FRAMU: Attention-based Machine Unlearning using Federated Reinforcement Learning

Thanveer Shaik, Xiaohui Tao, Lin Li, Haoran Xie, Taotao Cai, Xiaofeng Zhu, and Qing Li

***Abstract*—Machine Unlearning, an emerging field, addresses data privacy issues by enabling the removal of private or irrelevant data from the machine learning process. Challenges related to privacy and model efficiency arise from the use of outdated, private, and irrelevant data. These issues compromise both the accuracy and the computational efficiency of models in both machine learning and unlearning. To mitigate these challenges, we introduce a novel framework, Federated Reinforcement Learning with Attention-based Machine Unlearning (FRAMU). This framework incorporates adaptive learning mechanisms, privacy preservation techniques, and optimization strategies, making it a well-rounded solution for handling various data sources, either single-modality or multi-modality, while maintaining accuracy and privacy. FRAMU's strength lies in its adaptability to fluctuating data landscapes, its ability to unlearn outdated, private or irrelevant data, and its support for continual model evolution without compromising privacy. Our experiments, conducted on both single-modality and multi-modality datasets, revealed that FRAMU significantly outperformed baseline models. Additional assessments of convergence behavior and optimization strategies further validate the framework's utility in federated learning applications. Overall, FRAMU advances machine unlearning by offering a robust, privacy-preserving solution that optimizes model performance while addressing key challenges in dynamic data environments.**

***Index Terms*—Machine Unlearning, Privacy, Reinforcement Learning, Federated Learning, Attention Mechanism.**

I. Introduction

The widespread availability of decentralized and heterogeneous data sources has created a demand for machine learning models that can effectively leverage this data while preserving privacy and ensuring accuracy [1]. Traditional approaches struggle to handle the continuous influx of new data streams and the accumulation of outdated or irrelevant information, hindering their adaptability to dynamic data environments [2], [3]. Moreover, the presence of sensitive or private data introduces concerns regarding data breaches and unauthorized access, necessitating the development of privacy-preserving techniques [4]. The concept of the "right to be forgotten" allows individuals to have their personal information removed from online platforms, although there's no universal agreement on its definition or its status as a human right. Despite this, countries like Argentina, the EU, and the Philippines are working on regulations [1]. Therefore, there is a pressing need to advance the field of machine unlearning to ensure both adaptability and privacy in machine learning applications.

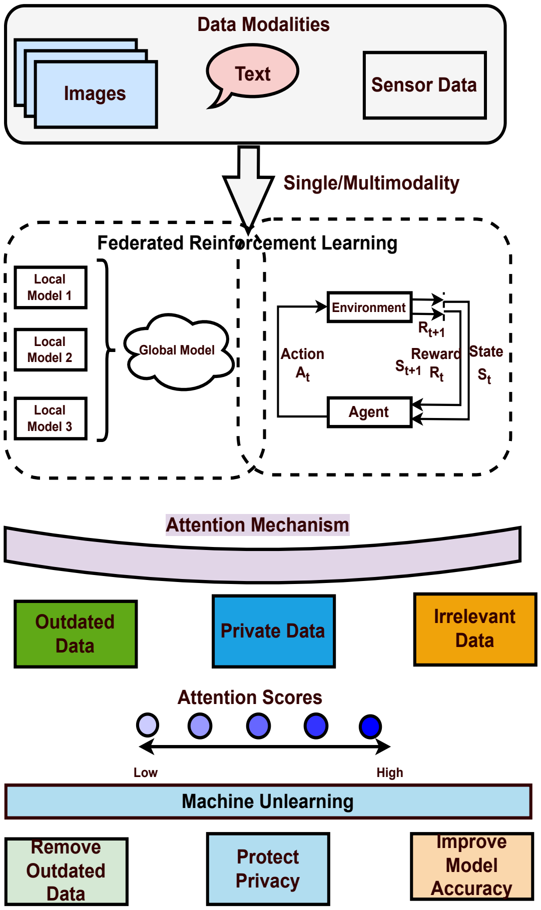


Fig. 1: Federated Reinforcement Learning to Unlearning

Example 1. *Consider the case of James Gunn, a renowned writer and director credited for the success of films like "Guardians of the Galaxy." In July 2018, Disney faced a dilemma when old tweets containing dark humor about sensitive subjects resurfaced, leading to Gunn's dismissal [5]. This incident triggered an outpouring of support from fans and*

Thanveer Shaik, Xiaohui Tao, and Taotao Cai are with the School of Mathematics, Physics and Computing, University of Southern Queensland, Queensland, Australia (e-mail: Thanveer.Shaik@usq.edu.au, Xiaohui.Tao@usq.edu.au, Taotao.Cai@usq.edu.au).

Lin Li is with the School of Computer and Artificial Intelligence, Wuhan University of Technology, China (e-mail: cathylilin@whut.edu.cn)

Haoran Xie is with the Department of Computing and Decision Sciences, Lingnan University, Tuen Mun, Hong Kong (e-mail: hrxie@ln.edu.hk)

Xiaofeng Zhu is with the University of Electronic Science and Technology of China (e-mail: seanzhuxf@gmail.com)

Qing Li is with the Department of Computing, Hong Kong Polytechnic University, Hong Kong Special Administrative Region of China (e-mail: qingprof.li@polyu.edu.hk).

[1] https://link.library.eui.eu/portal/The-Right-To-Be-Forgotten–A-Comparative-Study/tw0VHCyGcDc/

actors, advocating for his reinstatement through open letters and petitions. However, the removal of such content from social media platforms like Facebook and Instagram doesn't guarantee its complete erasure from the internet. Tools like Facebook's "Off-Facebook Activity"[2] *help users unlink their data from third-party apps and websites, but the information persists. In a 2014 case, a Spanish court ruled in favor of an individual requesting the removal of specific search results from Google [6]. The court deemed this information irrelevant and outdated, as the related debt had been settled long ago. The European Union also enforced the removal of these search results by Google. These instances underscore the critical need for the development of machine unlearning mechanisms. Such mechanisms are essential for eliminating outdated and private data from machine learning models while maintaining their accuracy. In an era of evolving data privacy regulations, ensuring individuals' "right to be forgotten" necessitates the development of robust machine unlearning techniques.*

Challenges. Considering today's digitally-connected environment data distributed in various forms, such as from sensors, text documents, images, and time series data. In unlearning outdated or private data, Machine unlearning presents unique challenges depending on whether you're dealing with a single type of data (known as single-modality) or multiple types (referred to as multimodality) [7]. For single-modality data, the issue primarily lies in the build-up of outdated or irrelevant information, which can negatively affect the model's effectiveness and precision. [8], [9]. On the other hand, multimodality situations are even more complicated; each type of data can have different characteristics and varying contributions to the overall model's performance. [10], [11]. As we discussed in the example 1, the need to unlearn outdated or private data is atmost important. This ensure individuals have the "right to be forgotten" about their information in public avenues. However, the unlearning needs to be happen in both single modality and multimodality data to make it an holistic unlearning.

Distributed learning systems, particularly Federated Learning, have made significant strides in enabling machine learning models to train on decentralized data, offering the dual advantage of reduced communication costs and enhanced privacy [12], [13]. Notable efforts have been made to incorporate Differential Privacy (DP) into these systems [14], ensuring robust privacy safeguards through techniques like DP-SGD and DP-FedAvg [15], [16]. However, these existing frameworks face limitations when confronted with the dynamic nature of data distribution, an intrinsic challenge in distributed learning [17]. Although some efforts have been made in machine unlearning to address data irrelevancy over time, such as the Split into Shards and Aggregating (SISA) training method, these solutions often operate in isolation from privacy-preserving mechanisms [18], [19]. This bifurcation leaves a crucial research gap, the absence of a unified approach that addresses both privacy concerns and the adaptability requirements in the face of ever-changing data landscapes. There is a need to bridge this gap by providing an integrated solution for robust privacy measures and efficient selective unlearning, thereby enabling machine learning models to be both secure and adaptable in dynamic, distributed environments.

To address these challenges, we propose Federated Reinforcement Learning with Attention-based Machine Unlearning Framework (FRAMU). By integrating federated learning, adaptive learning mechanisms, and privacy preservation techniques, FRAMU aims to leverage the diverse and dynamic nature of data in both single modality and multimodality scenarios while upholding privacy regulations and optimizing the learning process. Attention mechanism is incorporated into FRAMU to ensure the responsible and secure handling of sensitive information across modalities. FRAMU leverages reinforcement learning and adaptive learning mechanisms to enable models to dynamically adapt to changing data distributions and individual participant characteristics in both single modality and multimodality scenarios. This adaptability facilitates ongoing model evolution and improvement in a privacy-preserving manner, accommodating the dynamic nature of the data present in federated learning scenarios. In addition to addressing the challenges associated with unlearning outdated, private, and irrelevant data in both single modality and multimodality scenarios, FRAMU offers valuable insights into the convergence behavior and optimization of the federated learning process.

Contributions. We state our major contributions as follows:

- We propose a adaptive unlearning algorithm using attention mechanism to adapt to changing data distributions and participant characteristics in single-modality and multimodality scenarios.
- We develop a novel design to personalize the unlearning process using FedAvg mechanism [20] and unlearn the outdated, private and irrelevant data.
- We propose an efficient unlearning algorithm that demonstrates fast convergence and achieves optimal solutions within a small number of communication rounds.
- We conduct extensive experiments to demonstrate the efficiency and effectiveness of the proposed approach using real-world datasets.

Organization. In Section II, we review related works. Section III outlines the problem addressed in this study. We proposed framework FRAMU in Section IV. In Section V, we present the experimental setup and evaluation results of the proposed framework, along with convergence and optimization analysis. Section VI delves into the implications of the proposed framework. Finally, in Section VII, we conclude the paper.

II. Related Works

The importance of data privacy in distributed learning systems has garnered significant attention, especially when handling sensitive types of data like medical or behavioral information [21]. Differential Privacy (DP), a mathematically rigorous framework for ensuring individual privacy, has been widely adopted for this purpose [22], [23]. Efforts to integrate DP within distributed learning environments, particularly in Federated Learning, have been increasing [12], [13]. Abadi

[2] https://www.facebook.com/help/2207256696182627

et al. [15] developed a seminal approach called Deep Learning with Differential Privacy (DP-SGD), which adapts the Stochastic Gradient Descent (SGD) algorithm to meet DP standards by clipping gradients and injecting noise, thereby offering stringent privacy safeguards during deep neural network training. Building on this, McMahan et al. [16] further tailored DP mechanisms for Federated Learning through an extension called DP-FedAvg. While these methods effectively address privacy concerns, they often fall short in dealing with dynamic data distributions, a prevalent issue in distributed learning [17]. Specifically, data sets can evolve over time, rendering some information outdated or irrelevant, and the persistence of such data in the learning process can compromise model efficacy. Although machine unlearning approaches like SISA training have emerged to tackle this issue by enabling efficient selective forgetting of data, these methods are not yet designed to work synergistically with privacy-preserving techniques like DP [18], [19].

Federated Learning (FL) has substantially revolutionized distributed learning, enabling the training of machine learning models on decentralized networks while preserving data privacy and minimizing communication costs [24]. Among the pioneering works in this area is the FedAvg algorithm by McMahan et al. [20], which relies on model parameter averaging across local models and a central server. However, FedAvg is not without its limitations, particularly when handling non-IID data distributions [25]. Solutions like FedProx by Li et al. [26] have sought to address this by introducing a proximal term for improved model convergence. While other researchers like Sahu et al. [27] and Konečný et al. [28] have made strides in adaptive learning rates and communication efficiency, the realm of FL still faces significant challenges in dynamic adaptability and efficient machine unlearning. While privacy has been partially addressed through Differential Privacy [29] and Secure Multiparty Computation [30], these techniques often compromise on model efficiency. Additionally, the applicability of FL in diverse sectors like healthcare and IoT emphasizes the unmet need for a model capable of dynamically adapting to varied data distributions while preserving privacy and efficiency [31], [32].

Reinforcement Learning (RL) has garnered much attention for its ability to train agents to make optimal decisions through trial-and-error interactions with their environments [33], [34]. Several pivotal advancements have shaped the field, including the development of Deep Q-Networks (DQNs) [35]. DQNs collaborate traditional RL techniques with deep neural networks, significantly enhancing the system's ability to process high-dimensional inputs such as images. Furthermore, experience replay mechanisms have been integrated to improve learning stability by storing and reusing past experiences [36]. Mnih et al. [37] significantly accelerated the RL field by implementing DQNs that achieved human-level performance on a variety of complex tasks. However, there are evident gaps in addressing challenges posed by non-stationary or dynamic environments—situations where the statistical properties of the environment change over time. Under such conditions, an RL agent's ability to adapt quickly is paramount. Several approaches like meta-learning [38] and attention mechanisms [39], [40] have sought to remedy these issues to some extent. Meta-learning, for example, helps models quickly adapt to new tasks by training them on a diverse range of tasks. However, the technique does not offer a robust solution for "unlearning" or forgetting outdated or irrelevant information, which is crucial for maintaining performance in dynamic environments. In a similar vein, attention mechanisms help agents focus on important regions of the input space, but they also fail to address the need for efficient unlearning of obsolete or irrelevant data. This leaves us with a significant research gap, the lack of mechanisms for efficient unlearning and adaptability in RL agents designed for dynamic, non-stationary environments.

FL encounters challenges when faced with dynamic data distributions and the accumulation of outdated or irrelevant information, hampering its adaptability in evolving environments. RL has been instrumental in training agents for optimal decision-making in dynamic environments, yet it too grapples with the need to efficiently unlearn outdated or irrelevant data. These challenges underscore the importance of integrating Attention Mechanisms into the machine unlearning process. Unlike selective data deletion, attention mechanisms assign reduced weights to outdated, private, or irrelevant information. This dynamic adjustment of attention scores allows models to prioritize relevant data while disregarding obsolete or extraneous elements. By bridging the worlds of Federated Learning and Reinforcement Learning [41] with Attention Mechanisms, our study addresses the pressing need for an integrated solution that optimizes decision-making in distributed networks with changing data landscapes, all while preserving data privacy and adaptively forgetting outdated, private, or irrelevant information.

III. Preliminaries & Problem Definition

A. Objective

The primary objective of this research is to investigate the processes of unlearning outdated, private, and irrelevant data in machine learning models, with a focus on maintaining both model accuracy and computational efficiency. Due to diverse data modalities prevalent in today's digital landscape, our study explore the unlearning process in two ways: Single Modality and Multimodality. In Single Modality, we use only one kind of data, like traffic sensor readings, to make decisions. On the other hand, Multimodality involves using various kinds of data, like text records and images, to make better-informed decisions. This is especially useful in fields like healthcare, where a range of data types can be combined for more effective patient treatment. Given that we often get data from many different sources, it's important that our study considers both these approaches.

B. Single Modality

In the Single Modality setting, only one kind of data, such as traffic sensor readings, is used for decision-making. Although straightforward, this approach may lack broader context for more nuanced decisions.

TABLE I: Summary of Notations and Descriptions

Symbol	**Description**
AG	Set of agents in the model
ag	An individual agent in the set AG
S_i	States observed by an agent ag
A	Set of possible actions
$\pi_i(s,a)$	Policy followed by the agent
$R_i(s,a)$	Rewards for actions in different states
θ_i	Parameters of local models
θ_g	Parameters of global model
w_{ij}	Attention score for a data point j
M	Set of modalities in Multimodality setting
X_k	Data vectors for modality k
θ_k	Parameters for modality k
w_{ik}	Attention scores within a modality k
t	Time step
s_t	State at time step t
a_t	Action at time step t
r_t	Reward at time step t
R_t	Cumulative reward
$\pi(a_t\|s_t)$	Policy function
$Q(s_t,a_t)$	Q-function
γ	Discount factor
α_i	Attention score for feature i
$\Delta\theta_i$	Update sent by agent a_i
f	Function for calculating attention scores
w_{gi}	Global attention score for update from agent a_i
K	Number of local agents
α_{avg}	Average attention score
δ	Predetermined threshold for attention score
$ag \in AG$	A specific agent within the set of all agents AG
m	Number of modalities
$x_1, x_2, ..., x_m$	Data vectors for each modality
v_i	Feature vector for modality i
$\bar{w}_j$	Averaged attention score across modalities for data point j
λ	Mixing factor
T	The total number of training rounds
α	Learning rate for Q-value function updates
η	Scaling factor for attention score updates
β	Mixing factor for combining global and local model parameters
ε	Convergence threshold for global model parameters
w_k	Local model parameters for agent k
W	Global model parameters
A_i	Attention score for data point i
A_{ik}	Attention score for data point i within agent k
N	Total number of data points across all agents
n_k	Number of data points in agent k

Definition 1. *Let $AG = \{ag_1, ag_2, \dots, ag_n\}$ be a set of agents, where each agent $ag \in AG$ represents an entity like an IoT device, traffic point, wearable device, edge computing node, or content recommendation system. Each agent ag observes states $S_i = \{s_1, s_2, \dots, s_m\}$ and takes actions $A = \{a_1, a_2, \dots, a_k\}$ based on a policy $\pi_i(s,a)$. Rewards $R_i(s,a)$ evaluate the quality of actions taken in different states. Agents possess local models with parameters θ_i, while a central server maintains a global model with parameters θ_g.*

Example 2. *In the Single Modality setting, let $AG = \{ag_1, ag_2, \dots, ag_n\}$ be a set of agents. An agent ag can represent a real-world entity such as a traffic light in a city. These traffic lights observe various states $S_i = \{s_1, s_2, \dots, s_m\}$, such as the number and speed of passing cars, and change colors (actions $A = \{a_1, a_2, \dots, a_k\}$) according to an algorithmic policy $\pi_i(s,a)$. The system evaluates the effectiveness of the traffic light changes in reducing wait time or congestion (rewards $R_i(s,a)$). Each traffic light has its own local decision-making model characterized by parameters θ_i, and there is a global model for optimizing city-wide traffic flow with parameters θ_g.*

To address the challenge of preserving data privacy and adaptively forgetting private, outdated, or irrelevant information, attention scores w_{ij} are assigned to each data point j in the local dataset of agent $ag \in AG$. These attention scores, computed using a function f that considers the current model state or contextual information, guide the learning and unlearning process within each agent. By assigning higher attention scores to relevant data and potentially forgetting or down-weighting irrelevant data, the agents can effectively focus on the most informative and up-to-date information.

C. Multimodality

In the Multimodality setting, different kinds of data, like text and images, are collectively used for decision-making, especially relevant in fields like healthcare where multiple data types can be used for a more comprehensive understanding.

Definition 2. *In the Multimodality setting, let $M = \{1, 2, \dots, k\}$ represent the set of modalities, where k is the total number of modalities. Each modality $k \in M$ is associated with a set of data vectors $X_k = \{x_{k1}, x_{k2}, \dots, x_{kn}\}$, and has its local model with parameters θ_k. Attention scores w_{ik} are assigned to individual data points x_{ik} within each modality to guide the learning and unlearning process.*

Example 3. *In the Multimodality setting, consider a healthcare system as a collection of agents in set $M = \{1, 2, \dots, k\}$, where k represents different types of medical data (modalities) such as medical imaging and patient history. For instance, medical imaging (modality M_1) would have a set of MRI scans represented as data vectors $X_1 = \{x_{11}, x_{12}, \dots, x_{1n}\}$. Likewise, patient history (modality M_2) might involve a set of past diagnosis records represented as data vectors $X_2 = \{x_{21}, x_{22}, \dots, x_{2n}\}$. Each modality has a specialized machine learning model with parameters θ_1 for medical imaging and θ_2 for patient history. These models use attention mechanisms to weigh the importance of each data point, represented by attention scores w_{1k} for MRI scans and w_{2k} for patient history records. These scores guide the decision-making process in diagnosis and treatment.*

Tab. I summarizes the mathematical notations frequently used throughout this paper.

IV. Methodology

In an era marked by an ever-increasing influx of data, the need for adaptive machine learning models that can efficiently unlearn outdated, private, or irrelevant information is paramount. The methodology proposed in this paper addresses this necessity by introducing two key technical contributions. First, we propose an adaptive unlearning algorithm utilizing attention mechanisms to tailor the learning and unlearning processes in single-modality and then extend to multi-modality.

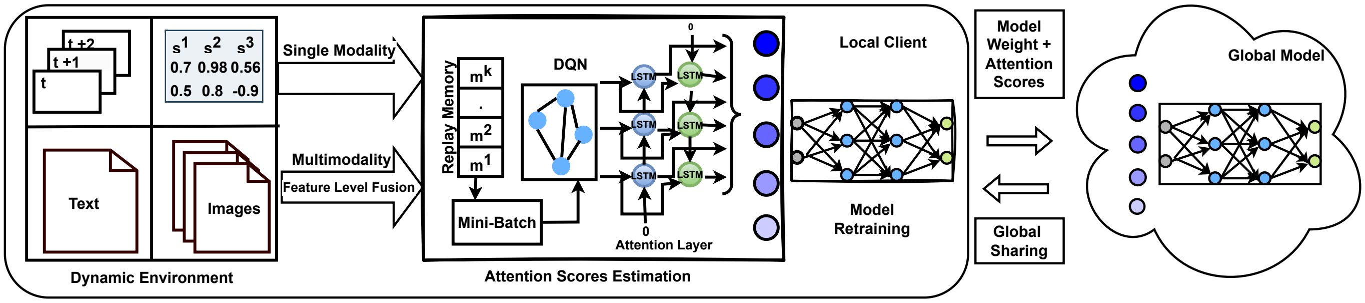


Fig. 2: Proposed adaptive algorithm, FRAMU, using attention mechanism

This innovative approach allows the model to adapt to dynamic changes in data distributions as well as variations in participant characteristics. Second, we put forth a novel design that employs the FedAvg mechanism [20] to personalize the unlearning process. This design ensures that the model is able to discard data that has become irrelevant, outdated, or potentially invasive from a privacy perspective, thus preserving the integrity of the learning model while adapting to new or changing data. The following sections will elaborate on these contributions, providing a detailed discussion of the proposed framework, Federated Reinforcement Learning with Attention-based Machine Unlearning (FRAMU) with single modality and multimodality, as depicted in Fig. 2.

A. FRAMU with Single Modality

At the core of FRAMU is an attention layer, serving as a function approximator, which enhances the learning process in local agents. Unlike conventional function approximators, this layer assigns attention scores to individual data points while approximating functions. The scores indicate the importance of each data point in the local model's learning process. As the agent interacts with its environment, it receives either rewards or penalties. These rewards and penalties serve as continuous feedback, which in turn updates and evolves the scores. Consider an agent operating in discrete time steps, where at time step t, the agent observes state s_t, takes action a_t, and receives reward r_t. The primary objective is to identify a policy $\pi(a_t|s_t)$ that maximizes the cumulative reward R_t. The Q-function, representing the expected cumulative reward with discount factor γ, is defined in Equation 1

$$Q(s_t,a_t)=\mathbb{E}[R_t \mid s_t,a_t]=r_t+\gamma\mathbb{E}[Q(s_{t+1},a_{t+1}) \mid s_t,a_t] \tag{1}$$

Incorporating the attention mechanism involves assuming that each state s_t consists of features $[x_1,x_2,...,x_n]$. The attention mechanism assigns scores α_i to these features:

$$\alpha_i=\text{Attention}(x_i,\text{context}) \tag{2}$$

The context include supplementary information like the prior state or action. The Q-function can then be approximated as a weighted sum of features:

$$Q(s_t,a_t)\approx\sum(\alpha_i\cdot x_i) \tag{3}$$

After each learning cycle, local agents send their model updates θ and attention scores α to the central server in the form of a tuple (θ,α).

Example 4. *For example, consider a scenario where an agent represents a traffic light management system, observing states like vehicle count, pedestrian presence, and weather conditions. Conventional function approximators might treat all these observed state features equally. However, with the attention mechanism, the agent could assign higher attention scores to vehicle count during rush hours, enabling it to make more context-aware decisions.*

B. Estimation of Attention Scores

FRAMU estimates attention scores at both local and global levels. At the local level, each agent computes attention scores for its data points by incorporating an attention mechanism into its local model. This mechanism allocates scores based on data point relevance or significance to the agent's task. For agent a_i with local model parameters θ_i, the attention score w_{ij} for data point j is computed using function f, possibly considering the model's state or other contextual information:

$$w_{ij}=f(s_j,\theta_i) \tag{4}$$

Global attention scores help the server prioritize updates or identify data points for global unlearning. For global model parameters θ_g, the global attention score for an update from agent a_i is computed as:

$$w_{gi}=f(\Delta\theta_i,\theta_g) \tag{5}$$

Here, $\Delta\theta_i$ represents the update sent by agent a_i, and f computes attention scores. This function consider the combined attention scores from local agents, as well as cues from the overall global context.

Example 5. *To put this into perspective, consider an IoT scenario where each agent is a temperature sensor in different parts of a building. One sensor near a heater might assign high attention scores to data points collected during the winter months. Another sensor near an air conditioner might find its summer data more relevant. On the central server, a global attention score could blend these attention metrics to identify which temperature patterns are generally more useful for, say, energy management across the building.*

C. Global Model Aggregation and Unlearning

The central server aggregates model updates from local agents using Federated Averaging [42]. Attention scores play a pivotal role in the unlearning process. Aggregated attention scores from all agents yield an average score:

$$\alpha_{\text{avg}} = \frac{1}{K} \sum \alpha_k \tag{6}$$

When the average attention score α_{avg} for a specific feature falls below a predetermined threshold δ, the server reduces the contribution of that feature in the global model based on attention scores as shown in Equation 7.

$$\theta_{\text{global'}} = g(\theta_{\text{global}}, \alpha_{\text{avg}}) \tag{7}$$

Example 6. *As an example, consider a wearable device network that tracks steps, heart rate, and sleep patterns. If many people stop wearing their devices to bed, the global attention score for sleep data might drop below a certain threshold. Consequently, the server can adjust the global model to focus less on sleep data, thereby aligning the model better with actual usage patterns.*

After global model updates and unlearning, the improved global model is transmitted back to local agents. This refined model demonstrates increased robustness and adaptability to changing data distributions due to the aggregation and unlearning processes. Consequently, local agents can potentially perform better within their respective operational environments. Revised global model parameters, denoted $\theta_{\text{global'}}$, are directly sent by the central server to individual local agents $\theta_k = \theta_{\text{global'}}$.

Example 7. *For instance, after undergoing unlearning and re-aggregation based on the attention scores, the central server might distribute a refined model back to the local agents. In the case of a content recommendation system, this could mean that outdated trending topics are given less priority, making the system more responsive to real-time user preferences.*

In the single-modality approach of the FRAMU framework, local agents use an attention layer to enhance learning by assigning dynamic scores to observed features. These agents then send their model updates and attention scores to a central server. The server employs Federated Averaging for model aggregation and uses the attention scores for global unlearning, thus refining the global model. The refined model is then sent back to the local agents. The use of attention scores at both local and global levels enhances the system's adaptability and robustness in handling changing data distributions.

D. FRAMU with Multimodality

In the FRAMU framework, addressing multimodality involves effectively integrating diverse types of data like images, text, audio, and sensor readings. This integration enhances decision-making and model performance while maintaining data privacy. Local agents fine-tune their models to each type of data, leading to a more robust and generalizable system that performs better in complex environments.

1) Modality-specific Attention Mechanisms: To effectively capture the relevance and importance embedded in data originating from diverse modalities, specific attention mechanisms tailored to each modality are introduced. Each modality is furnished with its own set of attention scores, which are attributed to data points within that particular modality. The role of these attention scores is to guide the learning and unlearning processes for each modality. This mechanism empowers local agents to concentrate their efforts on the most pertinent and informative data within their respective modalities.

The computation of attention scores for each modality j within the domain of agent $ag \in AG$ can be expressed as:

$$w_{ij} = f_j(s_{ij}, \theta_i), \tag{8}$$

where s_{ij} represents a data point from modality j within agent $ag \in AG$, while θ_i encapsulates the local model parameters of agent $ag \in AG$. The function f_j takes into consideration the modality-specific attributes and contextual nuances, thus enabling the calculation of modality-specific attention scores.

Let v_i denote the feature vector originating from modality j within the scope of agent $ag \in AG$. The process of feature-level fusion is shown in Equation 9.

$$v_i = [x_{i1}, x_{i2}, ..., x_{im}] \tag{9}$$

Example 8. *In a surveillance context, agents could be processing data feeds from public CCTVs, mobile devices, and social media posts to monitor for public safety. Each modality might have its own privacy implications. For instance, video feeds could employ attention mechanisms to automatically blur faces or license plates, focusing instead on object shapes, sizes, and movements that are pertinent to safety but not invasive of individual privacy.*

2) Unlearning and Adaptation in Multimodality: In the multimodal context, the unlearning process is enriched by the inclusion of attention scores from every modality. These scores serve as indicators of data relevance and informativeness. Should certain data points consistently garner low attention scores across multiple modalities, it suggests their diminished relevance or outdated nature. Leveraging attention scores from disparate modalities, the central server orchestrates the unlearning process by attenuating or removing the influence of such data points within the global multimodal model. This practice ensures that the model prioritizes the most informative and contemporary data. Consider w_{ij} as the attention score for data point j within modality i. The averaged attention score spanning modalities for a given data point is computed as:

$$\bar{w}_j = \frac{1}{m} \sum i = 1^m w_{ij} \tag{10}$$

If $\bar{w}_j$ descends below a predefined threshold, the central server enacts the down-weighting or elimination of that data point's influence within the global multimodal model. This preventive measure ensures that antiquated or irrelevant information does not undermine the decision-making process.

Throughout the adaptation phase, local agents harness the updated global multimodal model to refine their own local models. The interplay between the global and local model parameters is governed by a mixing factor, thereby enabling local agents to harness shared knowledge while retaining their modality-specific expertise. This strategic approach empowers local agents to elevate their decision-making proficiencies across varied modalities, fueled by the advancements inherent in the global model. The fusion of global and local model parameters can be denoted as:

$$\theta_i^{\text{new}} = \lambda \theta_{\text{global}} + (1 - \lambda)\theta_i^{\text{old}} \tag{11}$$

Where θ_i^{new} signifies the updated local model parameters for agent $ag \in AG$, θ_{global} embodies the refined global multimodal model parameters, θ_i^{old} encapsulates the previous local model parameters, and λ governs the mixing factor that regulates the equilibrium between global and local knowledge. The process of unlearning and adaptation within the multimodal context ensures that the global multimodal model remains pertinent and contemporary. Simultaneously, it empowers local agents to harness collective knowledge for heightened decision-making proficiency across diverse modalities.

Example 9. *Consider a smart home environment where various types of data are collected, such as energy usage patterns, voice command logs, and security camera footage. Over time, some data may be deemed too sensitive or private to keep, such as recorded conversations. These could receive low attention scores deliberately, flagging them for quicker 'forgetting' or deletion from the model, in compliance with privacy regulations or user preferences.*

E. Continuous Adaptation and Learning

Continuous Adaptation and Learning play pivotal roles within the FRAMU framework, ensuring its efficacy in dynamic and ever-evolving environments. These processes engender an iterative exchange of insights between local agents and the central server, further fostering the perpetual refinement of models at both the local and global levels.

1) Adapting to Local Changes: At the local level, agents must seamlessly adapt to the evolving circumstances inherent in their respective environments. In scenarios aligned with reinforcement learning paradigms, agents recalibrate their policies based on undertaken actions and observed rewards. Moreover, attention scores assigned to data points or features may dynamically shift as new data comes to the fore or as earlier data becomes less relevant. This innate capacity for dynamic adaptation assures the continuous relevance of each local agent's model. Let s_t denote the environmental state at time t, and a_t embody the action undertaken by the agent. Post-receipt of a reward r_t and transition to a novel state s_{t+1}, the agent endeavors to maximize the anticipated cumulative reward. The Q-value function $Q(s, a)$ stands as a surrogate for the anticipated cumulative reward ensuing from the selection of action a in the context of state s. Temporal-difference learning algorithms propel the updates to the Q-value function:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left[r_t + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t) \right] \tag{12}$$

Where α represents the learning rate, while γ encapsulates the discount factor.

In tandem with attention scores, A_i symbolizes the attention score attributed to data point i. Updates to the attention score are influenced by the temporal-difference error, denoted as δ:

$$A_i \leftarrow A_i + \eta |\delta|, \tag{13}$$

Where η functions as a scaling factor, and $\delta = r_t + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t)$.

By adapting to local changes through reinforcement learning mechanisms and dynamic attention score updates, local agents ensure that their models remain pertinent and up-to-date within their operational contexts. This process reflects the framework's commitment to continuous learning and real-time responsiveness.

Example 10. *Imagine an agent is responsible for analyzing social media posts for market research. Initially, it gathers all kinds of data, including personal user information. However, due to a change in privacy laws, this type of data collection becomes restricted. The local agent must then rapidly adapt, adjusting its attention scores to de-prioritize or ignore types of data that it's no longer permitted to process, thus preserving user privacy.*

2) Global Aggregation and Adaptation: As local agents perpetually learn and adapt, they communicate these updates to the central server, thereby fostering a continuous dialogue. The central server assumes the responsibility of aggregating this incoming information to update the global model. Simultaneously, the server monitors the attention scores shared by local agents. If these scores consistently indicate a decline in the significance of certain data points or features, the server may initiate a global unlearning process. This practice ensures that the global model remains contemporary and avoids becoming ensnared by obsolete information. Local agents transmit their updated model parameters, denoted as w_k for agent k, and attention scores A_{ik} for data point i within agent k, to the central server. This collection of updates is aggregated by the server to yield the updated global model parameters W, employing the principles of federated averaging:

$$W \leftarrow \frac{1}{K} \sum_k w_k, \tag{14}$$

Where K signifies the total number of local agents.

Attention scores contribute to the orchestration of global unlearning. A predetermined threshold, θ, serves as the reference point. If the averaged attention score across all agents for a specific data point dips below θ, the global model curtails the influence of that data point.

Example 11. *Consider multiple agents collecting data for city-wide traffic management. While the aggregated data can offer valuable insights into traffic patterns, it might also inadvertently reveal sensitive information, such as the frequent routes of individual citizens. In this case, the central server can use averaged attention scores to down-weight or exclude data points that risk breaching privacy, ensuring the global model remains both useful and ethical.*

3) Feedback Loop: Subsequent to the central server's update of the global model, this refined model is communicated back to local agents through a feedback loop. This reciprocal process connects the learning of local agents with the global model and vice versa. This iterative exchange enables local agents to leverage the updated global model for the initialization or refinement of their own models. This proves particularly advantageous when agents encounter novel or unfamiliar data encountered by other agents. The global model assumes the role of a shared knowledge repository, equipping all agents with insights to bolster their decision-making. The central server transmits the updated global model parameters W to local agents, who subsequently refine their respective models. This process leverages a mixing factor β to combine global and local model parameters:

$$w'_k \leftarrow \beta W + (1 - \beta) w_k, \tag{15}$$

Where $0 \leq \beta \leq 1$ regulates the degree to which the global model influences the local model.

Example 12. *After a new privacy policy takes effect, the central server updates the global model to ensure compliance. This update is then propagated back to all local agents. For instance, if a new policy restricts the use of location data, the updated global model will influence local agents to diminish or cease the collection of such data, thereby maintaining individual privacy.*

F. FRAMU Framework

Algorithm 1 FRAMU Framework

```
    Input: a set of LocalAgents, a CentralServer, $T$, $\theta$, $\alpha$, $\eta$, $\gamma$, $\beta$, $\varepsilon$;
    Output: Trained global model parameters $W$ for federated reinforcement learning.
 1: Initialize local model parameters $w_k$ for each agent $k$
 2: Initialize global model parameters $W$ at the central server
 3: Initialize attention scores $A_{ik}$ for each data point $i$ in agent $k$
 4: for $t = 1, 2, ..., T$ do
 5:     for each local agent $k$ do
 6:         Observe current states $s_{ij}$ for each modality $j$
 7:         Take action $a_t$ based on policy derived from $Q(s, a; w_k)$
 8:         Observe reward $r_t$ and next states $s'_{i,j}$ for each modality $j$
 9:         Compute TD error $\delta = r_t + \gamma \max_a Q(s'_{i,j}, a; w_k) - Q(s_{ij}, a_t; w_k)$
10:         Update $Q(s_{ij}, a_t; w_k) \leftarrow Q(s_{ij}, a_t; w_k) + \alpha\delta$
11:         Update attention scores $A_{ikj} \leftarrow A_{ikj} + \eta|\delta|$
12:     end for
13:     Send local model parameters $w_k$ and attention scores $A_{ikj}$ to CentralServer
14:     for each data point $i$ do
15:         if $\sum_k \frac{1}{m} \sum_j A_{ikj}/K < \theta$ then
16:             Reduce influence of data point $i$ in the global model
17:         end if
18:     end for
19:     Aggregate local model parameters to update global parameters:
20:     $W \leftarrow \sum_k \left(\frac{n_k}{N}\right) w_k$
21:     Send updated global model parameters $W$ to local agents
22:     for each local agent $k$ do
23:         Fine-tune local model with global model:
24:         $w'_k \leftarrow \beta W + (1 - \beta) w_k$
25:     end for
26:     if $|P(W_{t+1}) - P(W_t)| < \varepsilon$ then
27:         Break
28:     end if
29: end for
```

The algorithm 1 outlines the implementation of the FRAMU Framework. It initializes local and global model parameters and attention scores (lines 2-3). It then iterates through local agents to observe, select actions, and update Q-values and attention scores (lines 4-15). Local updates are sent to a central server (line 16), where averaged attention scores are used to diminish irrelevant data points in the global model (lines 17-21). Both local and global models are updated and shared (lines 22-25), followed by fine-tuning of local models based on the global model's performance (lines 26-32). The algorithm aims for adaptive decision-making in distributed networks.

V. Experimental Setup and Results Analysis

In order to evaluate the performance of FRAMU, we conducted a series of experiments using different baseline models and datasets. The experimental setup consisted of the following components: datasets, baseline models, evaluation metrics, and FRAMU configurations. For each dataset, we configured FRAMU with specific parameters related to unlearning thresholds and privacy preservation. The unlearning thresholds, such as outdated_threshold and irrelevant_threshold, were set based on domain knowledge and sensitivity analysis. The privacy_epsilon parameter was set to control the level of privacy preservation, ensuring compliance with privacy regulations.

TABLE II: Datasets for evaluation

Modality	Dataset	Outdated Data	Privacy Data	Irrelevant Data	Description
Single Modality	AMPds2 [43]	✓	✓	✓	Electricity, water, and natural gas consumption data .from a Canadian household.
	METR-LA [44]	✓	✗	✓	Traffic speed data from over 200 sensors in Los Angeles Metropolitan area.
	MIMIC-III [45]	✓	✓	✓	Health-related data from critical care units,including demographics, vital signs, laboratory results, and medications.
Multimodality	NYPD [46]	✓	✓	✓	Records of complaints filed with the New York City Police Department.
	MIMIC-CXR [47]	✓	✓	✓	Chest radiographs with associated radiology reports for medical image analysis tasks.
	Smart Home EnergyDataset (SHED) [48]	✓	✓	✓	Energy consumption data from smart home devices and appliances.

A. Datasets

In this study, publicly available datasets that encompass various modalities and address specific challenges related to outdated, private, and irrelevant data are adopted. Table II

TABLE III: Baseline Models

Data Type	Baseline Models	Characteristics
Single Modality	FedLU [49]	Federated learning model with knowledge graph embedding and mutual knowledge distillation.
	Zero-shot MU [50]	Baseline model for machine unlearning with error-minimizing-maximizing noise and gated knowledge transfer.
	SISA Training [18]	Framework with strategic data point limitation for optimized unlearning.
Multimodality	MMoE [51]	Multi-gate Mixture-of-Experts model for multimodal data with ensemble learning.
	CleanCLIP [52]	Fine-tuning framework to weaken spurious associations from backdoor attacks.
	Privacy-Enhanced Emotion Recognition (PEER) [53]	Baseline model with adversarial learning for privacy-preserving emotion recognition.

TABLE IV: FRAMU - Evaluation Results on Single Modality

Unlearning	Dataset		FedLU [49]			Zero-shot [50]			SISA [18]			FRAMU (Ours)	
			MSE	MAE	p-value	MSE	MAE	p-value	MSE	MAE	p-value	MSE	MAE
Outdated Data	**Original**	AMPds2	0.063	6.740	0.024	0.061	6.890	0.031	0.059	6.760	0.041	**0.046**	**5.570**
		METR-LA	0.079	7.140	0.016	0.082	7.210	0.038	0.078	7.090	0.029	**0.065**	**5.930**
		MIMIC-III	0.099	12.800	0.031	0.102	12.930	0.045	0.097	12.680	0.032	**0.083**	**10.650**
	Unlearned	AMPds2	0.060	6.630	0.015	0.055	6.860	0.029	0.056	6.690	0.036	**0.038**	**4.670**
		METR-LA	0.075	7.020	0.029	0.077	7.100	0.025	0.072	6.960	0.032	**0.052**	**4.910**
		MIMIC-III	0.095	12.650	0.023	0.098	12.820	0.041	0.094	12.580	0.017	**0.069**	**8.900**
Private Data	**Original**	AMPds2	0.052	6.780	0.014	0.054	6.930	0.037	0.053	6.810	0.041	**0.041**	**5.540**
		MIMIC-III	0.078	12.870	0.035	0.080	13.010	0.043	0.079	12.760	0.045	**0.064**	**10.600**
	Unlearned	AMPds2	0.049	6.670	0.011	0.052	6.910	0.035	0.051	6.740	0.015	**0.033**	**4.590**
		MIMIC-III	0.075	12.720	0.031	0.077	12.900	0.038	0.076	12.650	0.016	**0.053**	**8.860**
Irrelevant Data	**Original**	AMPds2	0.047	6.700	0.035	0.050	6.850	0.044	0.048	6.730	0.031	**0.037**	**5.440**
		METR-LA	0.054	7.100	0.027	0.056	7.170	0.041	0.055	7.050	0.025	**0.043**	**5.830**
		MIMIC-III	0.070	12.730	0.038	0.072	12.870	0.031	0.071	12.620	0.039	**0.057**	**10.410**
	Unlearned	AMPds2	0.045	6.590	0.011	0.047	6.830	0.036	0.046	6.660	0.029	**0.030**	**4.510**
		METR-LA	0.052	6.980	0.014	0.054	7.070	0.019	0.053	6.930	0.022	**0.035**	**4.750**
		MIMIC-III	0.068	12.580	0.029	0.070	12.760	0.024	0.069	12.510	0.027	**0.047**	**8.690**

provides detailed information about each dataset, including the data modality, number of instances, attributes, target variables, and specific characteristics pertinent to our study. In order to evaluate FRAMU, we conducted a comprehensive comparison of its performance against several contemporary baseline models. This comparative analysis was carried out in both single-modality and multimodality contexts as shown in Tab. III.

B. *Evaluation Metrics*

The FRAMU framework is evaluated using several important metrics: Mean Squared Error (MSE), Mean Absolute Error (MAE), Reconstruction Error (RE), Activation Distance (AD), and Relearn Time. A lower MSE or MAE score shows that the unlearning process is closely aligned with what was expected, indicating a high quality of unlearning. The RE measures how well the model can rebuild data that it has unlearned, with a lower score being better. AD measures the average distance between the predictions of the model before and after unlearning, using what is known as L2-distance, on a specific set of forgotten data. These metrics together give a well-rounded evaluation of how well the unlearning process is working.

C. *Single Modality Unlearning Results*

To evaluate the efficacy of FRAMU in unlearning outdated, private, and irrelevant data, we will analyze the results obtained from the experiments. The performance of FRAMU will be compared to the baseline models, namely FedLU, Zero-shot MU, and SISA training. It is important to note that the METR-LA dataset [44] is excluded from the private data experiments as it does not contain any private data. The performance metrics of FRAMU in unlearning outdated, private, and irrelevant data will be presented alongside the results of the baseline models for a comprehensive comparison as shown in Tab. IV. The p-values associated with these comparisons serve as indicators of the statistical significance of FRAMU's performance improvements.

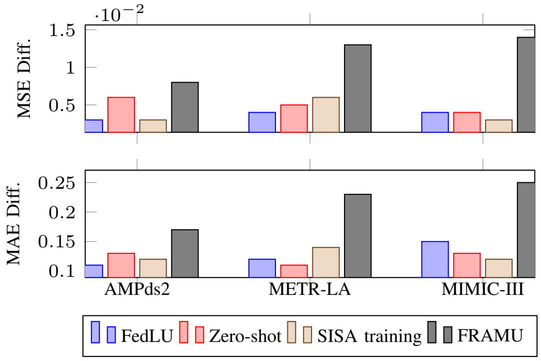


Fig. 3: Comparative Analysis of MSE and MAE Differences between Original and Unlearned Single-Modality Data

1) Outdated Data: Unlearning outdated data is crucial to maintain the accuracy and relevancy of trained models. Outdated data may introduce noise, biases, or patterns that no longer hold true in the current context. By selectively unlearning outdated data, FRAMU aims to adapt the model to the most up-to-date data distribution. When unlearning outdated data, FRAMU consistently achieves lower MSE and MAE compared to the baseline models across all datasets. This improvement is attributed to FRAMU's ability to adapt the model to the current data distribution by selectively unlearning outdated data, thereby ensuring that the model is trained on the most relevant and up-to-date information. The low p-values associated with the comparisons highlight the statistical significance of FRAMU's superiority in unlearning outdated data, clearly demonstrating that FRAMU significantly outperforms other models in this regard.

2) Private Data: Protecting the privacy of sensitive information is of utmost importance in many real-world applications. Unintentional retention of private data in the model can lead to privacy breaches and legal concerns. FRAMU incorporates privacy-preserving techniques during the unlearning process to ensure that sensitive information from private data is not retained. The METR-LA dataset was not considered for evaluating private data unlearning, as it doesn't contain privacy-sensitive data. In the case of private data, FRAMU consistently demonstrates superior performance in terms of both MSE and MAE. For example, in the AMPds2 dataset, FRAMU achieves an MSE of 0.038 and an MAE of 5.700, outperforming the best-performing baseline model, FedLU. This effectiveness can be traced back to the federated reinforcement

TABLE V: FRAMU - Evaluation Results on Multimodality

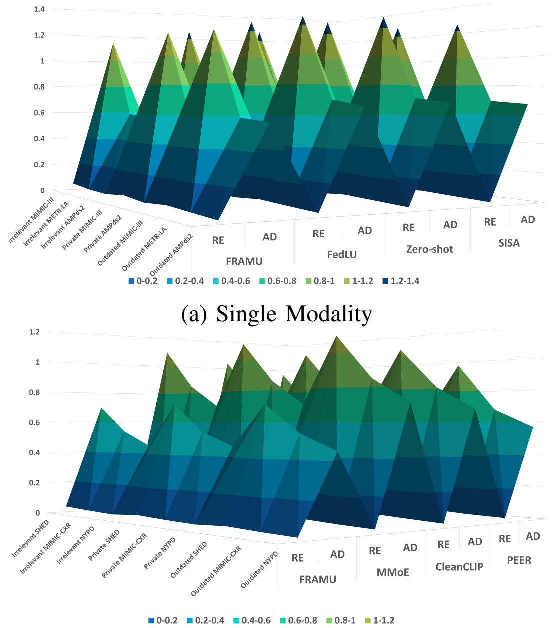
Unlearning	**Dataset**		**MMoE [51]**			**CleanCLIP [52]**			**PEER [53]**			**FRAMU (ours)**	
			MSE	**MAE**	**p-value**	**MSE**	**MAE**	**p-value**	**MSE**	**MAE**	**p-value**	**MSE**	**MAE**
Outdated Data	**Original**	NYPD	0.064	7.28	0.024	0.062	6.95	0.031	0.06	6.41	0.041	**0.055**	**5.77**
		MIMIC-CXR	0.075	8.71	0.016	0.079	8.31	0.038	0.074	7.67	0.029	**0.071**	**6.9**
		SHED	0.095	11.27	0.031	0.098	10.76	0.045	0.093	9.92	0.032	**0.089**	**8.93**
	Unlearned	NYPD	0.061	7.13	0.015	0.059	6.78	0.029	0.058	5.71	0.036	**0.042**	**4.54**
		MIMIC-CXR	0.071	8.55	0.029	0.075	8.12	0.025	0.07	6.84	0.032	**0.052**	**5.45**
		SHED	0.091	11.1	0.023	0.094	10.54	0.041	0.09	9.76	0.017	**0.067**	**7.07**
Private Data	**Original**	NYPD	0.053	7.33	0.014	0.055	7	0.037	0.054	6.45	0.041	**0.051**	**5.81**
		MIMIC-CXR	0.063	8.76	0.035	0.065	8.36	0.043	0.064	7.71	0.045	**0.062**	**6.94**
		SHED	0.078	11.34	0.035	0.08	10.82	0.044	0.079	9.98	0.031	**0.077**	**8.98**
	Unlearned	NYPD	0.051	7.17	0.011	0.053	6.82	0.035	0.052	6.31	0.015	**0.039**	**4.57**
		MIMIC-CXR	0.06	8.6	0.031	0.062	8.17	0.038	0.061	7.56	0.016	**0.046**	**5.48**
		SHED	0.075	11.17	0.011	0.077	10.61	0.036	0.076	9.81	0.029	**0.058**	**7.11**
Irrelevant Data	**Original**	NYPD	0.047	7.25	0.027	0.05	6.92	0.041	0.048	6.38	0.025	**0.046**	**5.74**
		MIMIC-CXR	0.054	8.66	0.038	0.056	8.27	0.031	0.055	7.63	0.039	**0.053**	**6.87**
		SHED	0.07	11.21	0.045	0.072	10.7	0.032	0.071	9.87	0.042	**0.069**	**8.88**
	Unlearned	NYPD	0.045	7.1	0.014	0.047	6.74	0.019	0.046	6.24	0.022	**0.034**	**4.52**
		MIMIC-CXR	0.052	8.5	0.029	0.054	8.08	0.024	0.053	7.48	0.027	**0.04**	**5.42**
		SHED	0.068	11.04	0.025	0.07	10.49	0.022	0.069	9.71	0.021	**0.052**	**7.04**

learning approach adopted by FRAMU, enabling collaborative learning across multiple parties while respecting data privacy constraints. The statistical significance of this performance improvement is further supported by the associated p-values, which unequivocally confirm the substantial and meaningful nature of FRAMU's enhancements in unlearning private data.

3) Irrelevant Data: Unlearning irrelevant data is essential to reduce noise and interference caused by data points that do not contribute to the underlying data distribution. Irrelevant data can introduce unnecessary patterns or outliers that negatively affect the model's understanding and prediction accuracy. By unlearning irrelevant data, FRAMU focuses on the most informative and relevant data instances, resulting in improved model performance. FRAMU exhibits remarkable performance in unlearning irrelevant data, consistently achieving the lowest MSE and MAE values compared to the baseline models. In the AMPds2 dataset, FRAMU achieves an MSE of 0.033 and an MAE of 5.600, outperforming the other models. The results are backed by low p-values, indicating its statistical significance over the baseline models, and underscore FRAMU's substantial advantage in unlearning irrelevant data.

A visual comparison of the differences in MSE and MAE between original and unlearned data for different datasets and baseline models as shown in Fig. 3. FRAMU consistently shows the highest differences, suggesting that it may be the most affected by the unlearning process. The other models show varying patterns of differences across the datasets.

FRAMU manifests superior performance relative to its counterparts across all datasets in RE and AD metrics as shown in Fig. 4a. To elucidate, in the AMPds2 dataset, FRAMU registers an RE and AD of 0.024 and 0.57, respectively, in contrast to FedLU's figures of 0.03 and 0.66. Similarly, within the METR-LA dataset, FRAMU attains average values of 0.033 and 0.59 for RE and AD, as opposed to FedLU's 0.038 and 0.7. In the case of the MIMIC-III dataset, FRAMU again excels, recording 0.044 and 1.16 against FedLU's 0.049 and 1.263 for RE and AD, respectively.



(a) Single Modality

(b) Multimodality

Fig. 4: Comparative Analysis of FRAMU performance with Baseline Models in RE and AD Metrics

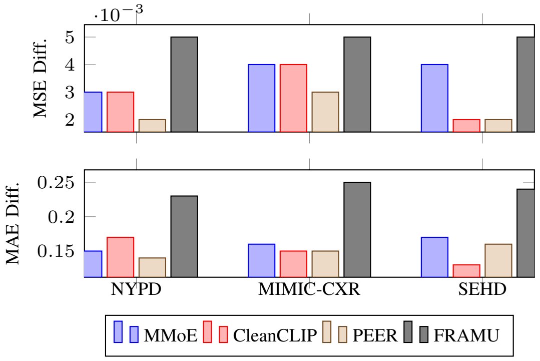


Fig. 5: omparative Analysis of MSE and MAE Differences between Original and Unlearned Multimodality Data

D. Multimodality Unlearning Results

In the multimodality experiment, the FRAMU framework handles multiple modalities of data, including images, text, and sensor data. The purpose of this experiment was to assess the performance of FRAMU in the context of unlearning outdated, private, and irrelevant data within a multimodal learning setting. To conduct the experiment, we utilized well-known benchmark datasets: MIMIC-CXR [47], NYPD Complaint Data [46], and SHED [48]. The evaluation primarily focused on measuring the reduction in error and performance improvement achieved by FRAMU compared to baseline models when unlearning outdated, private, and irrelevant data. The p-values associated with these comparisons are pivotal in highlighting the statistical significance of FRAMU's advancements.

1) Outdated Data: FRAMU achieves lower MSE, MAE, RE, and AD values compared to the baseline models across all datasets. For example, in the NYPD Complaint Data [46] dataset, FRAMU achieves an MSE of 0.047 and an MAE of 5.037, outperforming MMoE, CleanCLIP, and Privacy-Enhanced Emotion Recognition. Similar trends can be observed in the MIMIC-CXR [47] and SHED [48] datasets, where FRAMU consistently achieves better performance. FRAMU excels in capturing temporal changes and patterns within multimodal data. By unlearning outdated information and emphasizing the most recent and relevant features, FRAMU effectively reduces the impact of outdated patterns on predictive performance. This allows FRAMU to outperform the baseline models, which do not have mechanisms specifically designed for handling outdated data. This achievement is supported by the associated p-values, underlining the statistical significance of FRAMU's performance improvements. It affirms FRAMU's substantial advantage in unlearning outdated data over the baseline models.

2) Private Data: FRAMU continues to outperform the baseline models in terms of MSE and MAE values. In the NYPD Complaint Data [46] dataset, FRAMU achieves an MSE of 0.043 and an MAE of 5.067, outperforming the other models. This trend is also observed in the MIMIC-CXR [47] and SHED [48] datasets, where FRAMU consistently achieves lower values. FRAMU's attention-based machine unlearning framework plays a crucial role in preserving data privacy. By selectively attending to shared features across modalities while ignoring private information, FRAMU achieves a balance between privacy protection and predictive accuracy. This enables FRAMU to achieve superior performance compared to the baseline models, which may struggle to preserve privacy while maintaining predictive power. The p-values underscore that FRAMU significantly outperforms other models in unlearning private data.

3) Irrelevant Data: FRAMU again demonstrates superior performance. In the NYPD Complaint Data [46] dataset, FRAMU achieves an MSE of 0.038 and an MAE of 5.012, surpassing the baseline models. Similar trends can be observed in the MIMIC-CXR [47] and SHED [48] datasets, where FRAMU consistently achieves lower values. FRAMU's attention mechanism allows it to focus on the most relevant features and modalities for prediction while disregarding irrelevant or noisy information. This ability to selectively attend to informative features improves the overall predictive accuracy of FRAMU, leading to its statistically significant performance gains over the baseline models. The baseline models, lacking attention mechanisms, are less effective in filtering out irrelevant information, which may negatively impact their predictive performance. These p-values reinforce the fact that FRAMU significantly excels in unlearning irrelevant data.

The differences in MSE and MAE between original and unlearned data for different datasets and baseline models is presented in Fig. 5. FRAMU consistently shows the highest differences in both MSE and MAE, suggesting that it may be the most affected by the unlearning process. This could be interpreted as FRAMU being more responsive to unlearning, which might be aligned with its design to handle outdated, private, and irrelevant data. The other models show relatively similar patterns of differences, with slight variations across the datasets.

We evaluated the FRAMU performance in terms of RE and AD metrics and compared with the baseline model as shown in Fig. 4b. Across three distinct unlearning scenarios and datasets: NYPD, MIMIC-CXR, and SHED, FRAMU consistently outperforms its competitors. It achieves lower average RE and AD scores, indicating higher efficiency and applicability in machine unlearning tasks. This robust performance across diverse conditions establishes FRAMU as a leading option in this emerging research field.

E. Convergence Analysis

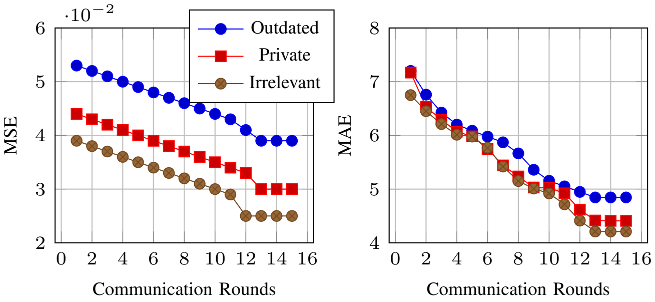


Fig. 6: Convergence Analysis

The convergence analysis of FRAMU, as shown in Figure 6, evaluates its performance over multiple communication rounds using MSE and MAE metrics across three types of data: Outdated, Private, and Irrelevant. The analysis reveals a consistent decline in both MSE and MAE values for all data categories as the number of communication rounds increases, confirming FRAMU's ability to refine its models and improve accuracy over time. Specifically, MSE values for Outdated, Private, and Irrelevant data show reductions from initial to final values of 0.053 to 0.039, 0.044 to 0.030, and 0.039 to 0.025, respectively. Similarly, MAE values also demonstrate improvements, with Outdated, Private, and Irrelevant data showing reductions from 7.201 to 4.845, 7.17 to 4.409, and 6.75 to 4.210, respectively.

This behavior indicates that FRAMU is effective in capturing underlying data patterns and optimizing its predictions. It continuously refines its models through iterative optimization, leading to a decrease in both MSE and MAE values. The analysis confirms the robustness of FRAMU in adapting to various types of data and highlights its effectiveness in progressively improving its predictive performance. Overall, FRAMU's strong convergence characteristics across different data categories demonstrate its versatility and capability in minimizing errors, making it a robust choice for various federated learning applications.

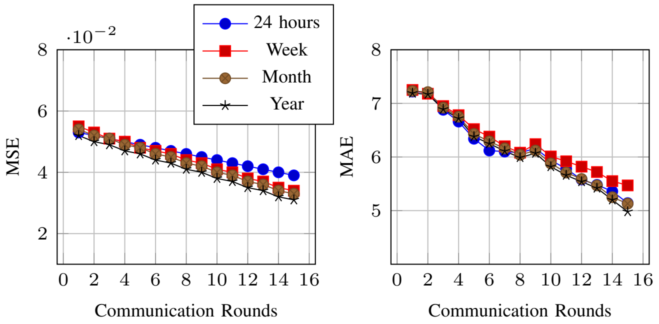


Fig. 7: Optimization Analysis - Outdated Data

F. Optimization

The performance of the FRAMU framework is evaluated through MSE and MAE metrics across various communication rounds and thresholds, as presented in Fig. 7 and Fig.. 8. Figure 7 investigates FRAMU's efficiency with outdated data across time durations ranging from 24 hours to a year. Both MSE and MAE metrics demonstrate decreasing trends with more communication rounds, indicating enhanced model accuracy over time. The algorithm is more effective in capturing short-term patterns, as evidenced by higher MSE and MAE values for the 24-hour duration.

Figure 8 shifts the focus to FRAMU's performance on private data, revealing that the algorithm not only maintains but also improves its accuracy compared to outdated data scenarios. Lower MSE and MAE values in the private data analysis affirm this. Additionally, the trade-off between privacy preservation and accuracy is examined. Although increasing privacy guarantees (lower ϵ values) generally lead to higher MSE and MAE, FRAMU still manages to maintain reasonable accuracy levels. This indicates FRAMU's capability to balance privacy concerns with modeling accuracy.

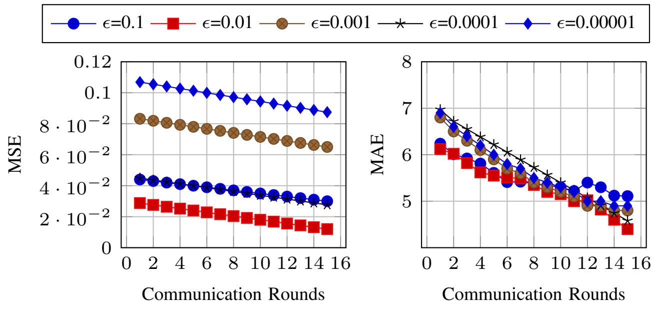


Fig. 8: Optimization Analysis - Private Data

VI. Research Implications

The FRAMU framework has significant academic implications in the field of machine unlearning, applicable to both single and multi-modality scenarios. It addresses five key areas: privacy preservation [54], adaptability to changing data, unlearning mechanisms, attention mechanisms for model aggregation, and optimization strategies for resource utilization and scalability.

In terms of privacy, FRAMU incorporates mechanisms that deter the model from excessively relying on sensitive information, successfully balancing privacy concerns with model performance. This offers a foundational approach for future privacy-preserving algorithms. FRAMU also exhibits adaptability by employing models that adjust to non-IID data and dynamic patterns, making it especially relevant for real-world applications with diverse and evolving data sets.

The framework includes unlearning mechanisms that discard outdated or irrelevant data, focusing computational efforts on current and relevant information. This not only maintains but can improve model accuracy over time. Its attention mechanisms refine model aggregation by prioritizing informative features, offering a template for developing more efficient federated learning systems. Lastly, FRAMU's optimization techniques minimize communication rounds while maintaining performance, contributing to the framework's efficiency and scalability. These aspects are empirically validated, confirming FRAMU's broad utility and potential for advancing federated learning research.

VII. Conclusion

The FRAMU framework represents a notable stride forward in federated learning, offering robust solutions for both single-modality and multimodality scenarios. It excels in key areas such as privacy preservation, adaptability, and optimization, as substantiated by statistical evaluations. However, the framework does have limitations in terms of computational complexity and scalability due to its retraining process. Future research should aim to address these issues, focusing on techniques like transfer learning and innovative communication methods to refine FRAMU's applicability. Overall, the ongoing improvements in FRAMU have the potential to significantly impact federated learning, setting the stage for advancements in data privacy and system performance.

References

[1] P. Kumar, G. P. Gupta, and R. Tripathi, "Tp2sf: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning," *Journal of Systems Architecture*, vol. 115, p. 101954, 2021.

[2] R. Nian, J. Liu, and B. Huang, "A review on reinforcement learning: Introduction and applications in industrial process control," *Computers & Chemical Engineering*, vol. 139, p. 106886, 2020.

[3] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb, "Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1342–1397, 2021.

[4] M. Al-Rubaie and J. M. Chang, "Privacy-preserving machine learning: Threats and solutions," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 49–58, 2019.

[5] C. N. Fortner, "Decision making within a cancel culture environment," tech. rep., US Army Command and General Staff College, 2020.

[6] J. Globocnik, "The right to be forgotten is taking shape: Cjeu judgments in gc and others (c-136/17) and google v cnil (c-507/17)," *GRUR International*, vol. 69, no. 4, pp. 380–388, 2020.

[7] K. Vasilevski, "Meta-learning for clinical and imaging data fusion for improved deep learning inference," 2023.

[8] M. Sun, J. Xiao, E. G. Lim, C. Zhao, and Y. Zhao, "Unified multimodality video object segmentation using reinforcement learning," *IEEE Transactions on Circuits and Systems for Video Technology*, 2023.

[9] A. Malekloo, E. Ozer, M. AlHamaydeh, and M. Girolami, "Machine learning and structural health monitoring overview with emerging technology and high-dimensional data source highlights," *Structural Health Monitoring*, vol. 21, no. 4, pp. 1906–1955, 2022.

[10] J. Ngiam, A. Khosla, M. Kim, J. Nam, H. Lee, and A. Y. Ng, "Multimodal deep learning," in *Proceedings of the 28th international conference on machine learning (ICML-11)*, pp. 689–696, 2011.

[11] T. Zhou, S. Ruan, and S. Canu, "A review: Deep learning for medical image segmentation using multi-modality fusion," *Array*, vol. 3, p. 100004, 2019.

[12] J. D. Fernández, S. P. Menci, C. M. Lee, A. Rieger, and G. Fridgen, "Privacy-preserving federated learning for residential short-term load forecasting," *Applied energy*, vol. 326, p. 119915, 2022.

[13] D. C. Nguyen, Q.-V. Pham, P. N. Pathirana, M. Ding, A. Seneviratne, Z. Lin, O. Dobre, and W.-J. Hwang, "Federated learning for smart healthcare: A survey," *ACM Computing Surveys (CSUR)*, vol. 55, no. 3, pp. 1–37, 2022.

[14] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, and B. He, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Transactions on Knowledge and Data Engineering*, 2021.

[15] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 308–318, 2016.

[16] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning differentially private recurrent language models," *arXiv preprint arXiv:1710.06963*, 2017.

[17] X. Chen and B. Wujek, "A unified framework for automatic distributed active learning," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 12, pp. 9774–9786, 2021.

[18] L. Bourtoule, V. Chandrasekaran, C. A. Choquette-Choo, H. Jia, A. Travers, B. Zhang, D. Lie, and N. Papernot, "Machine unlearning," in *2021 IEEE Symposium on Security and Privacy (SP)*, pp. 141–159, IEEE, 2021.

[19] M. Jegorova, C. Kaul, C. Mayor, A. Q. O'Neil, A. Weir, R. Murray-Smith, and S. A. Tsaftaris, "Survey: Leakage and privacy at inference time," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2022.

[20] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*, pp. 1273–1282, PMLR, 2017.

[21] Z. Wu, H. Wang, Z. Wang, H. Jin, and Z. Wang, "Privacy-preserving deep action recognition: An adversarial learning framework and a new dataset," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 4, pp. 2126–2139, 2020.

[22] J. Liang, Z. Liu, J. Zhou, X. Jiang, C. Zhang, and F. Wang, "Model-protected multi-task learning," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44, no. 2, pp. 1002–1019, 2020.

[23] 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*, pp. 265–284, Springer, 2006.

[24] P. Zhou, K. Wang, L. Guo, S. Gong, and B. Zheng, "A privacy-preserving distributed contextual federated online learning framework with big data support in social recommender systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, no. 3, pp. 824–838, 2019.

[25] Z. Ma, Y. Liu, Y. Miao, G. Xu, X. Liu, J. Ma, and R. H. Deng, "Flgan: Gan-based unbiased federatedlearning under non-iid settings," *IEEE Transactions on Knowledge and Data Engineering*, 2023.

[26] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE signal processing magazine*, vol. 37, no. 3, pp. 50–60, 2020.

[27] A. K. Sahu, T. Li, M. Sanjabi, M. Zaheer, A. Talwalkar, and V. Smith, "On the convergence of federated optimization in heterogeneous networks," *ArXiv*, vol. abs/1812.06127, 2018.

[28] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *arXiv preprint arXiv:1610.05492*, 2016.

[29] T. Zhu, D. Ye, W. Wang, W. Zhou, and S. Y. Philip, "More than privacy: Applying differential privacy in key areas of artificial intelligence," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 6, pp. 2824–2843, 2020.

[30] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1175–1191, 2017.

[31] T. Shaik, X. Tao, N. Higgins, R. Gururajan, Y. Li, X. Zhou, and U. R. Acharya, "Fedstack: Personalized activity monitoring using stacked federated learning," *Knowledge-Based Systems*, vol. 257, p. 109929, 2022.

[32] T. S. Brisimi, R. Chen, T. Mela, A. Olshevsky, I. C. Paschalidis, and W. Shi, "Federated learning of predictive models from federated electronic health records," *International journal of medical informatics*, vol. 112, pp. 59–67, 2018.

[33] W. Huang, J. Liu, T. Li, T. Huang, S. Ji, and J. Wan, "Feddsr: Daily schedule recommendation in a federated deep reinforcement learning framework," *IEEE Transactions on Knowledge and Data Engineering*, 2021.

[34] T. Hospedales, A. Antoniou, P. Micaelli, and A. Storkey, "Meta-learning in neural networks: A survey," *IEEE transactions on pattern analysis and machine intelligence*, vol. 44, no. 9, pp. 5149–5169, 2021.

[35] V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra, and M. Riedmiller, "Playing atari with deep reinforcement learning," 2013.

[36] T. Schaul, J. Quan, I. Antonoglou, and D. Silver, "Prioritized experience replay," *arXiv preprint arXiv:1511.05952*, 2015.

[37] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. Riedmiller, A. K. Fidjeland, G. Ostrovski, *et al.*, "Human-level control through deep reinforcement learning," *nature*, vol. 518, no. 7540, pp. 529–533, 2015.

[38] Z. Bing, D. Lerch, K. Huang, and A. Knoll, "Meta-reinforcement learning in non-stationary and dynamic environments," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 3, pp. 3476–3491, 2022.

[39] G. Brauwers and F. Frasincar, "A general survey on attention mechanisms in deep learning," *IEEE Transactions on Knowledge and Data Engineering*, 2021.

[40] I. Sorokin, A. Seleznev, M. Pavlov, A. Fedorov, and A. Ignateva, "Deep attention recurrent q-network," *arXiv preprint arXiv:1512.01693*, 2015.

[41] Z. Guan, Y. Li, Z. Pan, Y. Liu, and Z. Xue, "Rfdg: Reinforcement federated domain generalization," *IEEE Transactions on Knowledge and Data Engineering*, 2023.

[42] H. Miao, X. Zhong, J. Liu, Y. Zhao, X. Zhao, W. Qian, K. Zheng, and C. S. Jensen, "Task assignment with efficient federated preference learning in spatial crowdsourcing," *IEEE Transactions on Knowledge and Data Engineering*, 2023.

[43] S. Makonin, B. Ellert, I. V. Bajić, and F. Popowich, "Electricity, water, and natural gas consumption of a residential house in canada from 2012 to 2014," *Scientific data*, vol. 3, no. 1, pp. 1–12, 2016.

[44] Y. Li, R. Yu, C. Shahabi, and Y. Liu, "Diffusion convolutional recurrent neural network: Data-driven traffic forecasting," in *International Conference on Learning Representations (ICLR '18)*, 2018.

[45] A. E. Johnson, T. J. Pollard, L. Shen, L.-w. H. Lehman, M. Feng, M. Ghassemi, B. Moody, P. Szolovits, L. Anthony Celi, and R. G. Mark, "Mimic-iii, a freely accessible critical care database," *Scientific data*, vol. 3, no. 1, pp. 1–9, 2016.

[46] P. D. (NYPD), "Nypd complaint data current (year to date): Nyc open data," *NYPD Complaint Data Current (Year To Date) — NYC Open Data*, Apr 2023.

[47] A. E. Johnson, T. J. Pollard, S. J. Berkowitz, N. R. Greenbaum, M. P. Lungren, C.-y. Deng, R. G. Mark, and S. Horng, "Mimic-cxr, a de-identified publicly available database of chest radiographs with free-text reports," *Scientific data*, vol. 6, no. 1, p. 317, 2019.

[48] K. Dataset, "Smart home dataset with weather information," 2019.

[49] X. Zhu, G. Li, and W. Hu, "Heterogeneous federated knowledge graph embedding learning and unlearning," in *Proceedings of the ACM Web Conference 2023*, pp. 2444–2454, 2023.

[50] V. S. Chundawat, A. K. Tarun, M. Mandal, and M. Kankanhalli, "Zero-shot machine unlearning," *IEEE Transactions on Information Forensics and Security*, 2023.

[51] J. Ma, Z. Zhao, X. Yi, J. Chen, L. Hong, and E. H. Chi, “Modeling task relationships in multi-task learning with multi-gate mixture-of-experts,” in *Proceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining*, pp. 1930–1939, 2018.

[52] H. Bansal, N. Singhi, Y. Yang, F. Yin, A. Grover, and K.-W. Chang, “Cleanclip: Mitigating data poisoning attacks in multimodal contrastive learning,” *arXiv preprint arXiv:2303.03323*, 2023.

[53] M. Jaiswal and E. M. Provost, “Privacy enhanced multimodal neural representations for emotion recognition,” in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, pp. 7985–7993, 2020.

[54] X. Hu, T. Zhu, X. Zhai, W. Zhou, and W. Zhao, “Privacy data propagation and preservation in social media: A real-world case study,” *IEEE Transactions on Knowledge and Data Engineering*, 2021.