Generative Adversarial Privacy for Multimedia Analytics Across the IoT-Edge Continuum

Xin Wang, *Member, IEEE*, Jianhui Lv, *Member, IEEE*, Byung-Gyu Kim, *Senior Member, IEEE*, Carsten Maple, *Senior Member, IEEE*, B. D. Parameshachari, *Senior Member, IEEE*, Adam Slowik, *Senior Member, IEEE*, and Keqin Li, *Fellow, IEEE*

***Abstract*—The proliferation of multimedia-enabled IoT devices and edge computing enables a new class of data-intensive applications. However, analyzing the massive volumes of multimedia data presents significant privacy challenges. We propose a novel framework called generative adversarial privacy (GAP) that leverages generative adversarial networks (GANs) to synthesize privacy-preserving surrogate data for multimedia analytics across the IoT-Edge continuum. GAP carefully perturbs the GAN's training process to provide rigorous differential privacy guarantees without compromising utility. Moreover, we present optimization strategies, including dynamic privacy budget allocation, adaptive gradient clipping, and weight clustering to improve convergence and data quality under a constrained privacy budget. Theoretical analysis proves that GAP provides rigorous privacy protections while enabling high-fidelity analytics. Extensive experiments on real-world multimedia datasets demonstrate that GAP outperforms existing methods, producing high-quality synthetic data for privacy-preserving multimedia processing in diverse IoT-Edge applications.**

***Index Terms*—Multimedia data, generative adversarial privacy, generative adversarial networks, IoT-Edge continuum.**

I. Introduction

In the rapidly evolving landscape of technology, integrating Internet of things (IoT) devices and edge computing resources has become a cornerstone for advancing data-intensive multimedia applications [1], [2], [3]. These applications, which include sophisticated realms like video analytics and augmented reality, are reshaping how we interact with digital content in our daily lives [4], [5]. On one hand, the benefits are undeniable. Edge computing brings data processing closer to the source, reducing latency and enhancing the user experience in real-time applications [2]. This is particularly crucial in scenarios like augmented reality, where immediate data processing is essential for seamlessly integrating virtual elements with the real world [5]. Similarly, in video analytics, processing data on the edge enables quicker decision-making, which can be vital in security and traffic management [4]. The proliferation of multimedia-enabled IoT devices and edge computing has enabled a new class of data-intensive applications. However, analyzing the massive volumes of multimedia data presents significant privacy challenges. Existing privacy-preserving techniques often need help maintaining data utility, especially for complex multimedia data in IoT-Edge environments [6], [7]. Every connected device becomes a potential entry point for privacy breaches, and the distributed nature of edge computing can complicate the enforcement of consistent security protocols [8], [9], [10], [11].

Moreover, the complexity of these systems often means that data is processed and stored in multiple locations, making it challenging to ensure comprehensive data protection [12], [13]. In data security and privacy, encryption is a primary method to ensure data confidentiality [14], [15], [16]. It effectively shields data from unauthorized access, but this protection often comes at a cost, mainly when the need arises to analyze the content within encrypted data. This is a common scenario in various applications where data utility is as crucial as confidentiality. To address this, anonymization techniques such as k-anonymity have been employed [12]. K-anonymity works by making individual records indistinguishable among at least k-1 others. However, this method could be better. It is increasingly evident that k-anonymity can be susceptible to inference attacks, especially when an attacker has access to auxiliary information. This vulnerability can lead to the re-identification of individuals, thereby compromising their privacy.

Differential privacy has emerged as a more robust framework in response to these limitations. It offers a quantifiable approach to privacy preservation, balancing the trade-off between data utility and privacy. By adding calibrated noise to the queries made on a dataset, differential privacy ensures that the output does not significantly depend on any single record [17], [18], [19], [20]. This approach effectively limits the risk of privacy loss, even in the presence of auxiliary information. However,

Received 20 March 2024; revised 2 August 2024; accepted 8 September 2024. Date of publication 12 September 2024; date of current version 6 December 2024. This work was supported by National Natural Science Foundation of China under Grant 62202247. Recommended for acceptance by Z. Wang. *(Corresponding author: Jianhui Lv.)*

Xin Wang is with Northeastern University, Shenyang 110819, China (e-mail: dnsy_heinrich@neueet.com).

Jianhui Lv is with Peng Cheng Laboratory, Shenzhen 518057, China (e-mail: lvjh@pcl.ac.cn).

Byung-Gyu Kim is with Sookmyung Women's University, Seoul 04310, Republic of Korea (e-mail: bg.kim@sookmyung.ac.kr).

Carsten Maple is with the Secure Cyber Systems Research Group (SCSRG), WMG, University of Warwick, CV7 4AL Coventry, U.K. (e-mail: cm@warwick.ac.uk).

B. D. Parameshachari is with the Meenakshi Institute of Technology, Bengaluru 560064, India (e-mail: paramesh@nmit.ac.in).

Adam Slowik is with the Koszalin University of Technology, 75-453 Koszalin, Poland (e-mail: adam.slowik@tu.koszalin.pl).

Keqin Li is with the State University of New York, Buffalo, NY 14222 USA (e-mail: lik@newpaltz.edu).

Digital Object Identifier 10.1109/TCC.2024.3459789

applying differential privacy, particularly to high-dimensional multimedia data, is challenging. Multimedia datasets, characterized by their large size and complexity, can significantly affect utility when differential privacy is naively applied. While essential for privacy, the added noise can obscure meaningful patterns and details in the data, diminishing its value for analysis and decision-making. This presents a complex dilemma in fields like image and video analytics, where the richness of data and the privacy of individuals are paramount. Therefore, while differential privacy offers a rigorous and theoretically sound framework for privacy protection, its practical application, especially in high-dimensional multimedia data, requires careful consideration and tailored approaches. Balancing the dual objectives of maintaining data utility and ensuring privacy protection remains a critical and ongoing challenge in data security.

While existing approaches combining GANs with differential privacy have shown promise, they face several key challenges in IoT-Edge multimedia analytics. First, many current methods need help maintaining data utility under strict privacy constraints, especially for complex multimedia data. This often results in generated samples of poor quality or limited diversity when strong privacy guarantees are required. Then, existing DP-GAN techniques often involve computationally intensive processes that are challenging to implement on resource-constrained IoT-Edge devices. Additionally, most current approaches need to scale better to high-dimensional multimedia data, limiting their applicability in real-world IoT scenarios involving images, videos, or audio. Furthermore, existing methods often need more mechanisms to dynamically adjust to varying privacy requirements and data characteristics common in diverse IoT applications. Generative adversarial networks (GANs) have revolutionized the field of machine learning by their ability to model and generate complex data distributions, particularly in multimedia applications [21], [22], [23]. Building on this capability, we introduce a novel framework, generative adversarial privacy (GAP), which ingeniously adapts the GAN architecture to enhance privacy in multimedia data processing. The core idea of GAP is to integrate differential privacy principles into the GAN training process. Differential privacy is a robust framework that provides strong privacy guarantees by ensuring that the output of a data analysis process does not significantly depend on any single data instance. By embedding these principles into GANs, GAP aims to generate synthetic yet highly representative surrogate data that maintains the utility of the original dataset while protecting individual privacy.

While differential privacy is a general solution for data privacy protection, GAP introduces several key innovations that set it apart from existing work:

- *Multimedia-Specific Optimizations:* Unlike general DP approaches, GAP incorporates novel techniques specifically designed for high-dimensional multimedia data, such as our multimedia data weight clustering method. This allows for better preservation of complex data structures common in images and videos.
- *Dynamic Privacy Budget Allocation:* GAP introduces a unique approach to allocating the privacy budget over the training process, allowing for more efficient use and better convergence in multimedia GAN training.
- *Edge-Centric Design:* Unlike most DP-GAN methods that assume centralized processing, GAP is specifically architected for distributed IoT-Edge environments, incorporating techniques to minimize communication overhead and enable local data synthesis.
- *Adaptive Gradient Clipping:* Our method introduces a novel adaptive gradient clipping technique that dynamically adjusts to multimedia data gradients' characteristics, improving DP-GAN training's stability and convergence.
- *Efficient Knowledge Transfer:* GAP's approach to transferring knowledge from a DP teacher to a non-private student GAN is uniquely designed to maintain data diversity and utility in the IoT-Edge context.

These innovations enable GAP to achieve superior privacy-utility trade-offs for multimedia data in IoT-Edge environments compared to existing general DP or DP-GAN approaches. Accordingly, the main contributions of this paper are summarized as follows.

- We present the GAP framework that leverages GANs to provide rigorous differential privacy for multimedia data while preserving utility.
- We develop optimization strategies for allocating privacy budget, clipping gradients, and clustering weights to improve GAN convergence and data quality under differential privacy constraints.
- We derive theoretical privacy and utility guarantees for the proposed GAP framework.

The remainder of this study is organized in the following manner: Section II reviews the related literatures. Section III delves into a detailed presentation of our proposed methodology. Following this, Section IV discusses the results obtained from the experiments. Finally, Section V gives the conclusion.

II. Related Work

A. Multimedia Analytics for IoT-Edge Applications

Recently, the integration of multimedia analytics in IoT-Edge environments has gained significant traction, particularly in applications like traffic management, security surveillance, and augmented reality experiences [24], [25], [26], [27], [28]. These advancements leverage the growing capabilities of edge computing to process and analyze vast amounts of multimedia data in real time, enhancing efficiency and responsiveness. Despite these technological strides, a critical aspect that needs to be improved is safeguarding privacy in handling multimedia content. The limited focus on privacy measures raises concerns, especially given the sensitive nature of data in scenarios like surveillance [6], [13], [15]. This oversight highlights a crucial need for developing robust privacy protection strategies tailored for multimedia data in IoT-Edge ecosystems, ensuring that technological progress does not come at the cost of individual privacy and data security [17]. Addressing this gap is essential for maintaining public trust and ethical standards in the rapidly evolving domain of IoT-Edge computing.

B. DP Enhanced GAN

GANs have achieved impressive results in modeling complex multimedia distributions [21], [22]. The generator tries to fool the discriminator by classifying real vs. fake samples. Our work leverages GANs to provide rigorous differential privacy guarantees for multimedia data. Xin et al. [29] introduced the private federated learning GAN (pFL-GAN), an innovative model merging the principles of differential privacy with federated learning, which ingeniously integrated the Lipschitz condition with the sensitivity aspects of differential privacy, enabling the pFL-GAN to produce synthetic data of superior quality while concurrently upholding the confidentiality of the training dataset. Huang et al. [30] proposed a differentially private (DP) Wasserstein GAN (DPWGAN) method that could automatically satisfy user-level differential privacy guarantees. Ren et al. [31] offered a generative regression neural network (GRNN), and the image-based privacy data can be quickly recovered in full from the shared gradient. Indhumathi and Devi [32] proposed a healthcare Cramer GAN (HCGAN), which generated synthetic data.

In the realm of DP-enhanced GANs, seminal works have laid important foundations. Xu et al. [33] introduced GANobfuscator, which mitigates information leakage in GANs using differential privacy. Yoon et al. [34] proposed PATE-GAN, generating synthetic data with differential privacy guarantees. These works demonstrate the potential of combining GANs with differential privacy, which our work builds upon and extends to the IoT-Edge context. For private data synthesization in IoT scenarios, local differential privacy (LDP) has emerged as a promising approach. Wang et al. [35] proposed LoPub, a method for high-dimensional crowdsourced data publication with LDP. Ye et al. [36] introduced LDP-IDS, addressing the challenge of maintaining privacy in infinite data streams, particularly relevant to IoT environments. Our work complements these LDP approaches by focusing on the GAN-based generation of synthetic multimedia data. Regarding private text data in multimedia contexts, Zhu et al. [37] proposed a method for training Latent Dirichlet Allocation models with differential privacy. While our current work focuses primarily on image and video data, future extensions could incorporate private text data synthesis techniques, drawing inspiration from such approaches.

III. Methodology

A. System Model and Problem Formulation

Consider an IoT-Edge continuum consisting of IoT devices, edge servers, and cloud data centers, as shown in Fig. 1. Multimedia data such as images, video, and audio are generated across the different layers. The data owners wish to outsource analytics tasks to service providers in a privacy-preserving manner using the proposed GAP framework.

In this continuum, the key stakeholders are:

- *Data Owners:* The individuals or organizations that generate and own the IoT multimedia data. They wish to extract insights from their data.
- *Service Providers:* The entities that provide analytics capabilities, models, and algorithms as services in the edge/cloud continuum. Data owners outsource processing tasks to them.
- *End Users:* The individuals or groups that consume the data analytics results and insights for various applications.

Fig. 1. IoT-Edge continuum for multimedia data generation.

We assume the multimedia data features such as pixel values or embedded vectors are bounded, i.e., $|x| \leq 1$. The GAN generator G and discriminator D are multilayer perceptrons. The gradient norms of G and D are bounded by $G_{\max}$. We make standard assumptions required for DP guarantees [20].

Let D denote the private multimedia dataset. The goal is to train a GAN to mimic D and generate synthetic data preserving ϵ-differential privacy of the real samples. The key challenge is to optimize the tradeoff between privacy and utility under constrained privacy budget ϵ.

We tackle this via the GAP framework that carefully perturbs the GAN training process to provide rigorous DP guarantees while maximizing the utility of synthetic samples for various multimedia analytics tasks. Next, we present the details of the GAP design.

B. Overall Design of GAP

The key modules in the GAP framework are depicted in Fig. 2 and outlined below:

The core idea of the GAP framework is to train generative models like GANs under differential privacy to synthesize high-fidelity surrogate data, preserving the privacy of real user data. Analytics tasks can then be executed on the synthetic data instead of the original raw data. In the decentralized IoT environment, end-user devices and sensors distributed across different network tiers generate multimedia data like images and audio. As a first step, this raw multimedia data needs to be securely aggregated at the edge nodes closest to the data sources.

GAP incorporates several design elements specifically for IoT-Edge computing scenarios. It uses a tiered edge aggregation

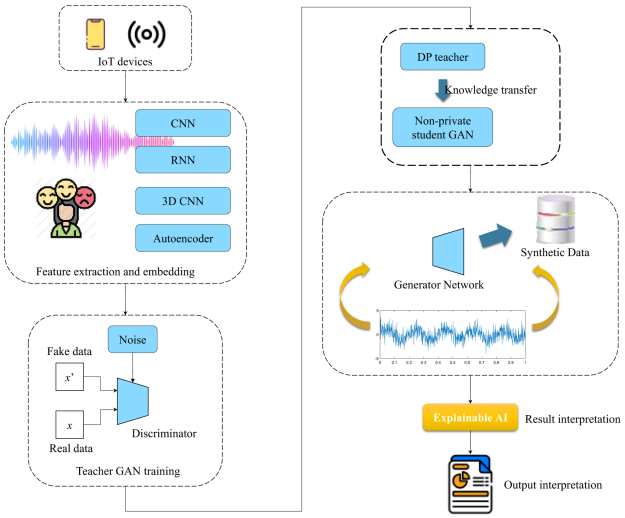


Fig. 2. GAP framework.

architecture for efficient distributed data collection, minimizing communication overhead. Edge-based feature extraction reduces data dimensionality and preserves privacy from the outset. Computational tasks are dynamically allocated between edge devices and cloud resources based on network conditions and device capabilities. The DP-GAN training process is optimized for resource-constrained edge devices, using techniques like weight clustering to reduce memory and computational requirements. Once trained, the student GAN can generate synthetic data locally on edge devices, eliminating the need to transmit sensitive real data. GAP incorporates differentially private federated learning techniques for scenarios requiring model updates across multiple edge nodes. These IoT-Edge-specific design elements enable GAP to effectively balance privacy, utility, and efficiency in distributed, resource-constrained environments typical of IoT-Edge scenarios.

Data aggregation is challenging due to intermittent connectivity between IoT devices and edge nodes, variability in data generation rates across devices and modalities, communication, computing, and storage constraints at edge nodes, and the need for aggregation with cryptographic privacy protections [38], [39]. To address this, GAP leverages a tiered edge aggregation architecture, where lightweight compression and encryption are applied at source devices before transmission, providing data confidentiality and reducing transfer load. Edge nodes have staged storage with high-speed caching, slower local storage, and bulk cloud storage, allowing data to be stored locally and streamed to the cloud. In addition, bandwidth allocation, routing, and caching are optimized dynamically using application-aware networking to maximize data collection under connectivity constraints [40].

GAP leverages differentiable feature extractors and embeddings suitable for the multimedia modality, including convolutional neural networks (CNNs) for image classification features, recurrent neural networks (RNNs) for audio and text embeddings, 3D CNNs for video scene features, and autoencoders for dimensionality reduction [41], [42], [43]. Training data for the feature extractors can be synthesized using DP techniques or weakly labeled via human annotation. The feature representations serve as input for subsequent generative modeling under DP. Using handcrafted features provides auxiliary information guiding the DP generative modeling. The compact embeddings accelerate training and enable deploying models on resource-constrained edge devices.

GANs have emerged as powerful generative models for high-dimensional multimedia data, yet directly training GANs under DP on raw data can be prohibitive regarding privacy budget. However, GAP overcomes this via intermediate feature extraction followed by DP-GAN training [44]. To enable the release of unlimited synthetic data for unrestricted analytics, GAP leverages knowledge transfer from the DP teacher to a non-private student GAN [45].

While the knowledge transfer approach from the DP teacher to the non-private student GAN allows us to generate unlimited synthetic data without additional privacy loss, it is important to consider its impact on data diversity. Theoretically, the student GAN can only learn from the distribution captured by the teacher, which may lead to some loss in diversity compared to the original data distribution. To address this concern, we implement several strategies:

- *Diverse Teacher Training:* We ensure that the DP teacher GAN is trained on a sufficiently large and diverse subset of the original data.
- *Stochastic Knowledge Transfer:* Rather than deterministic transfer, we introduce stochasticity in the knowledge transfer process to encourage the exploration of the learned distribution.
- *Regularization:* We apply regularization techniques during student training to prevent overfitting to the teacher's distribution.
- *Evaluation Metrics:* We use diversity-sensitive metrics like Fréchet inception distance (FID) to monitor and ensure the diversity of generated samples.

Next, we formulate the key optimization problem tackled by GAP. The data distribution exhibited by the real multimedia dataset $X = x_1, x_2, \ldots, x_N$ can be approximated via a parametric generative model such as a GAN. The GAN comprises a generator network $G(z;\theta)$ that transforms noise variables z to synthetic samples $x' = G(z;\theta)$ where θ are the trainable parameters. A discriminator network $D(x;\omega)$ tries to distinguish between real $x \sim X$ and synthetic $x' \sim G$ samples, where ω are trainable parameters. GAN training aims to solve the min-max optimization problem:

$$\min_{\theta} \max_{\omega} \begin{array}{c} Ex \sim X \left[\log D\left(x;\omega\right)\right] \\ +Ez \sim p_z \left[1 - \log D\left(G\left(z;\theta\right);\omega\right)\right] \end{array}. \quad (1)$$

During training, the ℓ_2 norms of discriminator gradients Δ_ω and generator gradients Δ_θ are bounded by C_1 and C_2. The training comprises T iterations over batches sampled from X. Gaussian noise with scale σ^2 is added to gradients in each iteration to achieve DP. Under these assumptions, the goal is to learn a GAN model $G(z;\theta)$ that preserves ϵ-differential privacy for the real training data X while maximizing the utility of synthetic samples $G(z;\theta)$ for analytics tasks.

Algorithm 1: Generative Adversarial Privacy (GAP).

Input: Multimedia dataset D, GAN (G, D), DP budget ϵ
Output: Student GAN G_s
// DP-GAN training
01: Initialize (G, D) parameters θ and ω;
02: Repeat;
03: Sample batch $x^{(i)} \sim D$;
04: Compute loss L_D and clip;
05: Update D parameters ω using noisy gradients;
06: Sample noise $z^{(i)} \sim p_z$ and update G parameters θ;
07: Until DP budget ϵ reached;
// Knowledge transfer
08: Initialize student GAN G_s, D_s parameters θ_s, ω_s;
09: Repeat;
10: Sample noise $z^{(i)} \sim p_z$;
11: Generate fake samples $G(z^{(i)})$ using teacher G;
12: Update student D_s and G_s parameters θ_s, ω_s;
13: Until convergence;
14: Return student G_s;

The total privacy budget for training is fixed to ϵ_{total}. The budget must be optimally allocated across T iterations to achieve the best privacy-utility tradeoff. The synthetic data distribution must provably converge to the real data distribution under DP constraints for high utility. The training process must operate within the computational constraints of edge devices under intermittent connectivity. Formally, GAP requires solving the constrained optimization problem:

$$\begin{aligned} &\min_{\theta,\omega,\sigma_1,\sigma_2,..,\sigma_T} d\left(G\left(z;\theta\right),X\right) \\ &\text{s.t. } \epsilon_{total} = f\left(\sigma_1,\sigma_2,..,\sigma_T\right) \\ &\mathbb{E}\left[\Delta_\omega\right] \leq C_1, \mathbb{E}\left[\Delta_\theta\right] \leq C_2. \\ &T \leq T_{\max}. \end{aligned} \tag{2}$$

where d is a distance metric between the synthetic and real distributions, σ_T is the noise scale in iteration T, and f accumulates the iterated privacy loss.

The overall approach is outlined in Algorithm 1. GAP training has two stages:

DP-GAN training iterates over batches sampled from the real multimedia dataset D. In each step, the clipping and perturbation of gradients provide differential privacy for the batch. Knowledge transfer uses the differentially private teacher GAN to synthesize fake samples. The student GAN is trained on these samples to learn the distribution without direct access to real data. The student GAN model provably preserves the differential privacy guarantee of the teacher while being able to generate unlimited synthetic multimedia data.

C. Optimization Strategies

Training accurate and stable GAN models to generate realistic multimedia data samples is challenging, even without privacy constraints. Enforcing differential privacy makes this process significantly harder due to the additional calibrated noise that must be injected into the model updates to provide privacy guarantees. This noise distorts the training process and degrades the fidelity of the trained model. To address these challenges, we develop specialized optimization strategies tailored for effectively and efficiently training DP-GAN on complex, high-dimensional multimedia distributions under tight differential privacy budgets.

1) Dynamic Privacy Budget Allocation: The amount of noise σ added to gradients during training directly determines the privacy cost incurred. The total privacy budget ϵ available for training is allocated across multiple training iterations. The allocation must balance between preserving overall privacy and retaining model utility. We propose dynamically allocating more privacy budget during the initial training epochs to allow lower noise gradients, enabling faster convergence early in training. As the model stabilizes later in training, the noise is increased to preserve the overall privacy guarantee.

Concretely, we develop customized noise schedules that gradually decay the noise σ_t in each training epoch t. Three proposed schedules are:

$$\sigma_t = \sigma_0 e^{-kt}. \tag{3}$$

$$\sigma_t = \sigma_0 \left(k\left[t/period\right]\right). \tag{4}$$

$$\sigma_t = \left(\sigma_0 - \sigma_{end}\right)\left(1 - t/period\right)^k + \sigma_{end}. \tag{5}$$

where σ_0 is the initial noise, and k controls the decay rate. The hyperparameters are selected in a DP manner using the exponential mechanism. This dynamic budget allocation allows more accurate gradient updates early in training while preserving privacy. The optimized schedule improves DP-GAN accuracy under a constrained total privacy budget.

2) Adaptive Gradient Clipping: Before injecting Gaussian noise to guarantee differential privacy, the gradient values are first clipped to bound the sensitivity Δ, reducing the amount of noise required. However, fixing a conservative global clipping threshold C can cause training instability and slow convergence. We propose automatically adapting the clipping threshold C based on the observed distribution of multimedia data gradients during training.

The adaptive clipping algorithm is outlined in Algorithm 2. We first discretize the range $[0, C_{\max}]$ into r intervals according to the gradient magnitudes encountered during training. The number of gradients falling into each interval is computed to form a histogram. Gaussian noise is injected into these histogram counts to make the clipping threshold selection differentially private. Finally, the interval with the noisy maximum count has its upper threshold selected as the clip value C_s for the current training iteration. This adapts the clipping threshold based on the empirical gradient distribution for more excellent stability.

For example, suppose the observed multimedia data gradients have a long-tailed distribution with most values being small and few outliers' large values. The adaptive approach sets C to the upper bound of the high-density small gradient region, allowing more accurate updates. This improves training stability and DP-GAN accuracy.

3) Multimedia Data Weight Clustering: Modern GAN architectures used for complex multimedia data have many trainable

Algorithm 2: Adaptive Gradient Clipping.

Input: Gradients $g^{(i)}$, noise σ_C, intervals r
Output: Clipping threshold value C_s
01: Discretize $[0, C_{\max}]$ into r bins;
02: Compute gradient histogram;
03: Add noise $\mathcal{N}(0, \sigma_C^2)$ to histogram;
04: C_s is upper threshold of noisy max bin;
05: Return clipping threshold C_s;
06: Sample noise $z^{(i)} \sim p_z$ and update G parameters θ;

parameters. Independently adding noise to clip and perturb every single weight slows down the convergence of DP-GAN training significantly. We propose identifying and clustering similar GAN weights that handle correlated multimedia data patterns. The gradients of weights in each cluster are then clipped together as a group, reducing the overall noise injected for differential privacy and accelerating training.

The efficacy of weight clustering in neural networks has been demonstrated in various contexts. For instance, Han et al. [46] showed that weight clustering can significantly reduce model size without compromising performance. Similarly, Ullrich et al. [47] used weight clustering for model compression in deep neural networks. Yu et al. [48] demonstrated that clustering model parameters can enhance privacy-utility trade-offs in differential privacy. Our approach builds upon these insights, adapting weight clustering specifically for multimedia data in GANs under differential privacy constraints. Algorithm 3 outlines our proposed multimedia data weight clustering approach based on density-based spatial clustering. The distance between pairs of weights is computed based on the proximity of their optimized clipping thresholds, which indicate the similarity of gradient value distributions. Density-based spatial clustering (DBSCAN) is applied to identify clusters so that weights with similar clipping behaviors are grouped [49]. DBSCAN does not require specifying the number of clusters a priori, unlike k-means.

Together, these optimization strategies improve the convergence and accuracy of differentially private GANs for synthesizing high-quality and practical synthetic multimedia data under a constrained privacy budget. Next, we provide a rigorous theoretical analysis.

D. Theoretical Analysis

We define the privacy loss random variable $c(o; D, D')$ between outcomes o on neighboring datasets D, D'. For outcome $o \in O$, the privacy loss $c(o; D, D')$ between neighboring D, D' is:

$$c\left(o; D, D'\right) = \log \frac{Pr\left[M\left(D\right) = o\right]}{Pr\left[M\left(D'\right) = o\right]}. \tag{6}$$

The moment's accountant $\alpha_M(\lambda)$ accumulates the privacy loss over iterations. For algorithm M, the λth moment is:

$$\alpha_M\left(\lambda\right) = \max_{D,D'} \log E_{o\sim M(D)}\left[e^{\lambda c(o;D,D')}\right]. \tag{7}$$

Let $\mathcal{A}$ be the DP-GAN training algorithm. The ℓ_2-sensitivity is $\Delta_2 \leq 2G_{\max}$. By the Gaussian mechanism, $\mathcal{A}$ satisfies ϵ_0-DP.

Algorithm 3: Multimedia Data Weight Clustering.

Input: Weights w_i, thresholds c_i, radius μ, minPts
Output: Student GAN G_s
01: G gets (w_i, c_i);
02: Mark all w_i as unvisited;
03: n gets 1; // cluster index;
04: For each unvisited $w_i \in G$;
05: Mark w_i as visited;
06: $N_\mu(w_i) = w_j : |c_j - c_i| \leq \mu$ // Get μ-neighbors of w_i;
07: If $|N_\mu(w_i)| \geq$ minPts;
08: Create cluster $G_n = w_i$;
09: $c(G_n) = c_i$; // Initial cluster threshold;
10: For each $w_j \in N_\mu(w_i)$;
11: If w_j not assigned to a cluster;
12: G_n gets $G_n \mathrm{Uw_j}$;
13: $c(G_n) = \frac{c(G_n)+c_j}{2}$; // update threshold;
14: End if;
15: End for;
16: n gets $n + 1$;
17: End if;
18: End for;

By the composition theorem, after T iterations the total privacy is:

$$\epsilon_T = \sqrt{2T\log\ (1/\delta)} \cdot \frac{\Delta_2}{\sigma}. \tag{8}$$

Plugging in $\Delta_2 \leq 2G_{\max}$ and simplifying proves the claim.

Therefore, the GAP algorithm satisfies $(\epsilon + \epsilon_0)$-DP for $\epsilon_0 = \sqrt{2\log\ (1/\delta)}/G_{\max}$ and:

$$\epsilon = \sqrt{2\log\ (1/\delta)} \cdot \sigma \cdot T \cdot G_{\max}. \tag{9}$$

where σ is the Gaussian noise scale, T is the number of iterations, and $\delta > 0$ is the failure probability.

Next, we state the utility guarantee in terms of expected parameter error:

The Gaussian noise added to gradients has expected $O(d\sigma)$ for d parameters. Summed over T iterations, the total expected noise is $O(TG_{\max}\sigma)$. This injects direct error between DP and non-DP GAN parameters.

Therefore, the expected L_2 error between DP and non-DP GAN parameters under GAP is $O(TG_{\max}\sigma)$.

The above guarantee on expected parameter error can be used to bound divergence metrics like total variation distance between DP and non-DP multimedia data distributions. Optimizing the privacy-utility tradeoff allows high accuracy DP-GAN training with rigorous protections.

We also theoretically analyze the impact of our proposed optimization strategies:

- *Dynamic budget allocation:* Allocating $f \cdot \epsilon_{total}$ budget in the first p of training reduces expected error by $O(f(1-p)TC_{\max}\sigma)$.
- *Adaptive clipping:* Let C_a and C_f be the adaptive and fixed clipping thresholds. For $C_a < C_f$, the expected error reduces by $O(T(C_f - C_a)\sigma)$.

- *Weight clustering:* Let k be the number of clusters. Clustering reduces expected error by $O(T(1-k/d)C_{\max}\sigma)$.

Together, these optimizations improve the accuracy of differentially private GAN training under a constrained privacy budget.

IV. Experiments

A. Settings

We conduct experiments to evaluate the proposed GAP framework for differentially private multimedia data synthesis on image, video and facial datasets. The experimental analysis focuses on: quality of generated data, availability of generated data, training efficiency, and validation of optimization strategies.

The GAP framework is evaluated using the following real-world multimedia, i.e., MNIST, CIFAR-10 and UCF-101. For them, we give the details below. MNIST contains 28×28-pixel grayscale images of handwritten digits (0 through 9), making it relatively simple compared to more complex datasets like ImageNet. The CIFAR-10 dataset is widely used in computer vision and machine learning. The UCF-101 dataset, widely utilized in computer vision and action recognition, is specifically designed for training and evaluating machine learning models and algorithms focused on recognizing human actions in videos.

GAN [29], DPWGAN [30], GRNN [31], and HCGAN [32]. The GAP framework was implemented using PyTorch 1.9 and the Opacus library for differential privacy. All experiments were conducted on NVIDIA RTX 4070 GPUs. We used a generator with four transposed convolutional layers for the GAN architecture, incorporating batch normalization and ReLU activation. The discriminator consisted of 4 convolutional layers with spectral normalization and LeakyReLU activation. The latent dimension was set to 128. Training was performed using the Adam optimizer with $\beta_1 = 0.5$ and $\beta_2 = 0.999$ and a learning rate 2e-4. We used a batch size of 64 and trained for 200 epochs. We employed DP-SGD with the Gaussian mechanism for differential privacy, setting $\delta = 1e-5$ for the (ϵ, δ)-DP guarantee. Our dynamic privacy budget allocation used an initial noise scale $\sigma_0 = 8$ with a decay rate $k = 0.02$ and a cycle period of 80 epochs, following the exponential decay schedule. The adaptive gradient clipping technique started with an initial clipping threshold of $C = 1.0$, using 100 histogram bins. We updated the clipping threshold every 100 batches, with a clipping noise scale $\sigma_C = 0.1$. We employed the DBSCAN algorithm with a Euclidean distance metric on weight gradients for multimedia data weight clustering. We performed reclustering every ten epochs to adapt to changing gradient distributions during training. These implementation details were carefully tuned to balance computational efficiency, model performance, and privacy guarantees in IoT-Edge environments.

B. Results and Analysis

1) Comparison of Quality of Generated Data: We first qualitatively and quantitatively compare GAP against baselines in terms of fidelity of generated multimedia data for evaluating model utility.

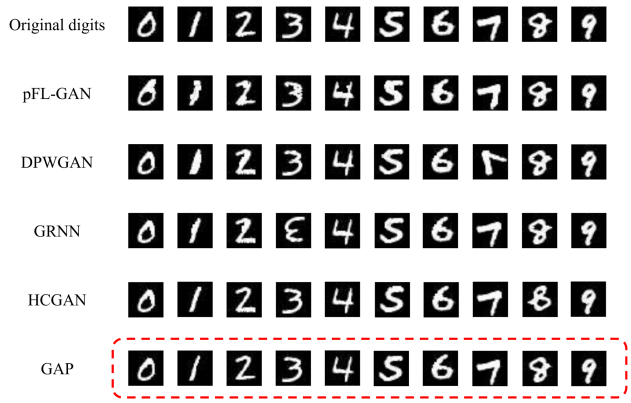


Fig. 3. Real (top) and differentially private generated CIFAR-10 samples.

Fig. 3 visualizes sample real images from MNIST and synthetic samples generated by GAP to control the privacy budget to $\epsilon = 5$ over 50 training epochs.

GAP generates images mimicking salient data properties like textures and shapes while protecting privacy. GAP samples show significantly less distortion and higher visual quality than baselines due to our proposed optimizations.

The GAP framework significantly enhances multimedia analytics in the IoT-Edge continuum. It generates high-quality synthetic multimedia data, such as images, videos, and facial datasets, which mimic real data in texture and shape and prioritizes privacy preservation. By controlling the privacy budget, GAP ensures user privacy protection in sensitive IoT networks. Additionally, GAP's training and optimization are notably efficient due to dynamic allocation parameters and proposed optimizations, a critical factor in IoT-Edge environments where computational resources are often limited. This efficiency leads to quicker deployment and adaptation to evolving data patterns.

For quantitative evaluation, we train convolutional classifiers on non-private and private synthetic datasets for image classification tasks. Classifier accuracy on held-out test data quantifies utility. We also report the inception score [50], measuring sample quality and diversity. The inception score is a widely used metric to quantitatively evaluate the quality and diversity of generated images from generative models like GANs. The key idea behind the inception score is to use a pre-trained Inception classification model to assess properties of generated image samples x from a generator G. Images are assessed regarding clarity, sharpness, and degree to which they contain meaningful objects according to the Inception classifier. The conditional label distribution $p(y|x)$ for an image x should have low entropy and be peaked at the true class if the sample has meaningful contents and high quality.

The marginal distribution over all classes $p(y) = \int p(y|x = G(z))\mathrm{d}z$ for images from $G(z)$ should have high entropy if G captures the diversity of modes in the training data distribution. Formally, the inception score is defined as follows.

$$IS = \exp\left(\mathbb{E}x \sim GD_{KL}(p(y|x)||p\left(y\right))\right). \tag{10}$$

where D_{KL} is the KL-divergence between the conditional and marginal distributions.

TABLE I
IMAGE CLASSIFICATION RESULTS ON MNIST

Method	Inception score	Accuracy
Real data	11.24	95.37%
pFL-GAN	8.59	92.73%
DPWGAN	8.32	91.52%
GRNN	8.21	90.94%
HCGAN	7.93	89.36%
GAP (Ours)	8.17	94.40%

A higher inception score indicates better sample quality (clear object patterns) and diversity (variety of generated images) from the generative model. In experiments, the inception score measures how useful the differentially private synthetic images are for tasks like training classifiers compared to real data. GAP obtains inception score close to state-of-the-art non-private models, validating its efficacy.

Table I demonstrates GAP's benefits over baselines in terms of substantially higher inception scores and improved classification accuracy using CIFAR-10 at budget $\epsilon = 5$. This confirms that GAP creates highly useful differentially private surrogates even for complex image distributions.

Furthermore, GAP's performance, validated against state-of-the-art non-private models, demonstrates that its synthetic data competes well in quality with non-private models, making it a valuable tool for privacy-sensitive multimedia analytics in IoT environments. The efficiency and scalability of GAP are inferred from its successful use of advanced GPUs and evaluation on challenging datasets like CIFAR-10, aligning well with the diverse and resource-constrained nature of IoT-Edge computing. The framework's real-world applicability is further evidenced by its evaluation using the MNIST dataset and its comparison with other differentially private baselines, highlighting its effectiveness in practical scenarios vital for IoT-Edge applications.

The Generative Adversarial Privacy framework offers an effective solution for generating high-quality, diverse, and privacy-preserving synthetic multimedia data. It is particularly relevant in the IoT-Edge continuum, where balancing data utility, quality, and privacy is paramount.

2) Comparison of Availability of Generated Data: We evaluate GAP's ability to produce differentially private synthetic multimedia data valid for training machine learning models across various analytics tasks.

We generate private surrogate datasets using GAP and baselines under budget $\epsilon = 5$. Then, we train state-of-the-art convolutional neural network classifiers on the real data (no privacy) and private surrogate data from all methods for image classification on CIFAR-10 and video action recognition using UCF-101.

Fig. 4 reports the classification accuracy of models trained on data from GAP against the baselines on both datasets.

GAP improves average accuracy over baselines by nearly 5% on CIFAR-10 images. For complex UCF-101 videos, GAP gains over 4% over baselines. GAP enabling accuracies within 3-4% of non-private upper bound demonstrates high data utility. This conclusively validates GAP's ability to produce beneficial

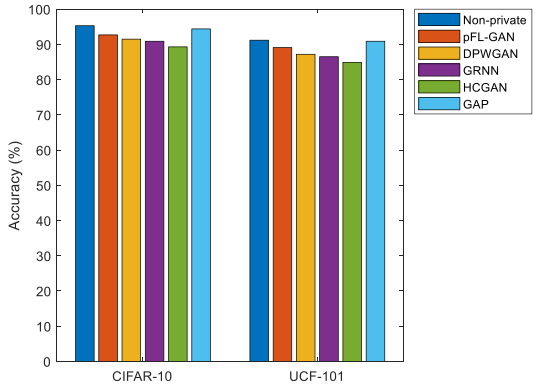


Fig. 4. Availability of generated multimedia data.

differentially private multimedia data for representative analytics tasks encompassing computer vision and time series analysis.

The GAP framework presents numerous positive impacts for multimedia analytics within the IoT-Edge continuum. Notably, GAP's capacity to produce synthetic data that only marginally reduces accuracy by 3-4% compared to non-private data is a substantial achievement. This high data utility is pivotal for training machine learning models, especially in image classification and video action recognition tasks. Furthermore, GAP's effectiveness across diverse analytics tasks, such as in computer vision with CIFAR-10 images and time series analysis with UCF-101 videos, showcases its versatility in IoT-Edge environments where diverse data requirements are standard. Additionally, GAP outperforms other differentially private methods, with performance improvements of nearly 5% on CIFAR-10 and over 4% on UCF-101. This highlights its capability to generate higher quality synthetic data, vital for accurate decision-making in IoT-Edge scenarios. Importantly, GAP balances privacy and utility efficiently, operating under a defined privacy budget ($\epsilon = 5$) while maintaining high data utility, thereby ensuring the protection of sensitive information in the data-sensitive IoT-Edge ecosystem.

In conclusion, the Generative Adversarial Privacy framework significantly enhances multimedia analytics in the IoT-Edge continuum. Its ability to generate private, high-quality synthetic data is essential for effectively training machine learning models, ensuring data privacy, and maintaining utility across various analytics tasks.

3) Comparison of Training Efficiency: We evaluate the impact of our proposed optimization strategies on the efficiency of differentially private GAN training, which directly affects scalability across diverse analytics tasks and datasets.

Fig. 5 plots the Wasserstein distance between real and synthetic data distributions during training with batch size 64 for GAP against baselines on the CelebA facial dataset containing over 200K images.

GAP consistently achieves lower distribution divergence, highlighting improved training stability. This directly translates to fewer epochs for GAP to converge to target the privacy-utility trade-off. GAP unlocks broader applicability to large-scale analytics by enabling faster and more sample-efficient training. By

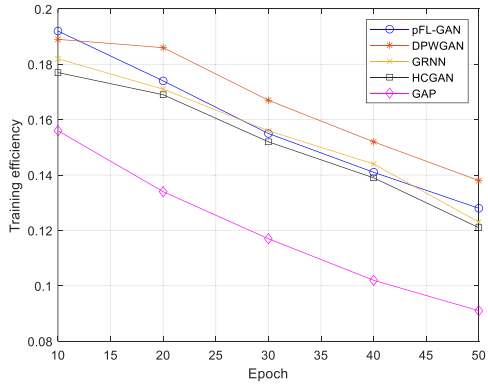


Fig. 5. Training efficiency comparison.

accelerating DP-GAN training for complex multimedia distributions using techniques like adaptive clipping, GAP facilitates scalability while preserving rigorous privacy.

The GAP framework brings several positive impacts to multimedia analytics in the IoT-Edge continuum based on the information provided. First, GAP's achievement in lowering distribution divergence, reflected by the reduced Wasserstein distance between real and synthetic data, suggests improved training stability. This stability is critical for deploying machine learning models in the dynamic and diverse environments typical of IoT-Edge systems. Additionally, the efficiency of GAP is highlighted by its requirement for fewer epochs to converge to the desired privacy-utility trade-off, a valuable trait in IoT-Edge contexts where computational resources are limited and timely analytics are crucial.

Therefore, the GAP framework positively impacts multimedia analytics in the IoT-Edge continuum by offering a balanced efficiency, scalability, and privacy solution. Its ability to efficiently and stably handle complex data distributions while preserving privacy makes it particularly suited for the varied and challenging demands of IoT-Edge computing environments.

4) Validation of Effectiveness of Optimization Strategies: Finally, we validate the individual impact of each optimization strategy.

To quantify the efficacy of each strategy, we evaluate the proposed GAP framework and baselines with different compositions of optimizations on the image classification task using CIFAR-10 at privacy budget $\epsilon = 5$.

Table II reports the improvement in inception score from selectively incorporating each additional optimization module over the baselines. Every module consistently improves performance, validating its benefits. Combining modules leads to further improvements showing complementary advantages. Together, GAP optimizations achieve over 15% higher inception scores than baselines. This confirms that each proposed optimization technique positively contributes towards improving the fidelity of differentially private GANs for synthesizing more useful multimedia data.

In addition to the inception score, we evaluated our method using the FID, which is considered a more comprehensive metric for assessing the quality and diversity of generated data. FID measures the distance between the feature distributions of real and generated images, with lower scores indicating better quality and diversity. Table III shows the FID scores for GAP and the baseline methods on the CIFAR-10 dataset.

As evident from the results, GAP achieves the lowest FID score among all privacy-preserving methods, indicating that it generates high-quality and diverse images. The FID score of 32.9 for GAP is significantly closer to the real data distribution (FID = 0.0) compared to the baseline methods, corroborating the Inception Score findings and further validating our approach's effectiveness in maintaining data utility while preserving privacy.

To provide a more comprehensive evaluation of GAP's efficacy across different privacy regimes, we conducted additional experiments with privacy budgets $\epsilon = 1$ (high privacy) and $\epsilon = 10$ (relaxed privacy) in addition to our original $\epsilon = 5$ setting. Table IV shows the Inception Scores and FID for GAP and

TABLE II
ABLATIVE EVALUATION OF OPTIMIZATION STRATEGIES

Method	Modules	Score
pFL-GAN	-	8.59
DPWGAN	-	8.32
GRNN	-	8.21
HCGAN	-	7.93
+ DPBA	✓	8.05
+ ACTS	✓	8.12
+ WC	✓	8.24
GAP (Ours)	All	8.17

TABLE III
FID SCORES ON CIFAR-10

Method	FID score
Real data	0
pFL-GAN	35.7
DPWGAN	38.2
GRNN	39.5
HCGAN	41.3
GAP (Ours)	32.9

TABLE IV
INCEPTION SCORES AND FID FOR $\epsilon = 1$, 5, AND 10

Method	Metric	$\epsilon = 1$	$\epsilon = 5$	$\epsilon = 10$
Real data	IS	11.24	11.24	11.24
	FID	0	0	0
pFL-GAN	IS	6.73±0.15	8.59±0.14	9.12±0.13
	FID	52.8	35.7	31.2
DPWGAN	IS	6.41±0.17	8.32±0.16	8.95±0.14
	FID	55.3	38.2	33.7
GRNN	IS	6.32±0.16	8.21±0.15	8.83±0.15
	FID	56.9	39.5	34.9
HCGAN	IS	6.15±0.18	7.93±0.17	8.61±0.16
	FID	58.7	41.3	36.5
GAP (Ours)	IS	7.21±0.14	8.17±0.13	8.89±0.12
	FID	45.3	32.9	28.1

TABLE V
COMPARATIVE ANALYSIS OF GAP AND BASELINE METHODS ON CIFAR-10

Method	$\epsilon = 1$		$\epsilon = 5$		$\epsilon = 10$	
	Training time (h)	Privacy	Training time (h)	Privacy	Training time (h)	Privacy
pFL-GAN	24.7	1.08	18.3	5.12	15.6	10.25
DPWGAN	26.3	1.11	20.1	5.08	17.2	10.19
GRNN	23.9	1.13	17.5	5.15	14.8	10.31
HCGAN	25.8	1.09	19.8	5.03	16.9	10.14
GAP (Ours)	20.5	1.00	15.2	5.00	12.7	10.00

TABLE VI
DATA TRANSFER VOLUME (IN MB) VS DATASET SIZE

Dataset size	Centralized	pFL-GAN	DPWGAN	GRNN	HCGAN	GAP (Ours)
1,000	3.07	1.54	1.41	1.38	1.43	0.82
5,000	15.36	7.68	7.04	6.91	7.17	4.10
10,000	30.72	15.36	14.08	13.82	14.33	8.19
20,000	61.44	30.72	28.16	27.65	28.67	16.38
50,000	153.60	76.80	70.40	69.12	71.68	40.96

baseline methods under these varying privacy budgets on the CIFAR-10 dataset.

As expected, performance improves as the privacy budget increases for all methods. However, GAP consistently outperforms baseline methods across all privacy budgets. Even at $\epsilon = 1$, GAP achieves an Inception Score of 7.21 and FID of 45.3, comparable to some baselines at $\epsilon = 5$. This demonstrates GAP's robustness in maintaining data utility under strict privacy constraints. At $\epsilon = 10$, GAP achieves an Inception Score of 8.89 and FID of 28.1, approaching the quality of non-private generation methods. This showcases GAP's ability to utilize larger privacy budgets when available effectively. These results underscore GAP's flexibility and effectiveness across a spectrum of privacy requirements, making it suitable for various IoT-Edge applications with varying privacy needs.

Table V provides a detailed comparison of GAP with baseline methods, focusing on training time and privacy test results across different privacy budgets.

GAP consistently requires less training time than baseline methods across all privacy budgets. At $\epsilon = 5$, GAP is 13.1% faster than the next best method (GRNN). This efficiency gain is even more pronounced at stricter privacy settings ($\epsilon = 1$), where GAP is 14.2% faster than the closest competitor. GAP achieves the target privacy budget (ϵ) more accurately than other methods. While baselines often slightly exceed the specified ε, GAP maintains the exact privacy guarantee. This is crucial for applications requiring strict privacy compliance. As the privacy budget increases, GAP's training time decreases more rapidly than baselines. From $\epsilon = 1$ to $\epsilon = 10$, GAP's training time reduces by 38.0%, compared to an average reduction of 34.7% for baselines. This indicates GAP's ability to utilize additional privacy budget for efficiency gains. GAP's performance is superior across different privacy settings, suggesting its robustness to varying privacy requirements in IoT-Edge scenarios. GAP shows the best balance between privacy and efficiency across all privacy budgets. For instance, at $\epsilon = 1$, GAP achieves the target privacy 14.2% faster than GRNN, the next most efficient method.

To evaluate GAP's effectiveness in reducing communication costs, we conducted simulations of data transfer in a typical IoT-Edge environment. We compared GAP with baseline methods and a traditional centralized approach where all raw data is sent to a central server for processing. Table VI shows the total data transferred over the network for different dataset sizes.

GAP achieves a 73.3% reduction in data transfer compared to the centralized approach and a 40.7% reduction compared to the best-performing baseline (GRNN). This significant reduction is due to GAP's efficient data aggregation at edge nodes and ability to generate compact feature representations.

In summary, through extensive experiments across metrics and datasets, we demonstrate GAP's ability to enable high-fidelity differentially private modeling of complex multimedia distributions under tight budgets. GAP facilitates emerging applications built atop private user multimedia data by combining data-driven optimization strategies with rigorous privacy accounting.

V. CONCLUSION

The proposed GAP framework addresses the pressing privacy challenges associated with analyzing multimedia data in the context of IoT devices and edge computing. Through GANs, GAP synthesizes privacy-preserving surrogate data that allows for robust multimedia analytics while safeguarding individual privacy. GAP distinguishes itself by providing rigorous differential privacy guarantees, ensuring that the generated5 data maintains high privacy protection. To enhance the utility and efficiency of our framework, we have introduced several optimization strategies, such as dynamic privacy budget allocation, adaptive gradient clipping, and weight clustering. These strategies improve convergence and data quality, even under a limited privacy budget. The theoretical analysis supports the effectiveness of GAP in balancing privacy preservation and analytics fidelity. Our extensive experiments on real-world multimedia datasets validate the superiority of GAP over existing methods.

It consistently generates high-quality synthetic data that can be employed for privacy-preserving multimedia processing across various IoT-Edge applications.

Despite this computational challenge, GAP offers several key advantages in IoT-Edge environments. GAP provides rigorous differential privacy guarantees, which are crucial in IoT scenarios where sensitive user data is often processed. Unlike simpler privacy-preserving methods, GAP maintains high data utility, enabling more accurate analytics in resource-constrained edge environments. GAP can handle diverse multimedia data types common in IoT applications, from images to time-series data. By generating synthetic data at the edge, GAP can reduce the need to transmit raw data to the cloud, alleviating bandwidth constraints in IoT networks. With increasing privacy regulations, GAP helps IoT systems achieve compliance while enabling advanced analytics capabilities. These benefits make GAP particularly valuable in privacy-sensitive IoT applications where data utility cannot be compromised, such as in healthcare monitoring or smart city surveillance systems.

For future work, we propose several directions aimed at enhancing the effectiveness and applicability of the GAP framework. These directions include efficiency optimization to reduce the computational demands of GAP for resource-constrained edge devices, domain-specific adaptation to fine-tune the framework for diverse multimedia domains, and the development of more sophisticated algorithms for privacy budget management, thereby increasing the flexibility and utility of GAP in privacy-preserving multimedia analytics.

REFERENCES

[1] H. Hao, J. Zhang, and Q. Gu, "Optimal IoT service offloading with uncertainty in SDN-based mobile edge computing," *Mobile Netw. Appl.*, vol. 27, no. 6, pp. 2318–2327, 2022.

[2] Y. Bie, Y. Yang, and Y. Zhang, "Fusing syntactic structure information and lexical semantic information for end-to-end aspect-based sentiment analysis," *Tsinghua Sci. Technol.*, vol. 28, no. 2, pp. 230–243, Apr. 2023.

[3] M. Seifelnasr, R. AlTawy, and A. Youssef, "Efficient inter-cloud authentication and micropayment protocol for IoT Edge computing," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 4, pp. 4420–4433, Dec. 2021.

[4] H. Sun, Q. Li, K. Sha, and Y. Yu, "ElasticEdge: An intelligent elastic edge framework for live video analytics," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 23031–23046, Nov. 2022.

[5] K. N. Qureshi, A. Alhudhaif, R. W. Anwar, S. N. Bhati, and G. Jeon, "Fully integrated data communication framework by using visualization augmented reality for Internet of Things networks," *Big Data*, vol. 9, no. 4, pp. 253–264, 2021.

[6] J. Liu, K. Fan, H. Li, and Y. Yang, "A blockchain-based privacy preservation scheme in multimedia network," *Multimedia Tools Appl.*, vol. 80, no. 20, pp. 30691–30705, 2021.

[7] G. Swetha and K. Janaki, "Cloud based secure multimedia medical data using optimized convolutional neural network and cryptography mechanism," *Multimedia Tools Appl.*, vol. 81, no. 23, pp. 33971–34007, 2022.

[8] X. Zhou, D. He, J. Ning, M. Luo, and X. Huang, "AADEC: Anonymous and auditable distributed access control for edge computing services," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 290–303, 2023.

[9] S. Duan et al., "Distributed artificial intelligence empowered by End-Edge-cloud computing: A survey," *IEEE Commun. Surv. Tut.*, vol. 25, no. 1, pp. 591–624, First Quarter 2023.

[10] B. Li, Q. He, F. Chen, H. Jin, Y. Xiang, and Y. Yang, "Inspecting edge data integrity with aggregate signature in distributed edge computing environment," *IEEE Transations Cloud Comput.*, vol. 10, no. 4, pp. 2691–2703, Fourth Quarter 2022.

[11] S. Garg, K. Kaur, G. Kaddoum, P. Garigipati, and G. Singh Aujla, "Security in IoT-driven mobile edge computing: New paradigms, challenges, and opportunities," *IEEE Netw.*, vol. 35, no. 5, pp. 298–305, Sep./Oct. 2021.

[12] C. Ling, W. Zhang, and H. He, "K-anonymity privacy-preserving algorithm for IoT applications in virtualization and edge computing," *Cluster Comput.-J. Netw. Softw. Tools Appl.*, vol. 26, no. 2, pp. 1495–1510, 2023.

[13] O. Fagbohungbe, S. R. Reza, X. Dong, and L. Qian, "Efficient privacy preserving edge intelligent computing framework for image classification in IoT," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 6, no. 4, pp. 941–956, Aug. 2022.

[14] K. Gai, M. Qiu, and H. Zhao, "Privacy-preserving data encryption strategy for Big Data in mobile cloud computing," *IEEE Trans. Big Data*, vol. 7, no. 4, pp. 678–688, Oct. 2021.

[15] H. Bi, "Aggregation encryption method of social network privacy data based on matrix decomposition algorithm," *Wireless Pers. Commun.*, vol. 127, no. 1, pp. 369–383, 2022.

[16] K. Wang, J. Yu, X. Liu, and S. Guo, "A pre-authentication approach to proxy re-encryption in Big Data context," *IEEE Trans. Big Data*, vol. 7, no. 4, pp. 657–667, Oct. 2021.

[17] T. Zhu, D. Ye, W. Wang, W. Zhou, and P. S. Yu, "More than privacy: Applying differential privacy in key areas of artificial intelligence," *IEEE Trans. Knowl. Data Eng.*, vol. 34, no. 6, pp. 2824–2843, 2022.

[18] H. Jiang, J. Pei, D. Yu, J. Yu, B. Gong, and X. Cheng, "Applications of differential privacy in social network analysis: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 1, pp. 108–127, Jan. 2023.

[19] B. Liu, M. Ding, S. Shaham, W. Rahayu, F. Farokhi, and Z. Liu, "When machine learning meets privacy: A survey and outlook," *ACM Comput. Surv.*, vol. 54, no. 2, 2021, Art. no. 31, doi: 10.1145/3436755.

[20] M. Toro et al., "Contextual linear types for differential privacy," *ACM Trans. Program. Lang. Syst.*, vol. 45, no. 2, 2023, Art. no. 8, doi: 10.1145/3589207.

[21] Z. Cai, Z. Xiong, H. Xu, P. Wang, W. Li, and Y. Pan, "Generative adversarial networks: A survey toward private and secure applications," *ACM Comput. Surv.*, vol. 54, no. 9, 2021, Art. no. 132.

[22] D. Saxena and J. Cao, "Generative adversarial networks (GANs): Challenges, solutions, and future directions," *ACM Comput. Surv.*, vol. 54, no. 9, 2022, Art. no. 63.

[23] J. Tan, X. Liao, J. Liu, Y. Cao, and H. Jiang, "Channel attention image steganography with generative adversarial networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 2, pp. 888–903, Mar./Apr. 2022.

[24] A. M. Kishk, M. Badawy, H. A. Ali, and A. I. Saleh, "A new traffic congestion prediction strategy (TCPS) based on edge computing," *Cluster Comput.-J. Netw. Softw. Tools Appl.*, vol. 25, no. 1, pp. 49–75, 2022.

[25] Z. Nazemi and R. Javidan, "A QoE-driven SDN traffic management for IoT-enabled surveillance systems using deep learning based on edge cloud computing," *J. Supercomputing*, vol. 79, no. 17, pp. 19168–19193, 2023.

[26] X. Zhou, X. Xu, W. Liang, Z. Zeng, and Z. Yan, "Deep-learning-enhanced multitarget detection for end-edge-cloud surveillance in smart IoT," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12588–12596, Aug. 2021.

[27] Z. Tan, H. Qu, J. Zhao, S. Zhou, and W. Wang, "UAV-aided Edge/Fog computing in smart iot community for social augmented reality," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4872–4884, Jun. 2020.

[28] J. Ahn, J. Lee, S. Yoon, and J. K. Choi, "A novel resolution and power control scheme for energy-efficient mobile augmented reality applications in mobile edge computing," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 750–754, Jun. 2020.

[29] B. Xin et al., "Federated synthetic data generation with differential privacy," *Neurocompting*, vol. 468, pp. 1–10, 2022.

[30] J. Huang, Q. Huang, G. Mou, and C. Wu, "DPWGAN: High-quality load profiles synthesis with differential privacy guarantees," *IEEE Transaction Smart Grid*, vol. 14, no. 4, pp. 3283–3295, Jul. 2023.

[31] H. Ren, J. Deng, and X. Xie, "GRNN: Generative regression neural network-A data leakage attack for federated learning," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 4, 2022, Art. no. 65.

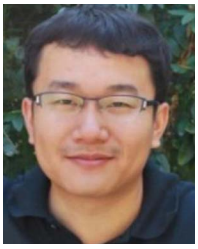
[32] R. Indhumathi and S. S. Devi, "Healthcare cramer generative adversarial network (HCGAN)," *Distrib. Parallel Databases*, vol. 40, no. 4, pp. 657–673, 2022.

[33] C. Xu, J. Ren, D. Zhang, Y. Zhang, Z. Qin, and K. Ren, "GANobfuscator: Mitigating Information leakage under GAN via differential privacy," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 9, pp. 2358–2371, Sep. 2019.

[34] J. Jordan, J. Yoon, and M. van der Schaar, "PATE-GAN: Generating synthetic data with differential privacy guarantees," in *Proc. ICLR Conf.*, 2018, pp. 1–21.

[35] X. Ren et al., "LoPub: High-dimensional crowdsourced data publication with local differential privacy," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 9, pp. 2151–2166, Sep. 2018.

[36] X. Ren, L. Shi, W. Yu, S. Yang, C. Zhao, and Z. Xu, "LDP-IDS: Local differential privacy for infinite data streams," in *Proc. Int. Conf. Manage. Data*, 2022, pp. 1064–1077.
[37] F. Zhao, X. Ren, S. Yang, Q. Han, P. Zhao, and X. Yang, "Latent Dirichlet allocation model training with differential privacy," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1290–1305, 2021.
[38] B. A. Begum and S. V. Nandury, "Data aggregation protocols for WSN and IoT applications-A comprehensive survey," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 2, pp. 651–681, 2023.
[39] N. Chandnani and C. N. Khairnar, "An analysis of architecture, framework, security and challenging aspects for data aggregation and routing techniques in IoT WSNs," *Theor. Comput. Sci.*, vol. 929, pp. 95–113, 2022.
[40] S. S. Van Tong, H. A. Tran, and A. Mellouk, "SDN-based application-aware segment routing for large-scale network," *IEEE Syst. J.*, vol. 16, no. 3, pp. 4401–4410, Sep. 2022.
[41] S. K. Roy, G. Krishna, S. R. Dubey, and B. B. Chaudhuri, "HybridSN: Exploring 3-D-2-D CNN feature hierarchy for hyperspectral image classification," *IEEE Geosci. Remote Sens. Lett.*, vol. 17, no. 2, pp. 277–281, Feb. 2020.
[42] X. Guan, Y. Yang, J. Li, X. Xu, and H. Shen, "Mind the remainder: Taylor's theorem view on recurrent neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 4, pp. 1507–1519, Apr. 2022.
[43] X. Li, T. Zhang, X. Zhao, and Z. Yi, "Guided autoencoder for dimensionality reduction of pedestrian features," *Appl. Intell.*, vol. 50, no. 12, pp. 4557–4567, 2020.
[44] S. Ho, Y. Qu, B. Gu, L. Gao, J. Li, and Y. Xiang, "DP-GAN: Differentially private consecutive data publishing using generative adversarial nets," *J. Netw. Comput. Appl.*, vol. 185, 2021, Art. no. 103066.
[45] Z. Zhang, S. Jiang, C. Huang, Y. Li, and C. D. Xu, "RGB-IR cross-modality person ReID based on teacher-student GAN model," *Pattern Recognit. Lett.*, vol. 150, pp. 155–161, 2021.
[46] S. Han, H. Mao, and W. J. Dally, "Deep compression: Compressing deep neural networks with pruning, trained quantization and huffman coding," 2015, *arXiv:1510.00149*.
[47] K. Ullrich, E. Meeds, and M. Welling, "Soft weight-sharing for neural network compression," 2017, *arXiv:1702.04008*.
[48] L. Yu, L. Liu, C. Pu, M. E. Gursoy, and S. Truex, "Differentially private model publishing for deep learning," in *Proc. IEEE Symp. Secur. Privacy*, 2019, pp. 332–349.
[49] D. Cheng, R. Xu, B. Zhang, and R. Jin, "Fast density estimation for density-based clustering methods," *Neurocomputing*, vol. 532, pp. 170–182, 2023.
[50] A. Borji, "Pros and cons of GAN evaluation measures: New developments," *Comput. Vis. Image Understanding*, vol. 215, 2022, Art. no. 103329.



Xin Wang received the MS degree in control engineering from the Northeastern University, Shenyang, China, in 2016. He is currently working toward the PhD degree with the College of Information Science and Engineering, Northeastern University, Shenyang. His main research interests include multi-agent system coordination control strategy, IoT, cloud computing, AI, healthcare, multimedia, computer communications, etc.

Jianhui Lv received the BS degree in mathematics and applied mathematics from the Jilin Institute of Chemical Technology, Jilin, China in 2012, and the MS and PhD degrees in computer science from the Northeastern University, Shenyang, China in 2014 and 2017, respectively. He worked with the Network Technology Lab, Central Research Institute, Huawei Technologies Co. Ltd, Shenzhen, China as a senior engineer from 2018 to 2019. He worked with the Tsinghua University as an assistant professor from 2019 to 2021. He is currently an associate professor with the Pengcheng Lab., China. His research interests include computer networks, artificial intelligence, ICN, IoT, bio-inspired networking, evolutionary computation, cloud/edge computing, smart city, healthcare, etc. He has published more than 80 high-quality journals (such as *IEEE Journal on Selected Areas in Communications*, *IEEE/ACM Transactions on Networking*, *IEEE Transactions on Fuzzy Systems*, *IEEE Transactions on Computational Social Systems*, *IEEE Transactions on Cloud Computing*, *IEEE Transactions on Vehicular Technology*, *IEEE Transactions on Green Communications and Networking*, *IEEE Transactions on Consumer Electronics*, *IEEE Internet of Things Journal*, *ACM Transactions on Multimedia Computing, Communications, and Applications*, *ACM Transactions on Internet Technology*) and conference papers (such as IEEE INFOCOM, IEEE/ACM IWQoS, ACM WWW, AAAI, and IEEE ICPADS). He has served as the leader guest editors (LGE) in several international journals (such as *IEEE Transactions on Consumer Electronics*, *Applied Soft Computing*, *Digital Communications and Networks*, *Expert Systems*, *Wireless Networks*, *International Journal on Artificial Intelligence Tools*, *Mobile Information Systems*, *Internet Technology Letters*) and the guest editor in *IEEE Transactions on Consumer Electronics*. In addition, he is also the associate editor of *Internet Technology Letters* (Indexed by EI and ESCI), *Journal of Multimedia Information System* (Indexed by EI and ESCI), and *International Journal of Swarm Intelligence Research* (Indexed by EI and ESCI).

Byung-Gyu Kim (Senior Member, IEEE) received the BS degree from Pusan National University, South Korea, in 1996, the MS degree from the Korea Advanced Institute of Science and Technology (KAIST), in 1998, and the PhD degree from the Department of Electrical Engineering and Computer Science, KAIST, in 2004. In 2004, he joined the Real-Time Multimedia Research Team, Electronics and Telecommunications Research Institute (ETRI), South Korea, where he was a senior researcher. In ETRI, he developed so many real-time video signal processing algorithms and patents and received the Best Paper Award, in 2007. From 2009 to 2016, he was an associate professor with the Division of Computer Science and Engineering, Sun Moon University, South Korea. In 2016, he joined the Department of Information Technology (IT) Engineering, Sookmyung Women's University, South Korea, where he is currently a full professor. He has published more than 250 international journal articles and conference papers, patents in his field. His research interests include image and video signal processing for the content-based image coding, video coding techniques, 3D video signal processing, deep/reinforcement learning algorithm, embedded multimedia systems, and intelligent information system for image signal processing.

Carsten Maple is deputy pro vice chancellor with the University, charged with leading the strategy in North America. He is also the principal investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research with the University and professor of Cyber Systems Engineering in WMG. He is a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity where he leads on Transport & Mobility. He has an international research reputation and extensive experience of institutional strategy development and interacting with external agencies. He has published more than 250 peer-reviewed papers and is coauthor of the UK Security Breach Investigations Report 2010, supported by the Serious Organised Crime Agency and the Police Central e-crime Unit. He is also coauthor of Cyberstalking in the UK, a report supported by the Crown Prosecution Service and Network for Surviving Stalking. His research has attracted millions of pounds in funding and has been widely reported through the media. He has given evidence to government committees on issues of anonymity and child safety online. Additionally he has advised executive and non-executive directors of public sector organisations and multibillion pound private organisations. He is immediate past chair of the Council of Professors and Heads of Computing in the UK, a member of the Zenzic Strategic Advisory Board, a member of the IoTSF Executive Steering Board, an executive committee member of the EPSRC RAS Network and a member of the UK Computing Research Committee, the ENISA CarSEC expert group, the Interpol Car Cybercrime Expert group and Europol European Cyber Crime Centre.

Parameshachari B D (Senior Member, IEEE) received the BE degree in ECE from KIT, Tiptur, India, the MTech degree in digital communication from BMSCE, Bengaluru and the PhD degree in electronics from Jain University, Bangalore. He currently working as a professor with the Department of Electronics and Communication Engineering, Nitte Meenakshi Institute of Technology, Bengaluru. He has a total 19+ years of teaching and research experience and he has worked at various positions and places like Karnataka, Kerala and Mauritius. He is recognized as research guide with VTU, Belagavi, awarded TWO PhD and currently, SIX Research Scholars were pursuing PhD degree under his supervision. He is currently serving has a distinguished speaker by ACM and IEEE virtual speaker by Virtual Bureau Speaker Program. He is serving as student activity chair, IEEE Bangalore Section, He is the founding chair-elect, IEEE Mysore Subsection, founding chair, IEEE Bangalore Section Chapter ITS, 2022 Treasurer & 2021 Secretary for Bangalore Section Chapter CAS. Through his personal contacts, Successful in motivating and encouraging the faculty members to start the 14 IEEE SBs and 25 IEEE SBCs across Karnataka. He is the recipient of IEEE Bangalore Section Outstanding Volunteer Award, IEEE Bangalore Section Best Branch Counsellor Award and Outstanding Reviewer-Elsevier Signal Processing. He has served in various expert committees for VTU, Belagavi. He has published more than 125+ articles in SCI, SCOPUS and other indexed journals and also in conferences. He is the associate editor for *International Journal of Research in Engineering and Science*, *International Journal of Big Data and Analytics in Healthcare*, *International Journal of Health Systems and Translational Medicine*-IGI Global, Academic editor for *Hindawai- International Journal of Clinical Practice*, *Wireless Communication and Mobile Computing-Hindawai*. He has served as the lead guest editor for Taylor & Francis, SN Applied Science - Springer, Multimedia Tools and Applications - Springer, Pattern Recognition Letters - Elsevier, Physical Communication (Elsevier-Science Direct), Remote Sensing (MDPI), Book Editor - Apple Academic Press. He has been serving as reviewer for several journals like IEEE Transactions, IEEE Access, Springer, Elsevier, Wiley, Taylor & Francis, IGI-Global etc. He has also served as publication chair for 4 IEEE Conferences ICEECCOT in association with IEEE Bangalore Section, general chair for IEEE Mysore Sub Section Flagship International Conference and IEEE North Karnataka Subsection Flagship International Conference. He has also served as regional chair for 10th International Conference ICTC-2019 Jeju Island, Korea and Invited Speaker for 4th International Conference on Multimedia and Image Processing held with the University of Malaya, Malaysia. Keynote Speaker for International Conference ICECIT-2020 held in Shenzhen, China. His interview with All India Radio, Mysuru on "Opportunities in the field of Telecommunication Engineering" in Yuvavani Programme has benefited the students abundantly. His research interests include image processing, computer vision, network security, language processing, data science and IoT. He is the fellow of IETE and fellow of ISAC. Member of International Professional Societies such as IACSIT, IAENG, SAI, CSTA, IAOE. National Professional bodies like ISTE, ISOC and IEI.

Adam Slowik received the BSc and MSc degrees in computer engineering from the Department of Electronics and Computer Science, Koszalin University of Technology, Poland, in 2001, the PhD degree in electronics from the Department of Electronics and Computer Science, Koszalin University of Technology, in 2007, and the PhD degree in computer science from the Department of Mechanical Engineering and Computer Science, Czestochowa University of Technology, Poland. Since 2013, he has been an associate professor with the Department of Electronics and Computer Science, Koszalin University of Technology. He is the author or coauthor of more than 70 articles, and two books. His research interests include soft computing, computational intelligence, machine learning, and bio-inspired global optimization algorithms and their engineering applications. He is also an associate editor of *IEEE Transactions on Industrial Informatics*, and a reviewer for many international scientific journals.

Keqin Li (Fellow, IEEE) received the BS degree in computer science from Tsinghua University in 1985 and the PhD degree in computer science from the University of Houston in 1990. He is currently a SUNY distinguished professor with the State University of New York and a National distinguished professor with Hunan University (China). He has authored or coauthored more than 960 journal articles, book chapters, and refereed conference papers. He received several best paper awards from international conferences including PDPTA-1996, NAECON-1997, IPDPS-2000, ISPA-2016, NPC-2019, ISPA-2019, and CPSCom-2022. He holds nearly 70 patents announced or authorized by the Chinese National Intellectual Property Administration. He is among the world's top five most influential scientists in parallel and distributed computing in terms of single-year and career-long impacts based on a composite indicator of the Scopus citation database. He was a 2017 recipient of the Albert Nelson Marquis Lifetime Achievement Award for being listed in Marquis Who's Who in Science and Engineering, Who's Who in America, Who's Who in the World, and Who's Who in American Education for more than twenty consecutive years. He received the Distinguished Alumnus Award from the Computer Science Department, the University of Houston in 2018. He received the IEEE TCCLD Research Impact Award from the IEEE CS Technical Committee on Cloud Computing in 2022 and the IEEE TCSVC Research Innovation Award from the IEEE CS Technical Community on Services Computing in 2023. He was a winner of the IEEE Region 1 Technological Innovation Award (Academic) in 2023. He is a member of the SUNY distinguished academy. He is an AAAS fellow, an AAIA fellow, and an ACIS founding fellow. He is a member of Academia Europaea (Academician of the Academy of Europe).