Generative Diffusion Models for Mobile Edge IoT Security: A Survey

Jiacheng Wang[a], Lijie Zhou[b], Xudong Wang[b], Changyuan Zhao[a], Lei Feng[b], Dusit Niyato[a] and Dong In Kim[c]

[a]College of Computing and Data Science, Nanyang Technological University, Singapore, 639798, Singapore
[b]State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[c]Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, 16419, South Korea

ARTICLE INFO

Keywords:
Internet of Things security
generative diffusion models
mobile edge IoT
intrusion detection

ABSTRACT

The rapid expansion of Internet of Things (IoT) systems has expanded the cyber attack surface across diverse applications, while IoT security remains constrained by heterogeneous, scarce, imbalanced, noisy, and partially observed data. In this context, given their significant successes in multidimensional data generation applications, generative diffusion models have emerged as a promising data-centric paradigm due to their strengths in generation and reconstruction-aware transformation. This survey reviews diffusion models for IoT security, covering two major directions: security data enhancement and direct threat analysis. We further summarize representative applications of diffusion models across different IoT scenarios, including industrial IoT, UAV networks, smart grids, healthcare IoT, and vehicular networks. We also summarize important research opportunities, including comprehensive model evaluation, efficient diffusion model training and inference, improved edge deployability, and stronger robustness under distribution shift, and outline future directions toward lightweight, robust, and deployment-aware frameworks.

1. Introduction

1.1. Background and Motivation

The rapid proliferation of internet of things (IoT) systems has greatly expanded the cyber attack surface across smart homes, industrial automation, healthcare, transportation, and edge-assisted sensing environments [34, 183, 167, 7]. Compared with conventional networked systems, IoT security is built on a much more challenging data foundation: security-relevant data are often heterogeneous, severely imbalanced, noisy, and partially observed [97, 48, 8, 71]. In mobile crowdsensing and edge-assisted IoT scenarios, security is further coupled with participant trust, location, and sensing-data leakage, and freshness-sensitive data collection, which makes centralized defense mechanisms difficult to apply directly [174, 42, 9, 166]. As a result, IoT security is a matter of designing better sensors and actuators, constructing usable security data, and enabling reliable threat inference during data collection and sharing. These characteristics expose the limitations of conventional intrusion detection and anomaly analysis methods, which typically assume sufficient labels, relatively stable data distributions, and clear feature representations [117, 201, 54]. Autoencoder-based and online anomaly detection methods have shown the value of unsupervised traffic modeling in

ORCID(s):

Table 1
Comparison Between IoT Security Issues and Those in Conventional Computer Networks

Category	Security Aspect	Conventional Computer Networks	IoT and Mobile Edge IoT Systems	Implication for This Survey
System environment	Attack surface [106]	• Servers, hosts, routers, and enterprise endpoints. • Relatively standardized configurations. • Centrally managed cloud services.	• Massive sensors, actuators, gateways, and mobile devices. • Widely deployed edge nodes and cyber-physical components. • Highly diverse devices, protocols, and deployment scenarios.	• Cross-device generalization. • Cross-protocol and cross-scenario modeling.
	Deployment environment [127]	• Security monitoring is often centralized. • Enterprise networks are hierarchically managed.	• Security functions are distributed across device, edge, and cloud layers. • Local communication constraints are critical.	• Edge-aware security frameworks. • Collaborative device–edge–cloud protection.
Data limitations	Data characteristics [43]	• Traffic and logs are usually more structured. • Monitoring infrastructure is relatively mature. • Data are easier to centralize.	• Data are heterogeneous, noisy, incomplete, and weakly labeled. • Data are generated under unstable sensing and communication conditions.	• Diffusion-based generation. • Denoising, reconstruction, and imputation.
	Class imbalance and rare events [53]	• Attack traces may be available from enterprise monitoring. • Public benchmarks and controlled testbeds are often available.	• Real attacks, faults, and safety-critical anomalies are rare. • Minority attack classes are costly to collect and annotate.	• Minority-class augmentation. • Synthetic security data construction.
	Observability [37]	• Network states, host logs, and system events are often complete. • Continuous monitoring is relatively feasible.	• Observations are frequently partial. • Packet loss, sensor failure, mobility, and intermittent connectivity are common.	• Conditional diffusion models. • Reconstruction-based and uncertainty-aware inference.
Operational constraints	Resource constraints [102]	• Security functions can often run on servers, desktops, or cloud platforms. • Computation and memory are usually sufficient.	• End devices and edge nodes have limited computation and memory. • Energy and latency constraints are strict.	• Lightweight diffusion models. • Compressed and deployment-aware inference.
	Threat dynamics [18]	• Threats are often analyzed in stable enterprise or cloud environments. • System boundaries are usually clearer.	• Threats are affected by physical processes, mobility, and environmental changes. • Device behaviors and attack patterns may evolve over time.	• Robustness under domain shift. • Concept-drift adaptation and cross-scenario transfer.

IoT and network environments, but their effectiveness still depends on representative training traffic, stable deployment settings, and sufficiently observable behavioral patterns [96, 99]. In real IoT environments, however, attack samples are scarce, device behaviors are diverse, and sensing quality is unstable [201, 48, 185]. Even advanced models are therefore constrained by the quality, quantity, and accessibility of the underlying data [48]. IoT security should thus be viewed as a broader data-centric problem involving data generation, reconstruction, analysis, and protection. Against this background, diffusion models have emerged as a promising technique at the intersection of generative modeling and IoT security [175, 135, 72]. In this broader intersection, two perspectives can be distinguished: 1) diffusion models for direct IoT security, and 2) diffusion models for optimizing IoT systems in ways that may indirectly benefit security. This survey considers both aspects, and the primary focus is the former perspective, namely studies in which diffusion models directly support security data enhancement, and threat analysis. Under this scope, diffusion models are attractive because they can learn minority or rare-event distributions for imbalanced intrusion learning [154, 184], and support direct analysis under noisy or incomplete observations through denoising, probabilistic imputation, forecasting, and reconstruction [86, 152, 142, 118]. Furthermore, to clarify the scope of this survey, Table 1 compares representative security characteristics of IoT systems with those of conventional computer networks [34]. Although IoT systems inherit many classical network security problems, such as intrusion detection, malware propagation, and unauthorized access [117], these problems become more difficult in IoT environments due to device heterogeneity, resource constraints,

unstable sensing and communication conditions, and limited labels. These differences explain why IoT security requires data-centric methods that can simultaneously support data enhancement and robust threat analysis [86].

Currently, related studies remain scattered across intrusion detection, industrial anomaly detection, and malware analysis [154, 152, 65]. Most focus on individual tasks or datasets, without clarifying the broader roles of diffusion models in the IoT security pipeline. This fragmentation makes it difficult to assess the research landscape, identify common technical trends, and understand deployment challenges [86, 152]. Motivated by this gap, this survey organizes the literature around two direct roles of diffusion models in IoT security: security data enhancement and threat analysis. In addition, to better reflect the recent growth of this area, we further performed a Google Scholar search using diffusion-model-related keywords combined with IoT security terms, and manually screened the retrieved papers for direct relevance. The resulting year-wise distribution, shown in Fig. 1, suggests a clear upward trend in the number of related studies in recent years. This increasing research activity further supports the timeliness and necessity of a focused survey on diffusion models for IoT security.

1.2. Related Surveys

Existing surveys related to this paper can be grouped into two major categories: surveys on IoT security and surveys on generative artificial intelligence (AI) and diffusion models. Both are relevant, but neither provides a focused review of diffusion models as direct tools for IoT security.

1) IoT security: Several recent surveys review IoT security from complementary system and application perspectives. For example, Dritsas *et al.* [34] provided a broad cybersecurity overview covering authentication, identity management, integrity, network protection, secure communication, and AI-enabled defense. Alotaibi *et al.* [6] focused on industrial IoT (IIoT), emphasizing security requirements, attack surfaces, AI-based defense, and edge-computing constraints. At the intrusion detection system (IDS) level, Rahman *et al.* [117] analyzed IoT intrusion detection in terms of models, features, datasets, loss functions, metrics, and computational efficiency, while Zhang *et al.* [201] further highlighted two persistent challenges in deep-learning-based IDS, namely spatiotemporal feature extraction and data imbalance. For anomaly-centric scenarios, Adhikari *et al.* [3] surveyed IoT anomaly detection across architectural layers and applications such as intrusion detection, fraud monitoring, and industrial automation. In medical IoT, Hassan *et al.* [55] emphasized dataset analysis together with federated learning and blockchain integration. Overall, these surveys clarify IoT threat models, and data characteristics, but they do not examine diffusion models as a dedicated methodological thread.

2) Generative AI and diffusion-model surveys: On the model side, Delgado *et al.* [89] provided the survey most closely related to this topic by reviewing generative-AI solutions for IoT security, including generative adversarial networks (GANs), variational autoencoders (VAEs), and diffusion models, but their goal was to map the broader

generative-AI landscape rather than diffusion-specific security workflows. Yang *et al.* [175] offered a general diffusion-model survey organized around efficient sampling, likelihood improvement, structured-data modeling, and applications, while Song *et al.* [133] focused on lightweight diffusion design and summarized strategies for reducing training and inference cost, which is highly relevant to resource-constrained IoT deployment. More specialized surveys also provided useful foundations: Yang *et al.* [181] reviewed diffusion models for time-series and spatio-temporal data across forecasting, anomaly detection, classification, and imputation; Liu *et al.* [86] organized diffusion-based anomaly detection into reconstruction, density, and hybrid-based paradigms while discussing efficiency, interpretability, robustness, edge–cloud collaboration, and large language model (LLM) integration; and Li *et al.* [82] focused on tabular diffusion models, especially their advantages, challenges, and future directions relative to GANs and VAEs. These studies are highly relevant because IoT security data are often temporal, structured, incomplete, and anomaly-centric. However, they remain mainly model-centric or data-centric, and do not explicitly organize the literature around diffusion roles in IoT security, such as attack-data augmentation and direct threat inference.

In summary, prior surveys have mainly reviewed either the IoT-security problem space or the diffusion-model methodology space. What remains missing is a focused survey on how diffusion models function directly within IoT security workflows. This survey aims to fill that gap by organizing the literature around two direct roles of diffusion models in IoT security: security data enhancement and threat analysis.

1.3. Scope and Contributions of This Survey

This survey focuses on the use of diffusion models for IoT security, rather than on the security, robustness, or attack surfaces of diffusion models themselves. Specifically, we consider studies in which diffusion models play a direct functional role in IoT-related security workflows, including data enhancement for security learning and direct threat analysis. Accordingly, we cover representative works on imbalance-oriented data augmentation, synthetic security data construction, intrusion detection from IoT network traffic, and anomaly detection from IIoT and multivariate sensor time series. The main contributions are as follows:

1. We provide a focused and systematic review of the emerging intersection between diffusion models and IoT security. Different from existing surveys that mainly discuss either IoT security mechanisms or diffusion models in general, this survey concentrates on how diffusion models directly support IoT security workflows.

2. We establish a role-oriented taxonomy of diffusion models for IoT security, covering two major directions: security data enhancement, and direct threat analysis. This taxonomy clarifies that diffusion models are useful for synthetic data generation and for reconstruction-based inference.

3. We review representative and recent studies in diffusion-based IoT security data enhancement, including sample-level rebalancing, pipeline-level augmentation, synthetic security data construction, and task-coupled generation.

We further summarize how these methods address data scarcity, class imbalance, noisy observations, and limited attack coverage in IoT environments.

4. We analyze diffusion models as inference-layer enabler for IoT systems. Specifically, we discuss their use in network intrusion detection, and IIoT multivariate time-series anomaly detection.

5. We identify major open challenges and future research directions, including evaluation beyond accuracy, efficient training and inference, edge deployment, robustness to domain shift, concept drift, and cross-domain transfer, and blockchain-assisted trustworthy collaboration.

This survey aims to offer readers a clear and systematic view of the emerging intersection between diffusion models and IoT security. By synthesizing representative studies, clarifying the functional roles of diffusion models in different security workflows, and summarizing their applications across diverse IoT scenarios, this survey provides useful guidance for researchers seeking new directions as well as practitioners interested in deploying diffusion-based solutions in real-world mobile edge IoT environments. As shown in Fig. 2, the remainder of this paper is organized as follows. Section 2 presents the foundations of IoT security data characteristics, existing countermeasures, and diffusion models. Section 3 reviews diffusion-based methods for IoT security data enhancement. Section 4 discusses diffusion models for direct IoT threat analysis. Section 5 summarizes applications of diffusion models in different IoT scenarios from data-oriented, and inference-oriented perspectives. Section 6 highlights open challenges and future research directions, including evaluation, efficiency, edge deployment, generalization, and blockchain-assisted trust. Finally, Section 7 concludes this paper.

2. Foundations

2.1. IoT Security Data Characteristics and Existing Countermeasures

IoT security spans diverse scenarios, including malicious traffic detection, network intrusion detection, and industrial anomaly detection [117, 177, 188]. These scenarios differ in security objectives and data forms. Intrusion detection in smart homes or edge networks often relies on packet- or flow-level tabular features [154][176], whereas industrial anomaly detection typically depends on multivariate sensor streams and control telemetry with strong temporal and physical dependencies [164, 203]. Hence, IoT security is strongly data-dependent, and its effectiveness is shaped by several difficult data characteristics.

1) *Heterogeneity, scarcity, and imbalance:* IoT security data come from diverse and weakly standardized sources, including traffic traces, device and gateway logs, wireless measurements, multivariate sensor records, and process-control signals [153]. These data vary widely in temporal structure, semantic meaning, feature granularity, and reliability, limiting direct transfer across datasets, protocols, and deployment environments [117]. Meanwhile, real

attacks and faults are rare, and high-quality labeled data are expensive to obtain, especially in operational settings [20]. This scarcity is closely tied to severe class imbalance, where benign traffic dominates and attack classes occupy only a small fraction of observations [154, 184]. Existing approaches include feature engineering, representation learning, transfer learning, cost-sensitive learning, and data augmentation [26]. Deep reinforcement learning (DRL)-based sensing and resource allocation strategies can further improve data collection efficiency by adapting sensing, communication, and computation policies to dynamic environments [75, 84]. However, these methods remain limited: feature engineering and transfer learning are often domain-specific; cost-sensitive learning does not create new minority-class evidence[1]; and oversampling or interpolation may replicate noise, unclear class boundaries, and fail to capture multimodal rare-attack structure [13]. Diffusion models are therefore promising because they can learn complex data distributions and generate diverse minority samples beyond simple duplication or local interpolation.

2) *Noise, uncertainty, and partial observability:* IoT data are often noisy because of packet loss, wireless instability, sensor drift, synchronization errors, and imperfect annotations [117, 203]. In addition, limited sensing coverage, constrained sampling, communication interruptions, and incomplete logging often lead to partial observability [146, 164]. Existing countermeasures include denoising, data imputation, robust temporal modeling, uncertainty-aware inference, and anomaly detection designed for incomplete observations [162]. DRL can also optimize sensing schedules or communication policies under resource constraints [75, 84]. Yet these methods often separate restoration from detection, rely on simplified assumptions about noise or missingness, and provide limited support for calibrated uncertainty under severe corruption [155]. By contrast, diffusion models offer a native denoising-and-reconstruction mechanism that can recover plausible structure from corrupted or incomplete inputs while supporting conditional generation, imputation, and uncertainty-aware inference in a unified probabilistic framework.

In summary, IoT security should be viewed not merely as a detection problem, but as a broader data-centric problem shaped by heterogeneity, scarcity, imbalance, noise, and partial observability. Existing methods provide only partial and fragmented remedies, which motivates growing interest in diffusion models as a unified framework for data enhancement and uncertainty-aware analysis.

2.2. Fundamentals of Diffusion Models

Diffusion models learn complex data distributions through a progressive noising-and-denoising process [58]. In the forward process, clean data are gradually corrupted with noise; in the reverse process, a denoising network reconstructs informative structure step by step from noisy states [175]. This formulation supports stable modeling of complex and multimodal distributions, as well as generation, reconstruction, and conditional recovery under uncertainty. Several variants are especially relevant to IoT security. Denoising diffusion probabilistic models (DDPMs) provide the

[1] Here, "minority-class evidence" refers to informative samples, patterns, or feature distributions associated with underrepresented classes, such as rare attack categories, that support reliable decision boundary learning [74].

probabilistic foundation [58]; conditional diffusion models incorporate labels, context, or partial observations for task-aware generation and inference [175]; and latent diffusion models improve efficiency by operating in compressed latent spaces [120]. Recent extensions to tabular data, multivariate time series, and incomplete observations are also highly relevant, since IoT intrusion detection often relies on structured traffic features, while industrial anomaly detection depends more on temporal sensor and process data [164].

For IoT applications, the key issue is expressiveness and deployability. Standard diffusion models often require many denoising steps, leading to substantial latency, memory, and energy cost [126]. This makes lightweight diffusion models particularly important in IoT and edge environments. Existing directions include knowledge distillation [168], quantization [151], pruning [41], efficient fine-tuning [62], signal-domain transformation [198], and algorithm-level optimization such as reducing sampling steps and accelerating reverse denoising [126, 133]. Lightweight design is therefore a practical prerequisite for enabling diffusion-based generation, and detection on resource-constrained IoT devices and edge gateways.

Compared with other generative AI models, diffusion models offer a useful balance for IoT security. In detail, relative to VAEs, diffusion models generally provide higher sample fidelity and better distributional coverage, although VAEs are often simpler and more efficient [202]. Relative to GANs, diffusion models are more stable and less prone to mode collapse, which is critical for rare-attack generation and long-tailed security data [61]. Relative to Transformer-based generators, diffusion models are more naturally suited to denoising, reconstruction, and conditional recovery from noisy or incomplete observations [161]. Their main limitation remains computational cost, which further motivates lightweight variants for practical deployment.

2.3. Why Diffusion Models Matter for IoT Security

The importance of diffusion models for IoT security can be understood from a need–capability matching perspective. As discussed above, IoT security is constrained by heterogeneous and imbalanced data, noisy and incomplete observations and strict resource limitations. Diffusion models matter because their generative and reconstruction capabilities align naturally with these challenges.

1) *Improving data quality under heterogeneity, scarcity, and imbalance:* Diffusion models can improve data quality under heterogeneous, scarce, and highly imbalanced conditions [20, 154, 184]. By learning complex minority-class and rare-event distributions, they support attack-data augmentation, synthetic sample generation, and missing-data recovery beyond simple duplication or interpolation. Compared with oversampling or cost-sensitive strategies, they better preserve distributional diversity and reduce overfitting to a few minority instances, thereby offering more realistic support for downstream intrusion learning.

2) *Supporting analysis under noise, uncertainty, and partial observability:* Diffusion models are also well suited to noisy, uncertain, and partially observed IoT data [164, 146]. Their denoising nature allows them to recover meaningful structure from corrupted, missing, or incomplete inputs, which is useful for data enhancement and for direct intrusion detection and anomaly analysis. This is especially important in industrial IoT, where abnormal behavior often appears as subtle deviations in multivariate temporal dynamics rather than as clearly separable attack signatures.

3) *Providing a unified and controllable framework across security tasks:* Beyond individual uses such as augmentation, diffusion models offer a unified generative and reconstruction-based framework that can adapt to multiple IoT security tasks. Through conditional generation, guided sampling, and task-aware reconstruction, they can incorporate labels, context, partial observations, or policy constraints into the modeling process [145]. This controllability can also extend to adjacent security-oriented decision and control problems, such as diffusion-enabled DRL for physical-layer secure communications and cross-layer covert communications [193, 87]. In such cases, diffusion models are used less for direct threat inference than for policy optimization under secrecy, energy, or covert-transmission constraints.

Compared with other generative AI models, diffusion models provide several distinctive advantages that are particularly relevant to IoT security. GANs have been widely adopted for intrusion-data augmentation and synthetic attack generation [36]. However, their adversarial training process is often unstable and susceptible to mode collapse, where only a subset of attack patterns is represented in the generated data. This limitation is problematic in IoT security because many attacks are inherently rare, heterogeneous, and long-tailed. Diffusion models learn data distributions through progressive denoising rather than adversarial competition, resulting in more stable training, improved distributional coverage, and higher diversity of generated samples. Consequently, diffusion models are better suited for constructing realistic attack datasets, augmenting minority classes, and preserving the statistical variability required for robust intrusion detection and anomaly analysis.

Diffusion models also offer important advantages over VAEs and Transformer-based generative models. Although VAEs are computationally efficient and useful for representation learning, their latent-space approximations often produce oversmoothed samples and may fail to capture the complex multimodal characteristics of heterogeneous IoT security data [147, 24]. Transformer-based generators excel at modeling sequential dependencies, but they are primarily designed for autoregressive prediction and are less naturally suited to denoising, reconstruction, imputation, and uncertainty-aware inference under noisy or incomplete observations [39, 11, 40]. In contrast, diffusion models inherently support these functions through their iterative reverse process, enabling them to recover missing information, reconstruct corrupted measurements, and quantify uncertainty while simultaneously generating high-fidelity synthetic data. These capabilities align closely with the fundamental challenges of IoT security, where heterogeneous data sources, imperfect sensing, missing observations, and evolving attack patterns are common.

In summary, the practical value of diffusion models depends heavily on deployability. In IoT environments, diffusion-based methods must satisfy strict latency, memory, and energy constraints [117, 133]. Therefore, lightweight architectures, efficient samplers, distilled models, compressed backbones, and task-adaptive fine-tuning are essential for translating diffusion-based capabilities into usable security functions at the device and edge levels [126]. Overall, diffusion models matter for IoT security not simply because they are strong generative models, but because they provide a unified, controllable, and deployment-aware framework for improving data quality and supporting threat inference.

3. Diffusion models for IoT Security Data Enhancement

High-quality security data, particularly in terms of completeness, reliability, and representativeness, is a fundamental prerequisite for data-driven IoT security, since the effectiveness of downstream tasks such as network intrusion detection, anomalous traffic analysis, and malicious attack identification is inherently constrained by the quality of the data used for training and evaluation [117]. However, due to the heterogeneity of IoT devices and protocols, the rarity and high collection cost of real attack events, and the limited realism of many publicly available testbeds, existing IoT security datasets are often heterogeneous, scarce, severely imbalanced, and insufficiently representative of operational deployment environments [207]. To address the challenges of IoT security data, data augmentation has attracted increasing attention as a practical way to improve downstream security learning performance. Conventional data augmentation methods, including random oversampling and interpolation-based resampling techniques, such as the synthetic minority oversampling technique (SMOTE) [25, 182], have long been used to mitigate data imbalance in security learning. However, their effectiveness remains limited, since they either replicate existing minority instances or synthesize new samples through local interpolation, which may increase the risk of overfitting, amplify noise, and distort class boundaries in complex data distributions [182, 33, 88].

Fig. 3 provides an overview of IoT security data challenges and the corresponding motivating techniques. This section will first introduce the generative data enhancement perspective to explain why diffusion models are well suited to addressing the key challenges of IoT security data, and then reviews their applications in two types of data enhancement for IoT: imbalance-oriented data augmentation and synthetic security data construction.

3.1. Generative Data Enhancement

The rapid development of deep generative models has introduced augmentation paradigms based on models such as VAEs and GANs, which aim to learn the underlying data distribution and generate more realistic minority-class samples for imbalanced learning [81, 4]. Nevertheless, existing studies suggest that the practical gains of such deep generative oversampling methods are often modest relative to their modeling and tuning complexity, while GAN-based methods in particular remain subject to well-known issues such as training instability, mode collapse, and sensitivity

to hyperparameter settings [148, 56, 85]. These limitations are especially restrictive in IoT security, where data are often heterogeneous, mixed-type, noisy, and severely long-tailed, thereby motivating the exploration of more stable and expressive generative mechanisms for security data enhancement [117].

Diffusion models offer a compelling alternative for IoT security data enhancement, potentially overcoming the limitations of traditional methods. By learning the underlying data distribution through a progressive noising-denoising process, diffusion models provide a more stable and expressive generative framework for complex security data than duplication-based, interpolation-based, or adversarial augmentation methods [58]. Specifically, diffusion models offer considerable flexibility in modeling complex distributions, enabling them to capture the heterogeneous, mixed-type, and highly non-linear characteristics commonly observed in IoT security data, where traffic patterns and sensor records are often shaped by device diversity, protocol variation, and deployment-specific context [146]. Diffusion models also offer improved distribution coverage and sample diversity, allowing them to better represent long-tailed attack classes whose samples are not only scarce but also structurally diverse, thereby reducing the bias of downstream models toward dominant benign or frequent attack categories [19]. Moreover, the conditional generation capability of diffusion models enables security samples to be synthesized under specified labels, contexts, or partial observations, which is particularly valuable for IoT security scenarios characterized by incomplete records, limited annotations, and partially observed attack behaviors [146]. The denoising mechanism within diffusion models further provides robustness to noisy and corrupted observations, making them well suited for practical IoT environments in which measurement errors, communication interference, and imperfect data collection are common [58, 80]. Their iterative generation process also acts as a form of implicit regularization, which can alleviate overfitting to a small number of minority samples and improve the generalization of augmentation-assisted security learning [58]. Lastly, the sampling process in diffusion models is inherently controllable, allowing the amount and type of generated data to be adjusted according to downstream learning objectives, class-rebalancing requirements, and available computational resources [146]. These properties suggest that diffusion models can serve as an effective data-enhancement mechanism for addressing heterogeneity, imbalance, noise, and partial observability in IoT security datasets.

3.2. Imbalance-Oriented Data Augmentation for IoT

A major challenge in IoT security is the severe imbalance between abundant benign data and scarce security-critical observations, such as rare attack traffic [12], anomalous device behaviors [38], and emerging malicious events [125]. Such an imbalance can lead downstream detection models to favor dominant classes during training, thereby weakening their sensitivity to minority attacks that are nevertheless of high security importance [12]. Conventional rebalancing methods, including random oversampling and interpolation-based resampling [182, 33], provide only partial relief, since they either replicate limited minority instances or synthesize new samples through local interpolation, which may

amplify noise, distort class boundaries, and offer insufficient support for heterogeneous IoT data distributions [33, 88]. More recent deep generative approaches [81, 4] improve sample synthesis flexibility, but their practical effectiveness remains constrained by issues such as training instability, limited distribution coverage, and reduced robustness under highly mixed-type and long-tailed security data [4]. In this context, diffusion models have been increasingly introduced as a data-level augmentation tool to learn the underlying distributions of minority classes and generate additional samples to rebalance training datasets [4]. The primary role of diffusion here is not to directly produce final intrusion decisions, but to alleviate the distributional bias of the training data. In this regard, diffusion models can improve the robustness and class-balanced performance of downstream IoT security models. Existing studies, such as [141, 154], treat diffusion models as class-rebalancing mechanisms used either before or within the task pipeline, with the common objective of improving the representation and detectability of rare security behaviors in highly skewed data distributions.

1) Sample-Level Rebalancing: A representative line of research uses diffusion models as standalone minority-sample generators before downstream learning, with the goal of enriching underrepresented security classes and reducing the distributional bias of the training data. In industrial cyber-physical system (ICPS) intrusion detection, severe class imbalance is a major challenge. Rare attack categories, such as user to root (U2R) and remote to local (R2L), may account for less than 1% of total network traffic [143]. To address this issue, the authors in [141] proposed an IDS based on the diffusion model (IDD), which is one of the earliest applications of diffusion models to ICPS network intrusion detection. They employ a DDPM to learn the feature distributions of rare attack classes and generate sufficient synthetic samples to construct a balanced training set, upon which a BiLSTM classifier is independently trained. Experiments on the NSL-KDD [143] and UNSW-NB15 [104] datasets demonstrate that IDD significantly outperforms conventional rebalancing baselines including random oversampling, VAE, and GAN, raising rare-class detection accuracy from approximately 30% under the original imbalanced setting to 65%.

Further addressing the challenge of adaptive class-wise sample allocation, the authors in [51] proposed an adaptive ordinary differential equation solver transformer network diffusion model (AOT-DDPM), a network traffic generation model that introduces an adaptive oversampling strategy directly into the reverse diffusion process. Unlike prior methods that generate a fixed number of synthetic samples per minority class, AOT-DDPM dynamically adjusts the number of samples per class by learning both the original data distribution and the per-class imbalance severity, thereby improving the quality and class-level calibration of the generated samples. Experiments on standard intrusion detection benchmarks confirm that this distribution-aware sampling mechanism yields superior detection accuracy compared to uniform diffusion-based augmentation.

While these works validate the feasibility of applying diffusion models in the original feature space, directly operating on high-dimensional IoT traffic features incurs substantial sampling cost and can struggle with heterogeneous

feature scales. To overcome these efficiency limitations, the authors in [139] proposed a latent diffusion-based augmentation framework that introduces an autoencoder to compress raw tabular IoT traffic into a compact latent space before performing the diffusion process. By shifting the generative modeling from the original high-dimensional feature space to a learned low-dimensional representation, this approach reduces sampling time by approximately 25% compared to data-space diffusion while preserving inter-feature dependencies. Comprehensive evaluations across three representative IoT attack types, specifically distributed denial-of-service (DDoS), Mirai, and man-in-the-middle [67], show that the latent diffusion augmentation achieves F1-scores of up to 0.99 for DDoS and Mirai detection, consistently outperforming SMOTE [25], GAN [148], VAE [197], and standard DDPM baselines [58] in both downstream IDS performance and intrinsic generative quality metrics.

2) Pipeline-Level Augmentation: Another line of work tightly couples the diffusion-based augmentation with the detection model within a unified architectural framework, enabling shared feature representations or end-to-end training between the generative and discriminative components. Fig. 4 shows the difference between two types of mechanisms for imbalance-oriented data augmentation with diffusion models. An early IoT-specific effort in pipeline-level augmentation focuses on few-shot intrusion scenarios. The authors in [171] proposed a few-shot intrusion detection model for few-shot attacks in IoT. The framework first transforms traffic features into image representations using gramian angular field (GAF) [160], and then employs an improved DDPM to augment scarce attack samples. The generated samples are subsequently used by an image-based detection network [140], achieving accuracy of up to 99.20% for few-shot detection and an average inference time as low as 23ms in IoT environments. This work demonstrates that diffusion-based augmentation can be effectively coupled with traffic visualization and downstream detection for few-shot IoT intrusion detection.

To further address class imbalance and feature representation limitations in IoT intrusion detection, the authors in [154] proposed an IoT intrusion detection model called DIFT, a unified framework that integrates a diffusion model with a time series Transformer. The diffusion model first learns minority-class feature patterns and generates a balanced dataset, after which the traffic data are locally feature-enhanced using a patching method [109] with shortened sequence length to improve processing efficiency. The Time Series Transformer then extracts both local and global features from the balanced data for multi-class detection. Evaluations on the ToN-IoT [103] and DS2OS [69] datasets demonstrate that this integrated design achieves superior detection performance compared to standalone detection approaches or VAE/GAN augmentation approaches, particularly for underrepresented attack categories. In particular, DIFT improves overall detection accuracy by 1.69% over the approach without data augmentation, by 0.42% over the VAE-based variant and by 0.17% over the GAN-based variant on DS2OS.

Extending this pipeline-level augmentation paradigm toward lightweight IoT deployment, the authors in [149] proposed LDCT-IDS, which couples diffusion-based class rebalancing with a compact hybrid detection architecture. It

employs a classifier-free guidance DDPM with dynamic conditional embedding to synthesize minority attack samples and rebalance the training data for intrusion detection. Compared with SMOTE [25], CGAN [100], and CVAE [132], LDCT-IDS achieves 99.92% and 99.28% accuracy on Edge-IIoTset [43] and CSE-CIC-IDS2018 [21], respectively, while keeping the model size around 72 KB and 69 KB. These results suggest that diffusion-based augmentation can enhance minority-class learning without sacrificing lightweight deployment.

3.3. Synthetic Security Data Construction

Beyond class rebalancing, diffusion models are also valuable for scenarios in which real IoT security data are costly to collect, difficult to annotate, or restricted by operational constraints. In many IoT scenarios, constructing high-quality security datasets is difficult due to limited protocol coverage, insufficient threat coverage, outdated attack scenarios, limited device diversity, and inadequate support for realistic deployment [125, 17]. Moreover, labeled data for IoT anomaly and intrusion analysis are expensive, time-consuming, and in some cases impractical to obtain [83]. Under such conditions, the objective shifts from simply expanding minority classes to constructing synthetic security-relevant data, such as attack traffic, malicious behavior, or other threat-related records. This is particularly important in scenarios where malicious events are rare, device environments are diverse, and the amount of labeled security data is limited [64, 131, 159]. Recent diffusion-based studies [20, 149] on synthetic IoT attack generation further suggest that data construction is emerging as a distinct role of diffusion models, separate from imbalance-oriented augmentation, with increasing attention to sample fidelity, dependency preservation, and utility for downstream detection.

1) Security Data Generation: Directly constructing realistic attack or malware-related samples from limited observations is a prerequisite for training robust IoT security models, particularly when certain threat categories are not merely underrepresented but fundamentally scarce due to the rarity of real-world incidents or the cost of controlled data collection. To address the challenge of determining how much data is actually needed and how to compensate for insufficient samples in IoT malware detection, the authors in [20] proposed a minimum sample size estimation method combined with DDPM-based synthetic traffic generation, as illustrated in Fig. 5 (a). Unlike prior data augmentation studies [141, 51, 139, 154, 19, 184] that assume a pre-existing dataset of moderate size, this work explicitly targets the data scarcity problem by first establishing a statistically grounded lower bound on the required sample count, and then employing a DDPM to generate synthetic traffic images that fill the gap between the available and required data volumes. Comparative experiments demonstrate that the samples generated by DDPM exhibit superior stability and predictability, achieving a 7% higher F1 score and 5% less variance over Deep Convolutional GAN (DCGAN) [52], confirming the suitability of the diffusion model for malware data synthesis under stringent sample-size constraints.

In addition, although several recent studies [64, 131, 159] focus on diffusion-based general network traffic synthesis, they provide transferable methodological foundations for IoT security data construction. NetDiffusion proposed in

[64] applies a protocol-constrained Stable Diffusion model to generate packet-level synthetic traces, achieving higher statistical fidelity and downstream performance than GAN-based alternatives while ensuring protocol compliance. It offers a practical basis for constructing protocol-compliant synthetic traffic that can support IoT security testing and IDS training. NetDiffus proposed in [131] converts one-dimensional time-series traffic into gramian angular summation field (GASF) images before applying a diffusion model, which provides a valuable way to preserve temporal correlations when constructing synthetic IoT security flows. DATG proposed in [159] highlights its utility for supplying diverse samples to IDSs. The authors further enhance long-range temporal modeling by integrating a self-attention mechanism into the DDPM denoising network. These packet- and flow-level synthesis techniques offer a readily adaptable foundation for constructing protocol-compliant and temporally faithful IoT security datasets.

2) Task-Coupled Synthetic Data Construction: While diffusion models have shown strong capability in constructing synthetic security data, standalone generation alone is often insufficient for practical IoT security applications. Samples optimized only for fidelity or diversity do not necessarily yield the greatest benefit for downstream tasks, especially when security data are heterogeneous, decision boundaries are subtle, and deployment settings impose constraints on efficiency and robustness. This issue has motivated the studies [78, 30, 206] that embed diffusion-based data construction directly into end-to-end security pipelines, where diffusion model-based sample synthesis is jointly aligned with downstream classification, anomaly detection, or collaborative intrusion learning.

To address the scarcity of stealthy false data injection attack (FDIA) samples in smart grid IoT, the authors in [78] proposed an adversarial attention-diffusion model for attack sample generation, as illustrated in Fig. 5 (b). The model injects attack vectors during the diffusion process while incorporating attention over grid topology and measurement nodes. This design enables the model to generate more realistic and stealthy FDIA samples than conventional generative baselines. These synthetic attacks can support the training and evaluation of FDIA detectors under limited real attack data, demonstrating the value of diffusion models for constructing domain-specific cyber-physical attack scenarios.

Several general network-security and malware-generation studies further provide transferable mechanisms for IoT security data construction, but direct IoT validation remains limited. To address the difficulty of detecting anomaly traffic under scarce and noisy security data, the authors in [30] proposed an anomaly traffic detection framework based on a denoising diffusion implicit model (DDIM). Instead of using diffusion as a standalone generator, the framework embeds DDIM-based synthetic sample construction into the overall detection pipeline, where anomaly traffic is first transformed into a unified image representation, then augmented through iterative denoising, and finally fed into a downstream classifier for anomaly recognition. Experiments on NSL-KDD show that the proposed framework achieves 95.56% accuracy and improves the anomaly traffic identification rate by 32.16%, demonstrating the effectiveness of embedding diffusion-based sample construction into end-to-end anomaly detection.

Table 2
Diffusion Models for IoT Security Data Enhancement

Category	Ref	Diffusion-based solution	Core idea	Pros	Cons
Imbalance-Oriented Data Augmentation	[141]	DDPM	DDPM is used to learn rare attack class distributions and generate synthetic minority samples for BiLSTM-based intrusion detection in ICPS.	✔ Improves rare-class detection ✔ Simple pre-training pipeline	✘ Fixed sample allocation per class ✘ High cost in original feature space ✘ Offline augmentation only
	[51]	AoT-DDPM	Transformer-based DDPM is used to generate balanced abnormal traffic samples with adaptive reverse sampling and ODE-accelerated generation.	✔ Adaptive class-wise sampling ✔ Better traffic distribution learning with Transformer network ✔ Fewer generation steps with ODE Solver	✘ Increased training complexity ✘ Sensitive to imbalance ratio estimation ✘ Offline augmentation only
	[139]	Latent diffusion model	An autoencoder is used to compress tabular IoT traffic into latent space and then diffusion model augments minority classes in the compressed representation.	✔ Lower sampling cost ✔ Preserves inter-feature dependencies	✘ Requires autoencoder pre-training ✘ Latent quality sensitive ✘ Offline augmentation only
	[171]	GDE	Traffic features are transformed into images via GAF, and an improved DDPM augments few-shot attack samples for image-based intrusion detection.	✔ Few-shot attack augmentation ✔ IoT-specific intrusion setting ✔ Integrates visualization and detection	✘ Few-shot distribution bias ✘ Image-transformation cost ✘ Multi-module pipeline complexity
	[154]	Diffusion-Transformer	Diffusion model is used to generate balanced minority-class data, and a Time Series Transformer jointly extracts local and global features for multi-class detection.	✔ End-to-end unified pipeline ✔ Enhanced feature representation	✘ Extra training complexity ✘ Transformer overhead
	[149]	Classifier-free guidance DDPM	Classifier-free guidance DDPM is used to synthesize minority attack samples via dynamic conditional embedding for a lightweight CNN-Transformer IDS.	✔ Lightweight framework ✔ Dynamic conditional control	✘ Guidance tuning complexity ✘ Static offline augmentation only
Synthetic Security Data Construction	[20]	DDPM	DDPM is used to generate synthetic malware traffic images to fill the gap between available and statistically required minimum sample counts.	✔ Sample-size aware generation ✔ Data-efficient augmentation ✔ Explainable fidelity validation	✘ Relies on sample size estimation ✘ Image-based representation ✘ Task-specific validation
	[78]	Adversarial attention-diffusion model	Diffusion is used to generate stealthy FDIA samples by injecting adversarial vectors and modeling grid topology with attention.	✔ Topology-aware attack synthesis ✔ Stealthy FDIA generation ✔ Attention-guided perturbation	✘ Perturbation injection sensitive ✘ Physical-model dependent ✘ Domain-specific validation

Further considering the heterogeneity of the traffic data, the authors in [206] proposed a novel method that integrates the Gaussian and multinomial denoising diffusion probabilistic model (GMDDPM) for data balancing with a convolutional neural network (CNN)-Transformer for classification, namely GMDDPM-CT. Unlike standard DDPM, which assumes a single Gaussian prior, GMDDPM incorporates a Gaussian mixture structure into the reverse diffusion process to better capture the multimodal nature of heterogeneous attack traffic distributions, where different attack types may occupy distinct regions of the feature space. This mixture-guided formulation enables the model to generate more structurally diverse synthetic samples that preserve inter-class separability, particularly for attack categories with limited available observations. Experimental evaluations on standard intrusion detection benchmarks demonstrate that GMDDPM produces synthetic samples with improved distributional fidelity and downstream classification utility compared to both conventional DDPM and GAN-based alternatives.

In addition, a related malware-security study in [16] showed that diffusion-based synthetic malware generation can outperform GAN-based and Wasserstein GANs with gradient penalty (WGAN-GP)-based approaches in downstream zero-day malware classification, achieving 8% improvement on malware classification performance. This result suggests that diffusion model-based security data construction may be especially valuable in IoT scenarios where real malicious samples are scarce or difficult to collect at scale.

3.4. Lessons Learned

As summarized in Table 2, the studies in this section demonstrate that diffusion models can serve as an effective data-layer enabler for IoT security, addressing both distributional skewness through sample-level [141, 51, 139] and pipeline-level [154, 19, 184, 149] rebalancing, and data scarcity through targeted synthetic construction [20, 64, 131,

159] and task-coupled generation [30, 206, 16]. By producing high-fidelity, structurally diverse, and class-balanced training samples, diffusion models help to improve the performance of downstream detection tasks, especially for rare-class detection accuracy.

Despite these advances, two common limitations constrain the practical impact of diffusion-based data enhancement for IoT security. Firstly, as generative fidelity increases, diffusion models face a risk of hallucination [157, 119], producing samples that are statistically plausible yet semantically invalid. This may introduce misleading decision boundaries into downstream models. Secondly, the iterative sampling process inherent to diffusion models imposes non-trivial computational overhead, and most existing methods have been validated only in offline settings without assessing whether they can meet the real-time latency, memory, and energy constraints of operational IoT edge devices. Therefore, future work should incorporate protocol-aware and semantics-constrained generation mechanisms to safeguard sample validity, and design edge-native diffusion architectures that bridge the gap between offline research and operational IoT deployment.

4. Diffusion Models for IoT Threat Analysis

The massive deployment of the IoT has significantly expanded system attack surfaces due to device heterogeneity, resource constraints, and diverse communication protocols. Moreover, modern attacks have evolved from traditional unauthorized access into dynamic, distributed intrusions, stealthy propagation, and protocol abuses. Consequently, IoT environments face highly complex and stealthy security threats [124]. Effective threat analysis in such environments requires models capable of learning the latent distribution of normal operational patterns and identifying subtle deviations indicative of malicious activity.

Conventional threat analysis approaches remain limited in security scenarios for modern IoT devices. Rule-based and signature-matching methods [105] are effective for known attacks but cannot detect zero-day or polymorphic threats. Classical machine learning models, such as support vector machines (SVMs) [173] and random forests [90], depend heavily on handcrafted features and struggle to model the high-dimensional nonlinear dependencies of heterogeneous IoT traffic. Deep discriminative models, including CNNs [29] and recurrent neural networks (RNNs) [111], improve feature learning but still require substantial labeled attack data, which are scarce in real IoT environments. Autoencoder-based methods [60] reduce the reliance on labels by reconstructing normal traffic, yet their reconstructions are often overly smooth and provide limited uncertainty quantification for subtle anomalies. These limitations motivate the exploration of more flexible and expressive methods that can model complex IoT traffic patterns, reconstruct inputs more precisely, and identify rare or unseen threats.

Building on this motivation, the following sections explore how generative models, particularly diffusion models, have been applied to the two core tasks of IoT threat analysis: intrusion detection from IoT network traffic and anomaly detection from IIoT multivariate sensor time series.

4.1. Generative Inference Improvement

Beyond data enhancement, generative models have also been widely exploited to directly improve inference in IoT security tasks such as intrusion detection and anomaly detection, based on models such as autoencoders [2, 10], VAEs [76, 194], and GANs [113, 44]. The aim is to learn the distribution of normal IoT behaviors and identify threats through reconstruction errors, likelihood deviations, or discriminator-based scoring. Early work such as [2] used denoising autoencoders to learn noise-robust traffic representations for intrusion detection under imperfect data collection. T-VAE proposed in [76] further improved distributional modeling flexibility through a transformer-based VAE. Complementing these reconstruction-based methods, a GAN-based framework was introduced in [44] which combines adversarial training with robust feature learning to detect intrusions and resist evasion attacks in dynamic IoT networks. Nevertheless, these methods often suffer from lossy compression, restrictive latent priors, and adversarial training instability that make them less suitable for heterogeneous IoT environments with long-tailed attack patterns, noisy observations, and evolving threat behaviors.

In this context, diffusion models offer a novel technical solution for IoT threat analysis. Diffusion models are valuable for data augmentation and for direct security inference, owing to their strong capabilities in feature extraction, probabilistic modeling, and conditional generation. The denoising process serves as a feature extractor that captures the multi-scale and entangled behavioral patterns of heterogeneous IoT data, which are difficult for conventional encoders to capture [58, 28]. The probabilistic modeling capability of diffusion models can effectively characterize the distribution of normal IoT behaviors in a tractable and expressive manner, thereby overcoming the lack of reliable confidence measures in deterministic detectors [150]. The conditional generation capability of diffusion models can incorporate auxiliary context such as partial observations, neighboring sensor readings, or class labels into threat inference, thereby supporting context-aware anomaly reasoning in incomplete and heterogeneous IoT environments [28, 154].

4.2. Intrusion Detection from IoT Network Traffic

IoT network intrusion detection aims to identify malicious behaviors from packet-level or flow-level traffic across heterogeneous terminals, edge nodes, and cloud services [23]. However, the diversity of IoT devices and protocols, the scarcity of labeled attacks, and the severe class imbalance of real traffic often cause conventional discriminative models [117] to learn biased and poorly transferable decision boundaries [101, 68]. Diffusion models address these limitations by learning the structure of network traffic through iterative denoising. Rather than merely augmenting

minority attack classes, diffusion models can support intrusion inference by reconstructing normal traffic [184, 77], measuring distributional deviations [46, 192, 158], and filtering noisy or adversarial perturbations [98]. This makes diffusion models particularly useful for detecting imbalanced, evolving, and previously unseen IoT attacks, where the key challenge is classification accuracy and robust modeling of normal and malicious traffic distributions.

1) Diffusion-Based Feature Extraction: One line of work uses diffusion models to enhance traffic representations for downstream intrusion classification. Instead of relying solely on discriminative feature learning, these methods exploit the structural priors learned during diffusion training to obtain more robust and compact flow representations. For example, Diff-IDS proposed in [184], converts network-flow features into image-like representations and uses a diffusion backbone with feature masking to extract discriminative traffic patterns for lightweight intrusion detection. This work demonstrates that the inductive bias acquired during denoising transfers directly to classification without retraining. Building on this lightweight feature-extraction paradigm, DMLITE [77] extended diffusion-based traffic representation learning to encrypted IoT environments, where raw payload statistics are no longer accessible. It combines a self-supervised diffusion model with contrastive multi-level feature fusion over visualized encrypted flows, and further introduces LLM-guided particle swarm optimization for adaptive feature selection. DMLITE achieves classification accuracies of 99.83% on the IoT benchmark Edge-IIoTset [43], on average improving accuracy by 3.7% over representative deep learning baselines and reducing training time by 41.9%. These results demonstrate the effectiveness of diffusion-driven feature representation in the encrypted-traffic regime.

2) Reconstruction-based Anomaly Scoring: Rather than extracting features for a labeled classifier, a complementary paradigm exploits the probabilistic reverse diffusion chain to derive anomaly scores directly. It measures the discrepancy between an input flow and its reconstructed normal counterpart, thereby enabling label-free detection of threats that are entirely absent from training. The theoretical foundation was established at the graph level by Gavrilev and Burnaev [46]. They showed that score-based generative models can support anomaly detection by reconstructing normal graph structure and measuring the discrepancy between original and reconstructed ego-graphs. This result provides an early foundation for adapting score-based inference to anomaly detection beyond conventional reconstruction-error-based methods. TabADM proposed in [192] then further extends this principle to tabular cybersecurity data, which shows that diffusion model can support stable unsupervised anomaly scoring for tabular data, thereby paving the way for flow-level IoT intrusion detection studies.

To detect intrusions without relying on labeled attack data, the authors in [158] proposed a DDPM-based unsupervised intrusion detection method for Unmanned Aerial Vehicle (UAV) networks, where the model is trained only on normal traffic flows and abnormality is identified through the discrepancy between the input flow and its denoised reconstruction. Evaluations show that the DDPM-based method performs uniformly better than methods based on seq2seq [138], VAE [70], and principal component analysis (PCA) [1], with higher accuracy, precision,

recall, F1-score, and area under the curve (AUC), demonstrating the feasibility of diffusion-based anomaly scoring for network intrusion detection. To address the practical challenge of detecting zero-day attacks and adversarially perturbed flows that remain close to normal traffic in observed feature space, the authors in [195] proposed NI-Diff, which pairs a VAE encoder with a latent diffusion model to reconstruct the latent distribution of each network flow under the learned normal prior. In this way, zero-day and adversarial flows can be detected through the divergence between the classifier output of the original flow and that of its diffusion-reconstructed counterpart. Experiments show that NI-Diff detects 97% of adversarial flows and 92% of zero-day threats while keeping the false positive rate below 2%, demonstrating that diffusion-based discrepancy scoring can support unified open-world intrusion detection beyond conventional closed-set classifiers.

Diffusion models are also being explored to improve the robustness and scalability of IoT intrusion detection under distributed and heterogeneous deployment settings. In practical IoT environments, traffic distributions often vary significantly across devices and network segments. To address these challenges, the authors in [95] proposed a federated intrusion detection framework that integrates distributed storage with diffusion-based modeling. By leveraging diffusion models to capture complex traffic distributions across decentralized IoT nodes, the framework enhances detection robustness while avoiding raw data sharing. Experimental results demonstrate that this collaborative diffusion-enabled approach improves detection performance against a range of IoT attacks, including reconnaissance, DoS, and DDoS, while strengthening deployment scalability.

4.3. Anomaly Detection from IIoT and Multivariate Sensor Time Series

In industrial IoT and sensor-rich environments, security incidents often manifest as anomalous patterns in multivariate time series rather than as conventional packet-level attacks. Unlike network flow features, IIoT sensor streams exhibit strong cross-variable coupling, non-stationary temporal dynamics, and extreme label scarcity, making the core challenge one of accurately characterizing the normal operational manifold from high-dimensional heterogeneous observations [110, 187]. Conventional approaches based on autoencoders, long short-term memories (LSTMs), and VAEs address this by learning normal distributions and flagging deviations via reconstruction errors or likelihood deviations [27, 114, 31], but their fixed distributional assumptions render them brittle under operating condition shifts, data drift, and cascading fault propagation common in real industrial deployments. The richer generative prior and flexible conditioning mechanisms of diffusion models offer potential for modeling such complex normal manifolds, motivating their adoption for IIoT anomaly detection.

1) Imputation-based Anomaly Scoring: A major line of work formulates anomaly detection as conditional imputation, where masked or corrupted segments are reconstructed from the surrounding context, and the imputation residual is used as the anomaly score. When anomalies concentrate in contiguous episodes, conventional reconstruction

methods become biased toward reproducing abnormal patterns, undermining detection reliability. To address this, DiffAD proposed in [165] selects high-density normal observations as conditioning context, and designs a conditional weight-incremental diffusion model to improve imputation fidelity over anomalous regions. ImDiffusion proposed in [28] further exploits the multi-step reverse diffusion process by aggregating intermediate denoising outputs for anomaly scoring. This mechanism converts the inherent stochasticity of diffusion into a robustness advantage, yielding an 11.4% F1 improvement in Microsoft's production monitoring system and strong performance on the industrial control dataset SWaT.

However, both methods rely on relatively simple conditioning signals and thus struggle to capture the complex contextual dependencies and diversified temporal patterns inherent in IIoT sensor streams. MAFCD proposed in [164] uses adaptive multi-view feature fusion to guide conditional diffusion with internal, external, and auxiliary temporal features, improving generalization across heterogeneous IIoT datasets. TSAD-C proposed in [59] extends this paradigm to contaminated training data by introducing a decontamination module before spatio-temporal graph conditional diffusion, thereby addressing the practical assumption that training data may contain unlabeled anomalies.

2) Prior-guided Reconstruction-based Scoring: Rather than relying on masking strategies, another line of work guides the reconstruction process with external structural knowledge, specifically physical signal priors or sensor topology, to sharpen the boundary between normal and anomalous behavior. PhysDiff proposed in [79] addresses the high false-positive rates caused by complex non-stationary dynamics in industrial sensor streams by introducing physics-guided signal decomposition before diffusion-based reconstruction. A Multi-channel Adaptive Fourier Decomposition isolates high-frequency oscillations and low-frequency trends as physically interpretable conditioning signals. By weighting reconstruction errors across frequency bands, PhysDiff enhances both anomaly localization and interpretability, outperforming state-of-the-art baselines on five benchmarks including the IIoT dataset SWaT. Similarly, Physics-Informed Diffusion proposed in [136] embeds physical constraints directly into the diffusion training objective through a weighted physics-informed loss, improving the model's ability to approximate the underlying physics-dependent temporal distribution of multivariate sensor data and demonstrating consistent F1 improvements on both synthetic and real-world IIoT datasets.

Beyond physical priors, graph-structured diffusion methods incorporate sensor topology or learned inter-variable relations. For example, the Diffusion Graph Model proposed in [73] focuses on the heterophily problem in multi-sensor systems, where connections between normal and anomalous data points may lead graph-based diffusion models to learn abnormal patterns. To mitigate this issue, it constructs a spatio-temporal joint graph and introduces anomaly-aware graph sparsification to reduce misleading normal-anomalous links. Contrastive augmentation is further used to enhance anomaly-free representations, leading to improved detection performance on SWaT.

Table 3
Diffusion Models for IoT Threat Analysis

Category	Ref	Diffusion-based solution	Core idea	Pros	Cons
Intrusion Detection from IoT Network Traffic	[184]	Diff-IDS	Diffusion backbone with feature masking is used to extract discriminative patterns from image-like network-flow representations for lightweight intrusion detection.	✔ Lightweight detection ✔ Denoising-enhanced features ✔ Compact model size	✘ Traffic visualization dependent ✘ Limited IoT dataset validation
	[77]	DMLITE	Self-supervised diffusion model is used to learn multi-level representations from visualized encrypted IoT traffic, with LLM-guided feature selection.	✔ Encrypted traffic support ✔ Multi-level feature fusion ✔ Adaptive feature selection	✘ Visualization preprocessing required ✘ LLM-assisted complexity ✘ Feature selection overhead
	[158]	DDPM	DDPM is trained on normal UAV traffic and uses denoised reconstruction discrepancy to identify abnormal network flows without attack labels.	✔ Label-free detection ✔ Normal-prior modeling	✘ Normal-data dependent ✘ Threshold sensitivity
	[195]	NI-Diff	VAE encoder and latent diffusion reconstruct each flow under a normal prior, and original-reconstruction prediction divergence detects zero-day and adversarial attacks.	✔ Zero-day detection ✔ Adversarial-flow detection ✔ Latent-space reconstruction	✘ VAE quality dependent ✘ Classifier discrepancy required
Anomaly Detection from IIoT and Multivariate Sensor Time Series	[164]	MAFCD	Multi-view adaptive conditional diffusion fuses internal, external, and auxiliary temporal features to guide anomaly reconstruction.	✔ Multi-view conditioning ✔ Adaptive feature fusion ✔ Heterogeneous dataset support	✘ Complex conditioning design ✘ Higher training complexity
	[79]	PhysDiff	Physics-guided signal decomposition conditions diffusion reconstruction with frequency-aware physical priors for anomaly scoring.	✔ Physics-guided reconstruction ✔ Frequency-aware scoring ✔ Better interpretability	✘ Physical-prior dependent ✘ Decomposition design sensitive
	[136]	Physics-informed diffusion	Physical constraints are embedded into the diffusion objective through a weighted physics-informed loss for unsupervised anomaly detection.	✔ Constraint-aware learning ✔ Physics-consistent modeling ✔ Improved normal manifold	✘ Requires physics knowledge ✘ Loss-weight tuning needed ✘ Model-specific constraints
	[73]	Diffusion graph model	Spatio-temporal graph diffusion uses anomaly-aware graph sparsification and contrastive augmentation to reduce misleading normal-anomalous links.	✔ Topology-aware modeling ✔ Heterophily mitigation ✔ Anomaly-free representations	✘ Graph quality dependent ✘ Sparsification sensitivity ✘ Contrastive design overhead

Fig. 6 compares all the four types of representative works about diffusion-based IoT threat analysis, where diffusion models play different roles to enhance security inference.

4.4. Lessons Learned

As summarized in Table 3, the studies in this section demonstrate that diffusion models can serve as an effective inference-layer enabler for IoT threat analysis, supporting security decisions for intrusion detection from IoT network traffic and anomaly detection from IIoT and multivariate sensor time series. Compared with conventional models [29, 111, 2, 194], diffusion models offer a richer generative prior, more stable training, and flexible conditioning that together enable more expressive normal behavior modeling and more reliable anomaly inference across heterogeneous IoT environments.

Yet several limitations remain that constrain the practical impact of diffusion-based threat analysis. Firstly, most existing methods are developed under fixed scene assumptions, either for specific traffic modalities and deployment settings [184, 77, 158] or for sensor systems with known physical priors [79, 136], and therefore often suffer noticeable performance degradation when deployment conditions shift. Secondly, the anomaly scoring mechanisms adopted by reconstruction- and discrepancy-based detectors usually rely on static thresholds [158, 195, 165, 164, 79], which cannot adapt to the gradual drift of normal IoT behavior and thus tend to increase false alarm rates under evolving traffic patterns or changing industrial operating conditions. Future work should therefore pursue scene-adaptive diffusion priors that generalize across dynamic IoT environments, and develop self-calibrating anomaly scoring mechanisms that track normal behavior evolution without manual recalibration.

5. Applications of Diffusion Models in Different IoT Scenarios

As illustrated in Fig. 7, diffusion models have been applied across diverse IoT scenarios, including industrial cyber-physical systems (CPSs), UAVs and satellite-terrestrial networks, smart grids, healthcare IoT, and vehicular networks. These applications can be broadly organized into two types: data-oriented applications for data augmentation, and inference-oriented applications for supporting security inferences.

5.1. Data-Oriented Applications

Generative diffusion models have been widely adopted as data-layer enablers across diverse IoT security domains, addressing domain-specific scarcity and imbalance challenges. Besides the solutions for general IoT intrusion detection discussed earlier, such as DIFT [154], latent diffusion-based IoT attack generation [139], and LDCT-IDS [149], diffusion models have also been increasingly applied to a broader range of domain-specific IoT scenarios, where data scarcity, rarity, and realism pose great challenges.

In industrial CPS, the authors in [141] employed a DDPM to learn rare attack class distributions and generate balanced training data, raising rare-class detection accuracy from approximately 30% to 65%. For IIoT physical equipment, fault events are inherently rare and exhibit large intra-class variability. FaultDiffusion proposed in [169] pre-trains a DDPM on abundant normal data and fine-tunes it via a positive-negative difference adapter to capture the normal-fault domain discrepancy. GI-DDPM, proposed in [172], further incorporates a Vision Transformer as a global information guide to align ViT-extracted features with diffusion model features, achieving fault diagnosis accuracy above 96% across varying data imbalance ratios for industrial rotating machinery.

In UAV networks and satellite-terrestrial integrated networks (STINs), the physical and operational constraints on data collection result in critically insufficient and unrepresentative labeled datasets. To address these challenges, the authors in [20] established a statistically grounded lower bound on required sample counts and then employed a DDPM to synthesize traffic images. STINIDF proposed in [57] collaboratively trains a conditional diffusion model across distributed STIN nodes via federated learning, generating globally representative synthetic traffic without requiring raw data sharing.

In addition, diffusion models have also been applied to smart grid IoT for augmenting scarce and hard-to-identify labeled false data injection attack (FDIA) samples. The authors in [78] proposed an adversarial attention-diffusion framework that injects attack vectors during the forward diffusion process while attending to grid topology and measurement nodes. This approach can generate evasion-capable FDIA samples validated on IEEE 14, 39, and 118 bus systems.

5.2. Inference-Oriented Applications

Beyond data enhancement, diffusion models have also been explored as inference-layer enablers for direct threat detection across diverse IoT scenarios. In addition to applications in industrial sensor systems as reviewed in Section 4 [165, 164, 79, 59, 136, 73], diffusion models have been increasingly applied to threat inference in other scenarios, such as UAV networks, STINs, healthcare IoT and infrastructure systems.

In space-air-ground integrated IoT systems, including UAV networks and satellite-enabled sensing platforms, security inference is particularly challenging due to highly dynamic operating environments, limited labeled attack data, and complex spatiotemporal dependencies. In UAV networks, dynamic complex topology and traffic label scarcity hinder conventional discriminative models from learning reliable decision boundaries. Beyond the previously mentioned DDPM-based unsupervised intrusion detection method [158], the authors in [50] also exploited the natural alignment between diffusion noise prediction and anomalous deviation detection to identify abnormal UAV sensor states without requiring labeled anomalies. In addition to detection, the authors in [193] leveraged diffusion model-enabled deep reinforcement learning to optimize multi-objective aerial collaborative beamforming against eavesdropping threats. This method demonstrates that diffusion models can also serve as policy generators for physical-layer security in UAV networks. To handle the high frame rates, large spatial scales, and the absence of labeled instances for satellite video anomaly detection, the authors in [15] proposed an unsupervised diffusion-based framework that learns normal scene distributions through denoising and detects deviations without motion modeling.

Diffusion-based security inference has also been increasingly applied in urban and human-centric IoT domains, including smart cities, healthcare IoT, and intelligent transportation systems. In smart city infrastructures, diffusion models have shown strong potential for safeguarding critical urban utilities and public environments. For example, an unsupervised diffusion-guided LSTM is proposed in [121] for anomaly detection in water distribution networks. It learns normal hydraulic and sensor behaviors from multivariate time-series data and identifies abnormal operational states without requiring labeled anomalies. Similarly, diffusion-based latent pattern learning has been applied to urban surveillance and satellite video analysis [196], enabling the detection of anomalous events in large-scale city monitoring and remote sensing scenarios. In healthcare IoT, secure data management imposes additional constraints on inference pipelines. The authors in [137] propose a retrieval-augmented generation (RAG)-empowered multi-modal LLM framework for secure internet of medical things (IoMT) data management, where a diffusion-based contract approach governs data access and incentive design, enabling security-aware inference over sensitive medical sensor streams while preserving task utility. In vehicular networks, the diversity of in-vehicle protocols and evolving attack patterns pose persistent challenges for intrusion detection. Recent works [14, 94] confirm that diffusion models are emerging as a promising direction for IoV IDS.

6. Open Challenges and Future Directions

6.1. Evaluation Beyond Accuracy

Future studies should move beyond accuracy-centric reporting and adopt evaluation criteria aligned with the specific role of diffusion models. For diffusion-based data generation, evaluation should consider sample fidelity, diversity, and downstream utility, namely whether synthetic data preserve security-relevant structures and improve learning under data scarcity and class imbalance [116, 144, 35, 5, 49, 191, 115]. More specifically, for direct security analysis, robustness, generalization, and low-latency decision quality are equally important [86, 117]. A model that performs well on static benchmarks may still fail in noisy, partially observed, or evolving IoT environments. Evaluation should therefore examine resilience to corrupted inputs, sensitivity to rare attacks, uncertainty calibration, and stability under distribution shift, while also accounting for response time, computational cost, data freshness, and security-aware sensing quality [180, 186].

6.2. Efficiency and Edge Deployment

Despite the significant potential of diffusion models, they still impose substantial computational overhead, especially during iterative sampling. This is a major obstacle in IoT and edge environments, where security functions often run on low-power devices, gateways, or resource-limited edge servers [117, 204, 63]. In such settings, the multi-step denoising process can hinder real-time detection and continuous monitoring. To address this concern, more work is needed on lightweight diffusion architectures, latent-space diffusion, model compression, and efficient inference. Important directions include reducing sampling steps without severely degrading performance, designing compact models suited to IoT data modalities, and applying pruning, quantization, distillation, consistency-model learning, caching, and hardware-aware optimization to improve deployability [204, 22, 205, 122, 134, 92, 93]. Besides, a further promising direction is collaborative edge–cloud design. Lightweight models at the edge may handle time-critical screening, while heavier diffusion procedures are offloaded for deeper analysis [170, 63]. Future research should thus treat energy consumption, memory footprint, communication cost, and end-to-end latency as key design objectives alongside predictive performance, especially in sensing–communication–computation integrated and privacy-sensitive mobile edge systems [178, 189].

6.3. Generalization, Drift, and Cross-Domain Transfer

IoT environments are highly dynamic, with both device populations and threat patterns evolving over time. Therefore, a central challenge is whether diffusion-based security methods can generalize across datasets, protocols, sensing modalities, and deployment domains. Many current studies still rely on closed-world evaluation, whereas real deployments face domain shift caused by behavioral change, sensing variation, firmware updates, and adaptive

attackers [128, 117, 163, 179]. Addressing concept drift and improving cross-domain transferability will be essential for practical adoption. For diffusion-based generators, this requires learning distributions that remain useful beyond narrow benchmarks [82, 144]. For detection or prediction tasks, it requires maintaining reliable decisions as normal behavior evolves and new attacks emerge. Continual learning, online adaptation, domain adaptation, and transfer learning are therefore important future directions [199, 66, 128, 45, 91, 112, 130]. This challenge is further amplified by the heterogeneity of IoT data, since security information is expressed differently across traffic traces, sensor streams, industrial telemetry, and wireless measurements. Future work should develop diffusion frameworks that capture invariant cross-domain structure while preserving domain-specific semantics, potentially through integration with representation learning, graph modeling, or temporal adaptation.

6.4. Diffusion Models and Blockchain-Assisted Trust

Another emerging direction is the integration of diffusion models with blockchain for IoT security. Blockchain can provide decentralization, auditability, and trusted coordination, while diffusion models contribute data generation, and augmentation capabilities [47, 123, 32, 108, 129]. Recent studies suggest that such a combination is promising in several scenarios. Nguyen *et al.* showed that generative-AI-enabled blockchain networks can benefit from diffusion-based optimization and support security-related services [107]. Wen *et al.* further incorporated blockchain and generative diffusion into a Generative IoT framework, where blockchain supports trusted management and diffusion models improve incentive design [161]. More directly, Manzano *et al.* combined Ethereum-based distributed storage, federated learning, and diffusion-based data augmentation for IoT intrusion detection, improving robustness under imbalanced data [95]. This direction opens a useful path toward trustworthy synthetic-data sharing, accountable collaborative training, and privacy-preserving incentive or access-control mechanisms in multi-stakeholder IoT systems [156, 200, 190]. Future work should further study lightweight blockchain–diffusion co-design, on-chain/off-chain task partitioning, and verifiable generation under resource-constrained edge settings.

7. Conclusion

This survey reviewed the emerging use of diffusion models in IoT security. Specifically, we categorized the integration of diffusion models into IoT security into two directions: diffusion for security data enhancement, and diffusion for direct threat analysis. This taxonomy highlights that diffusion models are valuable for synthetic data generation as well as for improving threat inference in heterogeneous, scarce, and noisy IoT environments. We further summarized data-oriented and inference-oriented applications across industrial IoT, UAV networks, satellite-terrestrial integrated networks, smart grids, healthcare IoT, vehicular networks, and other cyber-physical systems. Although the current body of work remains limited and fragmented, existing studies suggest that diffusion models offer a promising

unified framework for addressing several core IoT security challenges. In this regard, practical adoption still depends on overcoming important issues such as evaluation standardization, computational efficiency, edge deployment, robustness to drift, and domain shift. Therefore, future research should move toward lightweight, trustworthy, and system-aware diffusion frameworks that jointly consider security effectiveness and deployment constraints. We believe this survey can help clarify the research landscape and support further advances at the intersection of diffusion modeling and IoT security.

References

[1] Abdi, H., Williams, L.J., 2010. Principal component analysis. Wiley interdisciplinary reviews: computational statistics 2, 433–459.

[2] Abusitta, A., De Carvalho, G.H., Wahab, O.A., Halabi, T., Fung, B.C., Mamoori, S.A., 2023. Deep learning-enabled anomaly detection for IoT systems. Internet of Things 21, 100656. doi:10.1016/j.iot.2022.100656.

[3] Adhikari, D., Jiang, W., Zhan, J., Rawat, D.B., Bhattarai, A., 2024. Recent advances in anomaly detection in internet of things: Status, challenges, and perspectives. Computer Science Review 54, 100665. doi:10.1016/j.cosrev.2024.100665.

[4] Al-Ajlan, M., Ykhlef, M., 2024. A review of generative adversarial networks for intrusion detection systems: Advances, challenges, and future directions. Computers, Materials & Continua 81, 2053–2076. doi:10.32604/cmc.2024.055891.

[5] Alaa, A.M., van Breugel, B., Saveliev, E., van der Schaar, M., 2022. How faithful is your synthetic data? sample-level metrics for evaluating and auditing generative models, in: Proceedings of the 39th International Conference on Machine Learning, PMLR. URL: https://proceedings.mlr.press/v162/alaa22a.html.

[6] Alotaibi, B., 2023. A survey on industrial internet of things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. Sensors 23, 7470. doi:10.3390/s23177470.

[7] Alrawi, O., Lever, C., Antonakakis, M., Monrose, F., 2019. SoK: Security evaluation of home-based IoT deployments, in: 2019 IEEE Symposium on Security and Privacy, pp. 1362–1380. doi:10.1109/SP.2019.00013.

[8] Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A.N., Anwar, A.N., 2020. TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. IEEE Access 8, 165130–165150. doi:10.1109/ACCESS.2020.3022862.

[9] Alsheikh, M.A., Jiao, Y., Niyato, D., Wang, P., Leong, D., Han, Z., 2017. The accuracy-privacy trade-off of mobile crowdsensing. IEEE Communications Magazine 55, 132–139. doi:10.1109/MCOM.2017.1600737.

[10] Alsoufi, M.A., Siraj, M.M., Ghaleb, F.A., Al-Razgan, M., Al-Asaly, M.S., Alfakih, T., Saeed, F., 2024. Anomaly-based intrusion detection model using deep learning for iot networks. Computer Modeling in Engineering & Sciences 141, 823–845.

[11] An, Y., Wang, W., 2025. An internet of things (iot) intrusion detection system combining large language models (llms) and self-supervised learning, in: 2025 International Joint Conference on Neural Networks (IJCNN), pp. 1–8. doi:10.1109/IJCNN64981.2025.11229088.

[12] Anbiaee, Z., Dadkhah, S., Ghorbani, A.A., 2025. Figs: A realistic intrusion-detection framework for highly imbalanced iot environments. Electronics 14, 2917. doi:10.3390/electronics14142917.

[13] Araf, I., Idri, A., Chairi, I., 2024. Cost-sensitive learning for imbalanced medical data: a review. Artificial Intelligence Review 57.

[14] Asaouer, G., Boubiche, D.E., 2025. Generative ai-based intrusion detection systems for intra-vehicle networks. Ad Hoc Networks , 104031.

[15] Awasthi, A., Ly, S.T., Nizam, J., Mehta, V., Ahmad, S., Nemani, R., Prasad, S., Van Nguyen, H., 2024. Anomaly detection in satellite videos using diffusion models, in: 2024 IEEE 26th International Workshop on Multimedia Signal Processing (MMSP), IEEE. pp. 1–6.

[16] Bao, T., Trousil, K., Tran, Q.D., Di Troia, F., Park, Y., 2025. Generating synthetic malware samples using generative ai against zero-day attacks. IEEE Access .

[17] Belarbi, O., Spyridopoulos, T., Anthi, E., Rana, O., Carnelli, P., Khan, A., 2025. Gotham dataset 2025: A reproducible large-scale iot network dataset for intrusion detection and security research. Data in Brief doi:10.5281/zenodo.14502760. article information and dataset paper available online.

[18] Butun, I., Österberg, P., Song, H., 2020. Security of the internet of things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials 22, 616–644. doi:10.1109/COMST.2019.2953364.

[19] Cai, S., Zhao, Y., Lyu, J., Wang, S., Hu, Y., Cheng, M., Zhang, G., 2025. Ddp-dar: Network intrusion detection based on denoising diffusion probabilistic model and dual-attention residual network. Neural Networks 184, 107064. doi:10.1016/j.neunet.2024.107064.

[20] Camerota, C., Pappone, L., Pecorella, T., Esposito, F., 2024. Addressing data security in iot: Minimum sample size and denoising diffusion models for improved malware detection, in: 2024 20th International Conference on Network and Service Management (CNSM), IEEE. pp. 1–7.

[21] Canadian Institute for Cybersecurity, 2018. CSE-CIC-IDS2018 on AWS. Dataset. URL: https://www.unb.ca/cic/datasets/ids-2018.html.

[22] Castells, T., Song, H.K., Kim, B.K., Choi, S., 2024. Ld-pruner: Efficient pruning of latent diffusion models using task-agnostic insights, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, pp. 821–830.

[23] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P., 2019. Network intrusion detection for iot security based on learning techniques. IEEE Communications Surveys & Tutorials 21, 2671–2701.

[24] Chai, G., Wu, Y., Liu, J., 2026. Cdaf: A contrastive distribution alignment framework for generative augmentation in imbalanced iiot intrusion detection. IEEE Internet of Things Journal 13, 17774–17789. doi:10.1109/JIOT.2026.3664076.

[25] Chawla, N.V., Bowyer, K.W., Hall, L.O., Kegelmeyer, W.P., 2002. Smote: synthetic minority over-sampling technique. Journal of artificial intelligence research 16, 321–357.

[26] Chen, Q., Al Kontar, R., Nouiehed, M., Yang, X.J., Lester, C., 2025. Rethinking cost-sensitive classification in deep learning via adversarial data augmentation. INFORMS Journal on Data Science 4, 1–19.

[27] Chen, X., Deng, L., Huang, F., Zhang, C., Zhang, Z., Zhao, Y., Zheng, K., 2021. Daemon: Unsupervised anomaly detection and interpretation for multivariate time series, in: 2021 IEEE 37th International Conference on Data Engineering (ICDE), pp. 2225–2230. doi:10.1109/ICDE51399.2021.00228.

[28] Chen, Y., Zhang, C., Ma, M., Liu, Y., Ding, R., Li, B., He, S., Rajmohan, S., Lin, Q., Zhang, D., 2023. Imdiffusion: Imputed diffusion models for multivariate time series anomaly detection. arXiv preprint arXiv:2307.00754 .

[29] Cherfi, S., Boulaiche, A., Lemouari, A., Abouaissa, A., 2025. Enhancing intrusion detection in iot: Cnn integration with k-means for efficient and balanced classification. Expert Systems with Applications , 130122.

[30] Cui, F., Wang, X., Gu, R., Zhang, Q., Wang, J., Song, B., 2026. An improved anomaly traffic detection framework based on denoising diffusion implicit model. Journal of King Saud University Computer and Information Sciences doi:10.1007/s44443-026-00629-2.

[31] Dai, E., Chen, J., 2022. Graph-augmented normalizing flows for anomaly detection of multiple time series, in: International Conference on Learning Representations. URL: https://openreview.net/forum?id=45L_dgP48Vd.

[32] Dai, H.N., Zheng, Z., Zhang, Y., 2019. Blockchain for internet of things: A survey. IEEE Internet of Things Journal 6, 8076–8094. doi:10.1109/JIOT.2019.2920987.

[33] Dixit, A., Mani, A., 2023. Sampling technique for noisy and borderline examples problem in imbalanced classification. Applied Soft Computing 142, 110361. doi:10.1016/j.asoc.2023.110361.

[34] Dritsas, E., Trigka, M., 2025. A survey on cybersecurity in IoT. Future Internet 17, 30. doi:10.3390/fi17010030.

[35] D'Souza, A., M, S., Sarawagi, S., 2025. Synthetic tabular data generation for imbalanced classification: The surprising effectiveness of an overlap class, in: Proceedings of the AAAI Conference on Artificial Intelligence, pp. 16127–16134. doi:10.1609/aaai.v39i15.33771.

[36] Dunmore, A., Jang-Jaccard, J., Sabrina, F., Kwak, J., 2023. A comprehensive survey of generative adversarial networks (gans) in cybersecurity intrusion detection. IEEE Access 11, 76071–76094. doi:10.1109/ACCESS.2023.3296707.

[37] Dzaferagic, M., Marchetti, N., Macaluso, I., 2022. Fault detection and classification in industrial iot in case of missing sensor data. IEEE Internet of Things Journal 9, 8892–8900. doi:10.1109/JIOT.2021.3116785.

[38] Eda, R., Togawa, N., 2025. Anomalous iot behavior detection by lstm-based power waveform prediction, in: Proceedings of the 10th International Conference on Internet of Things, Big Data and Security (IoTBDS 2025), pp. 345–352. doi:10.5220/0013368900003944.

[39] Elouardi, S., Motii, A., Jouhari, M., Nasser Hassane Amadou, A., Hedabou, M., 2024. A survey on hybrid-cnn and llms for intrusion detection systems: Recent iot datasets. IEEE Access 12, 180009–180033. doi:10.1109/ACCESS.2024.3506604.

[40] EROL, A.G., DEMİRCİ, S., 2025. Llms for intrusion detection systems: A review, in: 2025 18th International Conference on Information Security and Cryptology (ISCTürkiye), pp. 1–6. doi:10.1109/ISCTrkiye68593.2025.11224813.

[41] Fang, G., Ma, X., Wang, X., 2023. Structural pruning for diffusion models. doi:10.48550/arXiv.2305.10924, arXiv:2305.10924.

[42] Feng, W., Yan, Z., Zhang, H., Zeng, K., Xiao, Y., Hou, Y.T., 2018. A survey on security, privacy, and trust in mobile crowdsourcing. IEEE Internet of Things Journal 5, 2971–2992. doi:10.1109/JIOT.2017.2765699.

[43] Ferrag, M.A., Friha, O., Hamouda, D., Maglaras, L., Janicke, H., 2022. Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning. IEEE Access 10, 40281–40306. doi:10.1109/ACCESS.2022.3165809.

[44] Gaber, T., Ali, T., Nicho, M., Torky, M., 2025. Robust attacks detection model for internet of flying things based on generative adversarial network (gan) and adversarial training. IEEE Internet of Things Journal .

[45] Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., Bouchachia, A., 2014. A survey on concept drift adaptation. ACM Computing Surveys 46, 44:1–44:37. doi:10.1145/2523813.

[46] Gavrilev, D., Burnaev, E., 2023. Anomaly detection in networks via score-based generative models. arXiv preprint arXiv:2306.15324 .

[47] Gholami, M., Ghaffari, A., Derakhshanfard, N., Ibrahimoglu, N., Kazem, A.A.P., 2025. Blockchain integration in iot: Applications, opportunities, and challenges. Computers, Materials & Continua 83, 1561–1605. doi:10.32604/cmc.2025.063304.

[48] Goldschmidt, P., Chudá, D., 2025. Network intrusion datasets: A survey, limitations, and recommendations. Computers & Security 156, 104510. doi:10.1016/j.cose.2025.104510.

[49] Goncalves, A., Ray, P., Soper, B., Stevens, J., Coyle, L., Sales, A.P., 2020. Generation and evaluation of synthetic patient data. BMC Medical Research Methodology 20, 108. doi:10.1186/s12874-020-00977-1.

[50] Gong, M., Du, J., You, J., 2025a. Diffuse to detect: A generalizable framework for anomaly detection with diffusion models applications to uavs and beyond. arXiv preprint arXiv:2510.22928 .

[51] Gong, X., Chen, S., Li, N., 2025b. A network traffic data generation model based on aot-ddpm for abnormal traffic detection. Evolving Systems 16, 15.

[52] Goodfellow, I.J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y., 2014. Generative adversarial nets. Advances in neural information processing systems 27.

[53] Gupta, N., Jindal, V., Bedi, P., 2022. Cse-ids: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems. Computers & Security 112, 102499. doi:10.1016/j.cose.2021.102499.

[54] Han, Z., Yang, Y., Bilal, M., Wang, W., Krichen, M., Alsadhan, A.A., Ge, C., 2023. Smart optimization solution for channel access attack defense under uav-aided heterogeneous network. IEEE Internet of Things Journal 10, 18890–18897.

[55] Hassan, S.R., Tanveer, M.U., Prajapat, S., Shabaz, M., 2025. A comprehensive survey on intrusion detection in internet of medical things: Datasets, federated learning, blockchain, and future research directions. ICT Express 11, 1291–1310. doi:10.1016/j.icte.2025.11.005.

[56] Hayaeian Shirvan, M., Moattar, M.H., Hosseinzadeh, M., 2025. Deep generative approaches for oversampling in imbalanced data classification problems: A comprehensive review and comparative analysis. Applied Soft Computing 170, 112677. doi:10.1016/j.asoc.2024.112677.

[57] He, J., Li, X., Zhang, X., Niu, W., Li, F., 2025. A synthetic data-assisted satellite terrestrial integrated network intrusion detection framework. IEEE Transactions on Information Forensics and Security 20, 1739–1754.

[58] Ho, J., Jain, A., Abbeel, P., 2020. Denoising diffusion probabilistic models, in: Advances in Neural Information Processing Systems, pp. 6840–6851.

[59] Ho, T.K.K., Armanfard, N., 2023. Contaminated multivariate time-series anomaly detection with spatio-temporal graph conditional diffusion models. arXiv preprint arXiv:2308.12563 .

[60] Hou, Y., He, R., Dong, J., Yang, Y., Ma, W., 2022. Iot anomaly detection based on autoencoder and bayesian gaussian mixture model. Electronics 11, 3287.

[61] Hu, C., Zhang, R., Li, B., Jiang, X., Zhao, N., Di Renzo, M., Niyato, D., Nallanathan, A., Karagiannidis, G.K., 2025. Generative ai-empowered secure communications in space–air–ground integrated networks: A survey and tutorial. IEEE Communications Surveys & Tutorials 28, 4156–4194.

[62] Hu, T., Zhang, J., Yi, R., Huang, H., Wang, Y., Ma, L., 2024. Sara: High-efficient diffusion model fine-tuning with progressive sparse low-rank adaptation. doi:10.48550/arXiv.2409.06633, arXiv:2409.06633. accepted by ICLR 2025.

[63] Javanmardi, S., Nascita, A., Pescapè, A., Merlino, G., Scarpa, M., 2025. An integration perspective of security, privacy, and resource efficiency in iot-fog networks: A comprehensive survey. Computer Networks 270, 111470. doi:10.1016/j.comnet.2025.111470.

[64] Jiang, X., Liu, S., Gember-Jacobson, A., Bhagoji, A.N., Schmitt, P., Bronzino, F., Feamster, N., 2023. Netdiffusion: Network data augmentation through protocol-constrained traffic generation. URL: https://arxiv.org/abs/2310.08543, arXiv:2310.08543.

[65] Kapoor, G., Nadipalli, S., Di Troia, F., 2025. Embedding-driven synthetic malware generation with autoencoders and cluster-tangent diffusion. Applied Sciences 15, 11791. doi:10.3390/app152111791.

[66] Karimian, M., Beigy, H., 2023. Concept drift handling: A domain adaptation perspective. Expert Systems with Applications 224, 119946. doi:10.1016/j.eswa.2023.119946.

[67] Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E.C.P., Xiong, P., Iqbal, S., Lamontagne, P., Ray, S., Ghorbani, A.A., 2023. Internet of things (iot) security dataset evolution: Challenges and future directions. Internet of Things 22, 100780.

[68] Khan, A.R., Kashif, M., Jhaveri, R.H., Raut, R., Saba, T., Bahaj, S.A., 2022. Deep learning for intrusion detection and security of internet of things (iot): current analysis, challenges, and possible solutions. Security and communication networks 2022, 4016073.

[69] Khare, S., Totaro, M., 2020. Ensemble learning for detecting attacks and anomalies in iot smart home, in: 2020 3rd international conference on data intelligence and security (ICDIS), IEEE. pp. 56–63.

[70] Kingma, D.P., Welling, M., 2013. Auto-encoding variational bayes. arXiv preprint arXiv:1312.6114 .

[71] Koroniotis, N., Moustafa, N., Sitnikova, E., Turnbull, B., 2019. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems 100, 779–796. doi:10.1016/j.future.2019.05.041.

[72] Kotelnikov, A., Baranchuk, D., Rubachev, I., Babenko, A., 2023. TabDDPM: Modelling tabular data with diffusion models, in: Proceedings of the 40th International Conference on Machine Learning, PMLR. pp. 17564–17579.

[73] Lan, D., Zhang, G., Guo, R., 2025. Diffusion graph model for time series anomaly detection via anomaly-aware graph sparsification and augmentation, in: Companion Proceedings of the ACM on Web Conference 2025, pp. 2207–2214.

[74] Leevy, J.L., Hancock, J., Khoshgoftaar, T.M., Zadeh, A.A., 2023. One-class classifier performance: Comparing majority versus minority class training, in: 2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI), IEEE. pp. 86–91.

[75] Lei, L., Tan, Y., Zheng, K., Liu, S., Zhang, K., Shen, X., 2020. Deep reinforcement learning for autonomous Internet of Things: Model, applications and challenges. IEEE Communications Surveys & Tutorials 22, 1722–1760. doi:10.1109/COMST.2020.2988367.

[76] Li, C., Kiat, Y.C., Jing, J., Long, C., 2025a. T-vae: Transformer-based variational autoencoder for perceiving anomalies in multivariate time series data. Expert Systems 42, e70078.

[77] Li, H., Kang, H., Liu, C., Wang, R., Li, J., Sun, G., Wang, J., Liang, S., Mao, S., 2025b. Encrypted traffic detection in resource constrained iot networks: A diffusion model and llm integrated framework. IEEE Transactions on Network Science and Engineering .

[78] Li, K., Li, F., Wang, B., Shan, M., 2024a. False data injection attack sample generation using an adversarial attention-diffusion model in smart grids. AIMS Energy 12.

[79] Li, L., Zhang, W., Yuan, S., Guo, H., Chen, W., 2025c. Physdiff: A physically-guided diffusion model for multivariate time series anomaly detection, in: The Thirty-ninth Annual Conference on Neural Information Processing Systems.

[80] Li, Y., Ruiz Luyten, M., van der Schaar, M., 2025d. Risk-sensitive diffusion: Robustly optimizing diffusion models with noisy samples, in: The Thirteenth International Conference on Learning Representations. URL: https://openreview.net/forum?id=bOWpXBABdu.

[81] Li, Z., Huang, C., Qiu, W., 2024b. An intrusion detection method combining variational auto-encoder and generative adversarial networks. Computer Networks 253, 110724. doi:10.1016/j.comnet.2024.110724.

[82] Li, Z., Huang, Q., Yang, L., Shi, J., Yang, Z., van Stein, N., Bäck, T., van Leeuwen, M., 2025e. Diffusion models for tabular data: Challenges, current progress, and future directions. arXiv preprint arXiv:2502.17119 doi:10.48550/arXiv.2502.17119, arXiv:2502.17119.

[83] Li, Z., Yao, W., 2024. A two stage lightweight approach for intrusion detection in internet of things. Expert Systems with Applications 257, 124965. doi:10.1016/j.eswa.2024.124965.

[84] Liang, W., Huang, W., Long, J., Zhang, K., Li, K.C., Zhang, D., 2020. Deep reinforcement learning for resource protection and real-time detection in IoT environment. IEEE Internet of Things Journal 7, 6392–6401. doi:10.1109/JIOT.2020.2974281.

[85] Lim, W., Yong, K.S.C., Lau, B.T., Tan, C.C.L., 2024. Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. Computers & Security 145, 103733. doi:10.1016/j.cose.2024.103733.

[86] Liu, J., Ma, Z., Wang, Z., Zou, C., Ren, J., Wang, Z., Song, L., Hu, B., Liu, Y., Leung, V.C.M., 2025a. A survey on diffusion models for anomaly detection. arXiv preprint arXiv:2501.11430 doi:10.48550/arXiv.2501.11430, arXiv:2501.11430.

[87] Liu, T., Liu, J., Zhang, T., Wang, J., Wang, J., Kang, J., Niyato, D., Mao, S., 2025b. Generative AI-driven cross-layer covert communication: Fundamentals, framework and case study. IEEE Communications Magazine 63, 128–134. doi:10.1109/MCOM.004.2500025.

[88] Liu, Y., Liu, Y., Yu, B.X.B., Zhong, S., Hu, Z., 2023. Noise-robust oversampling for imbalanced data classification. Pattern Recognition 133, 109008. doi:10.1016/j.patcog.2022.109008.

[89] López Delgado, J.L., López Ramos, J.A., 2024. A comprehensive survey on generative AI solutions in IoT security. Electronics 13, 4965. doi:10.3390/electronics13244965.

[90] Lu, C., Cao, Y., Wang, Z., 2024. Research on intrusion detection based on an enhanced random forest algorithm. Applied Sciences 14, 714.

[91] Lu, J., Liu, A., Dong, F., Gu, F., Gama, J., Zhang, G., 2019. Learning under concept drift: A review. IEEE Transactions on Knowledge and Data Engineering 31, 2346–2363. doi:10.1109/TKDE.2018.2876857.

[92] Luo, S., Tan, Y., Huang, L., Li, J., Zhao, H., 2023. Latent consistency models: Synthesizing high-resolution images with few-step inference. doi:10.48550/arXiv.2310.04378, arXiv:2310.04378.

[93] Ma, X., Fang, G., Wang, X., 2024. Deepcache: Accelerating diffusion models for free, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition.

[94] Mahmoudi, I., Boubiche, D.E., Athmani, S., Toral-Cruz, H., Chan-Puc, F.I., 2025. Toward generative ai-based intrusion detection systems for the internet of vehicles (iov). Future Internet 17, 310.

[95] Manzano, R., Zaman, M., Upadhyay, D., Goel, N., Sampalli, S., 2025. Federated learning framework based on distributed storage and diffusion model for intrusion detection on iot networks. IEEE Access .

[96] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., Elovici, Y., 2018. N-BaIoT—network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing 17, 12–22. doi:10.1109/MPRV.2018.03367731.

[97] Mengistu, T.M., Kim, T., Lin, J.W., 2024. A survey on heterogeneity taxonomy, security and privacy preservation in the integration of iot, wireless sensor networks and federated learning. Sensors 24, 968. doi:10.3390/s24030968.

[98] Merzouk, M.A., Beurier, E., Yaich, R., Boulahia-Cuppens, N., Cuppens, F., Khomh, F., 2025. Diffusion-based adversarial purification for intrusion detection, in: IFIP Annual Conference on Data and Applications Security and Privacy, Springer. pp. 351–370.

[99] Mirsky, Y., Doitshman, T., Elovici, Y., Shabtai, A., 2018. Kitsune: An ensemble of autoencoders for online network intrusion detection, in: Proceedings of the 25th Annual Network and Distributed System Security Symposium. doi:10.14722/ndss.2018.23204.

[100] Mirza, M., Osindero, S., 2014. Conditional generative adversarial nets. arXiv:1411.1784.

[101] Mishra, N., Pandya, S., 2021. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access 9, 59353–59377.

[102] Mosenia, A., Jha, N.K., 2017. A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing 5, 586–602. doi:10.1109/TETC.2016.2606384.

[103] Moustafa, N., Keshky, M., Debiez, E., Janicke, H., 2020. Federated ton_iot windows datasets for evaluating ai-based security applications, in: 2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom), IEEE. pp. 848–855.

[104] Moustafa, N., Slay, J., 2015. Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set), in: 2015 Military Communications and Information Systems Conference (MilCIS), pp. 1–6. doi:10.1109/MilCIS.2015.7348942.

[105] Nawaal, B., Haider, U., Khan, I.U., Fayaz, M., 2024. Signature-based intrusion detection system for iot, in: Cyber security for next-generation computing technologies. CRC Press, pp. 141–158.

[106] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., Ghani, N., 2019. Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. IEEE Communications Surveys & Tutorials 21, 2702–2733. doi:10.1109/COMST.2019.2910750.

[107] Nguyen, C.T., Liu, Y., Du, H., Hoang, D.T., Niyato, D., Nguyen, D.N., Mao, S., 2025. Generative AI-enabled blockchain networks: Fundamentals, applications, and case study. IEEE Network 39, 232–241. doi:10.1109/MNET.2024.3412161.

[108] Nguyen, Q.K., Dang, T., Kim, J., 2021. Blockchain for internet of things: A comprehensive survey. Sensors 21, 3721. doi:10.3390/s21113721.

[109] Nie, Y., Nguyen, N.H., Sinthong, P., Kalagnanam, J., 2022. A time series is worth 64 words: Long-term forecasting with transformers. ArXiv abs/2211.14730. URL: https://api.semanticscholar.org/CorpusID:254044221.

[110] Nizam, H., Zafar, S., Lv, Z., Wang, F., Hu, X., 2022. Real-time deep anomaly detection framework for multivariate time-series data in industrial iot. IEEE Sensors Journal 22, 22836–22849. doi:10.1109/JSEN.2022.3211874.

[111] Ogunseyi, T.B., Thiyagarajan, G., 2025. An explainable lstm-based intrusion detection system optimized by firefly algorithm for iot networks. Sensors 25, 2288.

[112] Pan, S.J., Yang, Q., 2010. A survey on transfer learning. IEEE Transactions on Knowledge and Data Engineering 22, 1345–1359. doi:10.1109/TKDE.2009.191.

[113] Park, C., Lee, J., Kim, Y., Park, J.G., Kim, H., Hong, D., 2022. An enhanced ai-based network intrusion detection system using generative adversarial networks. IEEE Internet of Things Journal 10, 2330–2345.

[114] Park, D., Hoshi, Y., Kemp, C.C., 2018. A multimodal anomaly detector for robot-assisted feeding using an lstm-based variational autoencoder. IEEE Robotics and Automation Letters 3, 1544–1551. doi:10.1109/LRA.2018.2801475.

[115] Patki, N., Wedge, R., Veeramachaneni, K., 2016. The synthetic data vault, in: 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), pp. 399–410. doi:10.1109/DSAA.2016.49.

[116] Qian, Z., Davis, R., van der Schaar, M., 2023. Synthcity: A benchmark framework for diverse use cases of tabular synthetic data, in: Advances in Neural Information Processing Systems, Datasets and Benchmarks Track, pp. 3173–3188.

[117] Rahman, M.M., Shakil, S.A., Mustakim, M.R., 2025. A survey on intrusion detection system in IoT networks. Cyber Security and Applications 3, 100082. URL: https://www.sciencedirect.com/science/article/pii/S2772918424000481, doi:10.1016/j.csa.2024.100082.

[118] Rasul, K., Seward, C., Schuster, I., Vollgraf, R., 2021. Autoregressive denoising diffusion models for multivariate probabilistic time series forecasting, in: Proceedings of the 38th International Conference on Machine Learning, PMLR. pp. 8857–8868.

[119] Rathkopf, C., 2025. Hallucination, reliability, and the role of generative ai in science. arXiv preprint arXiv:2504.08526 .

[120] Rombach, R., Blattmann, A., Lorenz, D., Esser, P., Ommer, B., 2022. High-resolution image synthesis with latent diffusion models, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 10684–10695.
[121] Rustam, F., Jurcut, A.D., Salauddin, M., 2026. Unsupervised diffusion-guided lstm for anomaly detection in water distribution networks. IEEE Access .
[122] Salimans, T., Ho, J., 2022. Progressive distillation for fast sampling of diffusion models, in: International Conference on Learning Representations. URL: https://openreview.net/forum?id=TIdIXIpzhoI.
[123] Sarhan, M., Lo, W.W., Layeghy, S., Portmann, M., 2022. HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. Computers & Electrical Engineering 103, 108379. doi:10.1016/j.compeleceng.2022.108379.
[124] Sasi, T., Lashkari, A.H., Lu, R., Xiong, P., Iqbal, S., 2024. A comprehensive survey on iot attacks: Taxonomy, detection mechanisms and challenges. Journal of Information and intelligence 2, 455–513.
[125] Shafi, M., Habibi Lashkari, A., 2025. Toward generating a large-scale iot-zwave intrusion detection dataset: Smart device profiling, intruders behavior, and traffic characterization. Internet of Things 34, 101747. doi:10.1016/j.iot.2025.101747.
[126] Shen, H., Zhang, J., Xiong, B., Hu, R., Chen, S., Wan, Z., Wang, X., Zhang, Y., Gong, Z., Bao, G., Tao, C., Huang, Y., Yuan, Y., Zhang, M., 2025. Efficient diffusion models: A survey. doi:10.48550/arXiv.2502.06805, arXiv:2502.06805.
[127] Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L., 2016. Edge computing: Vision and challenges. IEEE Internet of Things Journal 3, 637–646. doi:10.1109/JIOT.2016.2579198.
[128] Shyaa, M.A., Ibrahim, N.F., Zainol, Z., Abdullah, R., Anbar, M., Alzubaidi, L., 2024. Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems. Engineering Applications of Artificial Intelligence 137, 109143. doi:10.1016/j.engappai.2024.109143.
[129] Singh, S., Sharma, P.K., Yoon, B., Shojafar, M., Cho, G.H., Ra, I.H., 2021. Blockchain-based iot: Architecture, applications, and challenges. IEEE Internet of Things Journal 8, 4032–4048. doi:10.1109/JIOT.2020.3030965.
[130] Singhal, P., Walambe, R., Ramanna, S., Kotecha, K., 2023. Domain adaptation: Challenges, methods, datasets, and applications. IEEE Access 11, 6973–7020. doi:10.1109/ACCESS.2023.3237025.
[131] Sivaroopan, N., Bandara, D., Madarasingha, C., Jourjon, G., Jayasumana, A.P., Thilakarathna, K., 2024. NetDiffus: Network traffic generation by diffusion models through time-series imaging. Computer Networks 251, 110616. doi:10.1016/j.comnet.2024.110616.
[132] Sohn, K., Lee, H., Yan, X., 2015. Learning structured output representation using deep conditional generative models, in: Advances in Neural Information Processing Systems.
[133] Song, W., Ma, W., Zhang, M., Zhang, Y., Zhao, X., 2024. Lightweight diffusion models: A survey. Artificial Intelligence Review 57, 161. doi:10.1007/s10462-024-10800-8.
[134] Song, Y., Dhariwal, P., Chen, M., Sutskever, I., 2023. Consistency models, in: Proceedings of the 40th International Conference on Machine Learning, PMLR. pp. 32211–32252. URL: https://proceedings.mlr.press/v202/song23a.html.
[135] Song, Y., Sohl-Dickstein, J., Kingma, D.P., Kumar, A., Ermon, S., Poole, B., 2021. Score-based generative modeling through stochastic differential equations, in: International Conference on Learning Representations.
[136] Soni, J., Lange-Hegermann, M., Windmann, S., 2025. Physics-informed diffusion models for unsupervised anomaly detection in multivariate time series. arXiv preprint arXiv:2508.11528 .
[137] Su, C., Wen, J., Kang, J., Wang, Y., Su, Y., Pan, H., Zhong, Z., Hossain, M.S., 2024. Hybrid rag-empowered multimodal llm for secure data management in internet of medical things: a diffusion-based contract approach. IEEE Internet of Things Journal 12, 13428–13440.
[138] Sutskever, I., Vinyals, O., Le, Q.V., 2014. Sequence to sequence learning with neural networks. Advances in neural information processing systems 27.
[139] Sánchez-Carballo, E., Melgarejo-Meseguer, F.M., Rojo-Álvarez, J.L., 2026. Latent diffusion for internet of things attack data generation in intrusion detection. URL: https://arxiv.org/abs/2601.16976, arXiv:2601.16976.
[140] Tan, M., Le, Q., 2021. Efficientnetv2: Smaller models and faster training, in: Meila, M., Zhang, T. (Eds.), Proceedings of the 38th International Conference on Machine Learning, PMLR. pp. 10096–10106.
[141] Tang, B., Lu, Y., Li, Q., Bai, Y., Yu, J., Yu, X., 2023. A diffusion model based on network intrusion detection method for industrial cyber-physical systems. Sensors 23, 1141.
[142] Tashiro, Y., Song, J., Song, Y., Ermon, S., 2021. CSDI: Conditional score-based diffusion models for probabilistic time series imputation, in: Advances in Neural Information Processing Systems, pp. 24804–24816.
[143] Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A., 2009. A detailed analysis of the kdd cup 99 data set, in: 2009 IEEE symposium on computational intelligence for security and defense applications, Ieee. pp. 1–6. doi:10.1109/cisda.2009.5356528.
[144] Tu, R., Senane, Z., Cao, L., Zhang, C., Kjellström, H., Henter, G.E., 2024. Causality for tabular data synthesis: A high-order structure causal benchmark framework. arXiv preprint arXiv:2406.08311 arXiv:2406.08311.
[145] Ubukata, T., Li, J., Tei, K., 2024. Diffusion model for planning: A systematic literature review. arXiv preprint arXiv:2408.10266 .
[146] Villaizán-Vallelado, M., Salvatori, M., Segura, C., Arapakis, I., 2025. Diffusion models for tabular data imputation and synthetic data generation. ACM Transactions on Knowledge Discovery from Data 19, 1–32. doi:10.1145/3742435.
[147] Vyshnavi, A., Reddy, D., 2026. Synthnet: Vae–gan–driven synthetic data generation for iot network simulation and multi-class intrusion detection, in: 2026 4th International Conference on Knowledge Engineering and Communication Systems (ICKECS), pp. 1–6. doi:10.1109/ICKECS70176.2026.11527619.
[148] Wang, A.X., Chukova, S.S., Simpson, C.R., Nguyen, B.P., 2024a. Challenges and opportunities of generative models on tabular data. Applied Soft Computing 166, 112223.
[149] Wang, C., Tu, C., Wang, P., Song, Y., Wang, X., Guo, X., 2025a. Ldct-ids: A lightweight intrusion detection system for iot networks via denoising diffusion models and hybrid convolutional-transformer architecture. Research Square preprint URL: https://www.researchsquare.com/article/rs-8183839/v1, doi:10.21203/rs.3.rs-8183839/v1.

[150] Wang, F., Jiang, Y., Zhang, R., Wei, A., Xie, J., Pang, X., 2025b. A survey of deep anomaly detection in multivariate time series: Taxonomy, applications, and directions. Sensors 25. URL: https://www.mdpi.com/1424-8220/25/1/190.

[151] Wang, H., Shang, Y., Yuan, Z., Wu, J., Yan, J., Yan, Y., 2024b. Quest: Low-bit diffusion model quantization via efficient selective finetuning. doi:10.48550/arXiv.2402.03666, arXiv:2402.03666.

[152] Wang, J., Wang, Z., Wen, C., Liu, W., Liu, X., Wang, D., 2025c. Industrial anomaly detection based on improved diffusion model: A review. Cognitive Computation 17, 165. doi:10.1007/s12559-025-10517-y.

[153] Wang, N., Zhao, T., Mao, S., Wang, X., 2025d. Privacy-preserving wi-fi data generation via differential privacy in diffusion models, in: IEEE INFOCOM 2025 – IEEE Conference on Computer Communications, IEEE. pp. 1–10. doi:10.1109/INFOCOM55648.2025.11044673.

[154] Wang, P., Song, Y., Wang, X., Guo, X., 2025e. Dift: A diffusion-transformer for intrusion detection of iot with imbalanced learning. Journal of Network and Systems Management 33, 48. doi:10.1007/s10922-025-09926-z.

[155] Wang, S., Veldhuis, R., Brune, C., Strisciuglio, N., 2023. A survey on the robustness of computer vision models against common corruptions. arXiv preprint arXiv:2305.06024 .

[156] Wang, W., Yang, Y., Yin, Z., Dev, K., Zhou, X., Li, X., Qureshi, N.M., Su, C., 2022. Bsif: Blockchain-based secure, interactive, and fair mobile crowdsensing. IEEE Journal on Selected Areas in Communications 40, 3452–3469. doi:10.1109/JSAC.2022.3213306.

[157] Wang, X., Wang, J., Feng, L., Niyato, D., Zhang, R., Kang, J., Xiong, Z., Du, H., Mao, S., 2026. Hallucination in generative ai-enabled wireless communications: Concepts, issues, and solutions. IEEE Communications Magazine .

[158] Wang, Y., Ding, J., He, X., Wei, Q., Yuan, S., Zhang, J., 2024c. Intrusion detection method based on denoising diffusion probabilistic models for uav networks. Mobile Networks and Applications 29, 1467–1476.

[159] Wang, Z., Guan, Z., Liu, X., Qiao, M., Sun, X., Li, J., 2025f. Diffusion–attention traffic generation: Traffic generation based on the fusion of a diffusion model and a self-attention mechanism. Electronics 14. URL: https://www.mdpi.com/2079-9292/14/10/1977.

[160] Wang, Z., Oates, T., 2015. Imaging time-series to improve classification and imputation. URL: https://arxiv.org/abs/1506.00327, arXiv:1506.00327.

[161] Wen, J., Nie, J., Kang, J., Niyato, D., Du, H., Zhang, Y., Guizani, M., 2024. From generative AI to generative internet of things: Fundamentals, framework, and outlooks. IEEE Internet of Things Magazine 7, 30–37. doi:10.1109/IOTM.001.2300255.

[162] Wiessner, P., Bezirganyan, G., Sellami, S., Chbeir, R., Bungartz, H.J., 2024. Uncertainty-aware time series anomaly detection. Future internet 16, 403.

[163] Wu, J., Yang, Y., Yuan, W., Liu, W., Wang, J., Mao, T., Zhou, L., Cui, Y., Liu, F., Sun, G., Wu, N., Zheng, D., Xu, J., Ma, N., Feng, Z., Xu, W., Niyato, D., Yuen, C., Jing, X., Shi, Z., Liang, Y., Jin, S., Kim, D.I., Wang, J., Zhang, P., Yin, H., Zhang, J., 2025a. Low-altitude wireless networks: A survey. doi:10.48550/arXiv.2509.11607, arXiv:2509.11607.

[164] Wu, Z., Zhu, L., Yin, Z., Xu, X., Zhu, J., Wei, X., Yang, X., 2025b. Mafcd: Multi-level and adaptive conditional diffusion model for anomaly detection. Information Fusion 118, 102965. doi:10.1016/j.inffus.2025.102965.

[165] Xiao, C., Gou, Z., Tai, W., Zhang, K., Zhou, F., 2023. Imputation-based time-series anomaly detection with conditional weight-incremental diffusion models, in: Proceedings of the 29th ACM SIGKDD conference on knowledge discovery and data mining, pp. 2742–2751.

[166] Xiao, L., Jiang, D., Xu, D., An, N., 2018a. Secure mobile crowdsensing with deep learning. China Communications 15, 1–11. doi:10.1109/CC.2018.8485464.

[167] Xiao, L., Wan, X., Lu, X., Zhang, Y., Wu, D., 2018b. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? IEEE Signal Processing Magazine 35, 41–49. doi:10.1109/MSP.2018.2825478.

[168] Xie, S., Xiao, Z., Kingma, D.P., Hou, T., Wu, Y.N., Murphy, K.P., Salimans, T., Poole, B., Gao, R., 2024. Em distillation for one-step diffusion models. doi:10.48550/arXiv.2405.16852, arXiv:2405.16852. neurIPS 2024.

[169] Xu, Y., Chen, Z., Wang, R., Li, Y., Tang, F., Zhao, M., Liu, J., 2025. Faultdiffusion: Few-shot fault time series generation with diffusion model. arXiv preprint arXiv:2511.15174 .

[170] Yan, C., Liu, S., Liu, H., Peng, X., Wang, X., Chen, F., Fu, L., Mei, X., 2024. Hybrid sd: Edge-cloud collaborative inference for stable diffusion models. arXiv preprint arXiv:2408.06646 arXiv:2408.06646.

[171] Yan, Y., Yang, Y., Shen, F., Gao, M., Gu, Y., 2023. Gde model: A variable intrusion detection model for few-shot attack. Journal of King Saud University - Computer and Information Sciences 35, 101796. URL: https://www.sciencedirect.com/science/article/pii/S1319157823003506, doi:https://doi.org/10.1016/j.jksuci.2023.101796.

[172] Yang, H., Song, Y., Wang, D., Xing, J., Li, Y., 2025a. A global information-guided denoising diffusion probabilistic model for fault diagnosis with imbalanced data. Engineering Applications of Artificial Intelligence 147, 110312.

[173] Yang, K., Kpotufe, S., Feamster, N., 2022a. An efficient one-class svm for novelty detection in iot. Transactions on machine learning research .

[174] Yang, K., Zhang, K., Ren, J., Shen, X., 2015. Security and privacy in mobile crowdsourcing networks: Challenges and opportunities. IEEE Communications Magazine 53, 75–81. doi:10.1109/MCOM.2015.7180511.

[175] Yang, L., Zhang, Z., Song, Y., Hong, S., Xu, R., Zhao, Y., Zhang, W., Cui, B., Yang, M.H., 2024a. Diffusion models: A comprehensive survey of methods and applications. ACM Computing Surveys 56, 105:1–105:39. doi:10.1145/3626235.

[176] Yang, X., Ardakanian, O., 2023. Privacy through diffusion: a white-listing approach to sensor data anonymization, in: Proceedings of the 5th Workshop on CPS&IoT Security and Privacy, pp. 101–107.

[177] Yang, X., Ardakanian, O., 2025. Privdiffuser: Privacy-guided diffusion model for data obfuscation in sensor networks. Proceedings on Privacy Enhancing Technologies 2025, 40–55. doi:10.56553/popets-2025-0118.

[178] Yang, Y., Chen, Y., Wang, J., Sun, G., Niyato, D., 2024b. Embodied ai-empowered low altitude economy: Integrated sensing, communications, computation, and control (isc3). doi:10.48550/arXiv.2412.19996, arXiv:2412.19996.

[179] Yang, Y., Chen, Y., Wang, J., Sun, G., Niyato, D., Han, Z., 2026a. Leveraging the power of ensemble learning for secure low altitude economy. doi:10.48550/arXiv.2602.07725, arXiv:2602.07725.

[180] Yang, Y., Du, H., Xiong, Z., Xu, R., Niyato, D., Han, Z., 2025b. Exploring impacts of age of information on data accuracy for wireless sensing systems: An information entropy perspective. IEEE Transactions on Mobile Computing 24, 4907–4924. doi:10.1109/TMC.2025.3527587.

[181] Yang, Y., Jin, M., Wen, H., Zhang, C., Liang, Y., Ma, L., Wang, Y., Liu, C., Yang, B., Xu, Z., Bian, J., Pan, S., Wen, Q., 2024c. A survey on diffusion models for time series and spatio-temporal data. arXiv preprint arXiv:2404.18886 doi:10.48550/arXiv.2404.18886.

[182] Yang, Y., Khorshidi, H.A., Aickelin, U., 2024d. A review on over-sampling techniques in classification of multi-class imbalanced datasets: insights for medical problems. Frontiers in Digital Health 6, 1430245. doi:10.3389/fdgth.2024.1430245.

[183] Yang, Y., Sun, G., Du, H., Zhao, C., Xiong, Z., Niyato, D., Jamalipour, A., Han, Z., Letaief, K.B., 2026b. Leveraging generative ai for security defense of mobile edge-enabled digital twins: A survey. IEEE Transactions on Cognitive Communications and Networking .

[184] Yang, Y., Tang, X., Liu, Z., Cheng, J., Fang, H., Zhang, C., 2025c. Diff-ids: A network intrusion detection model based on diffusion model for imbalanced data samples. Computers, Materials & Continua 82, 4389–4408. doi:10.32604/cmc.2025.060357.

[185] Yang, Y., Wang, W., Xu, R., Srivastava, G., Alazab, M., Gadekallu, T.R., Su, C., 2022b. AoI optimization for UAV-aided MEC networks under channel access attacks: A game theoretic viewpoint, in: ICC 2022 – IEEE International Conference on Communications, pp. 1–6. doi:10.1109/ICC45855.2022.9838975.

[186] Yang, Y., Wang, W., Yin, Z., Xu, R., Zhou, X., Kumar, N., Alazab, M., Gadekallu, T.R., 2022c. Mixed game-based aoi optimization for combating covid-19 with ai bots. IEEE Journal on Selected Areas in Communications 40, 3122–3138. doi:10.1109/JSAC.2022.3215508.

[187] Yang, Y., Yang, X., Heidari, M., Khan, M.A., Srivastava, G., Khosravi, M.R., Qi, L., 2023a. Astream: Data-stream-driven scalable anomaly detection with accuracy guarantee in iiot environment. IEEE Transactions on Network Science and Engineering 10, 3007–3016. doi:10.1109/TNSE.2022.3157730.

[188] Yang, Y., Zhang, B., Guo, D., Wang, W., Li, X., Hu, C., 2023b. Ppfo: A privacy preservation-oriented data freshness optimization framework for mobile crowdsensing. IEEE Communications Standards Magazine 7, 34–40.

[189] Yang, Y., Zhang, B., Guo, D., Xiong, Z., Niyato, D., Han, Z., 2024e. Can we realize data freshness optimization for privacy preserving-mobile crowdsensing with artificial noise? IEEE Transactions on Mobile Computing 23, 11357–11374. doi:10.1109/TMC.2024.3396993.

[190] Yang, Y., Zhang, B., Guo, D., Xu, R., Kumar, N., Wang, W., 2023c. Mean field game and broadcast encryption-based joint data freshness optimization and privacy preservation for mobile crowdsensing. IEEE Transactions on Vehicular Technology 72, 14860–14874.

[191] Yoon, J., Jarrett, D., van der Schaar, M., 2019. Time-series generative adversarial networks, in: Advances in Neural Information Processing Systems.

[192] Zamberg, G., Salhov, M., Lindenbaum, O., Averbuch, A., 2023. Tabadm: Unsupervised tabular anomaly detection with diffusion models. arXiv preprint arXiv:2307.12336 .

[193] Zhang, C., Sun, G., Li, J., Wu, Q., Wang, J., Niyato, D., Liu, Y., 2025a. Multi-objective aerial collaborative secure communication optimization via generative diffusion model-enabled deep reinforcement learning. IEEE Transactions on Mobile Computing 24, 3041–3058. doi:10.1109/TMC.2024.3502685.

[194] Zhang, C., Xie, B., Huo, Z., 2025b. Unsupervised anomaly detection in time series data via enhanced vae-transformer framework. Computers, Materials, & Continua 84, 843.

[195] Zhang, M., De Lucia, M., Swami, A., Ashdown, J., Bastian, N.D., Restuccia, F., 2025c. Ni-diff: Zero-day and adversarial network intrusion detection with diffusion models, in: MILCOM 2025-2025 IEEE Military Communications Conference (MILCOM), IEEE. pp. 776–781.

[196] Zhang, M., Wang, J., Qi, Q., Ren, P., Sun, H., Zhuang, Z., Zhang, L., Liao, J., 2024a. Safeguarding sustainable cities: unsupervised video anomaly detection through diffusion-based latent pattern learning, in: Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence, pp. 7572–7580.

[197] Zhang, S., Chen, J., Chen, J., Chen, X., Huang, H., 2023. Data imputation in iot using spatio-temporal variational auto-encoder. Neurocomputing 529, 23–32.

[198] Zhang, X., Liu, D., Liu, H., Zhang, Q., Meng, H., Garcia, L.P., Chng, E.S., Yao, L., 2024b. Speaking in wavelet domain: A simple and efficient approach to speed up speech diffusion model, in: Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing, pp. 159–171. doi:10.18653/v1/2024.emnlp-main.9.

[199] Zhang, X., Zhao, R., Jiang, Z., Chen, H., Ding, Y., Ngai, E.C.H., Yang, S.H., 2025d. Continual learning with strategic selection and forgetting for network intrusion detection. arXiv preprint arXiv:2412.16264 arXiv:2412.16264.

[200] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J., 2019. Smart contract-based access control for the internet of things. IEEE Internet of Things Journal 6, 1594–1605. doi:10.1109/JIOT.2018.2847705.

[201] Zhang, Y., Muniyandi, R.C., Qamar, F., 2025e. A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance. Applied Sciences 15, 1552. doi:10.3390/app15031552.

[202] Zhao, C., Du, H., Niyato, D., Kang, J., Xiong, Z., Kim, D.I., Shen, X., Letaief, K.B., 2024a. Generative ai for secure physical layer communications: A survey. IEEE Transactions on Cognitive Communications and Networking 11, 3–26.

[203] Zhao, M., Peng, H., Li, L., Ren, Y., 2024b. Multivariate time series anomaly detection based on spatial-temporal network and transformer in industrial internet of things. Computers, Materials & Continua 80, 2815–2837. doi:10.32604/cmc.2024.053765.

[204] Zhao, Y., Xu, Y., Xiao, Z., Jia, H., Hou, T., 2024c. Mobilediffusion: Instant text-to-image generation on mobile devices, in: European Conference on Computer Vision, pp. 225–242.

[205] Zheng, X., Liu, X., Bian, Y., Ma, X., Zhang, Y., Wang, J., Guo, J., Qin, H., 2024. Bidm: Pushing the limit of quantization for diffusion models, in: Advances in Neural Information Processing Systems.

[206] Zhu, G., Yu, Y., Li, Z., Dai, Y., 2026. Gmddpm-ct: Advancing network intrusion detection through diffusion-based sample synthesis and deep learning. ICT Express .

[207] Zolanvari, M., Teixeira, M.A., Jain, R., 2019. Effect of imbalanced datasets on security of industrial IoT using machine learning. doi:10.48550/arXiv.1912.02651, arXiv:1912.02651.

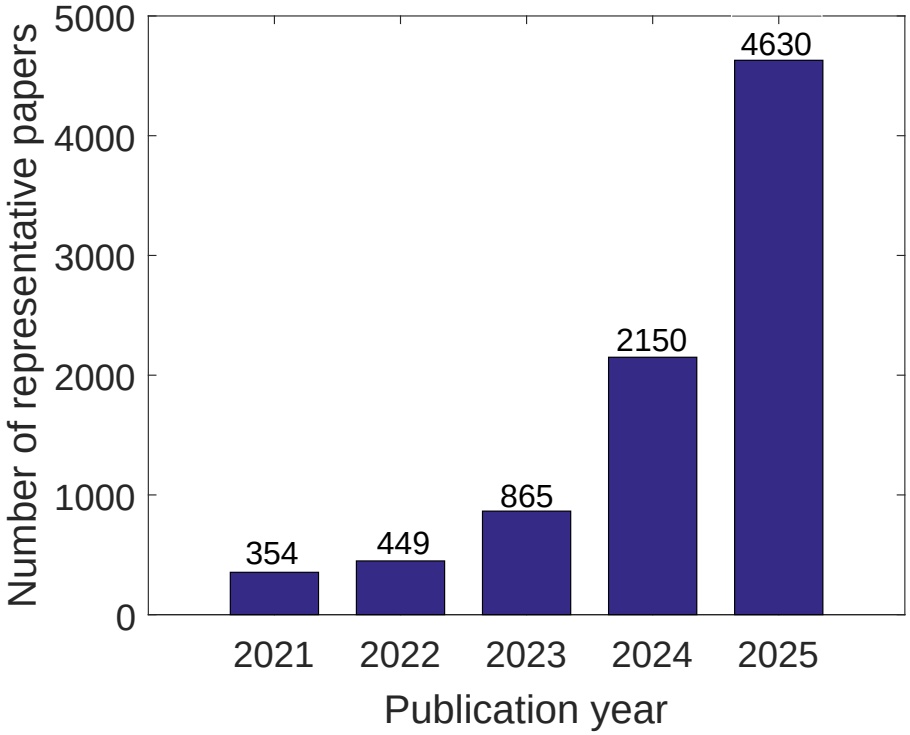

Figure 1: Publication trend of representative diffusion-model studies for IoT security from 2021 to 2025. The statistics were collected from Google Scholar using diffusion-model-related keywords combined with IoT security terms, followed by manual relevance screening.

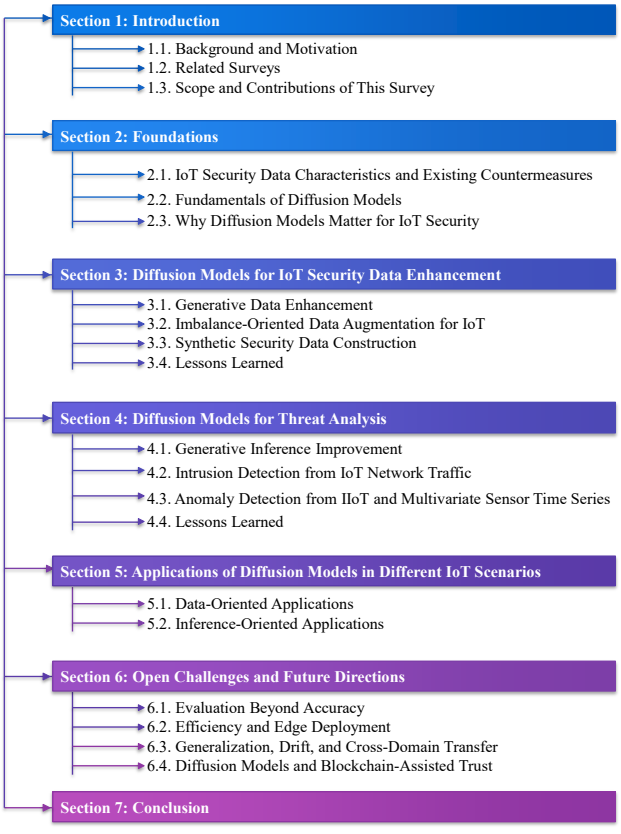

Figure 2: The main structure of the survey.

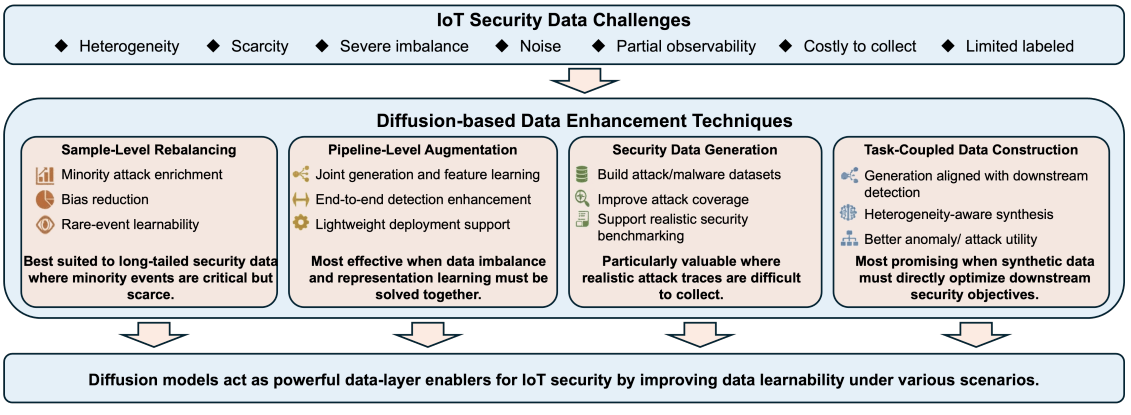

Figure 3: Overview of diffusion-based data enhancement for IoT security, showing the mapping from core data challenges to four types of diffusion-based enhancement techniques.

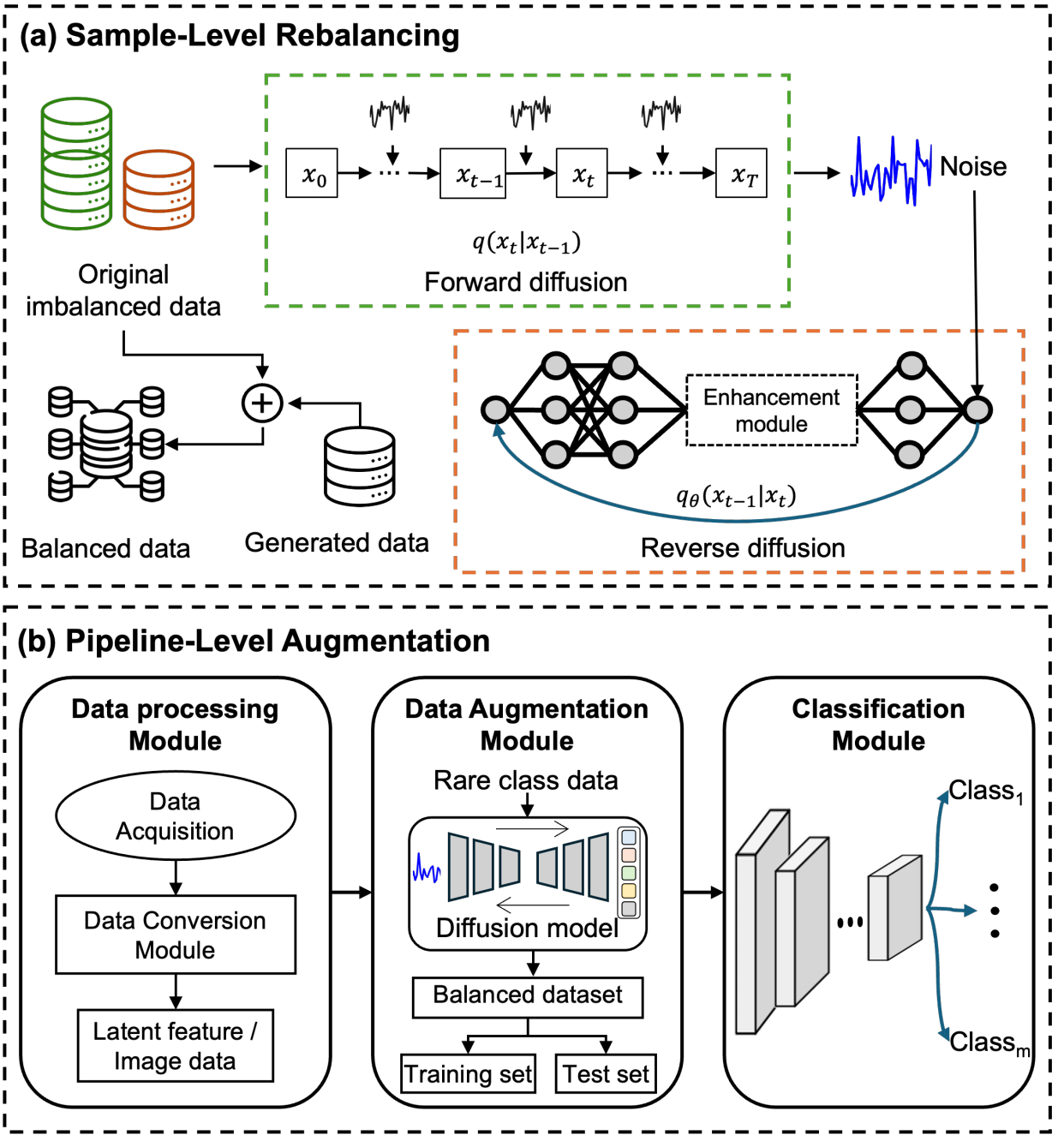

Figure 4: The process of imbalance-oriented data augmentation with diffusion models. Existing work can be classified into two types: (a) Sample-level rebalancing: This type focuses on generating high-quality data for rare classes through improved diffusion models. (b) Pipeline-level augmentation: This type integrates data processing, data augmentation and classification into a complete pipeline, focusing on concrete task performance.

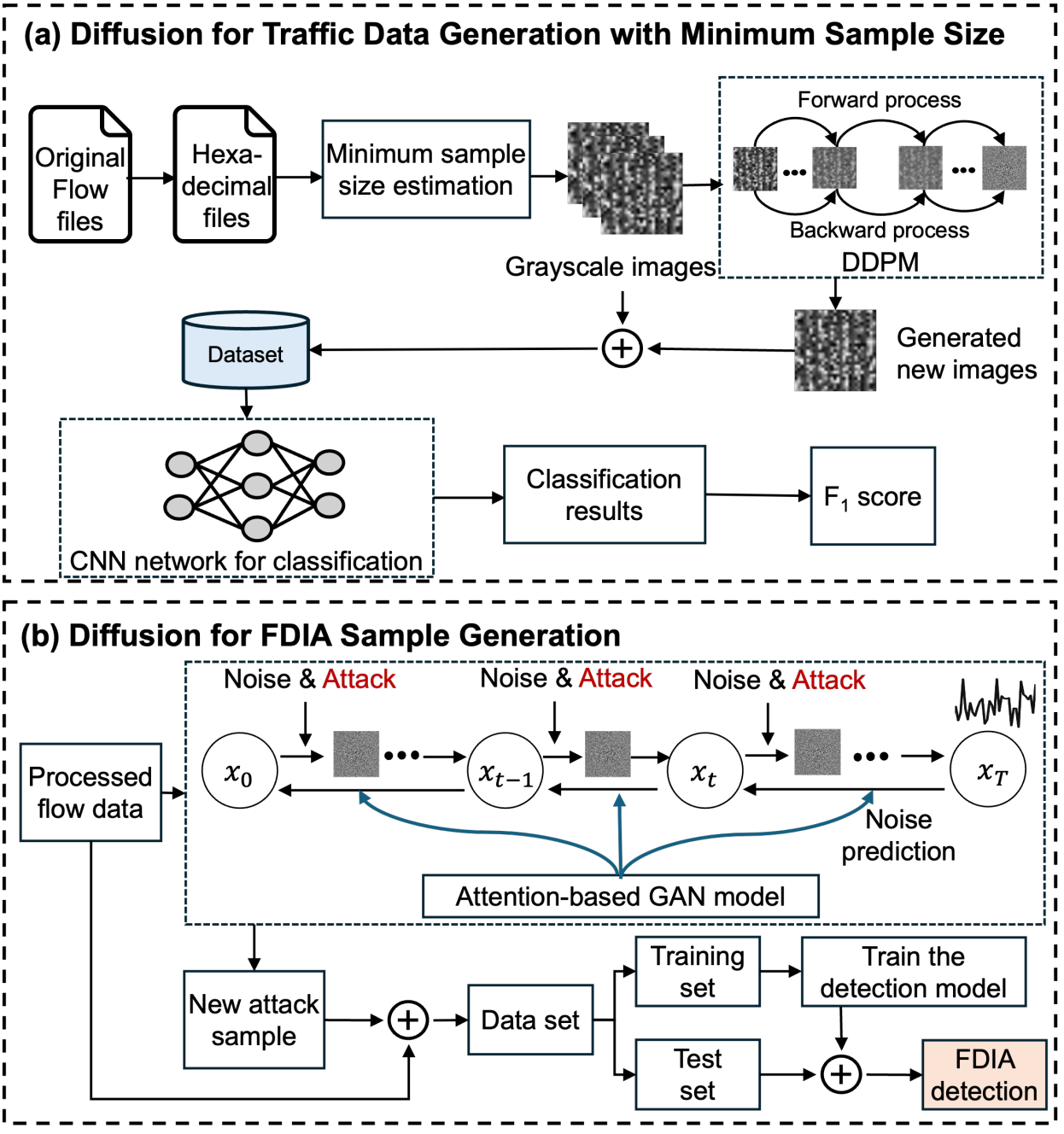

Figure 5: The diffusion-based synthetic security data construction methods. (a) A diffusion-based method proposed in [20] for traffic data generation with a minimum sample size. (b) A diffusion-based method proposed in [78] for FDIA sample generation in power cyber-physical systems.

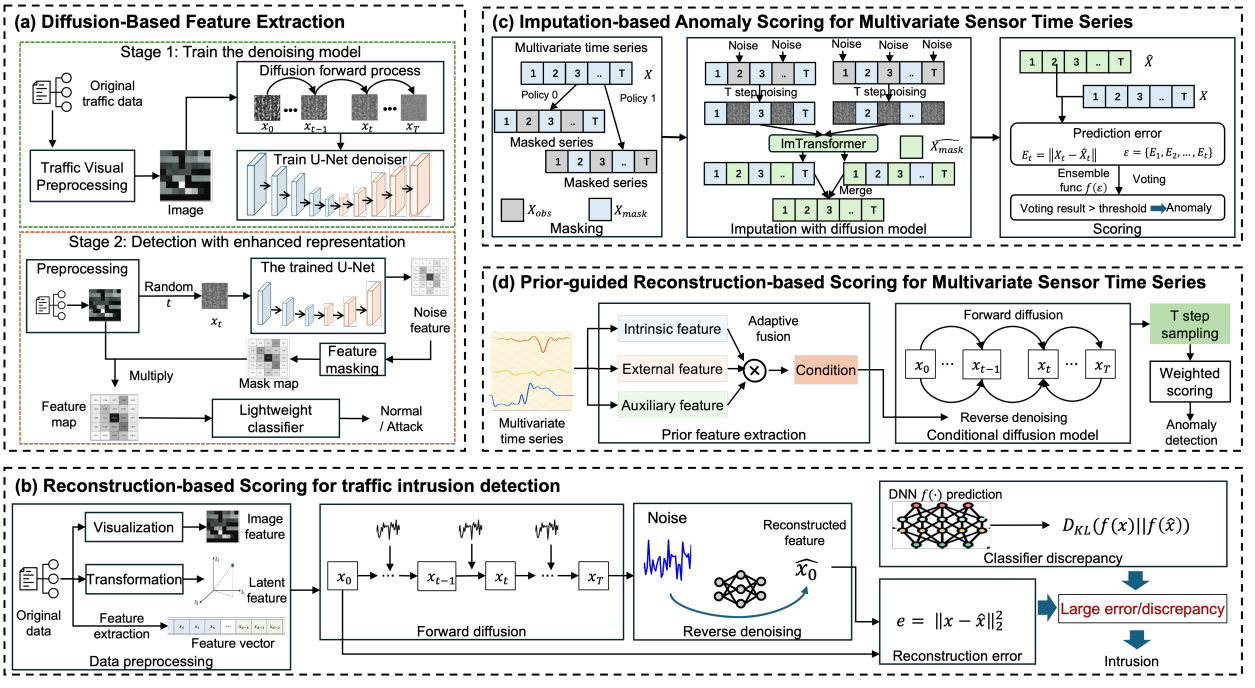

Figure 6: Overview of representative diffusion-based methods for IoT threat analysis. (a) illustrates diffusion-based feature extraction proposed in [184], where the preprocessed traffic feature is input to a diffusion model to obtain denoising-aware features for downstream intrusion detection. (b) presents the process of reconstruction-based intrusion detection methods in [158, 195], where traffic features are reconstructed through the reverse diffusion process and intrusions are identified from input-reconstruction discrepancies. (c) presents a representative imputation-based anomaly scoring method proposed in [28], where diffusion predicts masked observations and anomaly scores are derived from prediction errors between the original and imputed outputs. (d) presents a representative prior-guided reconstruction-based scoring method proposed in [164], where multi-level temporal features are adaptively fused as conditioning signals to guide the reverse diffusion process, and anomaly scores are derived from the weighted aggregation of multi-step reconstruction errors.

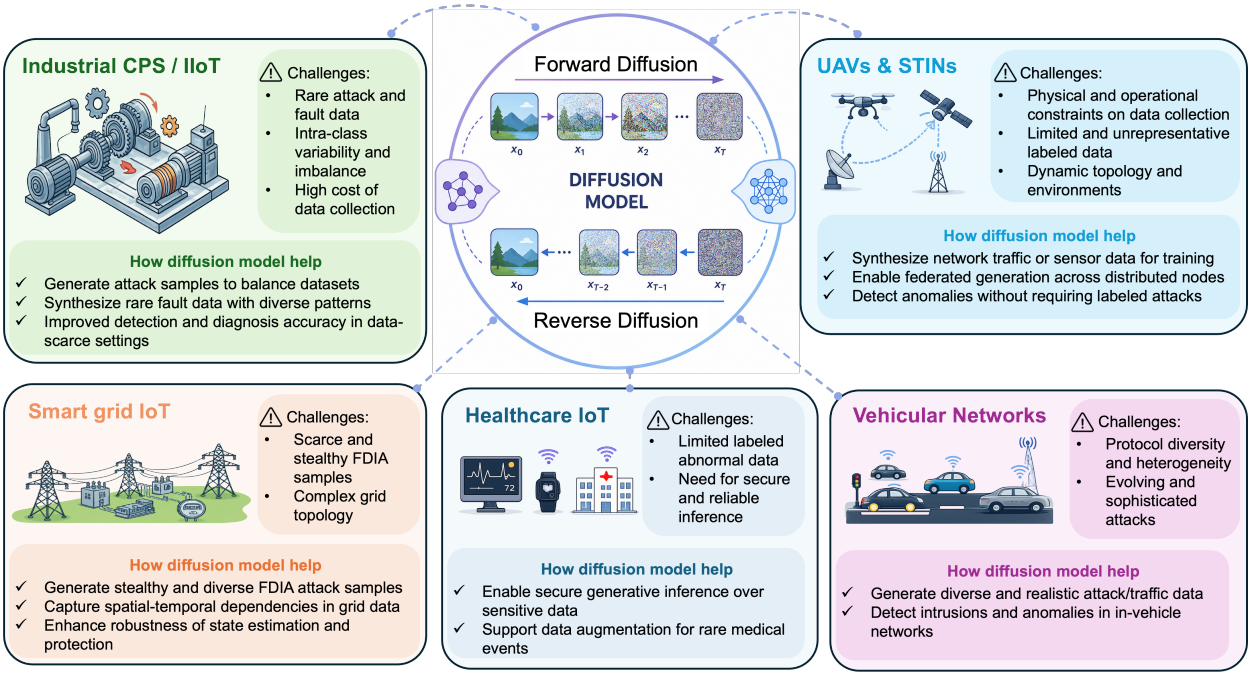

Figure 7: Applications of diffusion models in diverse IoT scenarios.