APOLLO: Differential Private Online Multi-Sensor Data Prediction with Certified Performance

Honghui Xu*, Wei Li†, Shaoen Wu*, Liang Zhao*, Zhipeng Cai†
*Department of Information Technology, Kennesaw State University, Marietta, USA
Email: {hxu10, swu10, lzhao10}@kennesaw.edu
†Department of Computer Science, Georgia State University, Atlanta, USA
Email: {wli28, zcai}@gsu.edu

***Abstract*—When multimodal AI systems increasingly utilize diverse data sources to achieve advanced understanding and interaction, they inevitably collect vast amounts of sensitive information, thus highlighting the urgent need for robust privacy safeguards, especially as these technologies expand into fields like healthcare, finance, and education. Existing research on data privacy in AI, encompassing adversarial training-based models, differential privacy-based models, and differentially private transform-based models, often neglects the inter-correlation inherent in multi-sensor data. To address this gap, we propose the differentiAl Private OnLine muLti-sensor data predictiOn model (APOLLO), which simultaneously considers intra-correlation and inter-correlation to enhance privacy protection while maintaining predictive performance. Under the proposed APOLLO framework, we design two implementations: APOLLO I, which ensures ϵ-differential privacy by adding Laplace noise to each correlated data segment, and APOLLO II, which applies additional noise to make the concatenated multi-sensor data realize ϵ-differential privacy. Furthermore, we conduct the theoretical analysis to reveal the relationship between performance influence and the privacy budget, providing guidelines for noise addition with the aim of achieving certified performance. Comprehensive experiments validate the effectiveness of the APOLLO model, establishing a new standard for privacy-preserving multi-sensor data prediction.**

***Index Terms*—Multi-sensor Data Analysis, Differential Privacy, Correlated Data Privacy**

I. Introduction

Nowadays, when plentiful advanced AI systems, such as multimodal large-scale language models (mLLMs), leverage the multimodal data (e.g., text, audio, and video) to achieve unprecedented levels of understanding and interaction [1], they unavoidably collect and analyze large amounts of sensitive information [2]. Especially, as the deployment of these technologies expands across various field, from healthcare [3] and finance [4] to education [5], robust privacy safeguards are essential to maintain public trust and compliance with regulatory standards. Therefore, it is indispensable to investigate multi-sensor data privacy protection for pursing the responsible advancement of AI models.

So far, there have been a large number of research works to study the data privacy protection in AI models. We can broadly categorize these works into three classes, including (i) adversarial training-based models [6], (ii) differential privacy-based models [7], and (iii) differentially private transform-based models [8]. Compared to adversarial training-based models, differential privacy-based models can provide a theoretical data privacy guarantee with a rigorous mathematical definition. While, differentially private transform-based models have an advantage over the naive differential privacy-based models because the side-effect of correlation on multi-sensor data on the trade-off between data privacy and model utility can be eliminated after data transformation. To be specific, these differentially private transform-based models take into account intra-correlation (*e.g.*, temporal correlation) to design the differential privacy mechanism for data privacy protection. However, in terms of multi-sensor data privacy protection, the existing works overlook the side-effect of inter-correlation (*e.g.*, the correlation between video and audio), which is a main kind of information during processing multi-sensor heterogeneous data. What's worse, no work carries out a theoretical analysis of the influence of learning performance while using differential privacy mechanism.

To fill this blank, we propose a differentiAl Private OnLine muLti-sensor data predictiOn model (APOLLO) by considering the intra-correlation and inter-correlation simultaneously to protect multi-sensor data privacy while maintaining the performance of online multi-sensor data prediction. Under this APOLLO framework, we further consider two kinds of implementations for the differential privacy mechanism, called APOLLO I and APOLLO II. In APOLLO I, we add Laplace noise to make each correlated data satisfy ϵ-differential privacy. In APOLLO II, we apply additional Laplace noise to make the concatenated multi-sensor data satisfy ϵ-differential privacy. Furthermore, we theoretically analyze the performance influence (including robustness and bias) while using additional Laplace noise for privacy preservation. Finally, comprehensive experiments are conducted to demonstrate the effectiveness of our proposed APOLLO model. Our multifold contributions are addressed as follows.

- This is the first work to propose a differential privacy online multi-sensor data prediction model by concurrently considering the intra-correlation and inter-correlation among multi-sensor heterogeneous data.
- Under a proposed APOLLO framework, we devise two

Corresponding Author: Zhipeng Cai

implementation options, called APOLLO I and APOLLO II, to realize the practical and feasible data privacy while using the online multi-sensor data prediction in the real-world applications.
- We provide rigorous theorems to reveal the relationship between performance influence and the privacy budget, which can be used as guidelines of adding noise for privacy protection with a aim of having a certified performance.
- We conduct real-data experiments to prove the effectiveness of our proposed APOLLO model and the correctness of our proposed theorems.

The rest of this paper is organized as follows. We briefly summarize the related works in Section II, present preliminaries in Section III, and formulate our APOLLO model in Section IV, Then, we conduct the differential privacy analysis of our proposed APOLLO model in Section V and propose rigorous theoretical analysis of robustness and bias of our proposed APOLLO I and APOLLO II in Section VI. Furthermore, we conduct real-data experiments on APOLLO and analyze all the results in Section VII. Finally, we end up with a conclusion in Section VIII.

II. Related Works

In this section, we summarize the related works on multi-sensor data prediction and review the current mainstream privacy-preserving learning approaches.

A. Multi-sensor Data Prediction Approaches

Multi-sensor data prediction approaches generally fall into two categories, including feature-level fusion models and prediction-level fusion models. (i) **Feature-level fusion models** transform multi-sensor data into a same feature space and then fuse these features into a joint feature representation to train a predictor, which take advantage of correlations across sensor data [9], [10]. Technically, simple methods like concatenation of raw sensor data features have been applied in the previous works for feature fusion. Besides, more advanced feature normalization, imputation, and dimensionality reduction techniques have also been investigated to further improve the prediction performance. (ii) **Prediction-level fusion models** combine the outputs of multiple predictors (*e.g.*, regression trees and neural networks) using ensemble methods, in which each predictor is built on data from an individual sensor [11], [12]. Compared to the feature-level fusion models, the prediction-level models avoid the challenges of feature fusion, but will lack the utilization of the correlations between sensor data in the process of prediction.

B. Privacy-Preserving Learning Approaches

Currently, the major techniques employed in machine learning for data privacy protection include adversarial training models, differential privacy approaches, and differentially private transform methods. (i) **Adversarial training-based models** generate adversarial examples, viewed as noise-disturbed data, to defend against inference attacks on both unimodal data [6] and multimodal data [13]. While adversarial training has appeal as a convenient and efficient technique for use in privacy-preserving learning systems, it suffers from an inability to ensure provable privacy protections. (ii) **Differential privacy-based approaches** use additional noise based on differential privacy mechanisms to ensure the theoretical guarantee of data privacy protection [14]. However, compared to non-correlated data, the additional noise should be enlarged for correlated data to keep the same degree of differential privacy protection [15], which sacrifices the performance (*e.g.*, accuracy) of learning models. (iii) **Differentially private transform-based methods** convert correlated data into an uncorrelated domain before applying differential privacy [8], where the side-effect of adding larger noise on learning performance can be eliminated due to the disappearance of data correlation after data transformation. Unfortunately, these existing transform-based methods can only be used to transform the homogeneous data with intra-correlation (that refers to correlation within a singular data instance, like temporal patterns in video or location dependence in a trajectory) into uncorrelated data domain but cannot be applied to the heterogeneous multimodal data with inter-correlation (that means correlation between separate data instances, such as relationships between two text documents or an audio segment and video clip). What's worse, all these existing privacy-preserving learning approaches did not conduct a theoretical analysis of the influence of learning performance while considering privacy protection.

In this paper, we propose a differentiAl Private OnLine muLti-sensor data predictiOn model (APOLLO) to achieve privacy enhanced online multi-sensor data prediction with certified performance influence. The novelty of our proposed APOLLO model lies in two aspects: (i) we take into account intra-correlation and inter-correlation among multi-sensor data to design additional noise for differential privacy protection; (ii) we theoretically investigate the influence of additional noise used in differential privacy on the learning performance.

III. Preliminaries

In this section, we introduce the basics of differential privacy and the correlated differential privacy.

Differential privacy (DP) is a robust privacy concept employed to safeguard the disclosure of individual data during computations. In simpler terms, it asserts that the likelihood of any differentially private output remains relatively stable even if noise is added into the original input. This constraint restricts the amount of information that the output can expose about any specific individual. ϵ-differential privacy is shown in Definition 1.

Definition 1: (ϵ-*Differential Privacy*) A randomized mechanism, $\mathcal{M}$ ($U \to \mathbb{R}$), satisfies ϵ-differential privacy, if for any two adjacent inputs $u, u' \in U$, there is

$$\Pr[\mathcal{M}(u)] \leq e^{\epsilon} \Pr\left[\mathcal{M}\left(u'\right)\right], \tag{1}$$

where ϵ is a positive real number and quantifies information leakage.

In order to realize differential privacy, a randomized mechanism, $\mathcal{M}$, can be constructed by a Laplace mechanism based on any real-value function f [16]. With respect to f, the global sensitivity S_f is defined as the maximum absolute distance between any two adjacent inputs in U, (*i.e.* $S_f = \sup_{u,u' \in U} |f(u) - f(u')|$). The Laplace mechanism for differential privacy is presented in Definition 2.

Definition 2: (*Laplace Mechanism*) The randomized mechanism, $\mathcal{M}$, which satisfies ϵ-differential privacy for function f, can be obtained via additive Laplace noise as

$$\mathcal{M}(u) = f(u) + Lap\left(0, S_f/\epsilon\right), \tag{2}$$

in which $Lap(0, S_f/\epsilon)$ is the Laplace distribution.

However, the vulnerability of current differential privacy mechanisms to data correlation was illustrated in [17]. The data correlation can be treated as a kind of side-channel information for attacks. Thus, the additional Laplace noise should be enlarged to eliminate the side effect of correlation for keeping the same differential privacy protection degree. To this end, the authors in [17] proposed a novel generalized Laplace mechanism presented in Definition 3 to offer privacy guarantees for correlated data.

Definition 3: (*Generalized Laplace Mechanism*) A randomized mechanism, $\mathcal{M}$, which satisfies ϵ-differential privacy for any real-value function f, can be obtained via additive Laplace noise as

$$\mathcal{M}(u) = f(u) + Lap\left(0, \frac{(1+C)S_f}{\epsilon}\right), \tag{3}$$

in which $C \in [0, 1]$ represents the correlation coefficient between input u with other data in the same dataset.

Besides, one significant property of differential privacy is its resilience to post-processing [18]. This property asserts that a differentially private output remains privacy-preserving even when subjected to arbitrary transformations using data-independent functions, thereby preserving its privacy guarantees. This post-processing property is described in Definition 4.

Definition 4: (*Post-Processing Property*) Suppose a randomized function $\mathcal{M}$ satifies ϵ-differential privacy and g is an arbitrary mapping from the set of possible outputs to an arbitrary set. Then,

$$\mathbb{E}(g(\mathcal{M}(u))) \leq e^{\epsilon}\mathbb{E}(g(\mathcal{M}(u'))), \tag{4}$$

where the expectation $\mathbb{E}$ is taken over the randomness in $\mathcal{M}$.

IV. APOLLO

Typically, service providers offer numerous online artificial intelligence (AI) services that utilize multi-sensor data collection. The data flow of online multi-sensor data prediction is shown in Fig. 1, where the multi-sensor data are collected from the users' device side and then the collected multiple sensor data are applied to realize the multi-sensor data prediction on the semi-honest server. Unfortunately, there is a risk of unauthorized interception of the transmitted data, potentially leading to privacy leakage [19]. Fortunately, previous research [20] has demonstrated the efficacy of the differential privacy mechanism for privacy protection in online AI services. Inspired by these works, we propose a differentiAl Private OnLine muLti-sensor data predictiOn model (APOLLO) to safeguard the privacy of these multi-sensor data prior to their transmission. In APOLLO model, differential privacy mechanism is executed on the users' device side to generate the privacy-preserving multi-sensor data, which will be transmitted to the server side for the final prediction. Our proposed APOLLO model can help users avoid privacy leakage caused by attackers who can leverage the eavesdropped multi-sensor data during transmission to infer the users' sensitive information via some effective deep learning attack models. The simplified data flow of our proposed APOLLO model is presented in Fig. 2.

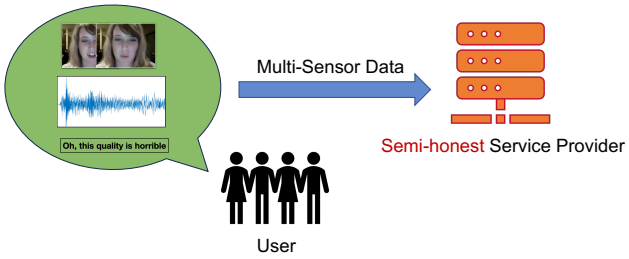


Fig. 1. Data Flow of Online Multi-Sensor Data Prediction

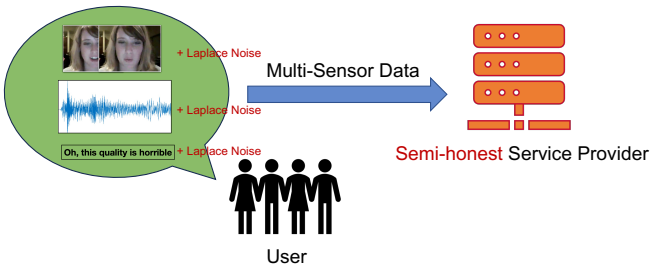


Fig. 2. Data Flow of Our APOLLO

Different from the previous differential private learning models, in order to realize privacy enhanced online multi-sensor data prediction, we consider both intra-correlation and inter-correlation among multi-sensor data in the design of additional Laplace noise to ensure the fulfillment of the differential privacy guarantee. Assume that there are total $\mathcal{P}$ types of data, and we denote the p-th time-series data as $(x_p^1, \cdots, x_p^T)$, where T represents the total time duration. Without loss of generality, we utilize the p-th data at time t, denoted as x_p^t, as an example for defining both intra-correlation and inter-correlation.

Building upon the concept of traditional temporal correlation, we define intra-correlation as below.

Definition 5: (***Intra-Correlation***) The intra-correlation of x_p^t

can be computed using the cosine distance, i.e.,

$$[c_{intra}]_p^t = \left| \frac{x_p^t \cdot x_p^{t+1}}{||x_p^t|| ||x_p^{t+1}||} \right|, \tag{5}$$

where $t \in [1, T]$ and $[c_{intra}]_p^t \in [0, 1]$.

Inspired by the definition of multiple correlation coefficient [21], we use the $\mathcal{P}$ types of data at time t, $(x_1^t, \cdots, x_{\mathcal{P}}^t)$, to define the inter-correlation as follows.

Definition 6: (***Inter-Correlation***) The inter-correlation can be calculated as:

$$[c_{inter}]_p^t = \sqrt{\frac{|Cov(M_{\mathcal{P}\times\mathcal{P}}^t)|}{|Cov([M_{\mathcal{P}\times\mathcal{P}}^t]^{-1})|}}, \tag{6}$$

where $M_{\mathcal{P}\times\mathcal{P}}^t$ represents a $\mathcal{P} \times \mathcal{P}$ covariance matrix, $[M_{\mathcal{P}\times\mathcal{P}}^t]^{-1}$ represents the inverse of the covariance matrix, $|Cov(M_{\mathcal{P}\times\mathcal{P}}^t)|$ denotes the determinant of $M_{\mathcal{P}\times\mathcal{P}}^t$, and $|Cov([M_{\mathcal{P}\times\mathcal{P}}^t]^{-1})|$ denotes the determinant of $[M_{\mathcal{P}\times\mathcal{P}}^t]^{-1}$. Each element $m_{ij}^t (i, j \in [1, \mathcal{P}])$ in this covariance matrix $M_{\mathcal{P}\times\mathcal{P}}^t$ is the covariance between the i-th data at time t (*i.e.*, x_i^t) and the j-th data at time t (*i.e.*, x_j^t), which can be computed below:

$$m_{ij}^t = \frac{(x_i^t - \bar{x_i^t}) \cdot (x_j^t - \bar{x_j^t})}{size(x_i^t)}, \tag{7}$$

where $\bar{x_i^t}$ is the mean of x_i^t, $\bar{x_j^t}$ is the mean of $\bar{x_j^t}$, and $size(x_i^t)$ is the size of x_i^t.

When considering the correlation among data, according to Definition 3, we should generate the privacy-preserving data $\tilde{x_p^t}$ as:

$$\tilde{x_p^t} = x_p^t + Lap\left(0, \frac{(1 + C_p^t) S_p^t}{\epsilon}\right), \tag{8}$$

where S_p^t represents the global sensitivity of x_p^t and C_p^t denotes the final correlation coefficient, which is equal to $\max\{[c_{intra}]_p^t, [c_{inter}]_p^t\}$ to eliminate the side influence of correlation on differential privacy protection [17].

Furthermore, we continue to investigate how the additional Laplace noise affects the multi-sensor data prediction performance. We define the multi-sensor data prediction model as a function $\mathcal{F}$, that maps inputs to a label from the set $\mathcal{K} = \{1, \cdots, K\}$, representing all possible labels. Let $x^t = [x_1^t, \cdots, x_{\mathcal{P}}^t]$ denote the concatenated multi-sensor data at time t, with label k. Typically, the multi-sensor data prediction model transform the input data x^t into a vector of scores denoted as $y(x^t) = (y_1(x^t), \cdots, y_K(x^t))$. Here, each score $y_i(x^t)$ is constrained to the range $[0, 1]$, and the sum of all scores for a given input is equal to 1, i.e., $\sum_{i=1}^K y_i(x^t) = 1$. The scoring function y is employed to interpret these scores as a probability distribution across the labels, and the prediction model $\mathcal{F}$ selects the label with the highest probability for its final output. For example, if $y_k(x^t) > \max_{i:i\neq k} y_i(x^t)$, we can make sure that the label of x^t is k.

In the following, we define two metrics, including robustness measurement and performance bias to study the influence of additional Laplace noise on learning performance. In terms of the model robustness, according to [22], we should make sure that a small change in the input does not alter the scores so much as to change the predicted label. Inspired by this idea, we give the definition of robustness measurement in Definition 7.

Definition 7: (***Robustness Measurement***) When we apply an additional noise α to the input data x^t for the multi-sensor data prediction with the score function y, the robustness measurement R can be defined as:

$$R = \frac{\mathbb{E}(y_k(x^t + \alpha))}{\mathbb{E}\left(\max_{i:i\neq k} y_i(x^t + \alpha)\right)}. \tag{9}$$

According to Definition 7, we can know that $R \in [0, \inf)$. If $R > 1$ (*i.e.*, $\mathbb{E}(y_k(x^t + \alpha)) > \mathbb{E}\left(\max_{i:i\neq k} y_i(x^t + \alpha)\right)$), the multi-sensor data prediction model is robust; otherwise, the multi-sensor data prediction model is not robust. Also, a larger R means a higher robustness of model.

Additionally, we can use the bias of scoring to measure the influence of additional noise on learning model performance [23]. In light of this, we define the performance bias in Definition 8.

Definition 8: (***Performance Bias***) If we add a noise α into the input data x^t for the multi-sensor data prediction with the score function y, we can define the bias of scoring B as follows.

$$B = \mathbb{E}\left(\left[y(x^t + \alpha) - y(x^t)\right]^2\right). \tag{10}$$

From Definition 8, we can see that $B \in [0, 1]$ since $y \in [0, 1]$, and a larger B indicates a higher performance bias.

In all, we can realize ϵ-differential privacy for the correlated data x_p^t by using additional Laplace noise $Lap\left(0, \frac{(1+C_p^t)S_p^t}{\epsilon}\right)$, shown in Eq. (8). Moreover, we want to conduct a comprehensive investigation about the influence of additional noise $\alpha = Lap\left(0, \frac{(1+C_p^t)S_p^t}{\epsilon}\right)$ on the multi-sensor data prediction model's robustness and bias. To be specific, our objective is to address two fundamental inquiries:

- What is the impact of privacy budget on the robustness of the multi-sensor data prediction model?
- How does privacy budget affect the bias of the multi-sensor data prediction?

In the context of online multi-sensor data prediction, users have two methods available for transmitting data to the server side for prediction. These methods include (i) transmitting multi-sensor raw data and (ii) transmitting multi-sensor data features. In our discussion, we have focused on the first option for problem formulation, but it's important to note that the problem formulation is equally applicable to the second option.

V. Differential Privacy Analysis

In this section, we elaborate on a rigorous privacy analysis for the correlated data and the multi-sensor data prediction model.

As shown in Eq. (8), we can add Laplace noise $Lap\left(0, \frac{(1+C_p^t)S_p^t}{\epsilon}\right)$ to the correlated data x_p^t to obtain the

privacy-preserving correlated data $\tilde{x_p^t}$ based on differential privacy while considering correlation among multi-sensor data. In Theorem 1, we give the privacy analysis for the correlated data x_p^t.

Theorem 1: Given the Laplace noise $Lap\left(0, \frac{(1+C_p^t)S_p^t}{\epsilon}\right)$ added into any one correlated data x_p^t, the disturbed correlated data $\tilde{x_p^t}$ meets ϵ-differential privacy.

Proof 1: According to [17], we denote $QS_p^t = (1+C_p^t)S_p^t$ as the correlated global sensitivity of the correlated data x_p^t. Let $\Pr[\cdot]$ be the Laplace distribution [24]. Accordingly, there is

$$\begin{aligned}\ln\frac{\Pr[x_p^t]}{\Pr[\tilde{x_p^t}]} &= \ln\frac{\frac{\epsilon}{2QS_p^t}e^{-\frac{\epsilon}{QS_p^t}|x_p^t|}}{\frac{\epsilon}{2QS_p^t}e^{-\frac{\epsilon}{QS_p^t}|\tilde{x_p^t}|}} \\ &= \frac{\epsilon}{QS_p^t}(|\tilde{x_p^t}| - |x_p^t|) \le \epsilon.\end{aligned} \tag{11}$$

Eq. (11) means that the disturbed correlated data $\tilde{x_p^t}$ meets ϵ-differential privacy.

In the multi-sensor data prediction process, we should concatenate multi-sensor data for the final prediction. Thus, when x_p^t is disturbed to be $\tilde{x_p^t}$ for privacy protection, the original concatnated multi-sensor data x^t will become the perturbed concatenated multi-sensor data $\tilde{x^t}$. In Theorem 2, we further show the differential privacy analysis for the concatnated multi-sensor data $\tilde{x^t}$ based on Theorem 1.

Theorem 2: When we use Laplace noise $Lap\left(0, \frac{(1+C_p^t)S_p^t}{\epsilon}\right)$ to make one disturbed correlated data $\tilde{x_p^t}$ satisfy ϵ-differential privacy, the perturbed concatnated multi-sensor data $\tilde{x^t}$, which is generated by combining the disturbed correlated data $\tilde{x_p^t}$ with the other $(\mathcal{P}-1)$ clean correlated data, will meet $\frac{\epsilon S^t}{(1+C_p^t)S_p^t}$-differential privacy.

Proof 2: Similar to the proof of Theorem 1, let $\Pr[\cdot]$ be the Laplace distribution. Accordingly, we have

$$\begin{aligned}\ln\frac{\Pr[x^t]}{\Pr[\tilde{x^t}]} &= \ln\frac{\frac{\epsilon}{2QS_p^t}e^{-\frac{\epsilon}{QS_p^t}|x^t|}}{\frac{\epsilon}{2QS_p^t}e^{-\frac{\epsilon}{QS_p^t}|\tilde{x^t}|}} \\ &= \frac{\epsilon}{QS_p^t}(|\tilde{x^t}| - |x^t|) \le \frac{\epsilon S^t}{(1+C_p^t)S_p^t},\end{aligned} \tag{12}$$

where $QS_p^t = (1+C_p^t)S_p^t$ as the correlated global sensitivity of the correlated data x_p^t and S^t is the global sensitivity of the concatenated multi-sensor data x_t. Eq. (12) infers that the perturbed concatnated multi-sensor data x^t satisfies $\frac{\epsilon S^t}{(1+C_p^t)S_p^t}$-differential privacy.

Through Theorem 1 and Theorem 2, we can get two conclusions: (i) when the condition $S_t \le (1+C_p^t)S_p^t$ is satisfied, the data privacy protection degree will increase after multi-sensor data concatenation operation. and (ii) if $S_t > (1+C_p^t)S_p^t$, the concatenation operation will bring the decrease of the data privacy protection degree.

So far, we provide a rigorous privacy analysis for the correlated data and the concatenated multi-sensor data based on the situation when we use additional Laplace noise to make one kind of data meet ϵ-differential privacy. However, more generally, according to Theorem 1, we can add Laplace noise $Lap\left(0, \frac{(1+C_i^t)S_i^t}{\epsilon}\right)(i \in [1, \cdots, \mathcal{P}])$ to the corresponding data x_i^t to ensure every kind of data meets ϵ-differential privacy for a privacy-preserving data transmission. When using different magnitude of noises for different kinds of data, it is hard for us to do the differential privacy analysis for the concatenated multi-sensor data. Therefore, in this article, we increase the Laplace noise from $Lap\left(0, \frac{(1+C_i^t)S_i^t}{\epsilon}\right)$ to the same $Lap\left(0, \frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}{\epsilon}\right)$ to ensure that the differential privacy budget for each correlated data x_i^t is equal or less than ϵ, which means that the privacy protection degree will not be decreased. Then, in Theorem 3, we further present the privacy analysis for the concatenated multi-sensor data under this situation.

Theorem 3: If we add $Lap\left(0, \frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}{\epsilon}\right)$ to each corrected data $\tilde{x_i^t}(i \in [1, \cdots, \mathcal{P}])$ for differential privacy protection, the perturbed concatenated multi-sensor data $\tilde{x^t}$ will satisfy $\frac{\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}$-differential privacy.

Proof 3: Let $\Pr[\cdot]$ be the Laplace distribution. Then, we have

$$\begin{aligned}\ln\frac{\Pr[x^t]}{\Pr[\tilde{x^t}]} &= \ln\frac{\frac{\epsilon}{2\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}e^{-\frac{\epsilon}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}|x^t|}}{\frac{\epsilon}{2\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}e^{-\frac{\epsilon}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}|\tilde{x^t}|}} \\ &= \frac{\epsilon}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}(|\tilde{x^t}| - |x^t|) \\ &\le \frac{\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}.\end{aligned} \tag{13}$$

Eq. (13) suggests that the perturbed concatnated multi-sensor data $\tilde{x^t}$ meets $\frac{\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}$-differential privacy.

Moreover, we think about how to use Laplace noise for each type of data $x_i^t(i \in [1, \cdots, \mathcal{P}])$ to guarantee that the perturbed concatenated multi-sensor data $\tilde{x^t}$ meets ϵ-differential privacy. Similarly, according to Theorem 1, we can add the same Laplace $Lap\left(0, \frac{S^t}{\epsilon}\right)$ to each $x_i^t(i \in [1, \cdots, \mathcal{P}])$ to make each $x_i^t(i \in [1, \cdots, \mathcal{P}])$ meet $\frac{(1+C_i^t)S_i^t\epsilon}{S^t}$-differential privacy. Then, we give Theorem 4 to show why this implementation of Laplace noise mechanism on each data can make the perturbed concatenated multi-sensor data $\tilde{x^t}$ meet ϵ-differential privacy.

Theorem 4: When add the same Laplace $Lap\left(0, \frac{S^t}{\epsilon}\right)$ to each $x_i^t(i \in [1, \cdots, \mathcal{P}])$ to each $x_i^t(i \in [1, \cdots, \mathcal{P}])$ for differential privacy protection, the perturbed concatenated multi-sensor data $\tilde{x^t}$ will satisfy ϵ-differential privacy.

Proof 4: Let $\Pr[\cdot]$ be the Laplace distribution. Accordingly,

there is

$$\ln \frac{\Pr[x^t]}{\Pr[\tilde{x^t}]} = \ln \frac{\frac{\epsilon}{2S^t} e^{-\frac{\epsilon}{S^t}|x^t|}}{\frac{\epsilon}{2S^t} e^{-\frac{\epsilon}{S^t}|\tilde{x^t}|}} = \frac{\epsilon}{S^t}(|\tilde{x^t}| - |x^t|) \leq \epsilon. \tag{14}$$

Eq. (14) shows that the perturbed concatnated multi-sensor data $\tilde{x^t}$ satisfies ϵ-differential privacy.

Finally, we use Corollary 1 to prove that the disturbed score function of the multi-sensor model $y(\tilde{x^t})$ satisfies ϵ-differential privacy if the perturbed concatenated multi-sensor data $\tilde{x^t}$ meets ϵ-differential privacy.

Corollary 1: When the perturbed concatenated multi-sensor data $\tilde{x^t}$ meets ϵ-differential privacy, the disturbed score function of the multi-sensor model $y(x^t)$ will satisfy ϵ-differential privacy as well.

Proof 5: Based on the post-processing property of differential privacy in Definition 4 and Theorem 4, we can obtain that the disturbed score function of the multi-sensor model $y(\tilde{x^t})$ satisfies ϵ-differential privacy.

VI. Theoretical Analysis of APOLLO Model

Our proposed APOLLO model realizes the privacy-preserving multi-sensor data prediction by implementing differential privacy mechanism on the multi-sensor correlated data. In this work, we consider two kinds of implementations for the differential privacy mechanism, called APOLLO I and APOLLO II. The APOLLO I is proposed based on Theorem 3, where we add the same Laplace noise to each correlated data in order to make the privacy budget for each correlated data equal to or less than ϵ. While, the APOLLO II is presented based on Theorem 4, where we apply the same additional Laplace noise to each correlated data so as to make the concatenated multi-sensor data satisfy ϵ-differential privacy. Theorem 3 and Theorem 4 have been given in Section V to finish the rigorous privacy analysis on APOLLO I and APOLLO II, respectively. In the following, we further thoroughly analyze APOLLO I and APOLLO II about the inter-influence between the utilization of Laplace noise and multi-sensor data prediction performance (*i.e.*, robustness and bias).

A. APOLLO I

In APOLLO, we can add the Laplace noise $Lap\left(0, \frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}{\epsilon}\right)$ to each correlated data $x_i^t (i \in [1,\cdots,\mathcal{P}])$ to ensure that the differential privacy budget for each correlated data is equal or less than ϵ. Then, according to Theorem 3, the disturbed concatenated multi-sensor data $\tilde{x}^t$ will uphold $\frac{\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}$-differential privacy. Moreover, Corollary 1 infers that the perturbed score function $y(\tilde{x}^t)$ of the multi-sensor model will also meet $\frac{\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}$-differential privacy. According to the aforementioned conclusions, we elaborate on the theoretical analysis of APOLLO I.

1) Privacy Budget v.s. Robustness: We use $(x^t+\alpha)$ instead of $\tilde{x^t}$ to represent the disturbed concatenated multi-sensor data for clear presentation. When the perturbed score function satisfies $\frac{\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}$-differential privacy, from [22], we can get

$$\mathbb{E}\left(y_k(x^t)\right) \leq e^{\frac{\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}} \mathbb{E}\left((y_k(x^t+\alpha)\right); \tag{15}$$

$$\mathbb{E}\left(y_i(x^t+\alpha)\right) \leq e^{\frac{\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}} \mathbb{E}\left((y_i(x^t)\right), (i \neq k). \tag{16}$$

Eq. (15) gives a lower-bound on $\mathbb{E}\left((y_k(x^t+\alpha)\right)$ and Eq. (16) gives a upper-bound on $\max\limits_{i:i\neq k}\mathbb{E}\left(y_i(x^t+\alpha)\right)$. Then, according to Eq. (15) and Eq. (16), we have

$$\frac{\mathbb{E}\left(y_k(x^t)\right)}{\mathbb{E}\left((y_k(x^t+\alpha)\right)} \times \frac{\mathbb{E}\left(\max\limits_{i:i\neq k} y_i(x^t+\alpha)\right)}{\mathbb{E}\left((\max\limits_{i:i\neq k} y_i(x^t)\right)} \leq e^{\frac{2\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}}. \tag{17}$$

Subsequently, we define one numerical property of the multi-sensor data prediction model implemented on the original multi-sensor data as:

$$R_o = \frac{\mathbb{E}\left(y_k(x^t)\right)}{\mathbb{E}\left((\max\limits_{i:i\neq k} y_i(x^t)\right)}. \tag{18}$$

Based on Eq. (9) and Eq. (18), we can rewrite Eq. (17) as

$$\epsilon \geq \frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}{2S^t} \ln(\frac{R_o}{R}). \tag{19}$$

From Eq. (19), we can obtain Theorem 5

Theorem 5: The viable span of the privacy budget expands as the model robustness increases.

We can also rewrite Eq (19) as

$$R \geq \frac{R_o}{e^{\frac{2\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}}} \tag{20}$$

Based on Eq. (20), we can get Theorem 6.

Theorem 6: The possibility of the model being robust increases with the increase of the privacy budget.

Furthermore, we show an exact robustness condition in Theorem 7.

Theorem 7: Let $\mathcal{F}$ be a multi-sensor data prediction model with a score function y. We apply the Laplace noise $\alpha = Lap\left(0, \frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}{\epsilon}\right)$ to each input data with label k. If there is

$$R_o \geq e^{\frac{2\epsilon S^t}{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}}, \tag{21}$$

$\mathcal{F}$ is robust to the additional noise α applied on each input data.

Proof 6: When Eq. (21) is satisfied, according to Eq. (19), we can compute $R \geq 1$, which suggests that the model $\mathcal{F}$ is robust according to Definition 7.

2) Privacy Budget v.s. Bias: We will use Lemma 1 and Lemma 2 [25] for analyzing the influence of Laplace noise $\alpha = Lap\left(0, \frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}{\epsilon}\right)$ on model bias.

Lemma 1: The expectation of Laplace noise $\alpha = Lap(0, \lambda)$ is

$$\mathbb{E}\left(Lap(0,\lambda)\right) = 0.$$

Lemma 2: The expectation of square Laplace noise α^2 is equal to

$$\mathbb{E}(\alpha^2) = \mathbb{E}(\alpha) + \mathrm{Var}(\alpha) = 2\lambda^2.$$

Since x^t is independent with the Laplace noise $\alpha = Lap\left(0, \frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}{\epsilon}\right)$ in the calculation of the data-independent function y, we can calculate the performance bias according to Lemma 1, Lemma 2, and Eq. (10) as below:

$$\begin{aligned} B &= \mathbb{E}\left(\left[y(x^t+\alpha) - y(x^t)\right]^2\right) \\ &= \mathbb{E}\left(\left[y(x^t) + y(\alpha) - y(x^t)\right]^2\right) \\ &= \mathbb{E}\left(\left[y(\alpha)\right]^2\right) \\ &= \mathbb{E}(\alpha^2) \\ &= \frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]} 2(1+C_i^t)^2 S_i^{t2}}{\epsilon^2}. \end{aligned} \tag{22}$$

According to Eq. (22), we can propose Theorem 8.

Theorem 8: The bias of multi-sensor data prediction performance increases with the decrease of the privacy budget.

Moreover, we can rewrite Eq. (22) as

$$\epsilon = \sqrt{\frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]} 2(1+C_i^t)^2 S_i^{t2}}{B}}. \tag{23}$$

Based on Eq. (23), we can obtain Theorem 9.

Theorem 9: The privacy budget can be reduced when there is a willingness to accept a greater model performance bias.

B. APOLLO II

We propose APOLLO II according to Theorem 4. To be specific, we can add the same Laplace noise $Lap\left(0, \frac{S^t}{\epsilon}\right)$ to each $x_i^t (i \in [1, \cdots, \mathcal{P}])$ for differential privacy protection to make the perturbed concatenated multi-sensor data $\tilde{x^t}$ satisfy ϵ-differential privacy. Subsequently, based on Corollary 1, we can obtain that the perturbed score function of the multi-sensor model $y(\tilde{x^t})$ also satisfies ϵ-differential privacy. According to the aforementioned conclusions, we continue to elaborate on the theoretical analysis of APOLLO II.

1) Privacy Budget v.s. Robustness: Following the similar analysis procedures from Eq. (15) to Eq. (20), we can easily obtain

$$\epsilon \geq \frac{1}{2}\ln(\frac{R_o}{R}); \tag{24}$$

and

$$R \geq \frac{R_o}{e^{2\epsilon}}. \tag{25}$$

From Eq. (24) and Eq. (25), we can get the same conclusions as Theorem 5 and Theorem 6. Besides, according to Eq. (24), we can obtain a robustness condition in Theorem 10.

Theorem 10: Let $\mathcal{F}$ be a multi-sensor data prediction model with a score function y. We apply the Laplace noise $\alpha = Lap\left(0, \frac{S^t}{\epsilon}\right)$ to each input data with label k to make the concatenated multi-sensor data achieve ϵ-differential privacy. If we have

$$R_o = \frac{\mathbb{E}\left(y_k(x^t)\right)}{\mathbb{E}\left(\left(\max\limits_{i:i\neq k} y_i(x^t)\right)\right)} \geq e^{2\epsilon}, \tag{26}$$

$\mathcal{F}$ is robust to the additional noise α applied on each input data.

Proof 7: If the input x_p^t satisfies ϵ-differential priacy, we can get Eq. (25), which can be written as $R \geq \frac{R_o}{e^{2\epsilon}}$. Then, once Eq. (26) is satisfied, we can obtain $R \geq 1$, which indicates that the model $\mathcal{F}$ is robust according to Definition 7.

2) Privacy Budget v.s. Bias: Similar to the analysis in Subsection VI-A2, we can compute the performance bias when using Laplace noise $\alpha = Lap\left(0, \frac{S^t}{\epsilon}\right)$ as below.

$$\begin{aligned} B &= \mathbb{E}\left(\left[y(x^t+\alpha) - y(x^t)\right]^2\right) \\ &= \mathbb{E}\left(\left[y(x^t) + y(\alpha) - y(x^t)\right]^2\right) \\ &= \mathbb{E}\left(\left[y(\alpha)\right]^2\right) \\ &= \mathbb{E}(\alpha^2) \\ &= \frac{2(S^t)^2}{\epsilon^2}. \end{aligned} \tag{27}$$

Eq. (27) can be written as Eq. (28).

$$\epsilon = \sqrt{\frac{2}{B}} S^t. \tag{28}$$

Based on Eq. (27) and Eq. (28), we can get the same conclusions as Theorem 8 and Theorem 9.

VII. Experiments

In this section, we first introduce our experiment settings and then present comprehensive experimental results. These experimental results can be used to demonstrate the effectiveness of the proposed APOLLO model, including APOLLO I and APOLLO II.

A. Experimental Settings

The datasets, baselines, performance metrics, network architectures, and hyper-parameter settings are described below.

1) Datasets: Our experiments employ two benchmark datasets, CMU-MOSI (MOSI) and CMU-MOSEI (MOSEI), for multi-sensor sentiment analysis. The **MOSI dataset** comprises 2189 subjective YouTube monologues, each with video, audio, and text expressing opinions on topics like movies. An integer sentiment score in $[-3, 3]$ manually tags each monologue, where -3 and 3 indicate the strongest negative and positive sentiments, respectively. As an enhancement over MOSI, the **MOSEI dataset** includes 23453 annotated video clips featuring more utterances, speakers, and subject diversity.

2) Baseline: MISA [26], Self-MM [27], and MMIM [28] represent the current state-of-the-art models on both the MOSI and MOSEI datasets for multi-sensor sentiment analysis. Accordingly, we utilize MISA, Self-MM, and MMIM as baseline models to benchmark performance.

3) Performance Metrics: Sentiment prediction on MOSI and MOSEI can be formulated as a 7-class classification task using integer labels in [-3,3], evaluated by the seven-class accuracy metric (Acc-7) [29]. Additionally, two binary accuracy (Acc-2) approaches are adoptable for measuring sentiment prediction performance. The first one is *Negative/Non-negative (Neg/Non-neg)* classification, where non-negative labels are indicated by non-negative scores [30]. The second one is calculated based on *Negative/Positive (Neg/Pos)* classes, with negative and positive classes denoted by corresponding negative and positive scores [31]. In summary, our experiments employ Acc-2 (Neg/Non-neg), F1 (Neg/Non-neg), Acc-2 (Neg/Pos), F1 (Neg/Pos), and Acc-7 as evaluation metrics.

4) APOLLO's Framework: Our APOLLO model is composed of two parts, including a differential privacy mechanism deployed on the users' side and a multi-sensor data prediction model on the semi-honest server side.

The multi-sensor data prediction model is composed of data pre-processing, autoencoding feature learning, and sentiment prediction modules. The neural network architectures of these three modules are described below. (i) **Data Pre-processing.** Facial Action Coding System (FACS) [32] extracts facial expression features encompassing facial action units and pose. An acoustic analysis framework (COVAREP) [33] obtains acoustic features including 12 MFCCs, pitch, voiced/unvoiced elements, glottal source parameters, and other emotion/tone related aspects. The pre-trained BERT [34] serves as the feature extractor for textual utterances. Therefore, the visual feature dimension is $d_v = 47$, the acoustic feature dimension is $d_a = 74$, and the textual feature dimension is $d_l = 784$. To align the multimodal features for encoding, we utilize *one Fully-Connected Layer with ReLU activation function and one Normalization Layer* to embed these features into the same dimensional space. (ii) **Autoencoding Feature Learning.** Within this autoencoder module, the encoder E uses *one Fully-Connected Layer with Sigmoid activation function* to extract the data features, and the decoder D employs *one Fully-Connected Layer* for reconstruction, avoiding learning unrepresentative encodings. Specifically, three separate autoencoders learn the feature representations for video, audio, and text data. (iii) **Sentiment Prediction.** In the prediction function G, *one Transformer Encoder Layer* is used for transformation, *one Fully-Connected Layer with a Dropout Layer plus a ReLU activation function* is used for fusion, and *one Fully-Connected Layer* is used to map all representations into one dimension for final prediction.

The differential privacy mechanism is applied in the users' side according to the design of APOLLO I and APOLLO II. For APOLLO I, as mentioned in subsection VI-A, Laplace noise $Lap\left(0, \frac{\max\limits_{i\in[1,\cdots,\mathcal{P}]}(1+C_i^t)S_i^t}{\epsilon}\right)$ is applied to each modality data to ensure that the differential privacy budget for each modality data is equal or less than ϵ. For APOLLO II, as stated in subsection VI-B, we can add the same Laplace noise $Lap\left(0, \frac{S^t}{\epsilon}\right)$ to each modality data for differential privacy protection to make the perturbed concatenated multi-sensor data satisfy ϵ-differential privacy.

5) Hyperparameter Settings: In the differential privacy mechanism, the global sensitivity of each modality data S_i^t, the correlation for each modality data C_i^t, and the global sensitivity of the concatenated multi-sensor data S^t should be dynamically calculated in the training process. We train the multi-sensor data prediction model with the batch size 128, the training epochs 500, and the learning rate $1e-4$. The proposed model is trained on Ubuntu OS system using 8 Nividia A100 GPU. More details of the proposed APOLLO model can be found at https://github.com/ahahnut/APOLLO.

B. Evaluation on Our APOLLO Model

In our privacy enhanced model, we should set one system parameters ϵ. The value of ϵ, which is the so-called "privacy budget", indicates the degree of privacy protection. A smaller ϵ implies a higher degree of data privacy protection. First of all, we implement our proposed APOLLO I with $\epsilon = 0.5, 1.0, 1.5, 2.0, 2.5, 3.0, 3.5, 4.0$ on MOSI dataset, and we present the evaluation results in Fig. 3. From Fig. 3, we can see that all metric results of our proposed APOLLO I is comparable to that of the three baselines, which indicates that our proposed APOLLO I can keep the utility of multi-sensor data prediction model and achieve privacy protection for multi-sensor data. Moreover, the proposed APOLLO II with the same various ϵ on MOSI is applied on MOSI dataset, and these evaluation results are shown in Fig. 4. In Fig. 4, the comparison results can be used to demonstrate that our proposed APOLLO II maintains the performance of the multi-sensor data prediction while realizing data privacy preservation. Furthermore, we run our proposed APOLLO I and APOLLO II on MOSEI datset, whose evaluation results are shown in Fig. 5 and Fig. 6, respectively. By observing all metric results, we can obtain the same conclusion that our proposed APOLLO model can achieve the trade-off between the multi-sensor data privacy protection and the utility of multi-sensor data prediction model.

Fig. 3. Performance Comparison on MOSI Dataset (Baselines v.s. APOLLO I with Various ϵ)

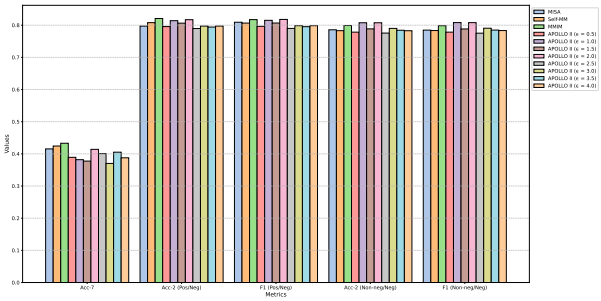


Fig. 4. Performance Comparison on MOSI Dataset (Baselines v.s. APOLLO II with Various ϵ)

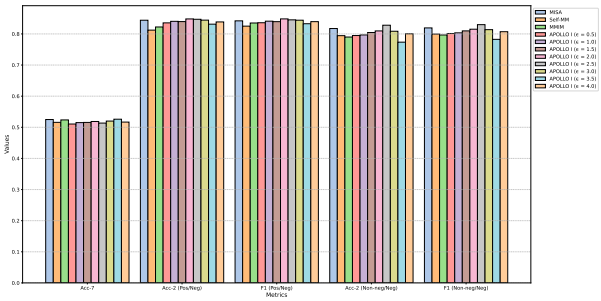


Fig. 5. Performance Comparison on MOSEI Dataset (Baselines v.s. APOLLO I with Various ϵ)

C. Evaluation Results (Privacy Budget v.s. Robustness)

During the training process of implementing APOLLO I with various $\epsilon = 0.5, 1.0, 1.5, 2.0, 2.5, 3.0, 3.5, 4.0$ on MOSI dataset, we can compute the corresponding robustness values of our proposed model. We use these robustness values to draw Fig. 7(a). From Fig. 7(a), it can be seen that the robustness of APOLLO I has an ascent trend with the increase of the privacy budget, which is consistent with Theorem 6. Additionally, we calculate three more groups of robustness values, including (i) the robustness of APOLLO I with various ϵ on MOSEI dataset, (ii) the robustness of APOLLO II with various ϵ on MOSI dataset, (iii) the robustness of APOLLO II with various ϵ on MOSEI dataset, shown in Fig. 7. According to the results in Fig. 7, we can conclude that the possibility of the model being robust increases with the increase of the privacy budget.

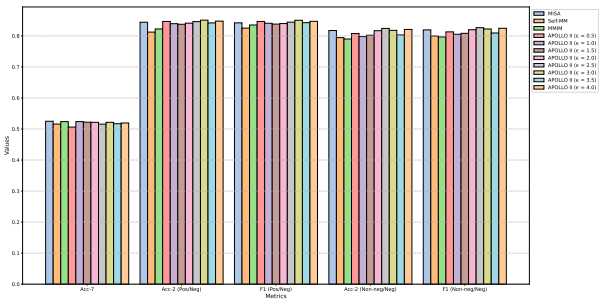
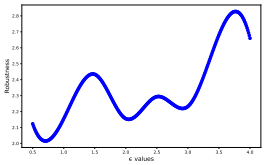
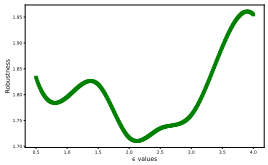


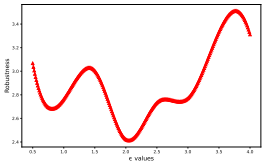
Fig. 6. Performance Comparison on MOSEI Dataset (Baselines v.s. APOLLO II with Various ϵ)



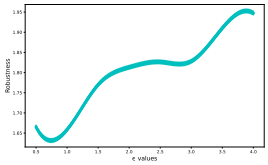
(a) Robustness of APOLLO I with Various ϵ on MOSI Dataset



(b) Robustness of APOLLO I with Various ϵ on MOSEI Dataset



(c) Robustness of APOLLO II with Various ϵ on MOSI Dataset

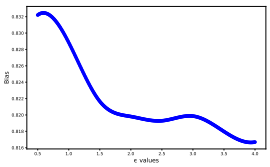


(d) Robustness of APOLLO II with Various ϵ on MOSEI Dataset

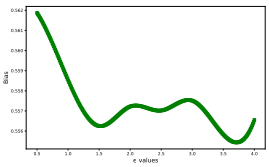
Fig. 7. Relationship between Robustness and Privacy Budget.

D. Evaluation Results (Privacy Budget v.s. Bias)

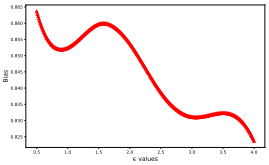
Similarly, the bias of our proposed model can be computed in the training process. To be specific, we obtain four groups of bias values, including (i) the bias of APOLLO I with various ϵ on MOSI dataset, (ii) the bias of APOLLO I with various ϵ on MOSEI dataset, (iii) the bias of APOLLO II with various ϵ on MOSI dataset, and (iv) the bias of APOLLO II with various ϵ on MOSEI dataset. These four groups of bias values are drawn in Fig 8. From Fig. 8, the bias has a descent trend with increasing the privacy budget, which is consistent with Theorem 8.



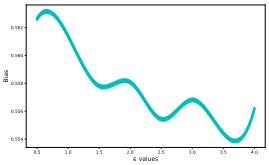
(a) Bias of APOLLO I with Various ϵ on MOSI Dataset



(b) Bias of APOLLO I with Various ϵ on MOSEI Dataset



(c) Bias of APOLLO II with Various ϵ on MOSI Dataset



(d) Bias of APOLLO II with Various ϵ on MOSEI Dataset

Fig. 8. Relationship between Bias and Privacy Budget.

VIII. Conclusion

In this paper, we create a differential private online multi-sensor data prediction model (APOLLO) to realize the privacy

enhanced multi-sensor data prediction with certified performance influence, where we consider the intra-correlation and the inter-correlation among multi-sensor data to design our proposed differential privacy mechanism. Under APOLLO framework, we design two kinds of APOLLO schemes (APOLLO I and APOLLO II) by taking into account the implementation ways of Laplace noise on multi-sensor data. Then, we propose a rigorous theoretical analysis on APOLLO I and APOLLO II to investigate the impact of privacy budget on the robustness and bias of the multi-sensor data prediction model. Finally, we conduct comprehensive experiments to illustrate that our proposed APOLLO model can maintain the performance of multi-sensor data prediction while protecting multi-sensor data privacy, and the observations from extensive experimental results of robustness and bias are consistent with our proposed theorems.

ACKNOWLEDGMENT

This work was partly supported by the National Science Foundation of U.S. (2146497, 2416872, 2315596, 2244219, 2343619).

REFERENCES

[1] B. McKinzie, Z. Gan, J.-P. Fauconnier, S. Dodge, B. Zhang, P. Dufter, D. Shah, X. Du, F. Peng, F. Weers *et al.*, "Mm1: Methods, analysis & insights from multimodal llm pre-training," *arXiv preprint arXiv:2403.09611*, 2024.

[2] L. Jiang, "Utilizing large languagemodels to detect privacy leaks in mini-app code," *arXiv preprint arXiv:2402.07367*, 2024.

[3] M. A. Rahman, "A survey on security and privacy of multimodal llms-connected healthcare perspective," in *2023 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2023, pp. 1807–1812.

[4] W. Zhang, L. Zhao, H. Xia, S. Sun, J. Sun, M. Qin, X. Li, Y. Zhao, Y. Zhao, X. Cai *et al.*, "Finagent: A multimodal foundation agent for financial trading: Tool-augmented, diversified, and generalist," *arXiv preprint arXiv:2402.18485*, 2024.

[5] M. A. Rahman, L. Alqahtani, A. Albooq, and A. Ainousah, "A survey on security and privacy of large multimodal deep learning models: Teaching and learning perspective," in *2024 21st Learning and Technology Conference (L&T)*. IEEE, 2024, pp. 13–18.

[6] K. Li, G. Luo, Y. Ye, W. Li, S. Ji, and Z. Cai, "Adversarial privacy-preserving graph embedding against inference attack," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6904–6915, 2020.

[7] Y. Wang, X. Wu, and L. Wu, "Differential privacy preserving spectral graph analysis," in *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer, 2013, pp. 329–340.

[8] H. Wang, Z. Xu, S. Jia, Y. Xia, and X. Zhang, "Why current differential privacy schemes are inapplicable for correlated data publishing?" *World Wide Web*, vol. 24, pp. 1–23, 2021.

[9] R. Pang, Y. Yang, A. Huang, Y. Liu, P. Zhang, and G. Tang, "Multi-scale feature fusion model for bridge appearance defect detection," *Big Data Mining and Analytics*, vol. 7, no. 1, pp. 1–11, 2023.

[10] M. H. Wang, L. Xing, Y. Pan, F. Gu, J. Fang, X. Yu, C. P. Pang, K. K.-L. Chong, C. Y.-L. Cheung, X. Liao *et al.*, "Ai-based advanced approaches and dry eye disease detection based on multi-source evidence: Cases, applications, issues, and future directions," *Big Data Mining and Analytics*, vol. 7, no. 2, pp. 445–484, 2024.

[11] N. C. Iyer, P. Nissimagoudar, P. Pillai, H. Gireesha, A. Kulkarni, and A. Okade, "Perception of autonomous vehicle for localization using camera and gps," in *International Conference on Soft Computing and Pattern Recognition*. Springer, 2021, pp. 86–96.

[12] U. Shin, K. Park, B.-U. Lee, K. Lee, and Kweon, "Self-supervised monocular depth estimation from thermal images via adversarial multi-spectral adaptation," in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*. IEEE, 2023, pp. 5798–5807.

[13] H. Xu, Z. Cai, D. Takabi, and W. Li, "Audio-visual autoencoding for privacy-preserving video streaming," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 1749–1761, 2021.

[14] Y. Wang, X. Wu, and D. Hu, "Using randomized response for differential privacy preserving data collection," in *EDBT/ICDT Workshops*. Springer, 2016, pp. 0090–6778.

[15] Z. Hu and J. Yang, "Differential privacy protection method based on published trajectory cross-correlation constraint," *Plos one*, vol. 15, 2020.

[16] F. Koufogiannis, S. Han, and G. J. Pappas, "Optimality of the laplace mechanism in differential privacy," *arXiv preprint arXiv:1504.00065*, 2015.

[17] C. Liu, S. Chakraborty, and P. Mittal, "Dependence makes you vulnerable: Differential privacy under dependent tuples," in *NDSS*. ISOC, 2016, pp. 21–24.

[18] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3*. Springer, 2006, pp. 265–284.

[19] P. Hu, Z. Wang, R. Sun, H. Wang, and M. Xue, "M4̂i: Multi-modal models membership inference," *arXiv preprint arXiv:2209.06997*, 2022.

[20] S. Rahimian, T. Orekondy, and M. Fritz, "Differential privacy defenses and sampling attacks for membership inference," in *Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security*. ACM, 2021, pp. 193–202.

[21] S. C. Kafle, "Correlation and regression analysis using spss," *Management, Technology & Social Sciences*, vol. 126, 2019.

[22] M. Lecuyer, V. Atlidakis, R. Geambasu, D. Hsu, and S. Jana, "Certified robustness to adversarial examples with differential privacy," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 656–672.

[23] T. Hellström, V. Dignum, and S. Bensch, "Bias in machine learning–what is it good for?" *arXiv preprint arXiv:2004.00686*, 2020.

[24] T. Eltoft, T. Kim, and T.-W. Lee, "On the multivariate laplace distribution," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 300–303, 2006.

[25] O. Arslan, "An alternative multivariate skew laplace distribution: properties and estimation," *Statistical Papers*, vol. 51, no. 4, p. 865, 2010.

[26] D. Hazarika, R. Zimmermann, and S. Poria, "Misa: Modality-invariant and-specific representations for multimodal sentiment analysis," in *Proceedings of the 28th ACM International Conference on Multimedia*. ACM, 2020, pp. 1122–1131.

[27] W. Yu, H. Xu, Z. Yuan, and J. Wu, "Learning modality-specific representations with self-supervised multi-task learning for multimodal sentiment analysis," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 35, no. 12, 2021, pp. 10 790–10 797.

[28] W. Han, H. Chen, and S. Poria, "Improving multimodal fusion with hierarchical mutual information maximization for multimodal sentiment analysis," *arXiv preprint arXiv:2109.00412*, 2021.

[29] A. Zadeh, R. Zellers, E. Pincus, and L.-P. Morency, "Multimodal sentiment intensity analysis in videos: Facial gestures and verbal messages," *IEEE Intelligent Systems*, vol. 31, pp. 82–88, 2016.

[30] A. Zadeh, P. P. Liang, S. Poria, P. Vij, E. Cambria, and L.-P. Morency, "Multi-attention recurrent network for human communication comprehension," in *Proceedings of the AAAI Conference on Artificial Intelligence*. AAAI, 2018, pp. 5642–5649.

[31] Y.-H. H. Tsai, S. Bai, P. P. Liang, J. Z. Kolter, L.-P. Morency, and R. Salakhutdinov, "Multimodal transformer for unaligned multimodal language sequences," in *Proceedings of the Conference. Association for Computational Linguistics. Meeting*. NIH Public Access, 2019, p. 6558.

[32] E. L. Rosenberg and P. Ekman, *What the Face Reveals: Basic and Applied Studies of Spontaneous Expression Using the Facial Action Coding System (FACS)*. Oxford University Press, 2020.

[33] G. Degottex, J. Kane, T. Drugman, T. Raitio, and S. Scherer, "Covarep-a collaborative voice analysis repository for speech technologies," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2014, pp. 960–964.

[34] J. Devlin, M. Chang, K. Lee, and K. Toutanova, "BERT: pre-training of deep bidirectional transformers for language understanding," *CoRR*, vol. abs/1810.04805, 2018. [Online]. Available: http://arxiv.org/abs/1810.04805