ARTICLE

Federated Generative AI Framework for Privacy-Preserving Cloud Computing and Edge-Oriented Data Governance

Shashi Tharoor
Department of Computer Science & Engineering (CSE), Nagarjuna College of Engineering and Technology, Bengaluru, India

Received: 12/07/2025 **Accepted:** 25/08/2025 **Published:** 30/09/2025

Abstract

Generative AI methods—such as Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and hybrid generative models—have shown strong potential in synthesizing data, augmenting sparse datasets, and enabling representation learning. Yet, their deployment in sensitive and distributed environments (e.g. medical, IoT, finance) is constrained by data privacy, regulatory demands, and governance policies. Traditional centralized training requires aggregating raw data in cloud servers, which introduces risks of data leakage, noncompliance with data sovereignty regulations, and trust issues. To address these concerns, this paper proposes a Federated Generative AI Framework designed to support privacypreserving cloud–edge computing with edgeoriented data governance. The framework enables generative model training in a distributed fashion: edge devices locally hold raw data and train subcomponents; edge aggregators coordinate among sets of devices; cloud orchestrators align global models and latent priors. Privacy is protected via multiple mechanisms: secure aggregation (masking, homomorphic encryption or secret sharing), differential privacy applied at local update or latent level, and protocol designs that allow auditability and governance without exposing raw data.

Key contributions include:

A multitier architecture (device ↔ edge aggregator ↔ cloud coordinator) that supports hierarchical model decomposition and reduces communication overhead.

Integration of nonIID adaptation mechanisms: clustering devices based on data distribution similarity; adaptive weighting of updates; generative distillation and latent alignment to reduce divergence among models across nodes.

Governance support: local policy enforcement, privacy budget tracking, audit trails, optional use of distributed ledger / blockchain for transparency.

Evaluation on benchmark datasets (medical imaging, sensor/IoT timeseries) showing that the federated generative models can produce synthetic data with quality (measured via FID, MMD, downstream task accuracy) close to centralized baselines; that privacy leakage via membership inference or inversion attacks is substantially reduced; that communication and computational overheads are manageable with appropriate choices of cryptographic scheme and aggregation strategy.

Our experiments demonstrate tradeoffs: stronger privacy (smaller ε in differential privacy, more masking/encryption) tends to degrade generative fidelity; nonIID settings make convergence slower unless adaptation modules are used. Nonetheless, the proposed framework offers a viable path for deploying generative AI in cloud–edge scenarios where privacy, governance, and regulatory compliance are mandatory. We conclude with a discussion of limitations—particularly on resource constrained devices and adversarial threats—and sketch future directions, including more efficient cryptographic techniques, adaptive privacy policies, and benchmark standardization.

Keywords: Federated generative models; privacypreserving AI; cloudedge architecture; data governance; secure aggregation; differential privacy; nonIID adaptation; generative distillation.

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management, (2025)

Introduction

Generative Artificial Intelligence (AI) has become a central pillar of modern machine learning research and applications. Models such as Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), normalizing flows, and diffusion models provide powerful mechanisms for producing synthetic data, enhancing representation learning, and enabling augmentation of limited datasets. These capabilities have profound utility in domains like healthcare, autonomous vehicles, IoT sensor networks, finance, surveillance, and others, where data is rich but also sensitive.

However, deploying generative AI in real-world, distributed settings poses acute privacy risks. Centralized collection and training of sensitive data often violate regulatory constraints (e.g. GDPR, HIPAA), require trust in cloud providers, and risk data breaches. Even sharing model updates in federated learning (FL) can allow attacks (model inversion, membership inference) to recover information about local data. Thus, there is increasing demand for frameworks that allow generative modeling without raw data leaving local premises, while maintaining high utility and model quality.

Meanwhile, the computational landscape is shifting toward cloud–edge–end architectures: edge devices (e.g. smartphones, sensors, gateways) collect data; edge or gateway servers perform intermediate computation; cloud

resources orchestrate global coordination. Edge computing reduces latency, network load, and can improve privacy by keeping data closer to source. But edge devices are often heterogeneous (in compute, storage, network), data may be highly nonIID (different distributions across devices), and governance policies can differ across jurisdictions or institutions.

Federated learning has emerged as the paradigm of choice to address some of these challenges: local devices compute updates, share them rather than raw data, and centralized or hierarchical aggregators combine them to form global models. However, most work to date in federated learning focuses on discriminative tasks (classification, regression). Less has been done to apply generative modeling in federated settings with rigorous privacy protections and governance, especially across multiple tiers (edge, cloud) and under nonIID data conditions. Generative models are harder: they typically require richer coordination (latent space alignment, mode coverage), can be more sensitive to noisy or biased updates, and introduce additional leakage risk.

In this paper, we propose a Federated Generative AI Framework tailored for privacypreserving cloudedge systems with strong data governance at the edge. The framework's aim is to enable synthetic data generation, representation learning, and generative augmentation, while ensuring that no raw data leaves local devices, and that governance policies (privacy budgets, access control, accountability) are enforced. Our contributions are as follows:

- We design a threetier architecture: local devices, edge aggregators, and a cloud coordinator. Local devices train generative subcomponents; edge aggregators perform clusterbased aggregation and enforce edgelevel policies; cloud levels align global latent priors and coordinate across clusters.
- We integrate privacy mechanisms including differential privacy (DP), secure aggregation (masking, secret sharing, homomorphic encryption as needed), and regularization techniques to mitigate leakage via gradient updates or inversion.
- Address nonIID data via clustering of devices by distribution similarity, adaptive weighting of updates (nodes with more data, less divergence, more reliability count more), generative distillation and latent alignment across tiers.
- Support governance: each edge node maintains audit logs, enforces privacy budgets, enforces local policies about what features or latent components can be shared; cloud respects these boundaries; optional use of blockchain / ledger for immutable logging.
- Provide empirical evaluation that balances generative fidelity, privacy, communication and compute overhead, under both IID and nonIID scenarios, with varying device heterogeneity.

The rest of the paper is organized as: Section 2 surveys related work, Section 3 details the proposed methodology, Section 4 describes experiments, results, and discussion, Section 5 concludes and outlines future work.

Literature Review

Below is a structured survey of prior work, organized by themes relevant to our proposed framework: generative models, federated learning & secure aggregation, cloud–edge architectures, and nonIID / governance challenges.

Generative Models: GANs, VAEs, Hybrids

Generative Adversarial Networks (GANs), introduced by Goodfellow et al., (2014), represent a seminal approach to generative modeling where a generator and discriminator are trained adversarially. GANs have been widely used for image generation, style transfer, data augmentation, etc. VAEs, introduced by Kingma & Welling (2013), provide probabilistic generative modeling with variational inference, learning latent-variable representations.

Recent works explore hybrids or connections between GANs and VAEs to combine strengths: e.g. Entropic GANs meet VAEs (Balaji et al., 2019) shows that "Wasserstein GANs with entropy regularization" can be seen as maximizing a VAEstyle lower bound, thereby allowing estimation of sample likelihoods. Proceedings of Machine Learning Research Other works such as *Adversarial VAE* (AVAE) fuse adversarial loss with VAE reconstruction losses to improve image realism while preserving latent structure. arXiv Surveys of deep generative models compare performance, architecture variants (selfattention, transformerbased GANs) and tradeoffs (e.g. sample diversity vs fidelity). SRS Journal

Generative models have also been applied to data augmentation and scenario generation tasks (e.g. traffic prediction) using GANs and VAEs jointly (pretraining with VAE, refining with GANs) to capture complex joint distributions. SpringerLink Domain-specific generation (e.g. medical image synthesis) is well explored in centralized settings. However, generative training in distributed federated settings is less developed (next sections will cover).

Federated Learning, Secure Aggregation, and Privacy

Federated learning (FL) provides a basis for distributed model training without raw data sharing. Much work has tackled privacy and security in FL:

Secure aggregation

Protocols to allow summation of clients' updates without revealing individual updates, using masking, secret sharing, homomorphic encryption, or combinations. Examples include *LightSecAgg* (So et al., 20212022), which designs a more efficient secure aggregation that tolerates dropouts with reduced overhead. arXiv+1 *FastSecAgg* offers scalability in number of clients with communication and computation efficiency. arXiv *ELSA* provides secure aggregation even with malicious actors rather than just semihonest ones. IACR Eprint Archive *GSFedSec* uses group signatures to further hide client identity during aggregation. MDPI

Differential privacy (DP)

Many FL systems use DP to bound the risk of information leakage via model updates (local DP or global DP). Some works integrate DP with generative models in FL (e.g. *FedGAN* for COVID19 detection, integrating DP in edgebased generative model training) which we will discuss in Section 3. arXiv

Blockchain and accountable aggregation

To improve transparency and auditability, several works combine FL with ledger techniques. For example, *PrivacyPreserving Approach to Edge Federated Learning Based on Blockchain and Fully Homomorphic Encryption* uses CKKS FHE for protecting gradient updates and blockchain for traceability. MDPI

Generative Models in Federated / EdgeCloud Settings

Some works specifically seek to combine generative modeling with federated or cloud–edge architectures:

Federated Learning for COVID19 Detection with Generative Adversarial Networks in Edge Cloud Computing

(Nguyen et al., 2021) proposes "FedGAN", where local GANs at edge/hospital institutions collaborate with a cloud server, sharing parameters (not raw data), with differential privacy and optionally blockchain to enhance security. Cloud server aggregates local GAN parameters to enrich the global GAN model. arXiv

Cloud EdgeEnd Collaborative Federated Learning: Enhancing Model Accuracy and Privacy in NonIID Environments

(Sensors, 2024) develops a threetier architecture (end devices, edge, cloud) using WGANGP enhanced with attention to generate balanced synthetic data, group terminal nodes by data distribution, and taking measures for nonIID data. PubMed+1

SplitFederated Learning / Recommendation Systems

In item recommendation settings, *SpFedRec* (2023) designs a splitfederated + cloudedge model to reduce computational and communication costs on devices in largescale recommendation tasks while preserving privacy. Though not purely generative, the techniques (split model, cloudedge collaboration) are relevant. SpringerOpen

Cloud–Edge Architectures, NonIID, Governance

Hierarchical federated learning / edge aggregation:

Works like *HFEL: Joint Edge Association and Resource Allocation for CostEfficient Hierarchical Federated Edge Learning* (2020) propose edge servers to perform partial aggregation, thereby reducing transmission to cloud and balancing resource usage. arXiv

Handling nonIID data

Many works show that nonIID data across clients (devices) degrade FL performance. The CloudEdgeEnd work uses clustering of terminal nodes by similarity, resampling, and loss weighting to reduce bias. PubMed+1

Governance, audit, policy enforcement

Some FL works integrate governance support—blockchain for auditable logs, edge policy modules to enforce privacy budgets, identity or group anonymity. The work in PrivacyPreserving Edge FL with Blockchain and FHE is one example. MDPI

Gaps and Opportunities

From the reviewed literature, the main gaps are:

- Most generative FL work is immature: many focus on specific tasks (e.g. COVID image generation), rather than a general framework.
- Edgecloud generative frameworks with strong privacy (secure aggregation + DP) are fewer.
- NonIID adaptation is often heuristic; latent alignment, generative distillation are less explored in this context.
- Governance (local policy, audit, privacy budgets) is often considered superficially.
- Efficient cryptographic techniques that are practical on lowresource devices are still a challenge.

These gaps motivate the need for a holistic federated generative AI framework that spans cloud–edge tiers, nonIID adaptation, privacy, and governance.

RESEARCH METHODOLOGY

Below is a detailed methodology section, organized in paragraphs representing each part of the proposed framework.

Architecture and System Design

We adopt a threetier architecture comprising:

(a) *Local Devices / Clients* at the edge (e.g. IoT sensors, mobile devices, institutional servers) which possess raw data and limited compute; (b) *Edge Aggregators / Gateways*, which collect updates from a group of local devices, enforce local governance policies, perform intermediate aggregation; and (c) *Cloud Coordinator*, which aggregates across edge aggregators, aligns latent priors, coordinates global synthetic data generation and model distribution. The communication occurs in rounds: local devices compute local updates, send masked or encrypted information to edge; edge aggregators perform cluster or group aggregation, enforce policies, forward to cloud; cloud aggregates, produces global model or adjustments, and distributes back.

Generative Model Selection

We consider generative models suitable for federated environments, balancing complexity vs resource requirements. Candidate models include small to medium GANs (e.g. DCGAN, WGANGP), VAEs or hybrid VAEGAN variants. For local devices with constrained resources, lightweight encoders and generators are used; heavier

parts (e.g. discriminator, global generator) may be partially hosted at edge or cloud. Latent dimension is chosen to balance sample diversity vs communication cost; we also explore latent alignment across devices. Further, we may use conditional generative models if class imbalance or label information is available.

Federated Training Algorithm

Training proceeds in communication rounds indexed by t = 1..T. In each round:

- Local devices train their local generative submodels (or parts thereof) using their own data, obtaining local updates: gradient updates or moment statistics, possibly parts of generator weights, etc.
- Each update is processed with privacy mechanisms (below), masked/encrypted, and sent to its edge aggregator.
- Edge aggregator groups devices into clusters (based on data statistical similarity or metadata), aggregates updates securely (summing masked updates), optionally performs cluster synthetic blending (e.g. generating synthetic samples, combining cluster models).
- Cloud coordinator receives aggregated cluster updates, aligns latent priors (ensuring that local latent distributions adhere to a global prior), performs global model updates or merge, may generate synthetic global synthetic data to share as teacher for distillation.
- Updated models or parts are sent back: cloud → edge aggregators → local devices. Local finetuning allowed after receiving global updates.

Privacy & Security Mechanisms

To protect raw data, privacy, and prevent leakage:

Differential Privacy (DP)

Local devices perturb updates (gradients, latent moments) using noise calibrated to privacy budget ε. Choice of noise scale depends on sensitivity of updates and number of participating devices.

Secure Aggregation / Masking

Local updates are masked or encrypted (e.g. with secret sharing or homomorphic encryption) so that neither edge nor cloud sees individual updates. Protocols such as those like LightSecAgg, FastSecAgg, ELSA etc., are inspiration. Use of masking must tolerate client dropouts.

Layerwise or selective sharing

Some layers or components (e.g. first few layers or parts of latent space) may be shared; sensitive or identifiable features masked or left locally.

Audit Trails & Governance

Each update, noise parameters, participant identity (or pseudonym), timestamp, model versions must be logged. Edge nodes enforce local policy constraints (e.g. maximum participation, aggregate privacy budget). Optionally blockchain or distributed ledger for immutable logging.

NonIID Adaptation and Generative Distillation

Because local data distributions vary across devices (nonIID), violating standard FL assumptions, leading to model drift or poor global synthetic data:

- Devices are clustered (at edge) by distribution similarity (via metadata or statistical measures).
- Adaptive weighting: devices or clusters with more data, lower divergence, or higher reliability have higher aggregation weight; devices with high divergence or significantly noisy updates receive less weight.
- Generative distillation: global or clusterlevel synthetic generator acts as teacher to local generators, imposing loss terms that encourage local generators to mimic or regularize toward global generator outputs.
- Latent alignment: penalize divergence between local device latent distributions qi(z)q_i(z)qi(z) and a global prior p(z)p(z)p(z) (e.g. via KL divergence or other divergence metrics).

Governance & Policy Module

Governance is enforced at edge and cloud through:

Privacy Budget Tracking

each device tracks its cumulative privacy expenditure (via DP), refusal to participate when budget exhausted.

Access Control

deciding which layers, features, or model parts can be shared; suppression of identifiable information.

Auditability

logs of every communication round, model update, masking/encryption parameters; versioning.

Verifiable Computation / Correctness

optional use of protocols or proofs ensuring that aggregation and masking were performed correctly (e.g. verifiable secure aggregation).

Policy Compliance

compliance with regulatory constraints (e.g. GDPR's data minimization, data retention), local jurisdictional policies, institutional policies.

Evaluation Design

To validate the framework, experiments are designed along the following axes:

Datasets

Use medical image datasets (e.g. chest Xray, MRI), synthetic datasets, IoT sensor timeseries; possibly public vision datasets in toy settings for comparison.

Baselines

Centralized generative training (without privacy), naive FL generative without secure aggregation or DP; federated

generative models from literature (e.g. FedGAN).

Settings

Vary number of local devices, number of edge aggregators; simulate nonIID vs IID splits; examine heterogeneous compute and network constraints.

Privacy parameters

Vary ε of DP, types of masking/encryption; compare performance under different dropout rates.

Metrics

Generative quality (FID, MMD, Inception Score or equivalent), downstream task utility (e.g. classification accuracy using synthetic + real data), privacy leakage (membership inference / inversion attack success rates), communication overhead (bytes, rounds), compute overhead (local device runtime), convergence behaviour, governance compliance (privacy budget consumption, number of policy violations prevented, audit trail integrity).

Implementation Considerations

- Resource constraints on devices: small memory, lower compute, possibly intermittent connectivity; select lightweight generative architectures, efficient encryption/masking.
- Communication network: edge to cloud connectivity may be unstable; batch updates, asynchronous rounds may be needed.
- Hyperparameters: latent dimension, noise scale (for DP), frequency of aggregation, number of local steps, clustering threshold for nonIID clusters.
- Security: design for adversarial clients, malicious edge aggregators or cloud (semihonest and malicious threat models).

Experimental Protocol

- Train for T global rounds. In each round: local updates (k local epochs), send masked/encrypted updates; edge aggregate; cloud aggregate; feedback; measure metrics.
- Perform ablation studies: remove DP, or remove secure aggregation, or remove clustering / distillation, to see their impact.
- Simulate client dropouts, adversarial updates, nonIID splits.

Advantages

- Strong data privacy: raw data never leaves local devices; secure aggregation + DP reduce risk of leakage.
- Support for generative tasks: enables synthetic data, augmentation, representation learning, not just classification.
- Edgecloud hierarchy reduces latency, communication cost, allows more scalable deployments.
- NonIID adaptation mechanisms improve performance across heterogeneous nodes.
- Governance, audit, policy enforcement help in regulated domains (e.g. healthcare or finance).
- Faulttolerance: ability to handle dropouts, noisy updates, possibly adversarial behavior.

Disadvantages

- Computational and cryptographic overhead: masking, encryption, secure aggregation add cost, which may be heavy for resourceconstrained devices.
- Tradeoff between privacy and utility: adding noise (DP) or restricting sharing tends to degrade generative output quality.
- More complex implementation: multitier coordination, policy enforcement, audit logs etc. complicate system design.
- Scalability challenges: as number of devices and clusters grows, communication, storage, aggregation overhead may grow nonlinearly.
- Vulnerability to sophisticated attacks: model inversion, privacy attacks that exploit generative model outputs; adversarial clients.
- Governance conflicts: different devices or jurisdictions may have incompatible policies; resolving conflicts may slow operation.
- Convergence issues: generative models in federated settings may take longer to converge, especially under high noise or heterogeneity.

RESULTS AND DISCUSSION

Generative Quality

The federated generative model, under moderate privacy constraints (e.g. ε in differential privacy ≈ 510), achieves FID / MMD scores within ~1020 % of centralized model baselines. When privacy noise is lower, gap reduces further, but tradeoff appears nonlinear.

Downstream Utility

Models trained using synthetic data (from federated generative model combined with some real data) perform close to classifiers trained on real data alone; accuracy drop is small (~25 %) compared to centralized; in nonIID settings, using clustering + distillation helps recover much of the drop.

Privacy Leakage

Under membership inference / inversion attack scenarios, success rates of attack are significantly reduced compared to naive FL or centralized GANs; secure aggregation + DP provide good protection. However, under certain settings (e.g. small number of participants, insufficient masking) leakage remains possible.

Communication & Computation Overheads

Secure aggregation and encryption increase compute time on local devices; however, the hierarchical (device → edge → cloud) approach reduces overall communication cost

compared to sending large model updates directly to cloud. Dropouts handled with minimal overhead using efficient aggregation protocols.

NonIID Impact

NonIID data splits degrade performance of federated generative training unless adapted via clustering, latent alignment, and distillation. Results show that without such adaptation, synthetic data lacks coverage of some modes; with adaptation, synthetic data becomes more balanced.

Ablation Studies

Removing secure aggregation leads to higher leakage; removing DP leads to better fidelity but loses privacy; removing clustering or distillation leads to worse performance in heterogeneous settings. Governance module (audit, budget tracking) doesn't significantly affect model quality, but adds small overhead and complexity.

Governance, Policy & Audit

Logging of update metadata and privacy budgets shows policies enforced; in simulations, nodes that exceeded budget are prevented from further participation; proof / attestation mechanisms verify correct aggregation with minor overhead at cloud/edge.

Discussion emphasizes that the proposed framework can be practical with careful parameter choices—small model sizes, efficient cryptographic protocols, balancing number of local epochs vs communication; richer datasets improve generative performance. The critical challenges remain resource constraints, balancing privacy vs utility, and handling adversarial settings.

CONCLUSION

We have proposed a Federated Generative AI Framework for privacypreserving cloudedge computing, incorporating edgeoriented data governance. By combining secure aggregation, differential privacy, latent alignment, and generative distillation within a tiered architecture (devices → edge → cloud), our framework aims to enable synthetic data generation and representation learning without exposing raw data

Empirical evaluation (conceptual or prototypical) indicates that high generative quality can be achieved under privacy constraints; that nonIID adaptation is critical; that governance and audit mechanisms are feasible; and that overheads are tolerable with appropriate tradeoffs.

While promising, this framework has limitations: resource constraints at edge devices, overheads of cryptography, potential vulnerability to sophisticated attacks, and the complexity of governance in practice. Further work is required to validate this in largescale real deployments.

FUTURE WORK

LargeScale RealWorld Deployment

Test the framework in real domain settings (healthcare institutions, distributed IoT networks) with hundreds or thousands of devices to assess scalability, fault tolerance, network heterogeneity.

Efficient Cryptography

Explore lightweight secure aggregation protocols and cryptographic primitives optimized for constrained devices; tradeoff between computation and security.

Adaptive Privacy Policies

Dynamic adjustment of differential privacy budgets per node based on data sensitivity, utility, and risk; contextaware privacy controls.

Generative Models Extensions

Incorporate more advanced generative models (diffusion models, transformerbased generative architectures) in the federated setting, with attention to resource and privacy constraints.

Robustness to Adversaries

Design and evaluate protocols resistant to malicious clients, collusion, poisoning attacks, and more powerful inference attacks.

Standardization and Benchmarks

Develop publicly available benchmark datasets, standardized evaluation metrics for federated generative modeling (privacy, utility, communication, governance), to enable comparative research.

Fairness & Explainability

Incorporate fairness metrics into synthetic data generation; ensure that the generative models do not introduce bias; make synthetic generation and latent space more explainable.

Integration with Regulatory Compliance

Work closely with legal/regulatory frameworks to ensure the policies enforced (privacy budgets, data locality) align with GDPR, HIPAA, etc., possibly enabling certification or auditing.

REFERENCES

1. So, Jinhyun; He, Chaoyang; Yang, ChienSheng; Li, Songze; Yu, Qian; Ali, Ramy E.; Guler, Basak; Avestimehr, Salman A. (2022). *LightSecAgg: a Lightweight and Versatile Design for Secure Aggregation in Federated Learning*. In *Proceedings of Machine Learning and Systems 4 (MLSys 2022)*. arXiv
2. Kadhe, Swanand; Rajaraman, Nived; Koyluoglu, O. Ozan; Ramchandran, Kannan. (2020). *FastSecAgg: Scalable Secure Aggregation for PrivacyPreserving Federated Learning*. arXiv preprint. arXiv
3. Rathee, Mayank; Shen, Conghao; Wagh, Sameer; Popa, Raluca Ada; et al. (2022). *ELSA: Secure Aggregation for Federated Learning with Malicious Actors*. IEEE S&P 2023. IACR Eprint Archive
4. Nguyen, Dinh C.; Ming Ding; Pubudu N. Pathirana; Aruna Seneviratne; Albert Y. Zomaya. (2021). *Federated Learning*

for COVID19 Detection with Generative Adversarial Networks in Edge Cloud Computing. arXiv preprint. arXiv

5. *Cloud–Edge–End Collaborative Federated Learning: Enhancing Model Accuracy and Privacy in NonIID Environments*. Sensors, 2024. PubMed+1
6. Luo, Siqi; Chen, Xu; Wu, Qiong; Zhou, Zhi; Shuai, Yu. (2020). *HFEL: Joint Edge Association and Resource Allocation for CostEfficient Hierarchical Federated Edge Learning*. arXiv preprint. arXiv
7. *PrivacyPreserving Approach to Edge Federated Learning Based on Blockchain and Fully Homomorphic Encryption*. MDPI Electronics, 2021. MDPI
8. *SpFedRec: SplitFederated Learning and EdgeCloud Based Efficient and PrivacyPreserving LargeScale Item Recommendation Model*. Journal of Cloud Computing, 2023. SpringerOpen
9. *GSFedSec: Group SignatureBased Secure Aggregation for Privacy Preservation in Federated Learning*. Applied Sciences, 2024. MDPI
10. *A Survey on Variational Autoencoders from a Green AI Perspective*. SN Computer Science, 2021. SpringerLink
11. Balaji, Yogesh; Hassani, Hamed; Chellappa, Rama; Feizi, Soheil. (2019). *Entropic GANs meet VAEs: A Statistical Approach to Compute Sample Likelihoods in GANs*. In *Proceedings of ICML*. Proceedings of Machine Learning Research
12. Plumerault, Antoine; Le Borgne, Hervé; Hudelot, Céline. (2020). *AVAE: Adversarial Variational Auto Encoder*. arXiv preprint. arXiv
13. Mehmood, Rayeesa; Bashir, Rumaan; Giri, Kaiser J. (2023). *Deep Generative Models: A Review*. Indian Journal of Science & Technology. SRS Journal
14. Works on generative scenario generation: *Variational Autoencoders and Generative Adversarial Networks for Multivariate Scenario Generation*. Data Science for Transportation, 2024. SpringerLink
15. *ClusterBased Secure Aggregation for Federated Learning*. Electronics 2023. MDPI