BILINGUAL PUBLISHING GROUP

Journal of Environmental & Earth Sciences

https://journals.bilpubgroup.com/index.php/jees

REVIEW

Environmental IoT under Attack: A Review of Adversarial Machine Learning in Monitoring Networks

***Hui Zeng* [1*], *Massudi Mahmuddin* [2]**

[1] *School of AI Engineering, Guangzhou College of Technology and Business, Guangzhou 510850, China*

[2] *School of Computing, Universiti Utara Malaysia, Sintok 06010, Malaysia*

ABSTRACT

Environmental Internet of Things (E-IoT) networks are also used in real-time air, water, soil, and ecological systems monitoring, which provides high-resolution data that is essential in environmental management and policy decision-making. When used in these networks, the implementation of machine learning (ML) will improve the predictive potential, anomaly detection, and automated decision-making. Nevertheless, the use of ML models brings with it additional security threats in the guise of adversarial machine learning (AML) attacks, which can alter the input to models, their training data, or parameters in order to trigger inaccurate predictions or to prevent the detection of events of interest. This review essentially offers a thorough analysis of E-IoT network AML threats, the distinct characteristics of resource-constrained, distributed, and dynamic environmental sensing environments. Along with the mechanisms, the attack surface, and the impacts that such attacks may have on monitoring reliability and decision-making, we classify AML attacks into evasion, poisoning, model extraction, and backdoor attacks. The review also provides a survey of defense techniques at data, model, and system levels, such as preprocessing, robust modeling, adversarial training, secure aggregation, and self-healing networks, and the advantages, weaknesses, and trade-offs of these techniques. Lastly, the challenges that are recognized as open include a lack of realistic datasets, coping with concept drift, resource limitations, and interdisciplinary research. Through the synthesis of existing information, this review will inform the development of resilient, safe, and reliable E-IoT networks

*CORRESPONDING AUTHOR:

Hui Zeng, School of AI Engineering, Guangzhou College of Technology and Business, Guangzhou 510850, China; Email: zh45669209@gmail.com

ARTICLE INFO

Received: 26 January 2026 | Revised: 27 February 2026 | Accepted: 8 March 2026 | Published Online: 12 June 2026

DOI: https://doi.org/10.30564/jees.v8i6.13235

CITATION

Zeng, H., Mahmuddin, M., 2026. Environmental IoT under Attack: A Review of Adversarial Machine Learning in Monitoring Networks. Journal of Environmental & Earth Sciences. 8(6): 89–103. DOI: https://doi.org/10.30564/jees.v8i6.13235

that will be able to support reliable environmental monitoring when subjected to adversarial attacks.
Keywords: Environmental IoT; Adversarial Machine Learning; Cybersecurity; Sensor Networks; Resilient Monitoring

1. Introduction

Environmental monitoring plays a significant role in comprehending, controlling, and reducing the impact of natural as well as human changes in the ecosystem[1,2]. As the world is increasingly focused on climate change, air and water pollution, loss of biodiversity, and management of natural disasters, timely and correct environmental data has become a necessity in scientific discovery, government policy, and industry. Conventional forms of environmental monitoring, typically relying on manual sampling and localized observation points, are proving to be inadequate in order to obtain the high-resolution and real-time data demanded in the contemporary environmental decision-making process. Environmental monitoring systems are uniquely sensitive to data integrity compared to other IoT domains such as healthcare or industrial automation. While errors in industrial IoT may result in economic losses and healthcare IoT failures affect individual patients, compromised environmental IoT (E-IoT) data can propagate across large spatial and temporal scales, influencing policy decisions, ecological management, and public safety. For instance, adversarial manipulation of air or water quality data may lead to flawed climate or environmental policies, while suppressed anomaly detection in wildfire or flood monitoring systems can delay disaster response with severe ecological and humanitarian consequences. Moreover, inaccurate environmental data may undermine public trust, distort regulatory compliance, and exacerbate long-term environmental degradation. These cascading impacts highlight that ensuring the integrity and robustness of E-IoT systems is not only a technical necessity but also a critical requirement for sustainable environmental governance and societal resilience[3].

The possibilities of E-IoT networks are enhanced even further through the introduction of machine learning (ML)[4]. Machine learning algorithms can be used to recognize patterns automatically, for predictive modelling, detect anomalies, and make decisions based on reports. As an example, ML models may forecast the distribution of air pollutants, determine early warning of forest fires, foresee the decline in water quality, or reveal abnormal ecological processes with little human intervention. Specifically, more sophisticated methods like deep learning and graph-based modeling enable the discovery of multifaceted spatio-temporal patterns of heterogeneous environmental data, whereas federated and edge-based learning methods can be used to train the model in a distributed manner without centralized data aggregation. These developments place ML-driven E-IoT as one of the foundations of intelligent environmental management to offer scientific knowledge as well as practical guidance to policymakers and industry stakeholders[5].

Nonetheless, the deployment of ML on a large scale in E-IoT networks also causes additional security and reliability issues. In contrast to traditional cybersecurity threats, where a threat to the hardware or network protocols is targeted, adversarial machine learning (AML) is a category of attack that is specifically aimed at taking advantage of the vulnerability in the ML models. Attackers may be able to modify the inputs, the training data, or the model parameters to ruin the system performance, cause false predictions, or deliver sensitive information. Such attacks may be devastating in the environmental monitoring field. To illustrate, minor changes in sensor measurements may trigger wrong pollution notifications, inability to alert about dangerous situations, like wildfires or floods, or imbalanced regulatory decisions. E-IoT systems are unique targets of adversarial interventions as a result of their combination of resource-constrained devices, distributed deployments, and changing environmental conditions[6].

The risks created by AML are complex[7–9]. Evasion attacks are designed to introduce precise manipulations to sensor data that induce misclassification of sensor inputs during inference time, which may deploy either false alarms or conceal important events in the environment. **Figure 1** illustrates the hierarchical structure of E-IoT networks, depicting sensor layers, edge devices, communication pathways, and cloud platforms, along with potential adversarial attack points. The attacks of poisoning are aimed at the training, and in that case, malicious data is inserted to control the model on a systematic basis. Model extraction, backdoor,

and Trojan attacks are other techniques used to attack the predictive models in order to replicate, bias, and/or control the model by using access to the model outputs or internal parameters. E-IoT systems are further vulnerable to them as they rely on distributed and often unattended devices, which are subjected to stringent energy and computational limits. **Table 1** summarizes the primary attack types and their mechanisms, along with the possible effects on environmental monitoring networks. Conventional defense systems designed to work with Information Technology (IT) or industrial systems might not be adequate or viable in this situation.

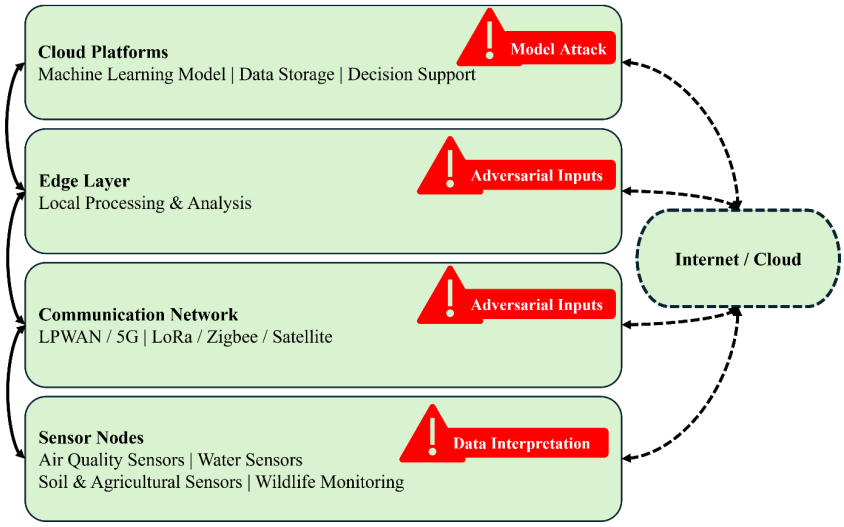

Figure 1. Hierarchical architecture of an environmental IoT network, including sensor nodes, edge devices, communication layers, and cloud platforms, with potential points of adversarial attack highlighted.

Table 1. Classification of adversarial machine learning attacks in environmental IoT networks, their target stages, mechanisms, examples, and potential impacts.

Attack Type	Target Stage	Mechanism	Example in Environmental Monitoring	Potential Impact
Evasion Attack	Inference	Perturbing sensor inputs to induce misclassification	Manipulating air quality sensor readings to trigger false safe air alerts	False alarms or missed events
Poisoning Attack	Training	Injecting malicious data into training sets	Altering water quality training data to mask high contamination	Model learns biased patterns
Model Extraction	Deployed Model	Systematic queries to reconstruct model parameters	Reconstructing wildfire prediction model for adversarial input crafting	Intellectual property theft, targeted attacks
Backdoor/Trojan	Training/Retraining	Embedding hidden triggers that activate under specific conditions	Introducing latent trigger in soil moisture model to suppress anomaly detection	Delayed or suppressed hazard alerts

In spite of the increasing awareness of adversarial threats, the study of AML in environmental IoT networks is still not unified. The current literature can be divided into general-purpose IoT security, sensor-specific or isolated ML models, with little regard to the environmental monitoring systems' peculiarities. The environmental data is generally very noisy, sparse, and highly correlated both in space and time, which creates opportunities as well as challenges to adversarial attacks. In addition, practical E-IoT implementations demand robust, energy-saving, and long-lasting models, and the construction and assessment of AML defenses are especially sophisticated. Having a detailed knowledge of the vulnerabilities, attack procedures, defense measures, and unresolved issues in this sector will be the key to obtaining robust environmental monitoring systems [10].

The main aim of the review is to make a systematic and integrative review of adversarial machine learning in environmental IoT networks. In particular, this article will (i) provide an overview of the architecture and data nature of E-IoT systems, (ii) categorize and discuss the range of AML threats applicable to environmental monitoring, (iii) examine the existing defense mechanisms on the data, model,

and system levels, and (iv) address the gaps in the existing research and prospects. This review aims to inform researchers and practitioners about the weaknesses and remedies of ML-enabled environmental monitoring by synthesizing existing knowledge, and such a synthesis can eventually result in the design of safer and more reliable E-IoT systems[11–13].

Besides being technically important, the insights of AML in the context of environmental IoT have a general societal and policy impact[14]. Regulatory compliance, public health advice, management of resources, and disaster response are based on accurate and reliable environmental data. E-IoT network vulnerabilities do not just affect the scientific credibility but also create potential risks to citizens and their relationship to the environment. Thus, the introduction of adversarial resilience into the E-IoT systems is not a technical issue; it is a condition for the responsible environmental regulations in the age of intelligent sensing and predictive analytics.

To conclude, environmental IoT and machine learning convergence have never presented such opportunities as they do now in terms of real-time, data-driven environmental monitoring[15,16]. However, this pivotal convergence also poses new risks to security with adversarial machine learning, which may jeopardize the integrity and safety of harsh monitoring systems. Figuring out the current level of research in environmental IoT on AML, categorizing types of attacks, exploring defense solutions, and outlining unresolved problems, this article is intended to serve as a reference point when developing a system of effective, reliable, and efficient environmental monitoring networks. The next sections describe the structure of E-IoT systems and the specifics of environmental data, analyze adversarial threats and defenses, and comment on up-and-coming challenges and future research directions, and finally assess adversarial resilience in environmental monitoring.

2. Environmental IoT Monitoring Networks and Machine Learning

The latest environmental monitoring is led by the Environmental Internet of Things (E-IoT) systems that have high-resolution and continuous observation capabilities superior to the conventional approaches of manual or station-based monitoring[17]. Such systems combine a variety of sensors, edge devices, communication networks, and cloud computing to gather, process, and analyze real-time environmental data. Machine learning (ML) adoption also promotes the functionality of such networks to allow them to predict analytics, detect anomalies, and make decisions automatically. It is in this section that the types of E-IoT architecture, how machine learning can be used in environmental monitoring, and the peculiarities of environmental data that define the design and security of the ML-based monitoring system are described in detail.

2.1. Architecture of Environmental IoT Networks

E-IoT systems are generally hierarchical in structure, and the needs of distributed sensing, data gathering, and computational efficiency[18]. On the bottom level, sensor nodes are being used to measure environmental parameters such as temperature, humidity, air pollutants, water quality indicators, soil moisture, or wildlife movement. Limited power, processing power, and storage of these sensors can often limit these sensors, which requires effective data gathering and local processing. Depending on the scale of deployment and the need to transmit data, sensor nodes are typically connected by wireless communication protocols, such as low-power wide-area network (LPWAN), Zigbee, LoRa, or cellular Internet of Things.

Edge devices or gateways are located above the sensor layer to aggregate and preprocess sensor data and pass it on to cloud servers or centralized platforms[19]. In E-IoT, edge computing can be incredibly useful in minimizing latency, conserving bandwidth, and performing initial analytical inspection. Cloud platforms at the highest tier offer comprehensive storage, multifaceted computing, and analytical services. Such systems have machine learning models that run on aggregate data across a range of sensors, and facilitate predictive information, trend analysis, and decision support. The multi-layered architecture enables E-IoT systems to work effectively in heterogeneous environments of large scale and also enables the adaptive and intelligent monitoring of the environment. **Table 2** gives the general overview of the main elements of E-IoT networks, reflects their functionality, some of the technologies they represent, and discloses the vulnerabilities that could be used by adversarial machine learning.

Table 2. Components of environmental IoT systems, their functions, examples, and potential vulnerabilities to adversarial machine learning.

Component	Function	Examples/Technologies	Vulnerabilities Related to AML
Sensor Nodes	Collect environmental data (temperature, humidity, pollutants, etc.)	Air quality sensors, water probes, soil moisture sensors	Input manipulation, spoofing, noise injection
Edge Devices	Aggregate, preprocess data, perform local computations	Gateways, microcontrollers, edge servers	Limited computational resources, susceptible to poisoned updates
Communication Layer	Transmit data between sensors, edge, and cloud	LPWAN, LoRa, Zigbee, Cellular IoT	Data interception, adversarial perturbation during transmission
Cloud Platforms	Central storage, high-performance computation, ML model hosting	Amazon Web Services (AWS) IoT, Azure IoT, Google Cloud IoT	Model extraction, backdoor injection, poisoning during retraining

2.2. Machine Learning in Environmental Monitoring

Machine learning has played a crucial role in E-IoT networks to convert raw sensor readings into actionable data. Environmental monitoring has a great variety of ML methods, including not only classical regression and classification models but also more sophisticated deep learning and graph-based methods. Continuous prediction is usually performed with the help of regression models, e.g., predicting the level of pollutants in the air, the rate of water flow, or the content of soil with nutrients. Some commonly used classification models, such as support vector machines and random forests, are used to identify anomalies or classify environmental events, such as classifying normal and hazardous levels of air quality [20].

Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are deep learning models that are more effective when modeling complex spatio-temporal patterns that exist in environmental data [21,22]. Graph neural networks (GNNs) have been used more often to learn relational and topological dependencies between sensor nodes in a network, including interactions between spatially distributed measurement points. Federated learning is also becoming a promising method of distributed environmental monitoring that enables ML models to be learned on a large population of edge devices without the need for a centralized system of data collection, which increases the level of data privacy and saves on the costs of transmissions. Together, these machine learning methods can make the E-IoT systems predict, detect anomalies, and warn about possible dangers in real-time and analyze the tendencies in the environment over the long term.

2.3. Characteristics of Environmental Data

The environmental data have their peculiarities that characterize them during comparison with other datasets within IoT and shape both the design and security of machine learning models. Noise and variability, which are caused by sensor imprecision, environmental noise, or missing measurements, are one of the distinguishing characteristics. The other important attribute is spatio-temporal correlation, which is an expression of the interdependence of environmental phenomena over space and time, e.g., the distribution of pollutants in air or water networks. The presence of these correlations makes environmental data very informative yet difficult to model because the traditional assumptions of independent and identically distributed (i.i.d.) data are frequently not true [23,24].

Cleaning environmental data also suffers from the issue of sparsity and missing values, especially in remote or unfavorable environments where sensor malfunction or loss of communication is the norm. Also, the processes of the environment tend to have concept drift, with the underlying patterns changing over time with seasonal variations, climate variations, or human actions. The machine learning models implemented in E-IoT networks should thus be adaptive, resilient to noise, and should also be able to withstand dynamic distributions. Behavior, being high-dimensional, heterogeneous, and temporally changing data simultaneously, presents both attacker possibilities to perform complex analysis and the possibility of adversarial manipulation, where minor perturbations have disproportionate effects on model predictions [25,26].

These distinctive characteristics of environmental data have direct implications for adversarial machine learning vulnerabilities. High noise levels and natural variability can obscure adversarial perturbations, making evasion attacks more difficult to detect while allowing attackers to embed malicious signals within normal fluctuations. Data sparsity and missing observations, which are common in remote sensing environments, can significantly increase the effectiveness of

poisoning attacks, as even a small number of manipulated samples may disproportionately influence model training and bias learned patterns. Furthermore, strong spatio-temporal correlations, while useful for improving predictive accuracy, may also enable adversarial effects to propagate across interconnected sensors, amplifying the impact of localized attacks and complicating detection. At the same time, these correlations can be leveraged defensively through cross-validation and anomaly detection across neighboring nodes. Finally, concept drift in environmental systems creates opportunities for adversaries to exploit outdated models, introducing perturbations that align with shifting data distributions and evade detection. Understanding these interactions is essential for designing robust AML defenses tailored to environmental monitoring contexts.

2.4. Security Implications of Machine Learning in E-IoT

Although the incorporation of ML into E-IoT networks has tremendous benefits in terms of analytics, it also brings emerging security issues. In contrast to the more conventional cyber threats, which are focused on network protocols, devices, or data integrity, adversarial machine learning attacks make use of the vulnerabilities within predictive models in particular. Such attacks are more likely to have an impact because of the dependence on ML models to make important environmental monitoring choices. Adversarial perturbations can be amplified by sensor noise, spatio-temporal correlations, and distributed data collection in a manner that is hard to detect and reduce. Also, edge devices and gateways tend to have a very restrictive resource budget, preventing them from being able to support computationally expensive defenses like adversarial training or model testing [27,28]. Therefore, it is important to have knowledge of the architecture, data, and ML usage of E-IoT networks to be able to evaluate the weaknesses of the system and establish protection mechanisms, which will be discussed later in this review.

3. Adversarial Machine Learning Threats in Environmental IoT

By introducing machine learning capabilities to environmental IoT (E-IoT) networks, there has been an impressive set of predictive and analytical power, but it has also opened the systems to a range of adversarial threats [4,29]. Adversarial machine learning (AML) attacks are not directed at communication protocols or physical devices, in contrast to conventional attacks, which focus on the behavior of prediction models. Such attacks may undermine the credibility of environmental surveillance, mislead important decision-making, and, worse still, put the safety of the population or environmental management in danger. This section offers a broad description of the nature of AML attacks applicable to E-IoT, how they are executed, on what components they impact, and what their impact could be on the environmental monitoring systems.

3.1. Taxonomy of Adversarial Attacks

Adversarial attacks in E-IoT may be generally classified into evasion attacks, poisoning attacks, model extraction attacks, and backdoor or Trojan attacks, whereby each is based on a different aspect of the ML lifecycle. Various attacks, such as evasion attacks, are attacks that happen during the inference phase, and an attacker intentionally manipulates the input data to cause misclassification or prediction errors. In environmental surveillance, it may mean the manipulation of sensor outputs to conceal high levels of pollutants, or creating a false alarm of some natural threat, e.g., flooding or wildfires. The attacks can be very nuanced and utilize small perturbations that are within sensor limits and are therefore hard to notice but have disproportionately large impacts on model outputs [30,31].

These attacks are aimed at the machine learning model teaching. In these attacks, the attackers introduce the training set with well-designed malicious data, which makes the model learn biased or malicious patterns. As an illustration, when an ML model is trained to identify an anomaly in water quality, the training data might be poisoned, which would make the model desensitized to a high level of contaminants and thus fail to alert to the issue and cause ecological damage. The problem of poisoning attacks is of particular concern to federated/distributed learning settings, where the outputs of several nodes are combined, and are more likely to be impacted by a malicious one [32].

Model extraction and inference attacks enable the attackers to rebuild or estimate proprietary models by presenting system queries in a systematic way. After an attacker is

aware of the framework or parameters of the model, it is a bit simpler to develop specific adversarial inputs. These attacks are not only a danger to the integrity of the system but to intellectual property as well, especially when using commercially deployed predictive models within an environmental monitoring context[33].

Lastly, backdoor attacks or Trojan attacks are those that entail inserting concealed triggers in the model when training it, which may later be triggered to induce certain erroneous responses. When applied to E-IoT, an attacker may place a latent vulnerability in a system that can be exploited under a specific environmental condition, or data pattern, to cause misclassification or suppressed detection of important events. These attacks are very strong in that they tend to be dormant as they are usually checked in the normal course of validation and only appear in certain situations, and are very difficult to identify and prevent[34].

3.2. Attack Surfaces in E-IoT Systems

There are several vulnerabilities to AML attacks in the lifecycle of an E-IoT system, including the data collection phase, all the way to the model deployment. Compromised or spoofed sensors may feed the ML model with altered data during the data collection phase, which amounts to evasion attacks on the source. During transmission, rivals can intercept or modify data packets to cause adversarial perturbation, either with the aid of weak encryption or insecure communication protocols. Poisoning attacks are also specifically vulnerable to the training phase, and are especially common in federated learning or in collaborative sensing networks, where the data is collected by many, potentially untrusted, sources. Evasion attacks take advantage of the weaknesses of the deployed ML model to generate erroneous predictions during real-time inference during model inference. Lastly, during model update/retraining, attackers can corrupt incremental learning operations, continuing to propagate past unnoticed vulnerabilities/backdoors. The interchangeability of such attack surfaces highlights the challenge of maintaining ML-enabled environmental monitoring networks[32,35–37].

3.3. Case Studies in Environmental Monitoring

Several studies have demonstrated the practical risks of AML in environmental contexts. For instance, adversarial perturbations in air quality monitoring systems have been shown to induce misclassification of pollution levels, potentially resulting in false safety alerts or regulatory noncompliance. In water quality monitoring networks, data poisoning experiments have illustrated how biased training sets can prevent detection of high contaminant concentrations. Similarly, wildfire detection systems relying on distributed sensors and ML-based prediction models are vulnerable to both evasion and poisoning attacks, which can delay critical alerts and exacerbate ecological and human damage. These examples highlight that even small-scale perturbations or carefully timed attacks can have outsized consequences due to the reliance on automated, ML-driven decision-making in environmental monitoring[38–40].

3.4. Impacts and Implications

AML attacks in E-IoT networks go beyond technical failures. Inaccurate forecasts may jeopardize the quality of environmental information, destroy the credibility of people, and lead to poorly informed policy choices[41]. Adversarial attacks can lead to a delay in responding or even cause unsuitable interventions in a safety-related situation, like flood warnings, wildfire alerts, or detecting hazardous emissions, which are dangerous to human lives, wildlife, and ecosystem conditions. Furthermore, the spread and resource-limited nature of most E-IoT systems increase the challenge in tracking and deterring adversarial behavior, as nodes may act independently with little processing power to conduct effective anomaly detection or verification.

AML threats in E-IoT are very insidious, especially because of high-impact consequences, a variety of attack surfaces, and limited resources[42]. Knowing these vulnerabilities is a requirement to create an effective defense mechanism, and this will be addressed in the following section. The systematic taxonomy of types of attacks, their mechanisms, and practical consequences will help researchers and system designers to devise specific approaches that increase the resilience of environmental monitoring networks.

4. Defense Mechanisms and Resilience Strategies

The identification of the adversarial machine learning (AML) threat to environmental IoT (E-IoT) networks has

led to the emergence of a variety of defense mechanisms that should enhance the resilience of the system [43]. These defenses are created in response to vulnerabilities in machine learning models, the training data, and deployment settings, unlike traditional cybersecurity measures. Plausible defense solutions need to take into account the peculiarities of the E-IoT, such as resource-constrained sensor nodes, heterogeneous deployment, spatio-temporal relationships, and the necessity to have reliable environmental information. It is an exhaustive background of the defense mechanisms in the form of data-level, model-level, and system-level strategies and how the data-level, model-level, and system-level defense mechanisms have been applied, limited, and compromised in the case of environmental monitoring.

4.1. Data-Level Defenses

Data-level security is aimed at improving the quality and resilience of data coming to machine learning models. A central method is data preprocessing, which is designed to eliminate noise, normalize inputs, and identify anomalies prior to reaching the model [44]. Statistics outlier detection methods, smoothing filters, sensor fusion, and more can be used to reduce the effects of corrupted or perturbed sensor measurements to make evasion attacks less effective. Also, the use of redundancy in sensor placement and cross-checking with a number of nodes can be used to determine discrepancies that are signatures of adversarial manipulation.

The other strategy that is important is robust data augmentation, whereby the models are trained on varied and representative data that mimics possible perturbations or anomalies [45]. The model is also made less susceptible to small, malignant alterations in sensor readings through exposing models to a broader spectrum of variations in inputs, including adversarial examples that can be synthetically generated. Additionally, data aggregation techniques, which are secure especially in federated or distributed learning, can minimize the threat of poisoning attacks through weights or filtering of contributions made by possibly untrusted sources. The data-level defenses are necessary, but they need to be well-tuned to ensure the balance between the high level of robustness and the limitations on computational power and real-time performance in E-IoT networks.

4.2. Model-Level Defenses

The model-level defenses intend to improve the inherent resistance of the machine learning algorithms to adversarial attacks [46]. Adversarial training is one of those commonly used methods, as models are directly trained on clean and adversarial perturbed samples. This exposure enables the model to gain decision boundaries that are not sensitive to small perturbations, hence reducing exposure to evasion attacks. Additional approaches are good architecture design, i.e., ensemble models, dropout regularization, or special-purpose layers that make adversarial inputs more difficult to be effective.

Estimation of uncertainty and confidence calibration are also essential aspects of model-level defenses [47]. Bayesian neural networks or Monte Carlo dropout technology can be employed to compute prediction uncertainty in models to indicate problematic input or abnormal structure. E-IoT systems can avoid such erroneous decisions made due to adversarial perturbation by labeling low-confidence predictions to be further verified or to be handled by humans. Nevertheless, they can add computational demands, which is a vital factor with edge-deployed models with a constrained energy budget.

4.3. System-Level Defenses

System-level defenses consider the larger network structure and protocols to be more resilient to AML attacks [42]. Federated learning can be securely aggregated using secure aggregation protocols, where malicious nodes are not allowed to affect the changes in the model to make collaborative training resistant to poisoning attacks. Likewise, multiple node redundancy and cross-validation can be used to identify anomalies due to localized adversarial manipulation, and adaptive sampling and dynamic sensor selection can be used to decrease the exposure to compromised nodes.

Moreover, system-level monitoring and anomaly detection frameworks may offer real-time monitoring of both the network activity and data trends as well as model behavior [48]. These frameworks usually integrate statistical analysis, time pattern identification, and domain information to identify anomalies that are signs of AML attacks. E-IoT systems can automatically adjust their sensing, data

routing, or model parameters based on the observed attacks through advanced strategies, e.g., self-healing networks, and thus increase their resilience without the need to adjust them manually.

System-level defenses have to trade off security against practical deployment as well as communication, energy, and real-time operational constraints. In very big or distant E-IoT networks, the capacity to introduce lightweight, distributed, and dynamic defense systems is vital in safeguarding not just the security but also the dependability of environmental surveillance[49].

4.4. Trade-Offs and Evaluation Challenges

Although the data, model, and system-level protections offer several tiers of defenses, their application on the E-IoT networks is associated with trade-offs. Indicatively, model resilience can be enhanced through strong preprocessing or adversarial training, but at the expense of higher computational cost, energy use, and latency[50]. Likewise, system-level redundancy has better detection but must add sensors and bandwidth, which might not be possible in resource-constrained deployments.

The assessment of the effectiveness of AML defences in E-IoT is a special problem as well[51]. The above defense mechanisms have been summarized in **Table 3**, and their strengths, weaknesses, and suitability in various E-IoT deployment scenarios have been noted. Environmental data are generally noisy, sparse, and highly correlated, which makes it difficult to measure model robustness. In addition, there are few realistic threat models and benchmarking data sets used in the environmental applications, and it is hard to measure the performance of defenses in the real attack environment. Nevertheless, the multi-level defences, properly adjusted according to the specifics of the E-IoT network, continue to be the most promising with regard to increasing the degree of adversarial resilience.

Table 3. Defense strategies for mitigating adversarial machine learning threats in E-IoT networks, classified by data, model, and system levels, with pros and limitations.

Defense Level	Strategy/Method	Description	Pros	Cons/Limitations
Data-Level	Preprocessing/Filtering	Remove noise, detect anomalies before feeding to ML models	Simple, low computational cost	May not detect sophisticated adversarial perturbations
Data-Level	Robust Data Augmentation	Train on adversarial or varied datasets	Improves model generalization	Requires careful calibration, extra training
Model-Level	Adversarial Training	Train model with adversarial examples	Directly improves robustness	Computationally expensive, increases latency
Model-Level	Uncertainty Estimation	Quantify prediction confidence to detect suspicious inputs	Helps flag potential attacks	Requires additional computational resources
System-Level	Secure Aggregation/Federated Learning	Reduce influence of compromised nodes in distributed learning	Enhances collaborative security	Communication overhead, complexity
System-Level	Self-Healing Networks	Reconfigure sensing, routing, or computation in response to detected attacks	Enables continuous resilience	Complex implementation, resource-intensive

5. Open Challenges and Future Directions

Although the threats of adversarial machine learning (AML) in environmental IoT (E-IoT) networks have been studied and mitigated to a large extent, there are still many obstacles that prevent the implementation of completely resilient systems. Exceptional features of environmental surveillance, such as decentralized and resource-limited deployments, spatio-temporal associations in information, and the fundamental importance of precise forecasting, pose difficulties in both technical and operational aspects[42]. The given section dwells upon the key open issues of AML in E-IoT and provides some possible future research directions, with references to the intersections of security, machine learning, and environmental science.

5.1. Lack of Realistic Datasets and Threat Models

The lack of realistic data that is representative of the environment, sensor noises, and adversarial conditions has become one of the most problematic issues in the development of AML studies concerning E-IoT[52]. The majority of publicly available data sets are either those that are not so large in number, do not have enough time resolution, or

do not contain examples of adversarial manipulation. This is a weakness in building and benchmarking solid models since it is not always possible to simulate attacks that are entirely applicable in the real world. Likewise, current threat modeling methods tend to rely on simplistic assumptions about attack methods and not take into account the complexities of how adversarial inputs, spatio-temporal relationships, and distributed sensing interact. To test the attacks and defenses in an environment that is similar to the conditions that are encountered in real environmental monitoring deployments, high-fidelity datasets and all-inclusive threat models are necessary.

5.2. Resource Constraints and Scalability

IoT networks in the environment are typically deployed in remote or harsh environments with severe power, computing, and communication constraints [53]. It can be computationally expensive and energy-consuming to implement powerful defenses, e.g., adversarial training, uncertainty estimation, or continuous anomaly detection. The challenge of balancing security and operational effectiveness is recurring, especially when a network is expanded to the level of thousands of sensors or a broad geographical area. Future studies should involve the development of lightweight, distributed, and adaptive defense features that are resilient without violating E-IoT infrastructural limitations. Space Unless the network is linear or acts as a complete system, edge-based algorithms, federated learning, and energy-aware algorithms are all potentially promising directions to resolve these challenges.

5.3. Handling Concept Drift and Environmental Dynamics

The environmental processes are dynamic in nature and have a seasonal variation, climatic change effects, and human-made disturbances. Such changes may cause concept drift, where the statistical characteristics of the environmental data change over time, and this may affect the performance of the machine learning models [54]. Opponents can use concept drift to unleash attacks that are not noticed by models that are trained on old data. A major research problem is to design models that can adapt to the changing environmental conditions and be resilient to adversarial perturbations. The factors that should be explored in the future include incremental learning, continual learning, and self-adaptive model architectures.

5.4. Integration of Trustworthy AI and Self-Healing Systems

With the growing impact that E-IoT networks have on policy and the decisions of people regarding their safety, the integration of the principles of reliable Artificial Intelligence (AI) becomes necessary [55]. This is in the form of ensuring that there is transparency, interpretability, fairness, and accountability in model predictions. These principles, along with adversarial resilience, can be used together to increase confidence in the outputs of environmental monitoring and help with regulatory compliance. In addition, self-healing systems, which identify, isolate, and neutralize compromised nodes or corrupted data streams, are also a promising direction for enhancing operational resilience. These systems would be able to automatically reconfigure sensing, computation, and communication pathways to keep them functioning reliably against constant attacks.

5.5. Interdisciplinary Research Opportunities

The overlap between the fields of environmental science, IoT infrastructure, and cybersecurity makes interdisciplinary research necessary [56,57]. The development of AML defenses needs the knowledge of domain specialists to interpret phenomena in the environment, sensor constraints, and the decisive thresholds of intervention. Cooperation between computer scientists, ecologists, environmental engineers, and policymakers can result in more credible threat models, more effective metrics of evaluation, and useful mitigation measures. Moreover, regulatory and policy frameworks that include AML strength under environmental monitoring standards may provide an incentive to implement strong and reliable systems.

5.6. Future Research Directions

The next generation of AML in E-IoT research ought to focus on the creation of standardized, realistic datasets and benchmarks that mirror the issues of real monitoring of the environment [54]. **Figure 2** illustrates the key open challenges in AML for E-IoT networks and maps potential research directions to address these gaps. Addressing scalability and

resource constraints requires lightweight, adaptable, and distributed defense systems. Long-term resilience will require models that can continuously learn their environment, which is dynamic and which have system-level self-healing and trust-enhancing capabilities. Lastly, an interdisciplinary solution combining cybersecurity, environmental monitoring, and regulatory aspects will offer a comprehensive model for constructing secure and reliable E-IoT networks that are able to meet scientific, industrial, and societal demands. A systematic overview of current research gaps and how they relate to E-IoT networks, as well as future research opportunities, is tabulated in **Table 4**.

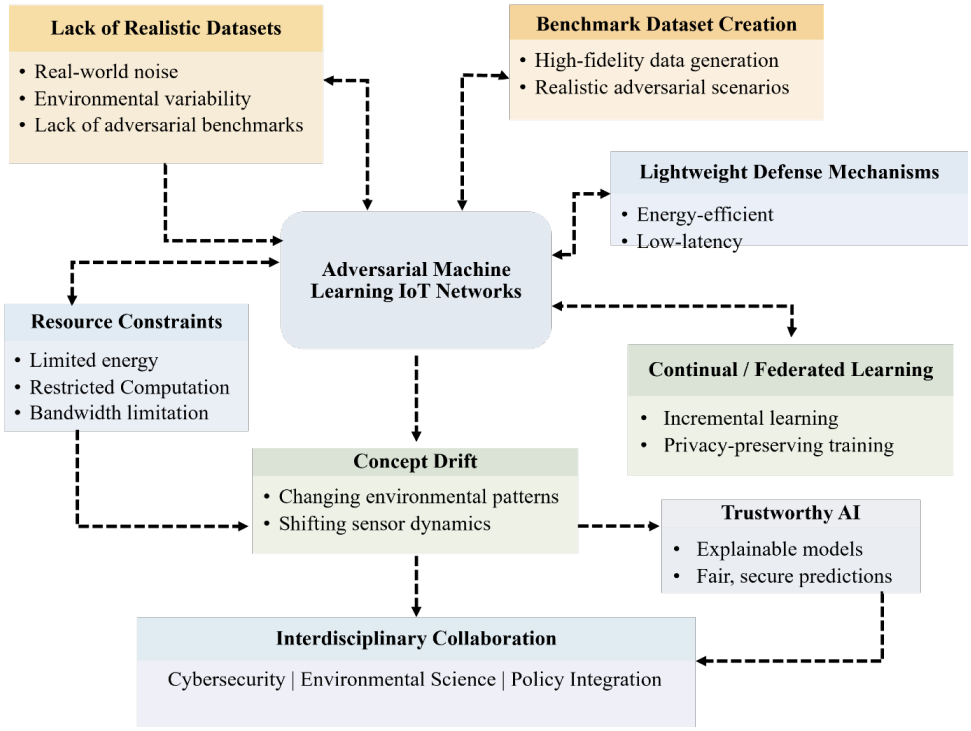

Figure 2. Conceptual roadmap of open challenges and future research directions for adversarial machine learning in environmental IoT networks.

Table 4. Open challenges in adversarial machine learning for environmental IoT networks, their implications, and potential research directions.

Challenge/Gap	Description	Implications for E-IoT	Potential Research Directions
Lack of Realistic Datasets	Few datasets capture sensor noise, environmental variation, and adversarial scenarios	Limits evaluation of defenses	Develop high-fidelity, benchmark datasets
Resource Constraints	Edge devices have limited energy, computation, and communication capacity	Limits feasibility of robust defenses	Lightweight, adaptive, distributed defenses
Concept Drift and Environmental Dynamics	Environmental conditions evolve over time, affecting model performance	Vulnerability to attacks exploiting outdated models	Incremental/continual learning methods
Integration of Trustworthy AI	Need for interpretable, fair, and accountable ML predictions	Supports regulatory compliance and public trust	Design explainable and trustworthy ML systems
Interdisciplinary Collaboration	Cybersecurity, environmental science, and policy knowledge often siloed	Limits holistic solutions	Promote interdisciplinary frameworks and standards

6. Conclusion

E-IoT networks, which are driven by machine learning, are a paradigm of monitoring and controlling the intricate environmental processes. These systems deliver new capabilities of real-time, high-resolution data collection, predictive analysis, and automated decision support and have been used in applications such as pollution monitoring and water quality management, wildfire detection, and climate research. Nonetheless, the implementation of machine learning on

such networks brings another category of threats called adversarial machine learning (AML) that fail the predictive models instead of conventional network or hardware objects.

The given review has offered an in-depth analysis of the latest situation in AML of environmental IoT networks. Section 2 described the design of E-IoT systems, with a special focus on the hierarchy of sensors, edge devices, and cloud platforms, along with the specific nature of the environmental data, such as noise, sparsity, spatio-temporal correlations, and concept drift. Section 3 analyzed the adversarial threat taxonomy, such as evasion, poisoning, model extraction, and backdoor attacks, and discussed their possible effect on the reliability, accuracy, and safety of environmental monitoring. Section 4 has covered defense mechanisms and system resilience strategies at data, model, and system levels, including methods like preprocessing, robust modeling, adversarial training, secure aggregation, and self-healing architectures. Section 5 emphasized unresolved issues and future research, such as the lack of realistic data, resource-related limitations, environmental dynamics, and interdisciplinary and trust-based solutions. The provided evidence indicates that the need to introduce adversarial resilience in the design and functioning of E-IoT networks is crucially important. Devoid of proper protection, adversarial attacks may undermine not just the accuracy of environmental forecasts but also the credibility of the policy choices, actions to protect the population, and ecological management efforts as well. To ensure that these networks are robust enough to work in the conditions of the environment and in the face of changing adversaries, the light-weight, adaptive, and distributed defense strategies, based on continuous learning and self-healing mechanisms, have to be developed.

Moreover, this review highlights the greater consequences of AML in E-IoT that are not directly related to technical performance. It requires credible and explainable models, realistic to benchmark, and interdisciplinary cooperation to match technology developments with ecological, societal, and regulatory goals. The systematic nature of the vulnerability awareness, the categorization of the attack mechanisms, the assessment of defenses, and the uncovering of the existing gaps can enable researchers, practitioners, and policymakers to design E-IoT systems that are not only intelligent and efficient but also secure, resilient, and trustworthy enough.

To sum up, environmental IoT and machine learning convergence suggest a revolutionary potential in the field of environmental monitoring and control. Simultaneously, threats from adversaries are quite dangerous and should be prevented in advance. The most effective way of ensuring robust, secure, and reliable E-IoT systems is to employ an integrated strategy incorporating data-, model-, and system-defenses and adaptive learning strategies and interdisciplinary cooperation. Further research and development in this direction is pivotal towards maximizing the potential of smart environmental surveillance and preserving the consistency and credibility of the information and judgments that constitute ecological sustainability and citizen safety.

Funding

This study is supported by the 2024 Foshan City Self-Funded Science and Technology Innovation Project “Research on Image Segmentation Technology Based on Convolutional Neural Networks in Crop Images” (Project Number: 2420001004686).

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

No new data were created or generated in this study. As this is a review, it is based on data and information from previously published sources, which are cited in the reference list.

Conflicts of Interest

The authors declare no conflict of interest.

AI Use Statement

The authors declare that no artificial intelligence (AI) tools were used in the preparation of this manuscript.

References

[1] Lindenmayer, D., Likens, G., 2018. Effective Ecological Monitoring, 2nd ed. CSIRO Publishing: Clayton, Australia. DOI: https://doi.org/10.1071/9781486308934

[2] Spellerberg, I.F., 2005. Monitoring Ecological Change, 2nd ed. Cambridge University Press: Cambridge, UK. DOI: https://doi.org/10.1017/CBO9780511614699

[3] Manduva, V.C., 2020. AI-Powered Edge Computing for Environmental Monitoring: A Cloud-Integrated Approach. International Journal of Emerging Trends in Science and Technology. 7(12), 1–21.

[4] Muniswamy, A., Rathi, R., 2024. A Detailed Review on Enhancing the Security in Internet of Things-Based Smart City Environment Using Machine Learning Algorithms. IEEE Access. 12, 120389–120413. DOI: https://doi.org/10.1109/ACCESS.2024.3450180

[5] Issa, J., Abdulrahman, L.M., Abdullah, R.M., et al., 2024. AI-Powered Sustainability Management in Enterprise Systems Based on Cloud and Web Technology: Integrating IoT Data for Environmental Impact Reduction. Journal of Information Technology and Informatics. 3(1), 156–176.

[6] Alkadi, S., Al-Ahmadi, S., Ismail, M.M.B., 2023. Better Safe Than Never: A Survey on Adversarial Machine Learning Applications towards IoT Environment. Applied Sciences. 13(10), 6001. DOI: https://doi.org/10.3390/app13106001

[7] Muthalagu, R., Malik, J., Pawar, P.M., 2025. Detection and Prevention of Evasion Attacks on Machine Learning Models. Expert Systems with Applications. 266, 126044. DOI: https://doi.org/10.1016/j.eswa.2024.126044

[8] Paladini, T., Monti, F., Polino, M., et al., 2023. Fraud Detection under Siege: Practical Poisoning Attacks and Defense Strategies. ACM Transactions on Privacy and Security. 26(4), 1–35. DOI: https://doi.org/10.1145/3613244

[9] Mega, G., 2022. AML Security—A Comprehensive Framework for Machine Learning Attacks [Master's Thesis]. Politecnico di Torino: Turin, Italy.

[10] Obaidat, M.A., Obeidat, S., Holst, J., et al., 2020. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. Computers. 9(2), 44. DOI: https://doi.org/10.3390/computers9020044

[11] Hart, J.K., Martinez, K., 2015. Toward an Environmental Internet of Things. Earth and Space Science. 2(5), 194–200. DOI: https://doi.org/10.1002/2014EA000044

[12] Ibitoye, O., Abou-Khamis, R., Shehaby, M.E., et al., 2019. The Threat of Adversarial Attacks on Machine Learning in Network Security—A Survey. arXiv preprint. arXiv:1911.02621. DOI: https://doi.org/10.48550/arXiv.1911.02621

[13] Fang, S., Xu, L.D., Zhu, Y., et al., 2014. An Integrated System for Regional Environmental Monitoring and Management Based on Internet of Things. IEEE Transactions on Industrial Informatics. 10(2), 1596–1605. DOI: https://doi.org/10.1109/TII.2014.2302638

[14] Hasan, S.M., Shahid, A.R., Imteaj, A., 2024. Evaluating Sustainability and Social Costs of Adversarial Training in Machine Learning. IEEE Consumer Electronics Magazine. 14(3), 27–34. DOI: https://doi.org/10.1109/MCE.2024.3458350

[15] Liu, X., Lu, D., Zhang, A., et al., 2022. Data-Driven Machine Learning in Environmental Pollution: Gains and Problems. Environmental Science & Technology. 56(4), 2124–2133.

[16] Bhavani, K., Gajendra, N., 2024. Smart Data-Driven Sensing: New Opportunities to Combat Environmental Problems. In: Kumar, A., Saini, H.K., Dubey, A.K., et al. (Eds.). Bio-Inspired Data-Driven Distributed Energy in Robotics and Enabling Technologies. CRC Press: Boca Raton, FL, USA. pp. 17–47. DOI: https://doi.org/10.1201/9781003530077-2

[17] Baranwal, A., 2025. IoT-Based Environmental Sensing Solutions for Smart City Monitoring. Smart City Insights. 2(1), 1–16.

[18] Zheng, R., Wang, H., Zhao, J., 2019. A Unified Management Framework for EIoT Systems Based on Metadata and Event Detection. IEEE Access. 7, 112629–112638. DOI: https://doi.org/10.1109/ACCESS.2019.2930290

[19] Burhan, M., Alam, H., Arsalan, A., et al., 2023. A Comprehensive Survey on the Cooperation of Fog Computing Paradigm-Based IoT Applications: Layered Architecture, Real-Time Security Issues, and Solutions. IEEE Access. 11, 73303–73329. DOI: https://doi.org/10.1109/ACCESS.2023.3294479

[20] Handayani, A.S., Soim, S.S., Agusdi, T.E., et al., 2021. Air Quality Classification Using Support Vector Machine. Computer Engineering & Applications Journal. 10(1), 55–69.

[21] Wang, S., Cao, J., Yu, P.Y., 2020. Deep Learning for Spatio-Temporal Data Mining: A Survey. IEEE Transactions on Knowledge and Data Engineering. 34(8), 3681–3700. DOI: https://doi.org/10.1109/TKDE.2020.3025580

[22] Amato, F., Guignard, F., Robert, S., et al., 2020. A Novel Framework for Spatio-Temporal Prediction of Environmental Data Using Deep Learning. Scientific Reports. 10(1), 22243. DOI: https://doi.org/10.1038/s41598-020-79148-7

[23] Teh, H.Y., Kempa-Liehr, A.W., Wang, K.I.K., 2020. Sensor Data Quality: A Systematic Review. Journal of Big Data. 7(1), 11. DOI: https://doi.org/10.1186/s40537-020-0285-1

[24] Bai, Y.-T., Jin, X.-B., Wang, X.-Y., et al., 2020. Dynamic Correlation Analysis Method of Air Pollutants

in Spatio-Temporal Analysis. International Journal of Environmental Research and Public Health. 17(1), 360. DOI: https://doi.org/10.3390/ijerph17010360

[25] Kachhoria, R., Mahalle, P.N., Bhagwat, S., 2025. Data Collection and Preprocessing for Environmental Monitoring Using Wireless Sensor Networks. In: Mahalle, P., Takale, D., Sakhare, S., et al. (Eds.). Machine Learning for Environmental Monitoring in Wireless Sensor Networks. IGI Global: Hershey, PA, USA. pp. 39–52. DOI: https://doi.org/10.4018/979-8-3693-3940-4.ch003

[26] Dritsas, E., Trigka, M., 2025. Machine Learning in Intelligent Networks: Architectures, Techniques, and Use Cases. IEEE Access. 13, 102724–102745. DOI: https://doi.org/10.1109/ACCESS.2025.3577968

[27] Gao, N., Xue, H., Shao, W., et al., 2022. Generative Adversarial Networks for Spatio-Temporal Data: A Survey. ACM Transactions on Intelligent Systems and Technology. 13(2), 1–25. DOI: https://doi.org/10.1145/3474838

[28] Gyamfi, E., Jurcut, A., 2022. Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets. Sensors. 22(10), 3744. DOI: https://doi.org/10.3390/s22103744

[29] Elhanashi, A., Dini, P., Saponara, S., et al., 2023. Integration of Deep Learning into the IoT: A Survey of Techniques and Challenges for Real-World Applications. Electronics. 12(24), 4925. DOI: https://doi.org/10.3390/electronics12244925

[30] Khazane, H., Ridouani, M., Salahdine, F., et al., 2024. A Holistic Review of Machine Learning Adversarial Attacks in IoT Networks. Future Internet. 16(1), 32. DOI: https://doi.org/10.3390/fi16010032

[31] Tellez, M., El-Tawab, S., Heydari, H.M., 2016. Improving the Security of Wireless Sensor Networks in an IoT Environmental Monitoring System. In Proceedings of the 2016 IEEE Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 29 April 2016; pp. 72–77. DOI: https://doi.org/10.1109/SIEDS.2016.7489330

[32] Wang, Z., Ma, J., Wang, X., et al., 2022. Threats to Training: A Survey of Poisoning Attacks and Defenses on Machine Learning Systems. ACM Computing Surveys. 55(7), 1–36. DOI: https://doi.org/10.1145/3538707

[33] Zhao, K., Li, L., Ding, K., et al., 2025. A Systematic Survey of Model Extraction Attacks and Defenses: State-of-the-Art and Perspectives. arXiv preprint. arXiv:2508.15031. DOI: https://doi.org/10.48550/arXiv.2508.15031

[34] Gao, Y., Doan, B.G., Zhang, Z., et al., 2020. Backdoor Attacks and Countermeasures on Deep Learning: A Comprehensive Review. arXiv preprint. arXiv:2007.10760. DOI: https://doi.org/10.48550/arXiv.2007.10760

[35] Celdrán, A.H., Sánchez Sánchez, P.M., Feng, C., et al., 2022. Privacy-Preserving and Syscall-Based Intrusion Detection System for IoT Spectrum Sensors Affected by Data Falsification Attacks. IEEE Internet of Things Journal. 10(10), 8408–8415. DOI: https://doi.org/10.1109/JIOT.2022.3213889

[36] Wang, Y., Sun, T., Li, S., et al., 2023. Adversarial Attacks and Defenses in Machine Learning-Empowered Communication Systems and Networks: A Contemporary Survey. IEEE Communications Surveys & Tutorials. 25(4), 2245–2298. DOI: https://doi.org/10.1109/COMST.2023.3319492

[37] Kalejaiye, A.N., 2024. Adversarial Machine Learning for Robust Cybersecurity: Strengthening Deep Neural Architectures against Evasion, Poisoning, and Model-Inference Attacks. International Journal of Computer Applications Technology and Research. 13(12), 72–95.

[38] Luo, L., Zhang, Y., Pearson, B., et al., 2018. On the Security and Data Integrity of Low-Cost Sensor Networks for Air Quality Monitoring. Sensors. 18(12), 4451. DOI: https://doi.org/10.3390/s18124451

[39] Mattos, V., Schmidt, J., Bhaya, A., et al., 2025. Design and Detection of Covert Man-in-the-Middle Cyberattacks on Water Treatment Plants. In Proceedings of the 2025 Workshop on Re-Design Industrial Control Systems with Security, Taipei, China, 13–17 October 2025; pp. 7–15. DOI: https://doi.org/10.1145/3733823.3764516

[40] Tran, L., Bartz, R., Sankaran, R., et al., 2025. Stateful Triage for Reliable and Secure Wildfire Monitoring at the Edge. In Proceedings of the 2025 IEEE Military Communications Conference (MILCOM 2025), Los Angeles, CA, USA, 6–10 October 2025; pp. 1–6. DOI: https://doi.org/10.1109/MILCOM64451.2025.11310040

[41] Alfahaid, A., Alalwany, E., Almars, A.M., et al., 2025. Machine Learning-Based Security Solutions for IoT Networks: A Comprehensive Survey. Sensors. 25(11), 3341. DOI: https://doi.org/10.3390/s25113341

[42] Huma, Z.E., Jan, S.U., Ahmad, J., et al., 2025. Adversarial Machine Learning in IoT Security: A Comprehensive Survey. ACM Computing Surveys. 58(8), 202. DOI: https://doi.org/10.1145/3785665

[43] Partida, A., Criado, R., Romance, M., 2021. Identity and Access Management Resilience against Intentional Risk for Blockchain-Based IoT Platforms. Electronics. 10(4), 378. DOI: https://doi.org/10.3390/electronics10040378

[44] Davis, J.J., Clark, A.J., 2011. Data Preprocessing for Anomaly Based Network Intrusion Detection: A Review. Computers & Security. 30(6–7), 353–375. DOI: https://doi.org/10.1016/j.cose.2011.05.008

[45] Rebuffi, S.A., Gowal, S., Calian, D.A., et al., 2021. Data Augmentation Can Improve Robustness. In Proceedings of the 35th Conference on Neural Information

Processing Systems (NeurIPS 2021), Online, 6–14 December 2021. Available from: https://openreview.net/pdf?id=kgVJBBThdSZ

[46] Madry, A., Makelov, A., Schmidt, L., et al., 2017. Towards Deep Learning Models Resistant to Adversarial Attacks. arXiv preprint. arXiv:1706.06083. DOI: https://doi.org/10.48550/arXiv.1706.06083

[47] Wu, B., Zhu, M., Zheng, M., et al., 2025. Defenses in Adversarial Machine Learning: A Systematic Survey From the Lifecycle Perspective. IEEE Transactions on Pattern Analysis and Machine Intelligence. 48(1), 876–895.

[48] Zhao, S., Chandrashekar, M., Lee, Y., et al., 2015. Real-Time Network Anomaly Detection System Using Machine Learning. In Proceedings of the 2015 11th International Conference on the Design of Reliable Communication Networks (DRCN), Kansas City, MO, USA, 24–27 March 2015; pp. 267–270. DOI: https://doi.org/10.1109/DRCN.2015.7149025

[49] Papalkar, R., Alvi, A.S., Jadhav, J., et al., 2024. Securing the Internet of Things: Investigating Common Attacks and Defense Strategies for a Resilient Ecosystem. In: Dagur, A., Shukla, D.K., Makhmadiyarovich, N.F., et al. (Eds.). Artificial Intelligence and Information Technologies. CRC Press: London, UK. pp. 516–523. DOI: https://doi.org/10.1201/9781003510833-83

[50] Hasan, M.M., Islam, M.M., 2022. High-Performance Computing Architectures for Training Large-Scale Transformer Models in Cyber-Resilient Applications. ASRC Procedia: Global Perspectives in Science and Scholarship. 2(1), 193–226. DOI: https://doi.org/10.63125/6zt59y89

[51] Krishna, R.R., Priyadarshini, A., Jha, A.V., et al., 2021. State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. Sustainability. 13(16), 9463. DOI: https://doi.org/10.3390/su13169463

[52] Ahmed, E.S.A., Yousef, M.E., 2019. Internet of Things in Smart Environment: Concept, Applications, Challenges, and Future Directions. World Scientific News. 134(1), 1–51.

[53] Pereira, F., Correia, R., Pinho, P., et al., 2020. Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment. Sensors. 20(22), 6420. DOI: https://doi.org/10.3390/s20226420

[54] Zhu, J.J., Yang, M., Ren, Z.J., 2023. Machine Learning in Environmental Research: Common Pitfalls and Best Practices. Environmental Science & Technology. 57(46), 17671–17689.

[55] Hoang, T.V., 2024. Impact of Integrated Artificial Intelligence and Internet of Things Technologies on Smart City Transformation. Journal of Technical Education Science. 19(Special Issue 01), 64–73. DOI: https://doi.org/10.54644/jte.2024.1532

[56] Lanfranchi, G., Crupi, A., Cesaroni, F., 2025. Internet of Things (IoT) and the Environmental Sustainability: A Literature Review and Recommendations for Future Research. Corporate Social Responsibility and Environmental Management. 32(6), 7648–7670. DOI: https://doi.org/10.1002/csr.70098

[57] Carr, M., Lesniewska, F., 2020. Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance. International Relations. 34(3), 391–412. DOI: https://doi.org/10.1177/0047117820948247