aim is to achieve continuous authentication as in the previous cited works related to mobile devices. The authors train a CNN using the raw augmented data and by means of the features extracted using the CNN and analysis of the principal components. They train a support vector machine that will provide the desired authentication.

3.2. Blockchain

Blockchain technology is a recent technology that is seeing increasing experimental use in Cybersecurity and that allows one to authenticate transactions between a group of users without the existence of a central trust authority, making it very attractive for its use in distributed environments as in the case of an IoT network. In preceding sections, we observed that Generative AI has applications in authentication. In this section, we review applications of Generative AI to Blockchain in IoT environments.

In [78], the authors provide a solution to the security and privacy challenges in IoT networks due to their complexity and massive data generation. They propose combining Blockchain and Machine Learning to create decentralized, secure and efficient network-management systems. The article focuses on using Generative Adversarial Networks to tackle the class imbalance issue in Intrusion-Detection Systems (IDSs), where abnormal data are significantly less frequent than normal data. A novel Imbalance GAN (IGAN) model is proposed to generate samples for minority classes, improving IDS performance. A smart house scenario is used to illustrate the approach.

The authors of [79] introduce a key secret-sharing scheme based on Generative Adversarial Networks to address key issues in Blockchain: low security, difficulty recovering lost keys and low communication efficiency. The scheme converts private keys from text to images, segments these images and encodes them using DNA coding for enhanced security. GANs treat the secret-sharing process as a classification task, distinguishing between qualified and unqualified participants. The system provides efficient secure recovery of keys while reducing the risk of key cracking. Simulation results demonstrate the method's high performance, security and communication efficiency.

Ref. [80] focuses on the challenges of implementing energy-efficient, secure and Quality of Service (QoS)-aware network slicing in the 6G environment using Software-Defined Networking (SDN) and Network Function Virtualization (NFV). It presents a deep network slicing model that employs Generative Adversarial Networks to optimize slice management based on capacity and QoS requirements. The authors utilize Directed Acyclic Graph (DAG)-based Blockchain technology, incorporating the Proof of Space algorithm to enhance scalability and reduce resource consumption. The study also introduces context-based authentication and secure handover techniques using Markov decision-making and a weighted product model. Additionally, it addresses load-balancing issues through hybrid neural decision trees and the Soft Actor-Critic algorithm for accurate load prediction. The proposed SliceBlock model is evaluated for its effectiveness in improving security and resource management in 6G networks.

Some security challenges in IoT networks within Smart Cities, such as centralism, data privacy and intrusion threats are studied in [81]. To tackle these issues, the authors propose

a Machine Learning-based Blockchain framework called Cycle-Consistent Generative Adversarial Network (CCGAN) for intrusion detection. The framework employs a three-level privacy model: the first level uses Blockchain for data authentication, the second one employs CCGAN for feature mapping and the third one focuses on classifying normal and attack instances. The proposed method utilizes the ToN-IoT and BoT-IoT datasets to enhance detection accuracy, achieving performance improvements over existing methods like XGBoost and DGRNN by 18.67% to 29.57% in recall and accuracy metrics. Overall, the study emphasizes the necessity for robust security measures in the evolving smart city infrastructure.

The work presented in [82] discusses the use of Federated Learning in decentralized applications for collaborative training, where each client device acts as a local AI model using Machine Learning. This approach reduces latency and enhances privacy by keeping data on the device. Applying Federated Learning in decentralized trading bots using Blockchain shows promise and the process is improved by using a fuzzy GAN environment to assist training. A Python bot interacts with the Binance API to place buy or sell orders for the BTC-USD pair, using historical data and Machine Learning for predictive analysis in trading.

In [83], the authors explore a privacy-preserving framework for integrating the Internet of Medical Things with Federated Learning to enhance intelligent medical services. Despite Federated Learning reducing privacy risks by avoiding data centralization, it remains vulnerable to inference attacks and single-point server failures. The proposed framework, called BFG, combines Blockchain, Differential Privacy and Generative Adversarial Networks to mitigate these issues. It addresses server failures, limits the success rate of poisoning attacks and improves security by adding noise to data and auditing model updates. Simulation experiments demonstrate the framework's effectiveness in balancing privacy, accuracy and robustness.

Privacy and security challenges in IoT-based healthcare is again the aim of [84]. Here, the authors propose a Blockchain solution enhanced with homomorphic encryption. The approach allows encrypted data to be processed without decryption, ensuring privacy throughout computations. Smart contracts within the Blockchain regulate data access and sharing, granting permissions only to authorized entities, while also creating audit trails for accountability. The proposed system improves both privacy and data-processing efficiency in healthcare. Through comparative analysis, it shows reduced communication costs and enhanced security, presenting a resilient and privacy-preserving model for IoT healthcare applications.

IoT devices usually do not posses a strong security mechanism, exposing them to multiple privacy risks, which include automatic data exchange or sharing of indirect identifiers through connected devices. Interest in their protection has increased, perhaps motivated by data-mining assaults on photographs. Ref. [85] discusses a novel privacy-preserving framework for facial recognition using GANs, clustering algorithms and Blockchain technology. It introduces the Privacy-Preserving Self-Attention GAN (PPSA-GAN) to generate realistic synthetic facial images while ensuring privacy. Mini-batch K-means clustering anonymizes these images by grouping them into distinct clusters and Blockchain is used to secure data storage and auditing through decentralized ledgers. The system is tested on the CelebA dataset, achieving high performance and accuracy in privacy preservation. This approach is designed for applications like identity verification, surveillance and medical image repositories, aiming to balance technological progress with data privacy.

In the same line as the preceding study, ref. [86] presents a Blockchain-based decentralized facial recognition system designed to address privacy and data security concerns in facial recognition technology. It segments facial traits into clusters managed by nodes, ensuring privacy and security. Generative Adversarial Networks are used for data obfuscation and facial data are securely encoded and stored in the Blockchain. The system demonstrated high accuracy (99.80%) on the CelebA dataset, highlighting its effectiveness for privacy-focused applications like biometrics. This approach combines advanced facial

recognition techniques with Blockchain for secure, decentralized data management and privacy protection.

Proof of work is used in some public Blockchains to show that a program realized the required work in order to propose a new block for the chain and it is known as a consensus mechanism as well. This requires a lot of computational efforts, so the authors of [87] propose an alternative consensus mechanism for Blockchain networks, particularly suitable for resource-constrained IoT environments, by replacing the computationally intensive proof of work with a Machine Learning-based decision-making system. The approach uses a GAN, specifically Vector GAN (VecGAN), to predict fraudulent transactions, thus reducing computation that is needed. VecGAN enhances fraud detection by augmenting imbalanced Blockchain data during classifier training and improves transaction verification accuracy by 3% compared to other methods. Additionally, it reduces resource consumption while improving block throughput by 50%.

In [88], the authors explore the integration of Blockchain and IoT, focusing on the potential security vulnerabilities and anomalies within Blockchain-based IoT networks. While Blockchain offers encryption, decentralization and secure ledger functions, experiments revealed its susceptibility to Distributed Denial of Service attacks, leading to network latency, bandwidth issues and hardware failures due to overheating. The study demonstrates that during DDoS attacks, IoT devices can overheat and block transaction rates drop significantly, with block loss rates reaching up to 81.3%. The findings highlight how temperature, latency and transaction anomalies can help identify cyber threats in Blockchain-IoT systems.

3.3. Cyber Threat Detection

There exists a strong relationship between efficiency and security: the more efficient we want a communication system to be, the more we usually find security breaches in it. Thus, IoT devices, which undoubtedly improve the quality of life, task automation and productivity by allowing access to data anytime and anywhere, produce, at the same time, an increase in the threat level in the systems that make use of them. Therefore, Cyber Threat Detection methods have become nowadays a crucial issue in the development and use of IoT networks. When we review works related to this field, we can consider works related to Intrusion-Detection Systems previously cited [50,55,58–61].

In the case of [50], the authors test successfully the introduced IDS with four attack types: Denial of Service (DoS) attack, i.e., injecting high priority message in a short cycle in order to produce a system collapse; Fuzzy attack, i.e., injecting messages of spoofed random ID and data values; and finally, injecting fake messages related to parameters included in the data transmitted. In the case of [55], the authors provide results with limited success on different attacks provided by public datasets containing several types of attacks including malware and DoS. In [58], the authors obtain satisfactory accuracy levels with different datasets when analyzing anomalous traffic and are able to detect information concerning different types of attacks contained in the datasets used, such as DoS and some types of malware. Gupta et al. in [59] offer different experiments to test the accuracy with different datasets and obtaining satisfactory results when applying the proposal to analyze traffic included in CICIDS 2017 Dataset, corresponding to different protocols such as HTTPS or SSH to detect DoS attacks, whereas detecting XSS and Brute Force attacks presents a poor performance. In the case of IoT-23 Dataset and NBAIoT Dataset, the accuracy also decreases when introducing attacks. Boppana et al's paper, [60], offers an analysis using a custom dataset and public flow-based MQTT traffic data. Due to its adversarial training strategy, the GAN with AE outperformed other models and attained a high detection accuracy score. In [61], the authors obtain a high accuracy rate for different types of DoS and BOT attacks, whereas the rate significantly decreases in some cases for Brute Force attacks and SQL injection.

In [89], the authors show that Adversarial AEs and Bidirectional GANs can be used to detect intruders based on an analysis of the network data. They use the IoT-23 dataset to

train the generative Deep Learning models to detect DDoS attacks and various botnets like Mirai, Okiruk and Torii. Their results show that GAN-based models overcome those based on Adversarial AEs when identifying and classifying the attacks.

Artificial Immune Networks are part of the family of algorithms known as Artificial Immune Systems, inspired by the work [90]. The authors of [91] propose a theoretical model that uses a Generative Adversarial Artificial Immune Network model for intrusion detection in IIoT systems. This model aims to improve the quality of an Artificial Immune Network-based classifier by introducing a generator AIN responsible for generating fake intrusion samples from a latent space against a discriminator, expecting that their proposal improves the training results obtained in a traditional GAN system that uses datasets.

One of the most common cyberattacks is DDoS, especially in IoT networks and those that are usually developed by a botnet, i.e., a network of compromised devices called bots and which are managed by a command and control server [92]. The aim of [93] is to apply a GAN for feature generation and classification of botnets. The authors work with the IoT-23 dataset and propose a GAN model with a feature-preserving generator with proper residual network and an effective loss model with a compact perception network. The data-perception network is specially designed for analysis and proposes a second model of scale fused bidirectional Long Short-Term Memory attention to discriminate between an attack and benign traffic for the classification process, improving the generator's efficiency with respect to generating fake data.

Another very common attack in IoT networks is replay attacks. In [94], the authors introduce REPLIOT, an ML-based tool for automatic testing replay attacks in a smart home environment. Among its references we find [95], where the authors propose a novel framework for detection methods relying on deep embeddings, either discriminative or generative based on GANs.

The aim of [96] is to study the problem of intrusion detection in Social Internet of Things based on collaborative edge computing. The authors propose an algorithm for intrusion detection based on a GAN, which is composed of three stages. Firstly, they use the feature-selection module to process the collaborative edge network traffic and then a GAN is used for intrusion detection in a single attack. Finally, they propose an intrusion-detection collaborative model that combines several intrusion-detection models as the preceding one at a single attack.

The work that is introduced in [97] combines distributional Reinforcement Learning with a GAN architecture to overcome trying to take advantage of these two approaches. The authors show how the GAN agent can be efficiently used to help the IDS, which is designed based on distributional Reinforcement Learning and improves IDS detection of some attacks. The process includes designing distributional Reinforcement Learning as a random process to find all possible returns from the immediate rewards and stochastic dynamics policy. Then, the GAN model is provided for data balancing and data augmentation for the minor profiles and building an algorithm that contains the outputs of the distributional Reinforcement Learning using the synthetic data generated by the GAN to empower anomaly detection, obtaining an IDS model that is tested satisfactorily with the DS2OS dataset.

The IDS model for IoT systems introduced in [98] classifies the multi-class with Normal and Generic, Exploits, Fuzzers and DoS as attack types. To do so, the authors design their IDS based on GANs to generate the synthetic data for minority attacks and balances the class load in the dataset UNSW-NB15. They reduce the number of features using a filter-based method. One of each two highly correlated features is dropped from the dataset, reducing the training time complexity of the model. They also modify the model with the use of various parameters, hyperparameters and regularization techniques in order to improve the model performance.

Ref. [99] proposes training a GAN model using Federated Learning. The authors use multiple local discriminators with multiple local datasets in the phase of generator learning. The IDS they proposed uses the multilevel discriminator model to distinguish the attack

traffic by continuously improving the quality of the generator to produce attacks similar to the original network traffic. The multilevel distributed GAN setup for anomaly detection is done with the KDD dataset and SWAT dataset.

In [100], the authors study the possibility of using uniquely synthetic data generated by a GAN for training Machine Learning models in Network IDS. Their results exhibit a high performance obtaining results similar to real-world IDS data and thus show the utility of this approach.

The work presented in [101] introduces a framework for detecting and generating new malware samples based on the raw byte code at the edge layer of the Internet of Things networks. The authors implement an automated representation learning model for extracting a conceptual space of the raw data. They use algorithms that are based on Deep Learning to generate new malware samples by utilizing the file header information and use a CNN to learn the conceptual and high-level features from the header's raw bytes. Then, they use a GAN to generate the signatures of previously unseen malware samples.

A collaborative intrusion detection for IoT networks is introduced in [102]. The authors analyze attacks targeting local models within edge nodes considering both threats, insider and external. They adopt a Federated Learning model with a collaborative generator–discriminator training and enhance the privacy preservation of the framework; Differential Privacy noise and dynamic threshold secret sharing are added to the uploaded model information and downloaded data.

Malware detection in an IoT smart agriculture environment is the aim of [103]. The proposal is divided intro three phases and uses jointly a malware-detection framework and image visualization strategies by means of the Discrete Wavelet Transform and GAN techniques. First, there is a feature extraction and data preprocessing, that is, extracting features from raw data and converting these extracted features into a grayscale image of a standard size that is later colorized to enhance classification accuracy.Then, the Discrete Wavelet Transform is applied to extract different coefficients from images and fuse them with the GAN model. Finally, a CNN is used for malware classification.

The aim of [104] is to search for a solution to detect the use of compromised IoT devices in an IoT environment. This paper presents a GAN-based solution that uses benign IoT traffic as well as global darknet data for training. The working assumption in this work is that the dataset used will help the system to identify anomalous IoT traffic as belonging to the same malicious distribution data used.

The motivation of [105] is to use GANs to increase the quantity of malicious code samples and convert the malicious code intro a binary format so a grayscale map is obtained and used to complete the malicious code visualization. The authors use a GAN to generate new malicious code images based on the image features in the original database; adding noises is also simulated. According to the results obtained, the data-enhancement method adds more usable features to the database than the approaches cited that used an analogous strategy.

IoT is increasingly adopting Android applications, so detecting malicious Android apps is a crucial issue and this is the authors' aim in [106]. They use graph-based classification using a graph neural network-based classifier to generate API graph embedding, reaching a high accuracy level in the Drebin dataset. However, adding fake relationships can make the graph-based learning not detect malicious software. Then, they use a GAN-based algorithm to attack the graph-based neural network Android malware classifier generating adversarial malware API graphs.

Another study that uses code images for malware identification is [107]. The authors use a technique that previously appeared in this survey and that combines a GAN with an AE. This acts as a generator that transfers learning to a discriminator in order to identify several types of malware threats that exploit the IoT network by means of RGB images that are obtained from malware samples. The original part of the work relies on AEs to learn underlying behavior patterns of benign and malicious software, enabling the generation of anomalous network traffic data to enhance detection effectiveness. Several architectures for

the AE are considered as convolutional and variational AEs. Moreover they allow image rotation and shuffling in order to increase the variation in the training data.

In [108], the authors collect benign and malware data to train a GAN-based system for threat detection. They focus on certain types of malware having both standard and metamorphic behavior. Machine Learning approaches often encounter difficulties in distinguishing between benign and malware behavior due to the benign activity continuing even under the malware action. Although a typical neural network classifier trained on a conventional advanced permanent threat with metamorphic behavior achieves a high level of accuracy, the false positive rate is also very high. The authors manage to reduce this rate by training a GAN to artificially synthesize malware data in order to make up the difference between the amount of benign and malware training data.

All the preceding citations concern the use of GANs to detect threats. In [109], the authors use a GAN to generate and store the dataset required to participate in the training process at each round of the Federated Learning, so the attacker can obtain a complete dataset containing the features of private data of the other participants. To break the model, the attacker simply has to distinguish itself as a regular participant during the training stage, so the attacker uses a GAN to generate samples that could forge the others'.

Table 3 depicts the datasets and the corresponding accuracy obtained for the proposed model to detect cyber threats in the works cited. In some of the accuracy values, we gave an average value, which is denoted by (avg) and this is due to the fact that the authors provide different accuracy values corresponding to different classes of the used datasets.

Table 3. Cyber Threat Detection accuracies.

Ref	Datasets	Accuracy (%)
[89]	IoT-23 dataset	Check reference [1]
[91]	IoT-Bot dataset	98.73%
[92]	Not provided	Not provided
[93]	IoT-23	Check reference [1]
[95]	Own dataset	Not provided
[96]	CSE-CIC-IDS2018, CIC-DDoS2019	CSE-CIC-IDS2018: 99.24% (avg), CIC-DDoS2019: 97.41% (avg)
[97]	DS2OS dataset	98.95% (avg)
[98]	UNSW-NB15	91%
[99]	KDD dataset SWAT dataset	KDD: 89.13% (avg), SWAT: 99%
[100]	UNSW-NB15, NSL-KDD, BoTIoT	UNSW-NB15: 90%, NSL-KDD: 84%, BoTIoT: 100%
[101]	Collected dataset, VX-Heaven dataset, IoT dataset, Packed dataset	Collected dataset: 97.56%, VX-Heaven dataset: 99.03%, IoT dataset: 99.96%
[102]	CIDIoT	CIDIoT (IID, Non-IID): 99%, 86.36%
[103]	Malimg, IoT-Malware	Malimg: 99.99%, IoT-Malware: 99.99%
[104]	IoT testbed	Not provided
[105]	Own dataset	Modified database: 94.64%, Original database: 97.23%
[106]	CICMalDroid 2020, Drebin	CICMalDroid 2020: 98.33%, Drebin: 98.68%
[107]	RGB	81.9%
[108]	Own dataset	Not provided
[109]	IoT Network Traffic Dataset, MNIST	Not provided

[1] In these cases, the reference includes several results obtained for different datasets and models.

3.4. IoT Software Security

The increasing use of smart devices in the setting of Smart Cities produced a considerable interest in Software-Defined Networking (SDN), a set of techniques that enable configuring a heterogenous large-scale network in a dynamic and efficient way in order to create grouping and segmentation that allow improving network monitoring and performance by means of software tools. One of the proposals to protect SDNs is given by IDSs, although identifying every attacking technique that could target SDNs is a difficult problem to handle given that most IDSs rely on classification algorithms and it is necessary to create new examples that can evade or deceive these IDSs to train them and enhance their efficiency. The aim of [110] is to create synthetic attack samples using a GAN and synthesize adversarial examples against the GAN, motivating the design of new defensive mechanisms.

In [111], the authors implement a GAN-based framework able to deceive an IDS by generating adversarial malicious traffic and use this to increase the retraining of the ML-IDS, enhancing its robustness against evasion attacks. Then, the authors deploy the IDS in an emulated SDN system to test the results by selecting a single instance of an IDS detecting a DOS attack. The objective in [112] is analogous using Wasserstein GAN.

The goal of [113] is to obtain an efficient solution of an IDS for an SDN network in terms of classification accuracy and interference time. To do so, the authors introduce a solution based on a Deep Sparse AE for unsupervised feature learning, a conditional GAN and Ensemble Learning to improve classification accuracies. They also design an FPGA-based packet-processing method using a high-speed networking platform to accelerate the pre-processing and post-processing phases of their proposal.

The aim of [114] is to research attacks against the forwarding nodes from multiple perspectives in software-defined IIoT. Concerning the difficulty in making a previous deployment of defense methods against various attacks, the authors' proposal consists of a system based on a deep reinforcement learning general attack-tolerance scheme to guide the benign traffic flow to bypass the attacked forwarded nodes. Moreover, they use a GAN to flexibly generate network traffic for training the attack-tolerance scheme.

IoT is an important part of the Metaverse, a future virtual reality technology, and its security is a major concern. In [115], the authors propose a Metaverse network intrusion-detection model in a 5G network based on GAN and using a deep autoencoder and a random forest strategy, whose purposes are, respectively, data optimization and imbalance processing; data feature extraction; and representation and classification. Another similar approach that uses a GAN combined with an AE that detects anomalies in imbalance data in a SDN network of smart devices is [116].

DDoS attacks are the challenge that [117] tries to face. Here, the authors propose an adversarial method for detection and defense against DDoS attacks in SDN environments. They use a GAN model to obtain an adversarial dataset with DDoS samples to train the IDS. The SDN controller collects flow records and then these are preprocesed to be used by a model based on an adversarial Deep Belief Network and a Long Short-Term Memory model for anomaly detection that produce sample timing features to detect IP records and identify adversarial DDoS attacks. This allows designing an abnormal defending strategy to provide the SDN controllers.

Segmentation produced by the use of SDN in IoT reduces the ramification of security breaches. The aim of the authors in [118] is to introduce an adaptive variational AE-based modified archery to enhance the security of IoT devices.

In [119], the authors try to address the problem of detecting two of the main attacks for an IoT device as DoS and botnet attacks. This paper proposes a Hybrid DoS Attack Intrusion-Detection System combining signature-based detection and anomaly-based detection The model to detect anomalies is based on a convolutional neural network with a GAN to establish a baseline for distinguishing between benign and malicious traffic.

The system introduced in [120] uses unsupervised learning to detect unknown attacks in an interval of 1 s using a GAN for anomaly detection in two different datasets. The

authors propose a mitigation algorithm in order to stop distributed DoS attacks from harming the network's operation. This algorithm decides which flows should be blocked by the controller. At the moment of anomaly detection, the mitigation modules check the IP that receives most flows and creates a suspect list, ensuring that only traffic towards the victim is blocked and, if there are multiple targets, when the traffic towards one diminishes, the mitigation algorithm will change the victim accordingly. The purpose of [121] is analogous, although the authors implement three different versions of the GAN model, using a traditional one, a deep convolutional GAN and a Wasserstein, whose behavior are compared.

Maddu and Rao in [122] introduce a system containing several steps, starting with a data-augmentation method based on a deep convolutional GAN. After extracting the features from the input data using a CenterNet-based approach as well as effective characteristics, ResNet152V2 with Slime Mold Algorithm (SMA)-based Deep Learning is implemented to classify the attacks in InSDN and Edge IIoT datasets. Once the network intrusion is detected, the proposed defense module is activated and then the SDN controller discards the related packets.

The authors of [123] propose a method to detect different attacks in SDN using improved Auxiliary Classifier Generative Adversarial Networks to solve the problem of data imbalance and an IDS, named TIBS, based on a Transformer and Inception-BiGRU-SA network. First, the encoder part is used to capture the connection globally and perform preliminary feature extraction on the input data. The datasets used in this study are CIC-IDS-2017 and CIC-DDoS-2019; both have features of different types of attacks. The results show a good level of accuracy, identifying various types of attack behaviors very efficiently.

The Distributed Network Protocol 3 (DNP3) is an industrial protocol for communication among intelligent devices and Industrial Control Systems (ICSs). The absence, in the version studied by the authors in [124], of authentication in the protocol made it vulnerable to several types of attacks as Man-in-the-Middle, spoofing, DoS or replay attacks. Therefore, it is essential to obtain a real-time, accurate and consistent IDS. In this paper, the authors introduce an anomaly-detection model capable of detecting anomalies and classify them into particular cyberattack types that combines an AE and a GAN with a high performance in terms of accuracy and can detect 13 Modbus/TCP cyberattacks, 5 DNP3 cyberattacks and potential anomalies related to operational data (i.e., time-series electricity measurements). The authors validate this in several Smart Grid evaluation environments showing the scalability and efficiency.

According to [125], one way to determine vulnerabilities in the DNP3 protocol is to cause device communication errors in fuzzing. The authors introduce a GAN that allows improving the passing rate and code coverage. Then, they propose a fuzzing framework to improve the fuzzing automation of DNP3. The authors simulate the DNP3 protocol and compare the fuzzer with other previous proposals, obtaining results that show a better performance.

3.5. Reinforced Encryption

Adversarial networks for encryption were first proposed in [126] as a game between three computers: the first's aim is encryption, the second one has decryption as its objective and the third one is the attacker that tries to obtain the plaintext exchanged between the first two. If these computers are neural networks, what we have is an adversarial training process that results in neural networks that can learn how to obtain confidentiality in their communications. Nowadays, we are continually using hybrid cryptography that uses two different types of cryptography, namely, symmetric cryptography and public key cryptography, where the second is used to encapsulate and protect the key that the first one uses to obtain confidentiality. The most widely used symmetric cryptosystem is AES, which is the standard recommended by NiST and it is very extended in IoT communications.

The authors of [127] explore enhancing the security of AES encryption by integrating a GAN and thus using a hybrid encryption with this cryptosystem and adversarial network

encryption. While AES uses fixed keys, making it vulnerable to attacks once keys are exposed, incorporating GAN offers added security since its encryption is not rule-based but learned through training. This prevents attackers from easily reversing the encryption. The proposed hybrid approach uses GAN to encrypt AES encrypted text further, ensuring, even if AES keys are compromised, attackers cannot decode the data.

A Deep Learning-based encryption and decryption network for safeguarding sensitive medical images in the Internet of Medical Things is presented in [128]. This proposal uses a Cycle-GAN framework to transform medical images into encrypted forms, protecting patient privacy. The decryption process is implemented as image reconstruction, while an ROI-mining network can extract key areas of interest (e.g., organs) from encrypted images without decryption, further enhancing privacy. Extensive experiments on chest X-ray datasets show that this method ensures efficiency and resists various attacks even when key-generation processes are known.

In [129], the authors try to address the security and energy efficiency of IoT devices, particularly in banking applications. They propose using Base + XOR encoding and Chaotic XOR Encryption (CXE) to optimize energy use and strengthen security. By applying these techniques, data transmission consumes less energy and time while maintaining security. Deep Learning, specifically Conditional Generative Adversarial Networks, is used to train the system for secure data generation and transmission. The CGAN-based model enhances security by encoding data during transmission, making it robust against attacks.

Providing methods that allow exchange information in a secure way, which includes confidentiality and authentication, in zero-trust environments as it is an IoT network is the problem that the authors of [130] try to address. Their proposal is a Blockchain-enabled zero-trust information-sharing protocol that is able to filter synthetic information and preserve privacy by using neural networks. They propose using neural networks for digital signature generation and verification. Their main contribution is the design of asymmetric cryptographic functions based on GANs for IoT environments. Their method can enable fuzzy encryption and signatures in low rate and loss transmission channels. A theoretical proof in specific adversary models of their design is included as well as a performance evaluation.

Homomorphic encryption is a type of encryption that allows one to make computations directly with the encrypted data without revealing any information on the confidential data. Thus, it has become very popular in IoT systems. Ref. [131] focuses on enhancing IoT security by utilizing a Conditional Generative Adversarial Network (CGAN) and Fully Homomorphic Encryption. It also proposes the use of an Algebraic Matrix-based CGAN to address time complexity issues in encryption and decryption processes, as traditional cryptographic techniques take longer to decrypt data. The combination of CGAN and Fully Homomorphic Encryption ensures the protection of IoT data with minimized encryption time and complexity compared to other existing algorithms. This article emphasizes the use of CGAN and Fully Homomorphic Encryption for IoT security, but also focuses on comparing time complexities of various cryptographic algorithms, including the Chaotic Algorithm and RSA and solving the decryption delay with mathematical optimizations.

In [132], the authors discuss how to enhance Cybersecurity in IoT systems by using Deep Learning techniques, specifically Conditional Generative Adversarial Networks. CGANs allow data encryption and decryption based on conditions set by generator and discriminator models. To address the time complexity in cryptography, the paper proposes using an Algebraic Matrix in CGAN (AMCGAN) combined with Fully Homomorphic Encryption. This approach reduces computational time by enabling simultaneous addition and multiplication of encrypted data; it is faster compared to traditional methods like RSA. The method aims to improve data security in IoT systems with minimal time complexity.

The authors of [133] aim to address the challenge of secure data transmission in the IoT using Deep Learning techniques, focusing on Generative Adversarial Networks. To overcome GAN limitations like mode collapse, the study proposes an enhanced Conditional GAN model with two generators and two discriminators. This model, combined

with cryptographic techniques like Algebraic Matrix Encryption and Fully Homomorphic Encryption, ensures secure data transmission. The Jaro–Winkler similarity measure evaluates the diversity of generated fake samples. The authors provide results in this work showing that the improved CGAN model outperforms existing methods in security and efficiency for IoT systems.

The growing use of the Industrial Internet of Things in manufacturing highlights concerns over data privacy. In [134], the authors try to give a solution by means of ML techniques for tasks like predictive maintenance. Sharing IIoT data with third parties can expose sensitive information. To address this, the authors propose a hybrid approach using Generative Adversarial Networks and Differential Privacy to protect sensitive IIoT data while maintaining the accuracy of ML tasks. Their method is tested on several IIoT datasets, showing it effectively preserves privacy without significant computational costs or accuracy loss. The article evaluates the model's efficiency using privacy metrics and demonstrates its practical application in an industrial setting.

Ref. [135] focuses on addressing privacy and security risks in the Industrial Internet of Things, emphasizing the growing importance of data protection in this context. It introduces a novel method based on Generative Adversarial Imitation Learning (GAIL) to identify security vulnerabilities in IIoT systems. By training privacy-protection agents using large datasets, this approach helps mitigate privacy data-leakage risks. The paper discusses key privacy concerns within IIoT, such as data-capture, encryption and homomorphism techniques. Simulation experiments validate the proposed method, showcasing its generalizability and effectiveness in enhancing privacy and security in IIoT environments.

In [136], the authors introduce a transmission system for large-scale images in order to avoid the high computational requirements of traditional cryptographic schemes. They generate a lossy encrypted dataset for the proposed low-noise encryption scheme and then they train the model using massive data transferred to the recognition network for the encrypted image by generating high-quality images from the halftoning decrypted images. To decrypt the image, it is necessary to eliminate the interference signal in the decrypted image, for which they use a high-quality image-generation model.

Ciphertext attribute-based encryption (CP-ABE) is a cryptographic method that allows encrypting data in such a form that only those entities that fit the access policies established at the encryption moment can recover the original data. The aim of [137] is the use of CP-ABE jointly with Generative AI to design and implement a method in fog computing settings. Generative AI is used in the encryption process by introducing flexibility incorporating in a dynamic way attributes into this process, so that encrypted texts are generated based on contextual attributes, which allows an adaptable Access Control to the changing requirements of secure data access.

3.6. IoT Data Traffic Generation

As we have already seen through this paper, accessing IoT traffic data plays a fundamental role in designing strategies that allow enhancing network security. However, this access is very rare for multiple reasons, mainly privacy issues. Thus, the strategy followed by many researchers is to generate synthetic IoT traffic. In [138], the authors use an autoencoder and a GAN to generate sequences of packet sizes that correspond to bidirectional flows. The autoencoder is trained to learn a latent representation of real sequences of packet sizes and then the GAN is trained to learn to generate latent vectors that can be decoded into realistic sequences.

The aim in [139] is also to generate synthetic IoT data traffic but including additional knowledge. The authors make use of a GAN model to produce this, introducing semantic knowledge over location and environment information as well as network structure knowledge. The proposal is able to generate such synthetic data from small real datasets with knowledge enhanced.

Another work aiming to obtain large amounts of IoT network traffic data is [140], where the author proposes an ML pipeline using the Conditional Generative Adversarial Network model to generate a synthetic dataset to be used later for security purposes.

The work presented in [141] proposes the use of Face Swapping-GAN (FS-GAN), a federated self-supervised learning model to support automatic traffic analysis and synthesis over a large number of heterogeneous datasets. FS-GAN is a model with multiple GANs, with a set of generators; each one is designed to generate synthesized data samples from the distribution of a single service traffic and, at the same time, every discriminator is trained to differentiate the created data samples and the real data samples of a local dataset. Then, Federated Learning is used to coordinate the local processes.

The object of study in [142] is the traffic data in Intelligent Transportation Systems, for which the lack of datasets large enough represents a challenge. This work presents a data-augmentation solution using GANs. The authors collect sensor-based traffic speed data with contextual labels and train a GAN-based model to generate realistic traffic data for specific days and times.The synthetic data obtained are used to augment the training data for multiple traffic-prediction models.

There exists a plethora of works that create datasets for training generative models with different purposes and that have been cited previously in the above sections. However the aim of [143] is to create datasets of malicious traffic that can be used later in other applications. Thus, the authors propose GothX, a flexible traffic generator to create both datasets of legitimate and malicious IoT traffic. The requirements for this are the following: an easy configuration of network topology; customization of traffic parameters; automatic execution of legitimate and attack scenarios; IoT network heterogeneity; and automatic labeling of generated datasets.

A singular application of Generative AI is provided in [144]. The huge amount of image collection in Smart City control that are transmitted from multiple sources include face images of individuals who even could not be aware of how their identity may be compromised. To preserve identity privacy of image data from a database, the authors introduce a Sensitivity Map Noise-Adding model based on Generative Adversarial Networks. The models work as a black-box model that does not require any architectural information or the parameters of the target model.

The purpose of [145] is precisely the opposite, i.e, mitigating noisy data. The data that IoT sensors collect are usually disturbed by noisy data, called out-of-distribution (OOD). Existing alternatives to remove noisy data have a huge storage and computational overload. Thus, the authors' aim in this work is introduce a way to remove the negative influence of OOD data in smart IoT from neural networks in an effective and efficient way. To do so, the authors propose a machine unlearning model based on a GAN that can restore the degraded model performance caused by these.

3.7. Penetration Testing

Identifying security breaches is an effective way to avoid attacks against a network environment before they occur, mainly in IoT environments where the characteristics of the network and the devices make them particularly susceptible to many types of attacks. Thus, Penetration Testing or Pentesting tries to identify such vulnerabilities by making controlled attacks against network services and devices. Nowadays the use of AI in Pentesting techniques is significantly increasing. The work presented in [146] tries to address security challenges in IoT security. There exist multiple concerns in this environment that have attracted significant research, but few studies assess security from an attacker's perspective. Penetration Testing is a common method to evaluate traditional Internet security, but it's costly and time-consuming. This paper proposes a Penetration Testing approach for IoT, using the belief–desire–intention (BDI) model to automate the process, improving testing efficiency. The methodology aims to simulate attacks to identify vulnerabilities and enhance IoT security.

In [147], the authors discuss the use of GANs for automating Penetration Testing in web applications, particularly in the context of Wireless Sensor Networks (WSNs) and the Internet of Things. Current methods, such as manual testing and signature-based Web Application Firewalls (WAFs), are often insufficient against sophisticated attacks like Cross-Site Scripting (XSS) and SQL Injection. The proposed framework employs conditional sequence generation to create realistic attack payloads that bypass WAFs by leveraging attack labels and features identified through semantic tokenization. This automated approach significantly reduces the effort involved in manual Penetration Testing, scaling well to large web platforms, and improves WAF rulesets by testing against ModSecurity and Amazon Web Services WAFs.

Ref. [148] explores the use of Artificial Intelligence, specifically Reinforcement Learning (RL), in automating Penetration Testing. It introduces Shennina, an AI-powered framework that simulates cyberattacks in a realistic test environment and validates its effectiveness in replicating advanced attack scenarios. The research focuses on generating datasets from these simulations, providing insights for improving attack-detection and -mitigation strategies. The study emphasizes the importance of AI in both offensive and defensive Cybersecurity measures, offering a practical methodology for analyzing and improving AI-powered Penetration Testing techniques.

Although we introduce the use of Large Language Models (LLMs) in the next section to several applications in IoT Cybersecurity, we finish this section by mentioning precisely an application of such LLMs in Penetration Testing. In [149], the authors explore the use of LLMs, such as GPT-3.5, to augment Penetration Testing by acting as AI sparring partners for human testers. The paper presents two main use cases: high-level planning of security tests and low-level vulnerability hunting. In the latter, the LLM was integrated with a vulnerable virtual machine, allowing it to analyze vulnerabilities and suggest attack vectors, which were executed automatically. The paper discusses initial promising results, possible improvements and ethical concerns regarding AI's role in Penetration Testing. It also suggests potential future uses of AI, like phishing simulation or automated report generation.

3.8. LLM

Language Representation Models or Large Language Models are Deep Learning models that are trained without supervision. The main difference with Recurring Neural Networks is that instead of processing inputs sequentially, LLMs process complete sequences in parallel, reducing significantly the training time. In [150], the authors explore the applications of Generative AI, including LLMs such as ChatGPT or DALL-E, in Cybersecurity, including highlighting its potential to enhance automated threat detection and response. GenAI can handle general security threats, allowing professionals to focus on critical issues requiring human intervention. It excels at detecting novel malware and improving system robustness. Tech companies like Google and Microsoft are integrating GenAI into Cybersecurity tools such as Security AI Workbench and Security Copilot. Despite its promise, GenAI faces challenges, including occasional inaccuracies, high training costs and potential misuse by cybercriminals.

BERT (Bidirectional Encoder Representations from Transformers) [151] is an LLM designed to pre-train deep bidirectional representations from unlabeled text. Unlike previous models, BERT captures both left and right context in all layers, enabling it to perform well on various Natural Language Processing (NLP) tasks like question answering and language inference without extensive task-specific modifications. Using a "masked language model" and "next sentence prediction" during pre-training, BERT achieves state-of-the-art results across eleven NLP tasks. Its fine-tuning approach allows for significant improvements in performance over prior models like ELMo and OpenAI GPT. In [152], the authors introduce SecurityBERT, a novel architecture leveraging BERT for Cyber Threat Detection in IoT networks. The model uses a privacy-preserving encoding technique called Privacy-Preserving Fixed-Length Encoding (PPFLE), combined with a Byte-Pair Encoder (BBPE) Tokenizer,

to effectively represent network traffic data. Experimental results using the Edge-IIoTset dataset show that SecurityBERT achieves 98.2% accuracy in identifying 14 attack types, outperforming traditional Machine Learning and hybrid models like CNN and Transformer-based architectures. With a small model size (16.7 MB) and rapid inference time (0.15 s), SecurityBERT is suitable for real-time analysis on resource-constrained IoT devices.

Ref. [153] is an example of the new LLM perspectives. The paper explores the transformative potential of Large Language Models in the telecom industry, detailing their capabilities and limitations. LLMs, such as GPT and BERT, can streamline telecom operations by enhancing tasks like anomaly resolution, technical specification comprehension and optimization in network technologies like Radio Access Networks (RANs). Companies like Huawei and Qualcomm are already integrating LLMs into their telecom products, offering solutions for mobile networks and customer service. The article highlights key challenges, such as adapting LLMs to domain-specific telecom data and outlines research directions to fully harness their potential.

In the same line as the preceding cited work, ref. [154] discusses the integration of LLMs, edge networks and multi-agent systems to enable intelligent decision-making at the network's edge. This approach envisions on-device LLMs collaborating to achieve network goals through collective intelligence, allowing for efficient task planning and problem-solving. It critiques cloud-based LLMs for their limitations and explores a game-theoretic approach for multi-agent collaboration. The article also outlines the design of wireless multi-agent generative AI systems, highlighting their potential in intent-based networking and emphasizing their advantages in handling complex, multi-modal tasks.

LLaMA (Large Language Model Meta AI) [155] is a collection of foundational language models with parameter sizes ranging from 7 B to 65 B, trained on trillions of tokens from publicly available datasets. The 13B model outperforms GPT-3 (175B) on most benchmarks despite being much smaller, while the 65B model is competitive with the best models like Chinchilla-70B and PaLM-540B. LLaMA's efficient performance on inference tasks makes it more accessible and cost-effective, potentially democratizing access to large LLMs. Unlike other models, LLaMA avoids proprietary datasets, supporting open-sourcing and broader research use. The Falcon series [156] introduces three causal decoder-only models Falcon-7B, 40B and 180B, trained on a vast dataset predominantly sourced from web data. The largest, Falcon-180B, trained on 3.5 trillion tokens, is the largest openly documented pretraining run. It outperforms models like PaLM and Chinchilla and rivals newer models like LLaMA 2 and Inflection-1, approaching the performance of PaLM-2-Large at lower pretraining and inference costs. The paper details the methods and custom tools used for efficient large-scale pretraining, including the use of 4096 A100 GPUs. The models and datasets are released under an open license to foster collaboration and open research. Falcon-180B is positioned among the top three language models globally. Ref. [157] introduces SecureFalcon, a Machine Learning model designed to detect software vulnerabilities efficiently. Built on the Falcon-40B model, SecureFalcon has 121 million parameters and is fine-tuned on specialized datasets like FormAI and FalconVulnDB. These datasets cover critical software weaknesses such as buffer overflows and memory errors. SecureFalcon achieves 94% accuracy in binary classification and 92% in multi-classification, outperforming models like BERT and traditional ML algorithms. Its ability to detect vulnerabilities with fast inference times makes it promising for integration into real-time code-completion tools, offering a faster alternative to resource-intensive formal verification methods like Bounded Model Checking.

As we have already shown, datasets are essential for AI method training and assessments. Ref. [158] introduces TeleQnA, the first benchmark dataset designed to assess Large Language Models' knowledge in telecommunications. It comprises 10,000 telecom-related questions, generated using an automated framework and enhanced by human input. The dataset is used to evaluate models like GPT-3.5 and GPT-4, revealing that while LLMs perform well on general telecom questions, they struggle with complex, standards-related queries. However, incorporating telecom-specific context improves their performance.

The study also compares LLMs with active telecom professionals, showing that LLMs can rival human expertise, underscoring their potential in the telecom industry. The dataset is publicly available on GitHub.

The authors of [159] introduce a novel approach to detecting IoT malware using code gadgets and GPT language models. By extracting code gadgets from IoT network traffic data, tokenizing them and vectorizing them using GPT's embedding layer, the model identifies malware with high accuracy. Evaluated on the IoT-23 and Malvis datasets, the approach achieved impressive F1-scores of 0.997 and 0.986, respectively. The results demonstrate GPT's ability to detect previously unseen malware variants, although challenges remain, such as model interpretability and the need for larger and more diverse datasets. The method offers promise for enhancing IoT device security.

Ref. [160] explores how generative AI models can transform wireless networks, particularly in the context of self-evolving networks. It envisions large GenAI models, trained on multimodal Telecom data, playing a central role in enabling autonomous networks by performing multiple tasks without needing dedicated AI models for each one. These models could enhance network operations like localization, spectrum management and resource optimization. The integration of GenAI in future 6G networks could foster collective intelligence among devices, boosting efficiency and reducing resource consumption, ultimately paving the way for self-driven, AI-powered wireless networks.

Dataset generation is the issue that [161] presents. Here, the authors introduce FormAI, a large dataset of 112,000 AI-generated C programs, created using GPT-3.5-turbo, with vulnerability classification. The dataset includes programs ranging from simple tasks to complex ones like encryption and network management. Each program is labeled with identified vulnerabilities using formal verification via the Efficient SMT-based Bounded Model Checker (ESBMC), which ensures accurate detection without false positives. The vulnerabilities are classified with Common Weakness Enumeration (CWE) numbers, making this dataset useful for training AI models. The study found that 51.24% of the generated programs contained vulnerabilities, highlighting the security risks in AI-generated code.

4. Discussion

The best defense strategy against a potential cyberattack is, apart from training users, to establish a solution that includes continuous monitoring, an adequate actualization and patching of the systems, effective incident management and the integration of Artificial Intelligence in such systems. This has proven to be very efficient and this is shown by the huge number of published works both in scientific journals and communications in international conferences (cf. the surveys referred to and their references). Artificial Intelligence is basically a system that has been trained to develop specific tasks without a previous programming. But perhaps, the introduction of Generative Artificial Intelligence is the greatest evolution of these autonomous methods and it is revolutionizing all the fields where this is applied and Cybersecurity is one of these.

Cybersecurity in IoT environments shows a high level of complexity and special challenges due to several factors, such as the heterogeneity and distributed character of IoT networks or the restrictions of computing resources, storage or energy consumption of the devices, among other factors. Generative Artificial Intelligence is a type of technology able to create original content for Deep Learning models that are previously trained with large datasets. Thus, the main difference between Generative Artificial Intelligence and the previous models, also known as Discriminative Artificial Intelligence, is that the first one can create content, whereas the second model basically is used for data classification.

4.1. GenAI Applied in IoT Cybersecurity

Among the content that a Generative Artificial Intelligence is able to create, we find image, music, speech and video generations that have possible applications in IoT Cybersecurity, for instance in Access Control or more precisely in authentication. Sensor capability might be affected for noise or illumination and these models can recreate the patterns they

have obtained from a large amount of training data and then use the acquired knowledge to create new data that could help to authenticate users' identity in changing conditions or help an Intrusion Detection Service to identify a menace, as we have seen throughout the paper in several cited applications.

Image generation has many applications in Cybersecurity given that a very usual technique is to encode data bytes as a matrix image, so data can be treated as images and thus we can benefit from the image-generation capacity to create realistic images, i.e., images non-necessarily identifiable by humans, but with the same features as the models included in the dataset. Thus, a classifier model can be trained to identify a much larger set of instances and provide Cybersecurity applications such as malware detection, allowing one to detect malicious software that usually has polymorphic and metamorphic characteristics. This is a key issue in IoT systems given that, on many occasions, the absence of authentication central entities can allow attackers to execute software in hardware that can cause fatal consequences.

Another important application is data synthetic creation. We have seen through most of the applications of this technology cited in the paper that the models usually include a data training stage, where huge amounts of data that fit with all the characteristics of the original data provided to the model are needed to achieve effectiveness in the task. This data augmentation is particularly useful when data origin or characteristics are special, such as health data or because they contain personal information. Sometimes, the dataset is not large enough to carry out an appropriate training process. A particular case is IoT traffic data, where this data traffic can contain benign or anomalous data that may help the IDS to detect possible intrusions that can affect data privacy or develop some kind of attack. This is specially useful for detecting some types of very common attacks in IoT devices such as DoS or DDoS attacks, usually developed by bots, whose presence in the network can be detected through data traffic analysis using this technique and thus prevent the attack before this takes place.

Table 4 collects the number of works that appear in all of the IoT Cybersecurity applications considered in this review. As we can observe, almost half of them are related to detecting anomalies in the IoT traffic, i.e., Access Control, which includes authorization and Cyber Threat Detection. Thus, we can derive, as it is in the essence of GenAI, that training is essential for the effectiveness of the several GenAI models applied in IoT Cybersecurity. However, works related to IoT Data Traffic Generation represent less than a 10% of the total number of collected works.

Table 4. Number of articles in every IoT Cybersecurity category.

Section	Number of Articles	Total Percentage (%)
Access Control	12	12.12%
AC—Authorization	16	16.16%
Blockchain	11	11.11%
Cyber Threat Detection	20	20.20%
IoT Software Security	16	16.16%
Reinforced Encryption	12	12.12%
IoT Data Traffic Generation	8	8.08%
Penetration Testing	4	4.04%

4.2. Growing Applications

Cryptographic applications appear among the possible case of use in IoT Cybersecurity for Generative Artificial Intelligence as well and as can be observed in Table 4 prove to be a growing case of study. Encryption reinforced with what is known as neural encryption is starting to be considered a useful possibility to achieve confidentiality in IoT networks. The result is a hybrid system that uses traditional cryptosystems to produce encrypted information that is later encrypted using a system of generative neural networks that produce encrypted messages and that correspond essentially to the same original data,

being apparently very difficult to break without knowledge of the methodology supporting the system. Key exchange is also another explored application of particular interest in distributed environments as is the case of IoT, where session keys are usually constructed in a collaborative way.

Blockchain is a cryptographic authentication technology that is becoming very popular in IoT networks because of its distributed nature as well. Blockchain does not need central authorities that provide certification for authentication, but the authentication process is provided by the members of the network themselves. Blockchain in collaboration with other techniques such as key exchange with Generative Artificial Intelligence models or Federated Learning is giving rise to several applications in Cybersecurity in IoT environments as member authentication or IDSs for Cyber Threat Detection.

Other possible applications are not as exploited as the preceding. Some Generative Artificial Intelligence tools allow one to generate code. This is not only a support for software developers, but also to help in software security, avoiding possible software vulnerabilities.

Another Cybersecurity technique that is starting to adopt Generative Artificial Intelligence methods is Penetration Testing. The special nature of IoT networks requires continuous monitoring and vulnerability analysis to avoid Cybersecurity attacks. Penetration Testing is a technique that consists in attacking the network in order to find vulnerabilities before they could be exploited by malicious parties. These methods can be very diverse and are closely related with the objective that is pursued, but always making use of the data-generation capabilities of these generative models. These may include data injection or simulating attacks and it is a promising and inspiring branch for future uses of Generative Artificial Intelligence.

To end this part, we find Large Language Models that make use of Deep Learning and that are trained in an unsupervised way with large datasets in a parallel approach. Very recent papers published in public repositories show their applicability in most of the preceding mentioned research lines in Cybersecurity.

4.3. Ethical Concerns

Let us finish this part with a brief reference to the ethical concerns involved in the use of GenAI in Cybersecurity. A maxim that any Cybersecurity specialist knows is that everything that is used to strengthen the defense of any system can also be used against it. A clear example of this is Penetration Testing, which is one of the application fields considered in this review. Thus, every ethical concern in this area should be considered. As instances of the possible malicious use of GenAI to create very sophisticated attacks, we can find the works [52,62–64,68–70,106], cited among the references. Here, the authors make use of the same techniques to design dangerous attacks that avoid every traditional Cybersecurity measure.

Another important aspect to take into account is that Generative AI can potentially amplify existing biases. As a consequence, a dataset that is used to train a GenAI model and that could be somehow biased might be derived from training datasets whose bias is increased and therefore the resulting model could be effective against this, but useless in another case, with harmful consequences.

5. Conclusions

In this paper, we conducted a review of the possibilities that Generative Artificial Intelligence offers for Cybersecurity applications in IoT networks. The intrinsic distributed and complex nature of these networks with devices that very often are very limited make them susceptible to multiple security challenges. The capability that Generative Artificial Intelligence methods offer to generate original content has shown its applicability in many diverse fields and due to the content features these methods show a direct application in determined Cybersecurity practices such as Access Control or threat detection. However, some recent inspiring proposals have shown a larger application field, which include

encryption to achieve confidentiality and privacy, Blockchain or Cybersecurity Forensic Techniques such as Secure Software or Pentesting. Concerning future research, a lot of works in the cited widespread research lines are being produced, but at the same time it is important to find solutions to unsolved problems related to new Cybersecurity applications.

Author Contributions: J.L.L.D. and J.A.L.R. authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Author Juan Luis López Delgado was employed by Elastacloud, Ltd. The remaining author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AE	Autoencoder
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMCGAN	Algebraic Matrix Conditional Generative Adversarial Network
API	Application Programming Interface
BBPE	Byte-Pair Encoder
BDI	Belief–Desire–Intention
BERT	Bidirectional Encoder Representations from Transformers
CCCGAN	Cycle-Consistent Generative Adversarial Network
CGAN	Conditional Generative Adversarial Network
ChatGPT	Chat Generative Pre-trained Transformer
CNN	Convolutional Neural Network
CP-ABE	Ciphertext Attribute-Based Encryption
CWE	Common Weakness Enumeration
CXE	Chaotic Exclusive OR Encryption
DAG	Directed Acyclic Graph
DDoS	Distributed Denial of Service
DGRNN	Deep Generalized Recurrent Neural Network
DL	Deep Learning
DNP3	Distributed Network Protocol
DoS	Denial of Service
ESBMC	Efficient SMT-based Bounded Model Checker
FS-GAN	Face Swapping-Generative Adversarial Network
FPGA	Field-Programmable Gate Array
GAIL	Generative Adversarial Imitation Learning
GAN	Generative Adversarial Network
GenAI	Generative Artificial Intelligence
ICS	Industrial Control System
IDS	Intrusion-Detection System
IGAN	Imbalance Generative Adversarial Network
IIoT	Industrial Internet of Things
GAN	Generative Adversarial Network
IoT	Internet of Things
HTTPS	Hypertext Transfer Protocol Secure
LLaMA	Large Language Model Meta AI
LLMs	Large Language Model

ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NFV	Network Function Virtualization
NLP	Natural Language Processing
OOD	Out-of-Distribution
PPFLE	Privacy-Preserving Fixed-Length Encoding
PPSA-GAN	Privacy-Preserving Self-Attention Generative Adversarial Network
QoS	Quality of Service
RAN	Radio Access Network
RGB	Red Green Blue
SDN	Software Defined Network
SSH	Secure Shell
VAE	Variational Autoencoder
VecGAN	Vector Generative Adversarial Network
WAF	Web Application Firewalls
XGBoost	Extreme Gradient Boosting
XOR	Exclusive OR
XSS	Cross Site Scripting

References

1. Evans, D. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*; White Paper; Cisco Internet Business Solutions Group, Cisco: San Jose, CA, USA, 2011. Available online: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed on 12 August 2024).
2. What Is the Internet of Things (IoT)? Available online: https://www.ibm.com/topics/Internet-of-things (accessed on 12 August 2024).
3. Mejias, U.A.; Couldry, N. Datafication. *Internet Policy Rev.* **2019**, *8* . [CrossRef]
4. Wiewiórowski, W. Cybersecurity and Data Protection: A Necessary and Powerful Duo (English), European Data Protection Supervisor. 28 September 2023. Available online: https://www.edps.europa.eu/press-publications/press-news/blog/Cybersecurity-and-data-protection-necessary-and-powerful-duo_en (accessed on 12 August 2024).
5. Cellular IoT Connections Reached 3.4 Billion in 2023. Available online: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook (accessed on 13 August 2024).
6. Alsheikh, M.; Konieczny, L.; Prater, M.; Smith, G.; Uludag, S. The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders. *IEEE Consum. Electron. Mag.* **2022**, *11*, 59–68. [CrossRef]
7. Simmons, A. Internet of Things (IoT) Architecture: Layers Explained. 13 November 2022. Available online: https://dgtlinfra.com/Internet-of-things-iot-architecture/ (accessed on 13 August 2024).
8. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A survey on enabling technologies, protocols and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
9. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
10. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [CrossRef]
11. Sun, L.; Du, Q. A review of physical layer security techniques for Internet of Things: Challenges and solutions. *Entropy* **2018**, *20*, 730. [CrossRef] [PubMed]
12. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of Things security: A top-down survey. *Comput. Netw.* **2018**, *141*, 199–221. [CrossRef]
13. Khan, M.A.; Salah, K. IoT security: Review, Blockchain solutions and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
14. Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion-Detection Systems in the Internet of Things: A comprehensive investigation. *Comput. Netw.* **2019**, *160*, 165–191. [CrossRef]
15. Abdul-Ghani, H.A.; Konstantas, D.; Mahyoub, M. A comprehensive IoT attacks survey based on a building-blocked reference model. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 355–373.
16. Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A survey on privacy and security of Internet of Things. *Comput. Sci. Rev.* **2020**, *38*, 100312. [CrossRef]
17. Tahsien, S.M.; Karimipour, H.; Spachos, P. Machine Learning based solutions for security of Internet of Things (IoT): A survey. *J. Netw. Comput. Appl.* **2020**, *161*, 102630. [CrossRef]
18. Sengupta, J.; Ruj, S.; Das Bit, S. A comprehensive survey on attacks, security issues and Blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]

19. Shah, Y.; Sengupta, S. A survey on classification of cyber-attacks on IoT and IIoT devices. In Proceedings of the 2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, USA, 28–31 October 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 406–413.
20. Liang, X.; Kim, Y. A survey on security attacks and solutions in the IoT network. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Virtual, 27–30 January 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 853–859.
21. Krishna, R.R.; Priyadarshini, A.; Jha, A.V.; Appasani, B.; Srinivasulu, A.; Bizon, N. State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. *Sustainability* **2021**, *13*, 9463. [CrossRef]
22. Bel, H.J.F.; Sabeen, S. A survey on IoT security: Attacks, challenges and countermeasures. *Webology* **2022**, *19*, 3741–3763.
23. Sasi, T.; Lashkari, A.H.; Lu, R.; Xiong, P.; Iqbal, S. A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *J. Inf. Intell.* 2023, *in press*. Available online: https://nrc-publications.canada.ca/eng/view/ft/?id=cac39ec4-3edc-4871-856a-a22de42cf3a1 (accessed on 15 August 2024).
24. Hou, K.M.; Diao, X.; Shi, H.; Ding, H.; Zhou, H.; de Vaulx, C. Trends and Challenges in AIoT/IIoT/IoT Implementation. *Sensors* **2023**, *23*, 5074. [CrossRef]
25. Kaur, R.; Gabrijelčič, D.; Klobučar, T. Artificial Intelligence for Cybersecurity: Literature review and future research directions. *Inf. Fusion* **2023**, *97*, 101804. [CrossRef]
26. Goodfellow, I.; Pouget-Abadie, J.; Mirza, M.; Xu, B.; Warde-Farley, D.; Ozair, S.; Courville, A.; Bengio, Y. Generative adversarial nets. In *Advances in Neural Information Processing Systems*; Curran Associates: Red Hook, NY, USA, 2014; pp. 2672–2680.
27. Jiang, J.; Han, G.; Liu, L.; Shu, L.; Guizani, M. Outlier Detection Approaches Based on Machine Learning in the Internet-of-Things. *IEEE Wirel. Commun.* **2020**, *27*, 53–59. [CrossRef]
28. Mazhar, T.; Talpur, D.B.; Shloul, T.A.; Ghadi, Y.Y.; Haq, I.; Ullah, I.; Ouahada, K.; Hamam, H. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. *Brain Sci.* **2023**, *13*, 683. [CrossRef] [PubMed]
29. Alahmadi, A.A.; Aljabri, M.; Alhaidari, F.; Alharthi, D.; Rayani, G.E.; Marghalani, L.A.; Alotaibi, O.B.; Bajandouh, S. DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions. *Electronics* **2023**, *12*, 3103. [CrossRef]
30. Bala, B.; Behal, S. AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. *Comput. Sci. Rev.* **2024**, *52*, 100631. [CrossRef]
31. Kuzlu, M.; Fair, C.; Guler, O. Role of Artificial Intelligence in the Internet of Things (IoT) Cybersecurity. *Discov. Internet Things* **2021**, *1*, 7. [CrossRef]
32. Alotaibi, B. A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions and Edge Computing Opportunities. *Sensors* **2023**, *23*, 7470. [CrossRef] [PubMed]
33. Diro, A.; Chilamkurti, N.; Nguyen, V.-D.; Heyne, W. A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms. *Sensors* **2021**, *21*, 8320. [CrossRef]
34. Gyamfi, E.; Jurcut, A. Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning and Datasets. *Sensors* **2022**, *22*, 3744. [CrossRef] [PubMed]
35. Sana, L.; Nazir, M.M.; Muddesar, I.; Lal, H.; Amjad, A. Anomaly Detection for Cyber Internet of Things Attacks: A Systematic Review. *Appl. Artif. Intell.* **2022**, *36*, 2137639. [CrossRef]
36. Manivannan, D. Recent endeavors in Machine Learning-powered Intrusion-Detection Systems for the Internet of Things. *J. Netw. Comput. Appl.* **2024**, *229*, 103925. [CrossRef]
37. Saadouni, R.; Gherbi, C.; Aliouat, Z.; Harbi, Y.; Khacha, A. Intrusion-Detection Systems for IoT based on bio-inspired and Machine Learning techniques: A systematic review of the literature. *Cluster Comput.* **2024**, *27*, 8655–8681. [CrossRef]
38. Shahin, M.; Maghanaki, M.; Hosseinzadeh, A.; Chen, F.F. Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion-Detection Systems. *Adv. Eng. Inform.* **2024**, *62*, 102685. [CrossRef]
39. Meziane, H.; Ouerdi, N. A survey on performance evaluation of Artificial Intelligence algorithms for improving IoT security systems. *Sci. Rep.* **2023**, *13*, 21255. [CrossRef]
40. Alwahedi, F.; Aldhaheri, A.; Ferrag, M.A.; Battah, A.; Tihanyi, N. Machine Learning techniques for IoT security: Current research and future vision with generative AI and Large Language Models. *Internet Things Cyber-Phys. Syst.* **2024**, *4*, 167–185. [CrossRef]
41. Ferrag, M.A.; Friha, O.; Maglaras, L.; Janicke, H.; Shu, L. Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications and Experimental Analysis. *IEEE Access* **2021**, *9*, 138509–138542. [CrossRef]
42. Rodríguez, E.; Otero, B.; Canal, R. A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things. *Sensors* **2023**, 23, 1252. [CrossRef]
43. AboulEla, S.; Ibrahim, N.; Shehmir, S.; Yadav, A.; Kashef, R. Navigating the Cyber Threat Landscape: An In-Depth Analysis of Attack Detection within IoT Ecosystems. *AI* **2024**, *5*, 704–732. [CrossRef]
44. Li, H.; Ge, L.; Tian, L. Survey: Federated Learning data security and privacy-preserving in edge-Internet of Things. *Artif. Intell. Rev.* **2024**, *57*, 130. [CrossRef]
45. Khazane, H.; Riduouani, M.; Salahdine, F.; Kaabouch, N. A Holistic Review of Machine Learning Adversarial Attacks in IoT Networks. *Future Internet* **2024**, *16*, 32. [CrossRef]
46. Aldhaheri, A.; Alwahedi, F.; Ferrag, M.A.; Battah, A. Deep Learning for Cyber Threat Detection in IoT networks: A review. *Internet Things Cyber-Phys. Syst.* **2024**, *4*, 110–128. [CrossRef]

47. Yinka-Banjo, C.; Ugot, O.A. A review of Generative Adversarial Networks and its application in Cybersecurity. *Artif. Intell. Rev.* **2020**, *53*, 1721–1736. [CrossRef]
48. Cai, Z.; Xiong, Z.; Xu, H.; Wang, P.; Li, W.; Pan, Y. Generative Adversarial Networks: A Survey Toward Private and Secure Applications. *ACM Comput. Surv.* **2021**, *54*, 1–38. [CrossRef]
49. Majeed, A. Attribute-Centric and Synthetic Data Based Privacy Preserving Methods: A Systematic Review. *J. Cybersecur. Priv.* **2023**, *3*, 638–661. [CrossRef]
50. Seo, E.; Song, H.M.; Kim, H.K. GIDS: GAN based Intrusion-Detection System for In-Vehicle Network. In Proceedings of the 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 28–30 August 2018; pp. 1–6.
51. Liu, Y.; Xiao, M.; Zhou, Y.; Zhang, D.; Zhang, J.; Gacanin, H.; Pan, J. An Access Control Mechanism Based on Risk Prediction for the IoV. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5.
52. Hou, T.; Wang, T.; Lu, Z.; Liu, Y.; Sagduyu, Y. IoTGAN: GAN Powered Camouflage Against Machine Learning Based IoT Device Identification. In Proceedings of the 2021 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Los Angeles, CA, USA, 13–15 December 2021; pp. 280–287.
53. Nukavarapu, S.K.; Nadeem, T. Securing Edge-Based IoT Networks with Semi-Supervised GANs. In Proceedings of the 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops), Kassel, Germany, 22–26 March 2021; pp. 579–584.
54. Fan, C.; Liu, P. Federated Generative Adversarial Learning. In *Pattern Recognition and Computer Vision: Third Chinese Conference, PRCV 2020, Nanjing, China, 16–18 October 2020*; LNCS 12307; Springer: Berlin/Heidelberg, Germany, 2020; pp. 3–15.
55. Siniosoglou, I.; Sarigiannidis, P.; Argyriou, V.; Lagkas, T.; Goudos, S.K.; Poveda, M. Federated Intrusion Detection In NG-IoT Healthcare Systems: An Adversarial Approach. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
56. Nayak, S.; Ahmed, N.; Misra, S. Deep Learning-Based Reliable Routing Attack Detection Mechanism for Industrial Internet of Things. *Ad. Hoc. Netw.* **2021**, *123*, 102661. [CrossRef]
57. Ullah, I.; Mahmoud, Q.H. A Framework for Anomaly Detection in IoT Networks Using Conditional Generative Adversarial Networks. *IEEE Access* **2021**, *9*, 165907–165931. [CrossRef]
58. Tabassum, A.; Erbad, A.; Ledba, W.; Mohamed, A.; Guizani, M. FEDGAN-IDS: Privacy-Preserving IDS Using GAN and Federated Learning. *Comput. Comm.* **2022**, *192*, 299–310. [CrossRef]
59. Gupta, N.; Shojafar, M.; Foh, C.H.; Tafazolli, R. An Efficient Distributed Intrusion-Detection System in IoT: GAN-Based Attacks and a Countermeasure. In Proceedings of the 2023 IEEE International Conference on Communications Workshops (ICC Workshops), Rome, Italy, 28 May–1 June 2023; pp. 1824–1829.
60. Boppana, T.K.; Bagade, P. GAN-AE: An unsupervised Intrusion-Detection System for MQTT networks. *Eng. Appl. Artif. Intell.* **2023**, *119*, 105805. [CrossRef]
61. Wu, Y.; Nie, L.; Wang, S.; Ning, Z.; Li, S. Intelligent Intrusion Detection for Internet of Things Security: A Deep Convolutional Generative Adversarial Network-Enabled Approach. *IEEE Internet Things J.* **2023**, *10*, 3094–3106. [CrossRef]
62. van den Oord, A.; Dieleman, S.; Zen, H.; Simonyan, K.; Vinyals, O.; Graves, A.; Kalchbrenner, N.; Senior, A.; Kavukcuoglu, K. WaveNet: A generative model for raw audio. *arXiv* **2016**, arXiv:1609.03499. Available online: https://arxiv.org/abs/1609.03499 (accessed on 30 September 2024).
63. Roy, A.; Memon, N.; Ross, A. MasterPrint: Exploring the vulnerability of partial fingerprint-based authentication systems. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2013–2025. [CrossRef]
64. Bontrager, P.; Roy, A.; Togelius, J.; Memon, N.; Ross, A. DeepMasterPrints: Generating MasterPrints for dictionary attacks via latent variable evolution. In Proceedings of the IEEE 9th International Conference on Biometry Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; pp. 1–9.
65. Merchant, K.; Nousain, B. Securing IoT RF Fingerprinting Systems with Generative Adversarial Networks. In Proceedings of the MILCOM 2019–2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 12–14 November 2019; pp. 584–589.
66. Chen, Z.; Peng, L.; Hu, A.; Fu, H. Generative Adversarial Network?based rogue device identification using differential constellation trace figure. *J. Wirel. Commun. Netw.* **2021**, *2021*, 72. [CrossRef]
67. Huang, D.; Al-Hourani, A. Physical Layer Spoof Detection and Authentication for IoT Devices Using Deep Learning Methods. *IEEE Trans. Mach. Learn. Commun. Netw.* **2024**, *2*, 841–854. [CrossRef]
68. Hitaj, B.; Gasti, P.; Ateniese, G.; Perez-Cruz, F. PassGAN: A Deep Learning Approach for Password Guessing. In *Applied Cryptography and Network Security*; Springer: Cham, Switzerland, 2019; pp. 217–237.
69. Nam, S.; Jeon, S.; Kim, H.; Moon, J. Recurrent GANs Password Cracker For IoT Password Security Enhancement. *Sensors* **2020**, *20*, 3106. [CrossRef] [PubMed]
70. Wong, H.; Luo, T. Man-in-the-Middle Attacks on MQTT-Based IoT Using BERT Based Adversarial Message Generation. In Proceedings of the KDD'20 Workshops: The 3rd International Workshop on Artificial Intelligence of Things (AIoT), San Diego, CA, USA, 24 August 2020.
71. Chen, S.; Ching-Chun, C.; Echizen, I. Steganographic Secret Sharing with GAN-Based Face Synthesis and Morphing for Trustworthy Authentication in IoT. *IEEE Access* **2021**, *9*, 116427–116439. [CrossRef]

72. Du, P.; Zheng, X.; Liu, L.; Ma, H. LC-GAN: Improving Adversarial Robustness of Face Recognition Systems on Edge Devices. *IEEE Internet Things J.* **2023**, *10*, 8172–8184. [CrossRef]
73. Meng, R.; Xu, X.; Wang, B.; Sun, H.; Xia, S.; Han, S. Physical-Layer Authentication Based on Hierarchical Variational Autoencoder for Industrial Internet of Things. *IEEE Things J.* **2023**, *10*, 2528–2544. [CrossRef]
74. Alhoraibi, L.; Alghazzawi, D.; Alhebshi, R. Generative Adversarial Network-Based Data Augmentation for Enhancing Wireless Physical Layer Authentication. *Sensors* **2024**, *24*, 641. [CrossRef] [PubMed]
75. Li, Y.; Liu, L.; Qun, H.; Deng, S.; El-Yacoubi, M.A.; Zhou, G. Adaptive Deep Feature Fusion for Continuous Authentication with Data Augmentation. *IEEE Trans. Mob. Comput.* **2023**, *22*, 5690–5705. [CrossRef]
76. Li, Y.; Ouyang, C.; Huan, H. AEGANAuth: Autoencoder GAN-Based Continuous Authentication with Conditional Variational Autoencoder Generative Adversarial Network. *IEEE Internet Things J.* **2024**, *11*, 27635–27650. [CrossRef]
77. Lai, C.; Zhang, X.; Zhang, H.; Li, G.; Yu, Y.; Zheng, D. GAN Augmentation-Based Continuous Authentication for Vehicular Digital Twin. In Proceedings of the ICC 2024-IEEE International Conference on Communications, Denver, CO, USA, 9–13 June 2024; pp. 5220–5225.
78. Bouzeraib, W.; Ghenai, A.; Zeghib, N. A Blockchain Data Balance Using a Generative Adversarial Network Approach: Application to Smart House IDS. In Proceedings of the 2020 International Conference on Advanced Aspects of Software Engineering (ICAASE), Constantine, Algeria, 28–30 November 2020; pp. 1–6.
79. Zheng, W.; Wang, K.; Wang, F.-Y. GAN-Based Key Secret-Sharing Scheme in Blockchain. *IEEE Trans. Cybern.* **2021**, *51*, 393–404. [CrossRef] [PubMed]
80. Abdulqadder, I.H.; Zhou, S. SliceBlock: Context-Aware Authentication Handover and Secure Network Slicing Using DAG-Blockchain in Edge-Assisted SDN/NFV-6G Environment. *IEEE Internet Things J.* **2022**, *9*, 18079–18097. [CrossRef]
81. Sugitha, G.; Solairaj, A.; Suresh, J. Block chain fostered cycle-consistent Generative Adversarial Network framework espoused intrusion detection for protecting IoT network. *Trans. Emerg. Telecommun.* **2022**, *33*, e4578. [CrossRef]
82. Carreño Aguilera, R.; Patiño Ortíz, M.; Aguilar Esteva, V.; Pacheco Bautista, D. Blockchain-based IoFLT Federated Learning in a fuzzy/GAN environment for a smart trading bot. *Fractals* **2023**, *31*, 235005.
83. Liu, W.; He, Y.; Wang, X.; Duan, Z.; Liang, W.; Liu, Y. BFG: Privacy protection framework for Internet of medical things based on Blockchain and Federated Learning. *Connect. Sci.* **2023**, *35*, 2199951. [CrossRef]
84. Ali, A.; Al-Rimy, B.A.S.; Alsubaei, F.S.; Almazroi, A.A.; Almazroi, A.A. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. *Sensors* **2023**, *23*, 6762. [CrossRef] [PubMed]
85. Ul Ghani, A.N.; Kun, S.; Rauf, M.A.; Alajmi, M.; Ghadi, Y.Y.; Algarni, A. Securing synthetic faces: A GAN-Blockchain approach to privacy-enhanced facial recognition. *J. King Saud Univ.-Comput. Inf. Sci.* **2024**, *36*, 102306. [CrossRef]
86. Ul Ghani, A.N.; Kun, S.; Rauf, M.A.; Khan, S.; Alajmi, M.; Ghadi, Y.Y.; Alkathani, H.K. Toward robust and privacy-enhanced facial recognition: A decentralized Blockchain-based approach with GANs and Deep Learning. *Math. Biosci. Eng.* **2024**, *21*, 4165–4186. [CrossRef]
87. Rawlins, C.; Sarangapani, J. Predicting IoT Distributed Ledger Fraud Transactions with a Lightweight GAN Network. *IEEE Trans. Mob. Comput.* **2024**, *23*, 7818–7829. [CrossRef]
88. Arachchige, K.G.; Branch, P.; But, J. An Analysis of Blockchain-Based IoT Sensor Network Distributed Denial of Service Attack. *Sensors* **2024**, *24*, 3083. [CrossRef]
89. Abdalgawad, N.; Sajun, A.; Kaddoura, Y.; Zualkernan, I.A. Generative Deep Learning to Detect Cyberattacks for the IoT-23 Dataset. *IEEE Access* **2022**, *10*, 6430–6441. [CrossRef]
90. Rucco, M.; Castiglione, F.; Merelli, E.; Pettini, M. Characterisation of the idiotypic immune network through persistent entropy. In Proceedings of the ECCS 2014, Lucca, Italy, 22–26 September 2014; Springer: Berlin/Heidelberg, Germany, 2016; pp. 117–128.
91. Sithungu, S.P.; Ehlers, E.M. GAAINet: A Generative Adversarial Artificial Immune Network Model for Intrusion Detection in Industrial IoT Systems. *J. Adv. Inf. Technol.* **2022**, *13*, 456–461. [CrossRef]
92. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
93. Geetha, K.; Brahmananda, S.H. Effective Internet of Things botnet classification by data upsampling using Generative Adversarial Network and scale fused bidirectional long short term memory attention model. *Concurr. Comput. Pract. Exp.* **2022**, *34*, 7380.
94. Lazzaro, S.; De Angelis, V.; Mandalari, A.M.; Buccafurri, F. Is Your Kettle Smarter Than a Hacker? A Scalable Tool for Assessing Replay Attack Vulnerabilities on Consumer IoT Devices. In Proceedings of the 2024 IEEE International Conference on Pervasive Computing and Communications (PerCom), Biarritz, France, 11–15 March 2024; pp. 114–124.
95. Burlina, P.; Joshi, N.; Wangetal, I. Where's Wally now? Deep generative and discriminative embeddings for novelty detection. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, 15–20 June 2019; pp. 11507–11516.
96. Nie, L.; Wu, Y.; Wang, X.; Guo, L.; Wang, G.; Gao, X.; Li, S. Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 134–145. [CrossRef]
97. Benaddi, H.; Jouhari, M.; Ibrahimi, K.; Ben Othman, J.; Amhoud, E.M. Anomaly Detection in Industrial IoT Using Distributional Reinforcement Learning and Generative Adversarial Networks. *Sensors* **2022**, *22*, 8085. [CrossRef] [PubMed]
98. Sharma, B.; Sharma, L.; Lal, C.; Roy, S. Anomaly based network intrusion detection for IoT attacks using Deep Learning technique. *Comput. Electr. Eng.* **2023**, *107*, 108626. [CrossRef]

99. Poongodi, M.; Hamdi, M. Intrusion-Detection System using distributed multilevel discriminator in GAN for IoT system. *Trans. Emerg. Telecommun.* **2023**, *34*, 4815. [CrossRef]
100. Rahman, S.; Pal, S.; Mittal, S.; Chawla, T.; Karmakar, C. SYN-GAN: A robust Intrusion-Detection System using GAN-based synthetic data for IoT security. *Internet Things* **2024**, *26*, 101212. [CrossRef]
101. Moti, Z.; Hashemi, S.; Karimipour, H.; Dehghantanha, A.; Jahromi, A.N.; Abdi, L.; Alavi, F. Generative Adversarial Network to detect unseen Internet of Things malware. *Ad. Hoc. Netw.* **2021**, *122*, 102591. [CrossRef]
102. Yao, W.; Zhao, H.; Shi, H. Privacy-Preserving Collaborative Intrusion Detection in Edge of Internet of Things: A Robust and Efficient Deep Generative Learning Approach. *IEEE Internet Things J.* **2024**, *11*, 15704–15722. [CrossRef]
103. Smmarwar, S.K.; Gupta, G.P.; Kumar, S. Deep malware detection framework for IoT-based smart agriculture. *Comput. Electr. Eng.* **2022**, *104*, 108410. [CrossRef]
104. Shaikh, F.; Bou-Harb, E.; Vehabovic, A.; Crichigno, J.; Yayimli, A.; Ghani, N. IoT Threat Detection Testbed Using Generative Adversarial Networks. In Proceedings of the 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Sofia, Bulgaria, 6–9 June 2022; pp. 77–84.
105. Wang, Z.; Wang, W.; Yang, Y.; Han, Z.; Xu, D.; Su, C. CNN and GAN based classification of malicious code families: A code visualization approach. *Int. J. Intell. Syst.* **2022**, *37*, 12472–12489. [CrossRef]
106. Yumlembam, R.; Isaac, B.; Yang, L. IoT-Based Android Malware Detection Using Graph Neural Network with Adversarial Defense. *IEEE Internet Things J.* **2023**, *10*, 8432–8444. [CrossRef]
107. Dong, H.; Kotenko, I. VAE-GAN for Robust IoT Malware Detection and Classification in Intelligent Urban Environments: An Image Analysis Approach. In *Risks and Security of Internet and Systems*; CRiSIS 2023, Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2024; Volume 14529, pp. 200–215.
108. Carter, J.; Mancoridis, S.; Protopapas, P.; Galinkin, E. IoT Malware Data Augmentation using a Generative Adversarial Network. In Proceedings of the 57th Hawaii International Conference of System Sciences 2024, Hawaiian Village, HI, USA, 3–6 January 2024; pp. 7572–7581.
109. Hao, R.; Hussain, R.; Parra-Ullari, J.M.; Vasilakos, X.; Nejabati, R.; Simeonidou, D. GAN-Based Privacy Abuse Attack on Federated Learning in IoT Networks. In Proceedings of the IEEE INFOCOM 2024—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 20–23 May 2024; pp. 1–2.
110. AlEroud, A.; Karabatis, G. SDN-GAN: Generative Adversarial Deep NNs for Synthesizing Cyber Attacks on Software Defined Networks. In *On the Move to Meaningful Internet Systems: OTM 2019 Workshops*; OTM 2019, Lecture Notes in Computer Science; Panetto, H., Debruyne, C., Hepp, M., Lewis, D., Ardagna, C., Meersman, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; Volume 11878.
111. Xuan Qui, C.P.; Hong Quang, D.; Duy, P.T.; Thi Thu Hien, D.; Pham, V.-H. Strengthening IDS Against Evasion Attacks with GAN-Based Adversarial Samples in SDN-Enabled Network. In Proceedings of the 2021 RIVF International Conference on Computing and Communication Technologies (RIVF), Hanoi, Vietnam, 19–21 August 2021; pp. 1–6.
112. The Duy, P.; Khac Tien, L.; Hoang Khoa, N.; Thu Hien, D.T.; Gian-Tuan Nguyen, A.; Pham, V.-H. DIGFuPAS: Deceive IDS with GAN and function-preserving on adversarial samples in SDN-enabled networks. *Comput. Secur.* **2021**, *109*, 102367.
113. Le, L.T.; Thinh, T.N. On the Improvement of Machine Learning Based Intrusion-Detection System for SDN Networks. In Proceedings of the 2021 8th NAFOSTED Conference on Information and Computer Science (NICS), Hanoi, Vietnam, 21–22 December 2021; pp. 464–469.
114. Wang, J.; Liu, J. Deep Learning for Securing Software-Defined Industrial Internet of Things: Attacks and Countermeasures. *IEEE Internet Things J.* **2022**, *9*, 11179–11189. [CrossRef]
115. Ding, S.; Kou, L.; Wu, T. A GAN-Based Intrusion Detection Model for 5G Enabled Future Metaverse. *Mob. Netw. Appl.* **2022**, *27*, 2596–2610. [CrossRef]
116. Zabeehullah; Arif, F.; Khan, N.A.; Ul Haq, Q.M.; Asim, M.; Ahmad, S. An SDN-AI-Based Approach for Detecting Anomalies in Imbalance Data within a Network of Smart Medical Devices. *IEEE Consum. Electron. Mag.* 2024, *accepted*. [CrossRef]
117. Chen, L.; Wang, Z.; Huo, R.; Huang, T. An Adversarial DBN-LSTM Method for Detecting and Defending against DDoS Attacks in SDN Environments. *Algorithms* **2023**, *16*, 197. [CrossRef]
118. Uma Mageswari, R.; Zafar Ali Khan, N.; Gowthul Alam, M.M.; Jerald Nirmal Kumar, S. Addressing security challenges in industry 4.0: AVA-MA approach for strengthening SDN-IoT network security. *Comput. Secur.* **2024**, *144*, 103907. [CrossRef]
119. Li, S.; Cao, Y.; Liu, S.; Lai, Y.; Zhu, Y.; Ahmad, N. HDA-IDS: A Hybrid DoS Attacks Intrusion-Detection System for IoT by Using Semi-Supervised CL-GAN. *Expert Syst. Appl.* **2024**, *238*, 122198. [CrossRef]
120. Brandão Lent, D.M.; da Silva Ruffo, V.G.; Carvalho, L.R.; Lloret, J.; Rodrigues, J.J.P.C.; Lemes Proença, M. An Unsupervised Generative Adversarial Network System to Detect DDoS Attacks in SDN. *IEEE Access* **2024**, *12*, 70690–70706. [CrossRef]
121. Zacaron, A.M.; Brandão Lent, D.M.; da Silva Ruffo, V.G.; Carvalho, L.F.; Lemes Proença, M. Generative Adversarial Network Models for Anomaly Detection in Software Defined Networks. *J. Netw. Syst. Manag.* **2024**, *32*, 93. [CrossRef]
122. Maddu, M.; Rao, Y.N. Network intrusion detection and mitigation in SDN using Deep Learning models. *Int. J. Inf. Secur.* **2024**, *23*, 849–862. [CrossRef]
123. Zhang, Y.; Wu, X.; Dong, H. TIBS: A Deep-Learning Model for Network Intrusion Detection for SDN Environments. In Proceedings of the 2024 9th International Conference on Computer and Communication Systems (ICCCS), Xi'an, China, 19–22 April 2024; pp. 419–426.

124. Siniosoglou, I.; Radoglou-Grammatikis, P.; Efstathopoulos, G.; Fouliras, P.; Sarigiannidis, P. A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments. *IEEE Trans. Net. Serv. Manag.* **2021**, *18*, 1137–1151. [CrossRef]
125. Yu, Z.; Wang, H.; Wang, D.; Li, Z.; Song, H. CGFuzzer: A Fuzzing Approach Based on Coverage-Guided Generative Adversarial Networks for Industrial IoT Protocols. *IEEE Internet Things J.* **2022**, *9*, 21607–21619. [CrossRef]
126. Abadi, M.; Andersen, D.G. Learning to Protect Communications with Adversarial Neural Cryptography. *arXiv* **2016**, arXiv:1610.06918. Available online: https://arxiv.org/abs/1610.06918 (accessed on 30 September 2024).
127. Zhao, Y.; Zhang, S.; Tu, Q.; Li, X. A hybrid AES encryption for IOT using Adversarial Network. In Proceedings of the 2021 7th International Conference on Computer and Communications (ICCC), Chengdu, China, 10–13 December 2021; pp. 2096–2100.
128. Ding, Y.; Wu, G.; Chen, D.; Zhang, N.; Gong, L.; Cao, M.; Qin, Z. DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 1504–1518. [CrossRef]
129. Palanisamy, I.; Santha, T. Machine Learning Based Secured Data Transmission for Banking Application. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 1184–1194.
130. Hao, X.; Ren, W.; Xiong, R.; Zhu, T.; Choo, K.-K.R. Asymmetric cryptographic functions based on generative adversarial neural networks for Internet of Things. *Future Gener. Comput. Syst.* **2021**, *124*, 243–253. [CrossRef]
131. Ramasamy, S.S.; Srinivasan, A.; Suba, M.; Kalaichelvi, V.; Swaminathan, S. Secured Data Transmission in IoT Using Homomorphic Encryption. *Int. J. Intell. Syst. Appl. Eng.* **2022**, *10*, 241–246.
132. Palanisamy, I.; Santha, T. Secured Data Transmission in IoT Using Deep Learning Technique for Data Encryption and Decryption Mechanism. *Math. Statiscian Eng. Appl.* **2022**, *71*, 1316–1330.
133. Palanisamy, G.A.; Rajappan, S.; Murugasamy, V. Enhancing Secure Data Transmission in IoT via Advanced Conditional Generative Adversarial Network and Encryption Techniques. *Trait. Signal* **2024**, *41*, 401–410. [CrossRef]
134. Hindistan, Y.S.; Yetkin, E.F. A Hybrid Approach with GAN and DP for Privacy Preservation of IIoT Data. *IEEE Access* **2023**, *11*, 5837–5849. [CrossRef]
135. Huang, C.; Chen, S.; Zhang, Y.; Zhou, W.; Rodrigues, J.J.P.C.; de Albuquerque, V.H.C. A Robust Approach for Privacy Data Protection: IoT Security Assurance Using Generative Adversarial Imitation Learning. *IEEE Internet Things J.* **2022**, *9*, 17089–17097. [CrossRef]
136. Zhang, D.; Shafiq, M.; Srivastava, G.; Gadekallu, T.R.; Wang, L. STBCIoT: Securing the Transmission of Biometric Images in Customer IoT. *IEEE Internet Things J.* **2024**, *11*, 16279–16288. [CrossRef]
137. Shruti; Rani, S.; Boulila, W. Securing Internet of Things device data: An ABE approach using fog computing and generative AI. *Expert Syst.* **2024**, e13691. [CrossRef]
138. Shahid, M.R.; Blanc, G.; Jmila, H.; Zhang, Z.; Debar, H. Generative Deep Learning for Internet of Things Network Traffic Generation. In Proceedings of the 2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC), Perth, Australia, 1–4 December 2020.
139. Hui, S.; Wang, H.; Wang, Z.; Yang, X.; Liu, Z.; Jin, D.; Li, Y. Knowledge Enhanced GAN for IoT Traffic Generation. In Proceedings of the WWW'22 Proceedings of the ACM Web Conference 2022, Virtual Event, Lyon, France, 25–29 April 2022; pp. 3336–3346.
140. Alabdulwahab, S.; Kim, Y.-T.; Seo, A.; Son, Y. Generating Synthetic Dataset for ML-Based IDS Using CTGAN and Feature Selection to Protect Smart IoT Environments. *Appl. Sci.* **2023**, *13*, 10951. [CrossRef]
141. Xiao, Y.; Xia, R.; Li, Y.; Shi, G.; Nguyen, D.N.; Hoang, D.T.; Niyato, D.; Krunz, M. Distributed Traffic Synthesis and Classification in Edge Networks: A Federated Self-Supervised Learning Approach. *IEEE Trans. Mob. Comput.* **2024**, *23*, 1815–1829. [CrossRef]
142. Dabboussi, A.H.; Jammal, M. Traffic Data Augmentation Using GANs for ITS. In Proceedings of the 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), Abu Dhabi, United Arab Emirates, 29 April–1 May 2024; pp. 66–73.
143. Poisson, M.; Carnier, R.; Fukuda, K. GothX: A generator of customizable, legitimate and malicious IoT network traffic. In Proceedings of the 17th Cyber Security Experimentation and Test Workshop, CSET'24, Philadelphia, PA, USA, 13 August 2024; pp. 65–73.
144. Yang, J.; Huang, Y.; Siddula, M.; Cai, Z. Noise Generation GAN Based Identity Privacy Protection for Smart City. In Proceedings of the 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI), Atlanta, GA, USA, 18–21 October 2021; pp. 338–347.
145. Ma, Z.; Yang, Y.; Liu, Y.; Liu, X.; Ma, J. Mitigate noisy data for smart IoT via GAN based machine unlearning. *Sci. China Inf. Sci.* **2024**, *67*, 132104. [CrossRef]
146. Chu, G.; Lisitsa, A. Penetration Testing for Internet of Things and Its Automation. In Proceedings of the 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, UK, 28–30 June 2018; pp. 1479–1484.
147. Chowdhary, A.; Kristshekhar, J.; Zhao, M. Generative Adversarial Network (GAN)-Based Autonomous Penetration Testing for Web Applications. *Sensors* **2023**, *23*, 8014. [CrossRef] [PubMed]

148. Karagiannis, S.; Fusco, C.; Agathos, L.; Mallouli, W.; Casola, V.; Ntantogian, C.; Magkos, E. AI-Powered Penetration Testing using Shennina: From Simulation to Validation. In Proceedings of the 19th International Conference on Availability, Reliability and Security, Ares'24, Vienna, Austria, 30 July 2024; p. 169.
149. Happe, A.; Cito, J. Getting pwn'd by AI: Penetration Testing with Large Language Models. In Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, ESEC/FSE 2023, San Francisco, CA, USA, 3–9 December 2023; pp. 2082–2086.
150. Sai, S.; Yashvardhan, U.; Chamola, V.; Sikdar, B. Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E and Other Models for Enhancing the Security Space. *IEEE Access* **2024**, *12*, 53497–53516. [CrossRef]
151. Devlin, J.; Chang, M.-W.; Lee, K.; Toutanova, K. Bert: Pre-Training of Deep Bidirectional Transformers for Language Understanding. In Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Minneapolis, MN, USA, 2–7 June 2019; Burnstein, J., Doran, C., Solorio, T., Eds.; Association for Computational Linguistics: Stroudsburg, PA, USA, 2019; Volume 1, pp. 4171–4186.
152. Ferrag, M.A.; Ndhlovu, M.; Tihanyi, N.; Cordeiro, L.C.; Debbah, M.; Lestable, T.; Thandi, N.S. Revolutionizing Cyber Threat Detection with Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices. *IEEE Access* **2024**, *12*, 23733–23750. [CrossRef]
153. Maatouk, A.; Piovesan, N.; Ayed, F.; De Domenico, A.; Debbah, M. Large Language Models for Telecom: Forthcoming Impact on the Industry. *arXiv* **2023**, arXiv:2308.06013. Available online: https://arxiv.org/abs/2308.06013 (accessed on 30 September 2024). [CrossRef]
154. Zou, H.; Zhao, Q.; Bariah, L.; Bennis, M.; Debbah, M. Wireless Multi-Agent Generative AI: From Connected Intelligence to Collective Intelligence. *arXiv* **2023**, arXiv:2307.02757. Available online: https://arxiv.org/abs/2307.02757 (accessed on 30 September 2024).
155. Touvron, H.; Lavril, T.; Izacard, G.; Martinet, X.; Lachaux, M.-A.; Lacroix, T.; Rozière, B.; Goyal, N.; Hambro, E.; Azhar, F.; et al. LLaMA: Open and Efficient Foundation Language Models. *arXiv* **2023**, arXiv:2302.13971. Available online: https://arxiv.org/abs/2302.13971 (accessed on 30 September 2024).
156. Almazrouei, E.; Alobeidli, H.; Alshamsi, A.; Cappelli, A.; Cojocaru, R.; Debbah, M.; Goffinet, E.; Hesslow, D.; Launay, J.; Malartic, Q.; et al. The Falcon Series of Open Language Models. *arXiv* **2023**, arXiv:2311.16867. Available online: https://arxiv.org/abs/2311.16867 (accessed on 30 September 2024).
157. Ferrag, A.F.; Battah, A.; Tihanyi, N.; Jain, R.; Maimut, D.; Alwahedi, F.; Lestable, T.; Thandi, N.S.; Mechri, A.; Debbah, M.; et al. SecureFalcon: Are We There Yet in Automated Software Vulnerability Detection with LLMs? *arXiv* **2024**, arXiv:2307.06616v2. Available online: https://arxiv.org/pdf/2307.06616 (accessed on 30 September 2024).
158. Maatouk, A.; Ayed, F.; Piovesan, N.; De Domenico, A.; Debbah, M.; Luo, Z.-Q. TeleQnA: A Benchmark Dataset to Assess Large Language Models Telecommunications Knowledge. *arXiv* **2023**, arXiv:2310.15051. Available online: https://arxiv.org/abs/2310.15051 (accessed on 30 September 2024).
159. Jones, R.; Omar, M.; Mohammed, D.; Nobels, C.; Dawson, M. IoT Malware Detection with GPT Models. In Proceedings of the 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE), Las Vegas, NV, USA, 24–27 July 2023; pp. 1749–1752.
160. Bariah, L.; Zhao, Q.; Zou, H.; Tian, Y.; Bader, F.; Debbah, M. Large Generative AI Models for Telecom: The Next Big Thing. *arXiv* **2023**, arXiv:2306.10249. Available online: https://arxiv.org/abs/2306.10249 (accessed on 30 September 2024). [CrossRef]
161. Tihanyi, N.; Bisztray, T.; Jain, R.; Ferrag, M.A.; Cordeiro, L.C.; Mavroeidis, V. The FormAI Dataset: Generative AI in Software Security through the Lens of Formal Verification. In Proceedings of the 19th International Conference on Predictive Models and Data Analytics in Software Engineering, PROMISE 2023, San Francisco, CA, USA, 8 December 2023; pp. 33–43.