Privacy and Security in Sustainable Smart City Applications

Subjects: Computer Science, Artificial Intelligence

Contributor: Sapdo Utomo , Adarsh Rouniyar , Hsiu-Chun Hsu , Pao-Ann Hsiung

Smart city applications that request sensitive user information necessitate a comprehensive data privacy solution. Federated learning (FL), also known as privacy by design, is a new paradigm in machine learning (ML).

sustainable smart cities federated learning adversarial attack

1. Introduction

The United Nations (UN) has advocated for the Sustainable Development Goals (SDGs), which have since become an indispensable cornerstone for research frameworks within the academic and scientific communities. The Sustainable Development Goals (SDGs) are an all-encompassing collection of seventeen goals, of which SDG 11 addresses the critical challenge of promoting sustainable cities and communities worldwide. Conversely, contemporary trends underscore the increasing demand for secure systems and user privacy. This imperative did not emerge spontaneously; it is rooted in a multitude of documented cases where users suffered adverse consequences due to insecure systems and data breaches. These users encompass a wide spectrum, including corporations, governmental entities, and private citizens [1][2].

The authors of [2] have documented that between 2018 and 2019, the United States experienced an alarming number of data breaches exceeding 10,000 cases. Notably, among these, 430 incidents were categorized as major data breaches [3]. In the European Union, since May 2018, over 160,000 cases have been officially reported. One particularly noteworthy instance revolves around the activities of Cambridge Analytica [4], which exploited fifty million Facebook profiles associated with American voters. Their objective was to develop an AI system capable of influencing electoral outcomes among targeted demographic groups.

The Equifax data breach in 2017 was a significant incident that affected nearly half of the United States' population. This breach compromised over 143 million data records [5][6]. Similarly, Orvibo, a company specializing in Internet of Things (IoT) management platforms, exposed over 2 billion records of private information, including camera recordings of conversations, on the Internet, without any password or security measures [7]. These incidents, among others, highlight the need for robust security solutions to protect user privacy.

Smart city applications often require access to sensitive user information, making it imperative to safeguard this data. Federated learning (FL), also known as "privacy by design", is a promising paradigm that preserves user

privacy by keeping personal data on local devices, also known as federated clients. Implementing FL can be seen as adding additional security layers to a system.

Previous studies have identified the limitations of machine learning in terms of preserving data privacy [8]. Adversaries can potentially derive training data from the gradients of machine learning models. Deep leakage from gradients (DLG) [9] and similar attacks [10][11] can recover information pixel by pixel for images and token by token for text. However, these attacks still face challenges in consistently converging and uncovering true labels.

Alternative research has proposed a method for reconstructing images from the parameter gradients of models by inverting gradients [12] using adversarial attacks. One limitation of this approach is its high computational cost—reconstructing a single image requires 24,000 iterations. Shen et al. [13] conducted a comprehensive study of adversarial threats to distributed machine learning and federated learning. Their findings suggest that FL has several advantages over distributed machine learning. The lack of communication requirements with other clients in FL significantly reduces the risk of privacy breaches. Additionally, distributed machine learning requires more collaboration with other clients or system nodes than FL.

It is worth noting that experts in the field have hypothesized that FL systems may offer enhanced security compared to centralized systems. The insights gained from the previous research, as cited in reference [14], establish the foundation for the subsequent analysis. This analysis primarily focuses on identifying potential vulnerabilities and areas where data could be compromised in the event of a security breach. The scope of the investigation includes a comparative assessment of attack probabilities and the extent of potential losses between centralized systems and the FL paradigm.

Figure 1 illustrates a generalized cloud-based architecture for smart cities, along with potential attack scenarios. This architecture typically collects data from a variety of IoT devices, such as wearable devices, smart sensors, and data loggers, which are used to support applications in areas such as intelligent monitoring, intelligent transportation, and intelligent healthcare. The collected data is then transmitted to edge computing servers, which significantly reduces data transport latency to and from centralized cloud data centers.

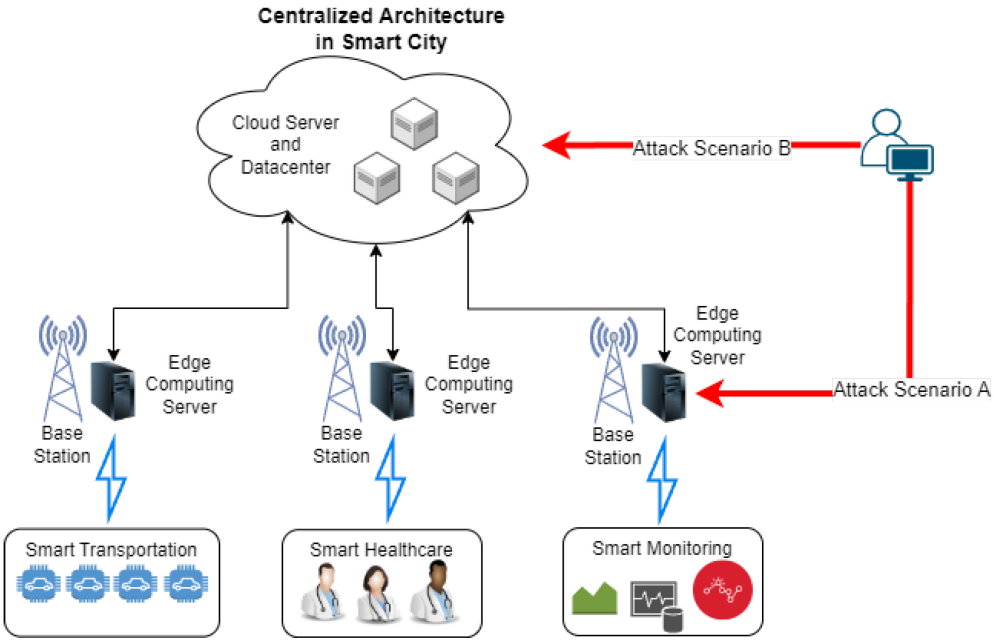

Figure 1. Attack scenarios in cloud-based architecture.

Edge computing plays a crucial role in facilitating real-time data processing and decision-making, a key requirement for applications demanding immediate responses, such as autonomous vehicles, robotics, and monitoring systems [15][16][17][18][19][20]. By employing edge processing and filtering, only relevant information is transmitted to the cloud, thereby reducing network traffic [20][21]. This optimization is particularly beneficial for applications with limited bandwidth.

Furthermore, edge computing enhances data security and privacy by limiting data exposure to external cloud services and keeping sensitive data within a local network. This approach aligns with best practices to safeguard data privacy [16][17][21]. The concept of edge AI has gained prominence with the advent of edge AI devices, such as the NVIDIA Jetson Xavier AGX (NVIDIA, China), NVIDIA Jetson TX2 (NVIDIA, China), NVIDIA Jetson Xavier NX (NVIDIA, China), Google Coral Dev Board (Google Coral, Taiwan, China), and Intel NUC (Intel, Beijing, China). These devices are equipped with graphical processing units (GPUs) and substantial computational capabilities, enabling advanced AI applications at the network's edge [22][23][24][25][26].

Two potential attack scenarios that may occur in cloud architecture are illustrated in **Figure 1**. Attack scenario A targets the edge server, which plays a critical role as a data storage and processor for a wide variety of IoT devices. This data often includes confidential and sensitive information [16][17][21]. If an attack is successful, unauthorized actors could gain access to the confidential information of numerous clients, which could have significant financial consequences.

Attack scenario B focuses on compromising the cloud server, which stores a significantly larger amount of data than the edge server. The cloud server acts as a centralized repository for all data collected from interconnected edge servers. The Orvibo incident [7] serves as a prime example, demonstrating how an attacker was able to access over two billion records from a cloud server with relative ease.

2. Privacy and Security in Sustainable Smart City Applications

In previous studies, diverse methods have been investigated to address security and privacy concerns within the realm of smart cities and the Internet of Things (IoT). These methods encompass the deployment of deep-learning-based intrusion detection systems, blockchain technology, and anomaly detection techniques, among others. The overarching objective of these approaches is to comprehensively fortify overall security measures. Additionally, several novel computational frameworks and architectures have been proposed to augment privacy protection. The emergence of edge GPU devices, equipped with substantial computational capabilities facilitated by GPUs, has given prominence to the concept of edge AI. Consequently, the notion of training AI models at the edge has garnered significance and viability.

In the realm of smart city applications, Singh et al. [27] introduced DeepBlockScheme, a solution that combines deep learning with blockchain technology to enhance security. To illustrate its practicality, the authors conducted a case study within the domain of vehicle manufacturing. Another study by Kumar et al. [28] employed blockchain and machine learning to enhance privacy and security in IoT-driven smart cities. In this context, a blockchain module ensures secure IoT data transmission. Principal component analysis (PCA) is applied to process raw IoT data into a new representation, and an intrusion detection system, the gradient boosting anomaly detector (GBAD), flags unauthorized access attempts. Despite the data integrity benefits offered by blockchain, its implementation introduces computational complexity, particularly in resource-constrained environments [29]. It is noteworthy that in contemporary blockchain systems like Ethereum, data stored on blockchains is commonly publicly accessible by default, posing potential privacy concerns for individuals [30].

Prior studies have introduced various frameworks and architectures aimed at supporting IoT technologies in the context of smart cities. In [31], the authors leverage blockchain and software-defined networking to ensure secure data communication, privacy, and reduced computational costs. They incorporate deep learning within the cloud architecture, enhancing smart industry production with valuable analysis. Another approach is presented in [20], where the authors utilize mobile edge computing (MEC) and the Stackelberg principle-based game theory implemented through the alternating direction method of multipliers (ADMM) within an IoT environment. This method efficiently schedules tasks for distributed devices, resulting in rapid algorithm convergence.

Addressing challenges in multimedia data management, [16] introduces the Short Supply Circuit Internet of Things (SSCIoT). This research primarily focuses on tackling data processing challenges when cloud access is limited or unavailable. The architecture emphasizes the utilization of mobile edge computing and fog computing over cloud computing to deliver quicker responses to users.

Numerous researchers have explored the integration of federated learning (FL) within the IoT and smart city domains, deviating from conventional approaches involving data transfer to multiple points. The foundational principle of FL revolves around maintaining data on the client side, as discussed earlier, aiming to fortify system security and privacy. In the prior research [32], researchers introduced a federated trustworthy AI (FTAI) architecture

tailored to meet seven key requirements of trustworthy AI (TAI) outlined by the European Union [33]. Specifically, the proposed method delves into TAI requirements two and three, focusing on robustness, safety, privacy, and data governance.

In a comprehensive survey [34], researchers explored FL's implementation for IoT, covering aspects such as data exchange, offloading, caching, attack detection, location services, mobile crowdsensing, privacy, and security. The study extensively discussed FL's applications across various domains, including smart healthcare, transportation, UAVs, cities, and industries. Challenges associated with FL-IoT implementations, such as adversarial attacks, non-IID data, low convergence rates, and heterogeneous client computational resources, were thoroughly outlined. In a distinct study [35], researchers integrated FL and blockchain technology to enhance privacy and scalability within smart healthcare systems. It is noteworthy that this conceptual architecture lacks empirical evidence regarding its implementation results.

Adversarial attacks on IoT systems and their ramifications have been subject to extensive investigation in prior research. In [36], researchers delved into the impact of both nontargeted and targeted adversarial attacks, employing methods such as the fast gradient signs method (FGSM) and projected gradient descent (PGD) on CNN-based IoT device identification. The study revealed a degradation in identification accuracy with increasing perturbation and iteration step size. In [37], the authors scrutinized adversarial attacks on deep-learning-based intrusion detection within IoT networks, comparing the effectiveness of two deep learning techniques: feedforward neural networks (FNNs) and self-normalizing neural networks (SNNs). Results indicated that SNNs exhibited greater resistance to adversarial samples in IoT datasets.

Moreover, [38] introduced a partial-model adversarial attack on IoT systems using machine learning (ML). Their findings underscored the vulnerability of ML-based IoT systems to adversarial attacks, particularly when an adversary targeted only 8 out of 20 IoT devices, achieving an 83% success rate. In [39], researchers assessed the efficacy of adversarial attacks on ML-based detection of denial-of-service (DoS) attacks in IoT smart home networks. The introduction of adversarial samples into the test data resulted in a 47.2% decrease in model accuracy, with subsequent improvements observed after employing adversarial training.

As previously highlighted, adversarial attacks extend their impact to both ML and deep learning (DL) models, with federated learning (FL) not immune to such vulnerabilities [13][29][30][40][41][42][43][44][45][46]. In an endeavor to fortify defenses against poisoning attacks, [47] introduced a method utilizing generative adversarial networks (GANs) to generate auditing data during the training process. This approach incorporates a mechanism to identify and eliminate adversaries by auditing the accuracy of their models and integrating a GAN into the federated learning server. The GAN's role involves constructing an auditing dataset capable of detecting adversaries by evaluating the correctness of participant models.

In the pursuit of robust federated learning, [40] introduces the robust framework for federated learning (RFFL). This framework is crafted to adeptly identify and eliminate malicious behaviors in a cautious and iterative manner before aggregating model updates. By adopting this approach, RFFL establishes a robust learning framework, effectively

mitigating the risks associated with data poisoning and model update poisoning attacks. This methodology shares commonalities with the work presented in [47], where a similar notion of implementing filtering on the federated server before aggregation is employed. However, both approaches raise concerns regarding the overall robustness of the global model against adversarial attacks, as they do not incorporate adversarial samples into their model training, thereby questioning the ability to create a truly robust model.

Addressing adversarial attacks in federated learning poses a significant challenge, with [41][44][46] highlighting the complexities involved. Notably, [41] acknowledges the inherent difficulties of implementing adversarial training in a federated setting, primarily attributed to the data-intensive requirements of such training. Previous research endeavors have been dedicated to identifying effective approaches to overcome these challenges.

The integration of FL and IoT has transitioned from a conceptual possibility to a practical reality, facilitated by the emergence of mini-computers equipped with GPUs, commonly known as “edge GPUs”. These devices enable the processing of multimedia data at the edge, giving rise to the concept of “edge AI” [22][23][24][25][26]. This evolution has spurred increased research initiatives exploring the application of AI at the edge. For instance, in a study conducted by [22], researchers utilized the NVIDIA Jetson Nano to develop a model for detecting vehicles and pedestrians on rural roads. Through extensive testing of well-established models, including MobileNetv1, MobileNetv2, Inceptionv2, Pednet, and Multiped, they demonstrated the effective functionality of these models on the NVIDIA Jetson Nano.

Another exploration by Mathur et al. [24] delved into the feasibility of on-device FL. In this investigation, Android smartphones and the Nvidia Jetson TX2 played a pivotal role. These devices were leveraged to train a model following the federated learning methodology through the utilization of the Flower framework. The training process involved the CIFAR-10 dataset for the Nvidia Jetson TX2 and the Office-31 dataset for Android clients. The findings from this study provide compelling evidence for the viability of training AI models on edge devices, especially with lightweight models such as ResNet18. Moreover, Truong et al. [26] harnessed the power of FL to train a lightweight anomaly detection model tailored for industrial control systems. By embracing FL, the learning process was significantly expedited, with completion times reduced to a matter of minutes. The research involved the use of four NVIDIA Jetson Nanos as federated clients, demonstrating the potential for efficient AI training on edge devices.

In order to address the aforementioned security and privacy issues associated with sustainable smart city applications, adversarial training strategies have been implemented within the framework of federated learning. These methodologies have been specifically developed to overcome the challenges that arise from clients having limited datasets, with the ultimate goal of developing a robust global model. This approach exhibits potential for improving the security and privacy aspects of smart city applications and is viable when federated clients are outfitted with GPU support.

References

1. Cheng, L.; Liu, F.; Yao, D.D. Enterprise data breach: Causes, challenges, prevention, and future directions. WIREs Data Min. Knowl. Discov. 2017, 7, e1211.
2. Neto, N.N.; Madnick, S.; Paula, A.M.G.D.; Borges, N.M. Developing a Global Data Breach Database and the Challenges Encountered. J. Data Inf. Qual. 2021, 13, 1–33.
3. Neto, N.N.; Madnick, S.; Paula, A.M.G.D.; Borges, N.M. Cyber Security Data Breaches. 2020. Available online: https://databreachdb.com/ (accessed on 1 October 2023).
4. Cadwalladr, C.; Graham-Harrison, E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Guardian 2018, 17, 22.
5. Wang, P.; Johnson, C. Cybersecurity incident handling: A case study of the Equifax data breach. Issues Inf. Syst. 2018, 19, 150–159.
6. Zou, Y.; Mhaidli, A.H.; McCall, A.; Schaub, F. “I’ve Got Nothing to Lose”: Consumers’ Risk Perceptions and Protective Actions after the Equifax Data Breach. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, MD, USA, 12–14 August 2018; pp. 197–216.
7. Leong, Y.Y.; Chen, Y.C. Cyber risk cost and management in IoT devices-linked health insurance. Geneva Pap. Risk Insur. Issues Pract. 2020, 45, 737–759.
8. Nair, A.K.; Raj, E.D.; Sahoo, J. A robust analysis of adversarial attacks on federated learning environments. Comput. Stand. Interfaces 2023, 86, 103723.
9. Zhu, L.; Liu, Z.; Han, S. Deep Leakage from Gradients. arXiv 2019, arXiv:1906.08935.
10. Lim, J.Q.; Chan, C.S. From Gradient Leakage To Adversarial Attacks In Federated Learning. In Proceedings of the 2021 IEEE International Conference on Image Processing (ICIP), Anchorage, AK, USA, 19–22 September 2021; pp. 3602–3606.
11. Zhao, B.; Mopuri, K.R.; Bilen, H. iDLG: Improved Deep Leakage from Gradients. arXiv 2020, arXiv:2001.02610.
12. Geiping, J.; Bauermeister, H.; Dröge, H.; Moeller, M. Inverting gradients-How easy is it to break privacy in federated learning? In Proceedings of the 34th International Conference on Neural Information Processing Systems, Red Hook, NY, USA, 6–12 December 2020; pp. 16937–16947.
13. Shen, S.; Zhu, T.; Wu, D.; Wang, W.; Zhou, W. From distributed machine learning to federated learning: In the view of data privacy and security. Concurr. Comput. Pract. Exp. 2022, 34, e6002.
14. Hsiung, P.A.; Utomo, S.; A, J.; Rouniyar, A.; Hsu, H.C.; Jiang, G.H.; Chang, C.H.; Tang, K.C. Trustworthy AI and Federated Learning for Sustainable Smart Cities. 2023. Available online: https://smartcities.ieee.org/newsletter/january-2023/trustworthy-ai-and-federated-learning-for-sustainable-smart-cities (accessed on 29 September 2023).

15. Vu Khanh, Q.; Nguyen, V.H.; Minh, Q.N.; Dang Van, A.; Le Anh, N.; Chehri, A. An efficient edge computing management mechanism for sustainable smart cities. Sustain. Comput. Inform. Syst. 2023, 38, 100867.
16. Debauche, O.; Mahmoudi, S.; Guttadauria, A. A New Edge Computing Architecture for IoT and Multimedia Data Management. Information 2022, 13, 89.
17. Badidi, E.; Mahrez, Z.; Sabir, E. Fog Computing for Smart Cities' Big Data Management and Analytics: A Review. Future Internet 2020, 12, 190.
18. Sittón-Candanedo, I.; Alonso, R.S.; García, O.; Muñoz, L.; Rodríguez-González, S. Edge Computing, IoT and Social Computing in Smart Energy Scenarios. Sensors 2019, 19, 3353.
19. Zhang, D.G.; Ni, C.H.; Zhang, J.; Zhang, T.; Yang, P.; Wang, J.X.; Yan, H.R. A Novel Edge Computing Architecture Based on Adaptive Stratified Sampling. Comput. Commun. 2022, 183, 121–135.
20. Lv, Z.; Chen, D.; Lou, R.; Wang, Q. Intelligent edge computing based on machine learning for smart city. Future Gener. Comput. Syst. 2021, 115, 90–99.
21. Li, H.; Ota, K.; Dong, M. Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing. IEEE Netw. 2018, 32, 96–101.
22. Barba-Guaman, L.; Eugenio Naranjo, J.; Ortiz, A. Deep Learning Framework for Vehicle and Pedestrian Detection in Rural Roads on an Embedded GPU. Electronics 2020, 9, 589.
23. Rajagopal, A.; Bouganis, C.S. perf4sight: A toolflow to model CNN training performance on Edge GPUs. In Proceedings of the 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW), Montreal, BC, Canada, 11–17 October 2021; pp. 963–971.
24. Mathur, A.; Beutel, D.J.; de Gusmão, P.P.B.; Fernandez-Marques, J.; Topal, T.; Qiu, X.; Parcollet, T.; Gao, Y.; Lane, N.D. On-device Federated Learning with Flower. arXiv 2021, arXiv:2104.03042.
25. Ahmed, K.M.; Imteaj, A.; Amini, M.H. Federated Deep Learning for Heterogeneous Edge Computing. In Proceedings of the 2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA), Pasadena, CA, USA, 13–15 December 2021; pp. 1146–1152.
26. Truong, H.T.; Ta, B.P.; Le, Q.A.; Nguyen, D.M.; Le, C.T.; Nguyen, H.X.; Do, H.T.; Nguyen, H.T.; Tran, K.P. Light-weight federated learning-based anomaly detection for time-series data in industrial control systems. Comput. Ind. 2022, 140, 103692.
27. Singh, S.K.; Azzaoui, A.E.; Kim, T.W.; Pan, Y.; Park, J.H. DeepBlockScheme: A Deep Learning-Based Blockchain Driven Scheme for Secure Smart City. Hum. Centric Comput. Inf. Sci. 2021, 11, 1–12.
28. Kumar, P.; Kumar, R.; Srivastava, G.; Gupta, G.P.; Tripathi, R.; Gadekallu, T.R.; Xiong, N.N. PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning

for IoT-Driven Smart Cities. IEEE Trans. Netw. Sci. Eng. 2021, 8, 2326–2341.

29. Yamany, W.; Moustafa, N.; Turnbull, B. OQFL: An Optimized Quantum-Based Federated Learning Framework for Defending Against Adversarial Attacks in Intelligent Transportation Systems. IEEE Trans. Intell. Transp. Syst. 2023, 24, 893–903.
30. Kairouz, P.; McMahan, H.B.; Avent, B.; Bellet, A.; Bennis, M.; Bhagoji, A.N.; Bonawitz, K.; Charles, Z.; Cormode, G.; Cummings, R.; et al. Advances and Open Problems in Federated Learning. arXiv 2021, arXiv:1912.04977.
31. Singh, S.K.; Jeong, Y.S.; Park, J.H. A deep learning-based IoT-oriented infrastructure for secure smart City. Sustain. Cities Soc. 2020, 60, 102252.
32. Utomo, S.; John, A.; Rouniyar, A.; Hsu, H.C.; Hsiung, P.A. Federated Trustworthy AI Architecture for Smart Cities. In Proceedings of the 2022 IEEE International Smart Cities Conference (ISC2), Paphos, Cyprus, 26–29 September 2022; pp. 1–7.
33. Floridi, L. Establishing the rules for building trustworthy AI. Nat. Mach. Intell. 2019, 1, 261–262.
34. Nguyen, D.C.; Ding, M.; Pathirana, P.N.; Seneviratne, A.; Li, J.; Vincent Poor, H. Federated Learning for Internet of Things: A Comprehensive Survey. IEEE Commun. Surv. Tutorials 2021, 23, 1622–1658.
35. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Gener. Comput. Syst. 2022, 129, 380–388.
36. Bao, Z.; Lin, Y.; Zhang, S.; Li, Z.; Mao, S. Threat of Adversarial Attacks on DL-Based IoT Device Identification. IEEE Internet Things J. 2022, 9, 9012–9024.
37. Ibitoye, O.; Shafiq, O.; Matrawy, A. Analyzing Adversarial Attacks against Deep Learning for Intrusion Detection in IoT Networks. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Big Island, HI, USA, 9–13 December 2019; pp. 1–6.
38. Luo, Z.; Zhao, S.; Lu, Z.; Sagduyu, Y.E.; Xu, J. Adversarial machine learning based partial-model attack in IoT. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, New York, NY, USA, 13 July 2020; pp. 13–18.
39. Anthi, E.; Williams, L.; Javed, A.; Burnap, P. Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks. Comput. Secur. 2021, 108, 102352.
40. Hu, F.; Zhou, W.; Liao, K.; Li, H.; Tong, D. Toward Federated Learning Models Resistant to Adversarial Attacks. IEEE Internet Things J. 2023, 10, 16917–16930.
41. Hong, J.; Wang, H.; Wang, Z.; Zhou, J. Federated Robustness Propagation: Sharing Robustness in Heterogeneous Federated Learning. arXiv 2022, arXiv:2106.10196.

42. Zhu, J.; Yao, J.; Liu, T.; Yao, Q.; Xu, J.; Han, B. Combating Exacerbated Heterogeneity for Robust Models in Federated Learning. arXiv 2023, arXiv:2303.00250.
43. Chen, Z.; Tian, P.; Liao, W.; Yu, W. Zero Knowledge Clustering Based Adversarial Mitigation in Heterogeneous Federated Learning. IEEE Trans. Netw. Sci. Eng. 2021, 8, 1070–1083.
44. Shah, D.; Dube, P.; Chakraborty, S.; Verma, A. Adversarial training in communication constrained federated learning. arXiv 2021, arXiv:2103.01319.
45. Jere, M.S.; Farnan, T.; Koushanfar, F. A Taxonomy of Attacks on Federated Learning. IEEE Secur. Priv. 2021, 19, 20–28.
46. Zizzo, G.; Rawat, A.; Sinn, M.; Buesser, B. FAT: Federated Adversarial Training. arXiv 2020, arXiv:2012.01791.
47. Zhao, Y.; Chen, J.; Zhang, J.; Wu, D.; Blumenstein, M.; Yu, S. Detecting and mitigating poisoning attacks in federated learning using generative adversarial networks. Concurr. Comput. Pract. Exp. 2022, 34, e5906.