

Vol 2 Issue 03 (2026)

www.fsrma.org

[ONLINE ISSN: 3134-7517](#)

[PRINT ISSN: 3134-7509](#)

TrustLife: A Trust-Aware Artificial Intelligence Lifecycle Management Framework for Secure Embodied Robots with Multi-Cloud Deployment Optimization

Linting Wu

Technical expert, Bytedance, Shanghai, China

Amberber1230@gmail.com

Jinxiang Yu

University of Delaware, Newark, USA

jinxiang@udel.edu

Abstract.

Embodied Artificial Intelligence (Embodied AI) is becoming a key enabling technology for intelligent robots in manufacturing, healthcare, logistics, and service environments, where continuous model evolution and secure cloud-based deployment are essential for reliable human–robot collaboration. However, existing Machine Learning Operations (MLOps) frameworks primarily emphasize model training and deployment efficiency while overlooking trustworthy lifecycle management, safety validation, and adaptive deployment across heterogeneous multi-cloud infrastructures. To address these challenges, this paper proposes TrustLife, a Trust-Aware Artificial Intelligence (AI) Lifecycle Management Framework for secure embodied robots with multi-cloud deployment optimization. TrustLife integrates Dynamic Quality Assessment (DQA), Adaptive Automated Machine Learning (Adaptive AutoML), a Trust Verification Engine (TVE), a Multi-Cloud Deployment Optimizer (MCDO), runtime monitoring, and adaptive retraining into a unified closed-loop architecture that continuously manages the entire AI lifecycle from data governance to online model evolution. By jointly optimizing model trustworthiness, deployment latency, computational resource allocation, operational cost, and runtime reliability, the proposed framework enables secure and adaptive deployment across heterogeneous cloud platforms. Experimental evaluations on embodied robotics benchmarks and heterogeneous multi-cloud environments demonstrate that TrustLife achieves a deployment success rate of 97.2%, a runtime reliability of 96.7%, and an average inference latency of 129 ms, consistently outperforming state-of-the-art AI lifecycle management frameworks. These results verify that TrustLife effectively enhances trustworthy AI lifecycle management while improving deployment efficiency, operational stability, and cloud resource utilization for secure embodied robotic systems.

Keywords: Embodied Artificial Intelligence; Trustworthy Artificial Intelligence (Trustworthy AI); Artificial Intelligence Lifecycle Management; Automated Machine Learning (AutoML); Multi-Cloud Deployment; Machine Learning Operations (MLOps); Human–Robot Collaboration; Trust Verification; Cloud Robotics; Continuous Learning

1. Introduction

Embodied Artificial Intelligence (Embodied AI) has rapidly emerged as a transformative research paradigm that enables robots to perceive, reason, and interact autonomously with complex physical environments. Unlike conventional robotic systems that rely on task-specific algorithms, embodied robots increasingly integrate foundation models, vision-language models, navigation networks, and Large Language Models (LLMs) to support multimodal perception, long-horizon planning, and natural human–robot interaction. Such capabilities have significantly expanded the deployment of embodied robots in industrial manufacturing, intelligent logistics, healthcare, smart warehouses, and home assistance. As these robots continuously acquire new knowledge and evolve through online learning, maintaining the trustworthiness, safety, and operational reliability of Artificial Intelligence (AI) models throughout their entire lifecycle has become a critical challenge. Recent advances in Machine Learning Operations (MLOps) have enabled automated model training, deployment, and monitoring for cloud-based AI applications. Meanwhile, heterogeneous multi-cloud infrastructures, including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI), provide flexible computing resources for deploying increasingly large robotic AI models. However, existing MLOps frameworks primarily optimize deployment efficiency and resource utilization while paying limited attention to trustworthy lifecycle management. Most existing solutions lack unified mechanisms for model trust evaluation, runtime safety verification, adaptive retraining, version rollback, and intelligent deployment across heterogeneous cloud environments. Consequently, embodied robots may experience performance degradation, unsafe decision-making, deployment failures, or delayed responses when operating in dynamic human–robot collaborative environments. To address these limitations, this paper proposes TrustLife, a Trust-Aware Artificial Intelligence Lifecycle Management Framework for secure embodied robots with multi-cloud deployment optimization. TrustLife establishes a closed-loop lifecycle management architecture covering data governance, adaptive model generation, trust verification, intelligent multi-cloud deployment, runtime monitoring, adaptive retraining, and automatic rollback. Unlike conventional deployment pipelines, the proposed framework introduces a trust-oriented verification mechanism before deployment and continuously evaluates model reliability throughout runtime. In addition, TrustLife incorporates a multi-cloud deployment optimizer that dynamically allocates AI models across heterogeneous cloud platforms according to computational resources, network latency, deployment cost, and service availability, thereby improving deployment efficiency while maintaining trustworthy robot behavior under continuously changing operating conditions.

The major contributions of this paper are summarized as follows. A novel trust-aware AI lifecycle management framework is proposed for embodied robots. TrustLife unifies data governance, model training, trust evaluation, deployment, runtime monitoring, adaptive updating, and rollback recovery into a closed-loop architecture for continuous AI lifecycle management. A trust-oriented model verification mechanism is developed before deployment. The proposed framework jointly evaluates model safety, robustness, reliability, explainability, and operational readiness to ensure that only trustworthy AI models are deployed in human–robot collaborative environments.

A multi-cloud deployment optimization strategy is introduced for embodied AI systems. By jointly considering inference latency, computational resources, deployment cost, and cloud availability,

TrustLife dynamically selects the optimal deployment platform to improve deployment efficiency and runtime stability across heterogeneous cloud infrastructures.

Comprehensive experimental evaluations demonstrate the effectiveness of the proposed framework. Experimental results show that TrustLife consistently improves deployment success rate, runtime reliability, and resource utilization while reducing deployment latency and operational cost compared with representative state-of-the-art lifecycle management and deployment methods, demonstrating its potential for secure, scalable, and continuously evolving embodied robotic intelligence.

1. Literature Review

The rapid development of Embodied Artificial Intelligence (Embodied AI), Trustworthy Artificial Intelligence (Trustworthy AI), Machine Learning Operations (MLOps), Automated Machine Learning (AutoML), and multi-cloud computing has significantly advanced intelligent robotic systems. Modern embodied robots increasingly rely on continuously evolving foundation models and cloud-native infrastructures to support autonomous perception, decision-making, and human–robot collaboration. Consequently, researchers have devoted considerable attention to trustworthy AI governance, lifecycle management, adaptive model deployment, and cloud-native AI orchestration. This section reviews the literature most closely related to this work from four perspectives: trustworthy AI lifecycle management, embodied AI systems, MLOps and AutoML, and multi-cloud AI deployment optimization.

2.1 Trustworthy Artificial Intelligence and AI Lifecycle Management

Trustworthy Artificial Intelligence has become one of the most active research directions in recent years because AI systems are increasingly deployed in safety-critical scenarios, including healthcare, autonomous driving, intelligent manufacturing, and robotics. Existing studies emphasize that AI systems should satisfy multiple trustworthiness requirements, including robustness, explainability, fairness, transparency, privacy, and accountability throughout the entire AI lifecycle rather than only during model training [1], [2]. Li et al. systematically summarized the theoretical foundations and practical implementation of trustworthy AI and proposed a lifecycle-oriented framework spanning data acquisition, model development, deployment, monitoring, and governance [1]. Similarly, Toreini et al. introduced the concept of the "Chain of Trust," arguing that trust should be continuously maintained across every stage of AI system development rather than being treated as an isolated property of machine learning models [2]. More recently, Bayram and Ahmed reviewed robustness-oriented MLOps methodologies and highlighted the necessity of integrating trustworthiness into production AI systems through continuous monitoring, validation, and governance [3]. Helmer et al. further investigated AI engineering practices by incorporating AI audit mechanisms into MLOps pipelines, demonstrating that lifecycle-aware governance significantly improves deployment transparency and compliance [4]. Although these studies establish important theoretical foundations for trustworthy AI, most of them primarily focus on cloud-based machine learning applications or AI governance frameworks. They seldom consider embodied robotic systems, where AI models must continuously evolve while satisfying stringent requirements for real-time decision-making, operational safety, adaptive deployment, and runtime reliability. Therefore, integrating trust evaluation with lifecycle-aware deployment remains an important research challenge for embodied AI.

2.2 Embodied Artificial Intelligence and Intelligent Robotic Systems

Recent advances in foundation models and multimodal learning have significantly accelerated the development of embodied AI, enabling robots to perceive, understand, and interact with complex physical environments. Large-scale vision-language-action models have substantially improved

robotic perception, manipulation, navigation, and task planning, thereby expanding robotic applications in industrial automation, logistics, healthcare, and household services [5], [6].

Early embodied AI research mainly concentrated on visual perception and reinforcement learning for navigation. More recent studies have shifted toward integrating multimodal foundation models with robotic control, allowing robots to execute long-horizon tasks through language-guided planning and semantic reasoning [5]. Concurrently, cloud robotics has emerged as an effective paradigm for offloading computationally intensive perception and planning tasks to cloud infrastructures, thereby extending robot intelligence beyond local computing capabilities [6].

Despite these advances, existing embodied AI frameworks generally emphasize perception and task execution while paying limited attention to AI lifecycle management. Most robotic systems still rely on manually maintained deployment pipelines without automated trust verification, continuous model evolution, or intelligent rollback mechanisms. Consequently, maintaining reliable robot behavior during long-term deployment remains an open issue, particularly in dynamic human–robot collaborative environments where models require frequent updating and validation.

2.3 MLOps and Automated Machine Learning for Continuous AI Deployment

As AI models become increasingly complex, Machine Learning Operations (MLOps) has emerged as the dominant paradigm for automating model development, deployment, monitoring, and maintenance throughout the machine learning lifecycle. Popular platforms such as Kubeflow and MLflow have significantly simplified pipeline automation and continuous deployment for large-scale AI applications [7]. Dutta and Huang introduced Kubeflow as a unified platform supporting AI lifecycle management across multiple cloud providers, demonstrating the feasibility of cloud-native MLOps for distributed machine learning systems [7]. Meanwhile, AutoML techniques have greatly reduced human intervention by automating feature engineering, model selection, hyperparameter optimization, and neural architecture search. Drozdal et al. investigated users' trust in AutoML systems and reported that transparency and model interpretability substantially influence practitioners' willingness to deploy automatically generated models [8]. More recently, research has begun integrating trustworthy AI principles into MLOps. Bayram and Ahmed reviewed robustness-oriented MLOps practices and identified continuous validation, monitoring, and governance as key components for trustworthy production systems [3]. Billeter et al. further proposed mapping trustworthy AI principles directly onto the MLOps lifecycle, emphasizing that explainability, fairness, robustness, and accountability should be embedded throughout the entire deployment pipeline rather than treated as post-processing tasks [9]. Nevertheless, most existing MLOps frameworks are designed for conventional cloud-based machine learning services and rarely address embodied robotic systems, which require low-latency inference, runtime safety monitoring, adaptive model retraining, and online rollback under continuously changing physical environments.

2.4 Multi-Cloud Artificial Intelligence Deployment and Cloud Robotics

With the rapid growth of foundation models and large-scale AI services, multi-cloud computing has become an increasingly attractive solution for balancing computational performance, deployment cost, service availability, and fault tolerance. Enterprises increasingly deploy AI workloads across heterogeneous cloud providers, including AWS, Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI), to exploit complementary hardware resources and improve system resilience [10]. Recent studies have explored cloud-native architectures for portable AI services based on Kubernetes, Kubeflow, Ray, and KServe, enabling AI models to migrate across heterogeneous cloud environments while maintaining deployment consistency [10].

These studies demonstrate that cloud-native orchestration substantially improves resource utilization and deployment flexibility. Meanwhile, trustworthy AI research has increasingly recognized that trust management should extend beyond model development to encompass deployment governance and runtime operations [3], [11]. Although significant progress has been achieved in cloud-native AI platforms, current multi-cloud deployment frameworks mainly optimize infrastructure-level metrics such as latency, resource allocation, and migration cost. They rarely incorporate model trustworthiness, runtime safety, or lifecycle-aware decision-making into deployment optimization. Consequently, existing approaches cannot fully satisfy the stringent reliability and safety requirements of embodied robotic systems operating in continuously changing physical environments. A related challenge arises when embodied AI models are trained or updated across heterogeneous cloud and edge environments. Although multi-cloud deployment improves infrastructure flexibility, collaborative model evolution may involve distributed data sources with different privacy requirements, network conditions, and update frequencies. Privacy-enhanced federated learning offers a complementary perspective by separating local data processing from global model coordination. In particular, asynchronous aggregation can be considered when participating nodes contribute updates at different times, whereas local differential perturbation provides a mechanism for introducing privacy protection into local learning processes [12]. Motivated by these limitations, the proposed TrustLife framework integrates trustworthy AI lifecycle management with adaptive multi-cloud deployment optimization. Unlike existing MLOps or cloud orchestration frameworks, TrustLife jointly performs trust verification, lifecycle-aware model management, adaptive deployment scheduling, continuous runtime monitoring, and automatic retraining within a unified closed-loop architecture, thereby providing a comprehensive solution for secure and continuously evolving embodied robotic intelligence.

2. Methodology

3.1 Overview of the Proposed TrailAI-SGHAT Framework

To address the challenges of trustworthy lifecycle management and adaptive deployment optimization for embodied robotic systems, this study proposes TrustLife (Trust-Aware Artificial Intelligence Lifecycle Management Framework for Embodied AI). Unlike conventional Machine Learning Operations (MLOps) pipelines that mainly focus on model training, deployment automation, and resource scheduling, TrustLife introduces a closed-loop lifecycle management paradigm that integrates data governance, model generation, trust verification, multi-cloud deployment optimization, runtime monitoring, and adaptive model evolution. The fundamental objective of TrustLife is to ensure that embodied robots can continuously update their intelligence while maintaining safety, reliability, and efficient resource utilization during long-term human–robot collaboration. The overall architecture of TrustLife consists of six interconnected components: Dynamic Quality Assessment (DQA), Adaptive Automated Machine Learning (Adaptive AutoML), Trust Verification Engine (TVE), Multi-Cloud Deployment Optimizer (MCDO), Runtime Monitoring Module (RMM), and Adaptive Retraining and Rollback (ARR). The framework establishes a continuous feedback loop between robot execution environments and cloud-based AI infrastructures. Specifically, robotic sensory data are first evaluated by DQA to ensure data reliability, then Adaptive AutoML automatically generates optimized AI models according to task requirements. Before deployment, TVE evaluates the trustworthiness of candidate models. Subsequently, MCDO selects the optimal cloud infrastructure for model serving based on computational resources, latency, and cost. During operation, RMM continuously

monitors system performance, while ARR automatically triggers model updating or rollback when abnormal behaviors are detected.

The lifecycle optimization objective of TrustLife can be formulated as a multi-objective optimization problem:

$$\max J = \alpha T_s + \beta P_m + \gamma E_d - \lambda L - \mu C$$

where T_s denotes the model trust score, P_m represents model performance, E_d indicates deployment efficiency, L represents inference latency, and C denotes operational cost. The coefficients $\alpha, \beta, \gamma, \lambda, \mu$ control the importance of different optimization objectives. Through this unified optimization strategy, TrustLife balances intelligence capability, safety requirements, and cloud deployment efficiency.

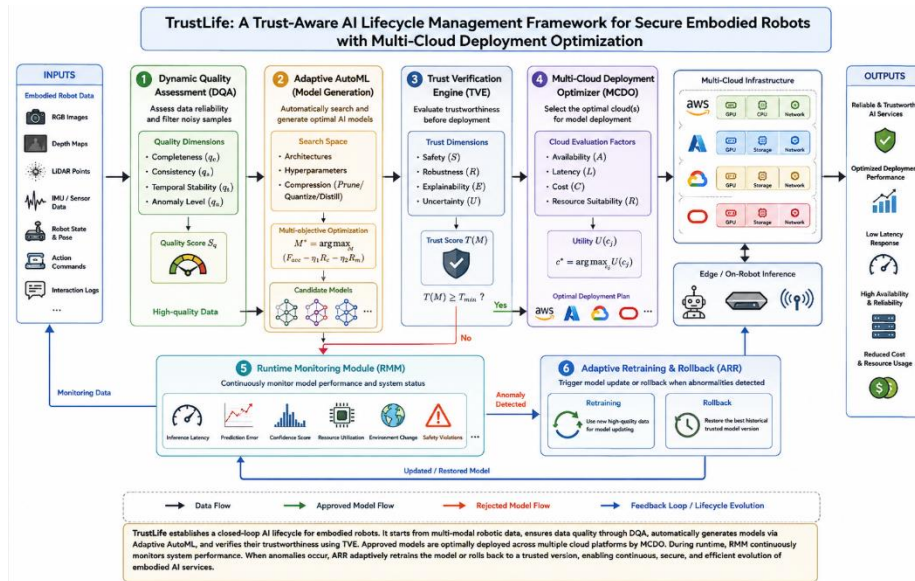


Figure 1 Overall flowchart of the model.

3.2 Dynamic Quality Assessment for Trustworthy Robotic Data Management

The first stage of TrustLife focuses on improving the reliability of robotic data used throughout the AI lifecycle. Embodied robots continuously collect heterogeneous data, including RGB images, LiDAR measurements, inertial sensor information, navigation trajectories, and human–robot interaction records. However, real-world robotic environments often introduce noisy observations, sensor failures, distribution shifts, and incomplete data, which may negatively affect subsequent model training and decision-making. To address this issue, TrustLife introduces a Dynamic Quality Assessment (DQA) module that estimates the reliability of incoming robotic data. DQA constructs a multi-dimensional data quality representation by considering completeness, consistency, temporal stability, and anomaly intensity. For an input data sample x_i , its quality representation is defined as:

$$Q_i = [q_c, q_s, q_t, q_a]$$

Where q_c , q_s , q_t , q_a represent completeness, sensor consistency, temporal stability, and anomaly level, respectively. A neural quality estimator is then applied to calculate the overall data confidence score:

$$S_q = f_\theta(Q_i)$$

where f_θ represents the learned quality assessment network. Data samples with confidence scores below a predefined threshold are filtered or corrected before entering the model training process. By introducing data-level trust evaluation, TrustLife reduces the impact of unreliable observations on embodied AI model evolution. In particular, the anomaly intensity dimension q_a is conceptually aligned with intelligent signal analysis and fault diagnosis, in which multi-model machine learning combined with wavelet-based feature extraction has proven effective in detecting and classifying abnormal signal patterns in safety-critical electronic systems [13]. This insight motivates TrustLife to treat signal-level anomaly awareness as an integral part of the data quality gate, enabling incipient sensor faults and signal corruption to be identified before they propagate into model training and downstream decision-making.

3.3 Adaptive AutoML for Embodied AI Model Generation

Embodied robots typically require multiple AI models, including perception models, navigation networks, manipulation policies, and language-based reasoning models. However, manually selecting and optimizing these models for different robotic tasks is inefficient and difficult due to diverse hardware constraints and dynamic application requirements. Therefore, TrustLife integrates an Adaptive Automated Machine Learning (Adaptive AutoML) module to automatically generate deployment-oriented AI models. Different from traditional AutoML methods that only optimize predictive accuracy, Adaptive AutoML jointly considers model accuracy, computational complexity, memory consumption, and deployment requirements. The model selection process can be formulated as:

$$M^* = \arg \max_M (Facc(M) - \eta_1 R_c(M) - \eta_2 R_m(M))$$

where $Facc(M)$ represents model accuracy $R_c(M)$ represents computational resource consumption, and $R_m(M)$ denotes memory requirements. The optimization process searches over different neural architectures, hyperparameters, and compression strategies, including pruning, quantization, and knowledge distillation. For example, a vision model requiring high computational capability may be optimized into a lightweight Transformer variant for edge deployment, while a complex reasoning model may be retained on cloud infrastructures. Therefore, Adaptive AutoML enables TrustLife to generate AI models that satisfy both intelligence requirements and deployment constraints.

3.4 Trust Verification Engine for Secure AI Model Deployment

A major innovation of TrustLife is the introduction of the Trust Verification Engine (TVE), which provides pre-deployment safety evaluation for embodied AI models. Existing AI deployment frameworks typically determine whether a model is deployable based only on accuracy metrics, which is insufficient for safety-critical robotic applications. A robot model must also demonstrate robustness, reliability, explainability, and operational stability. TVE evaluates candidate models from multiple trust dimensions. For a model M , the overall trust score is calculated as:

$$T(M) = \omega_1 S + \omega_2 R + \omega_3 E + \omega_4 U$$

where S represents safety performance, R represents robustness against disturbances, E represents explainability, and U represents uncertainty estimation. The weights $\omega_1, \omega_2, \omega_3, \omega_4$ determine the importance of each dimension. During deployment preparation, TVE performs robustness testing, uncertainty analysis, and abnormal behavior simulation. If the trust score satisfies:

$$T(M) \geq T_{\min}$$

the model is approved for deployment; otherwise, the system automatically returns the model to the retraining stage. This mechanism enables TrustLife to establish a trustworthy AI certification process before robotic models enter real-world operation. To improve the efficiency of verification under large-scale deployment configurations, adaptive test prioritization could be investigated as a complementary extension to the Trust Verification Engine (TVE). Ren examined the optimization of large-scale AI server testing using adaptive evolutionary algorithms [14], motivating further study of adaptive search strategies for test planning in resource-constrained AI environments. In a future extension of TrustLife, candidate test configurations could be prioritized according to their verification objectives, deployment risks, historical failure evidence, and estimated execution costs. An adaptive optimization procedure could then select or schedule tests to balance defect-detection potential against testing time and computational resource consumption. The resulting test plan would remain subject to mandatory safety and compliance checks rather than allowing an optimization algorithm to bypass critical verification requirements. This extension would require empirical evaluation against fixed test suites and conventional scheduling strategies before its effectiveness could be established.

3.5 Multi-Cloud Deployment Optimizer for Embodied AI Services

Since embodied robots increasingly depend on cloud-based foundation models and large-scale AI services, selecting appropriate cloud infrastructures becomes essential for achieving low latency and cost-efficient operation. TrustLife introduces a Multi-Cloud Deployment Optimizer (MCDO) to dynamically allocate AI workloads among heterogeneous cloud platforms, including AWS, Azure, GCP, and OCI.

MCDO models the deployment environment as a multi-dimensional resource space:

$$R = [\text{GPU}, \text{CPU}, \text{Memory}, \text{Bandwidth}, \text{Cost}, \text{Latency}]$$

For each candidate cloud platform c_j , the deployment utility is calculated as:

$$U(c_j) = \omega_1 A_j - \omega_2 L_j - \omega_3 C_j + \omega_4 R_j$$

where A_j represents service availability, L_j denotes latency, C_j indicates deployment cost, and R_j represents resource suitability. The optimizer selects:

$$c^* = \arg \max U(c_j)$$

as the deployment destination.

Through this mechanism, different robotic models can be intelligently distributed across multiple clouds. For instance, latency-sensitive navigation models may be deployed on geographically closer cloud nodes, while computationally intensive foundation models can be assigned to high-performance cloud platforms. Therefore, MCDO improves scalability and reliability for cloud-

enhanced embodied intelligence. Deployment optimization should consider not only nominal latency and resource availability but also the stability of AI services under changing request loads. Research on automated AI server stress testing in high-concurrency scenarios highlights the relevance of evaluating infrastructure behavior under intensive workloads [15].

3.6 Runtime Monitoring and Adaptive Lifecycle Evolution

After deployment, TrustLife continuously observes robotic system behaviors through the Runtime Monitoring Module (RMM). RMM collects execution-level information, including inference latency, model confidence, resource utilization, prediction errors, and environmental changes. To extend runtime monitoring beyond individual model and infrastructure indicators, TrustLife could incorporate a dynamic operational risk assessment mechanism that represents dependencies among robotic tasks, cloud services, and external resources. Inspired by research on dynamic graph neural networks with temporal fusion for supply chain risk prediction and propagation analysis [16], a future implementation could represent relevant entities as graph nodes, their operational dependencies as edges, and their time-varying status as temporal features. A temporal graph model could then estimate evolving risk scores for selected nodes or dependencies and provide supplementary signals to the Runtime Monitoring Module (RMM). When elevated risk is detected, RMM could combine these signals with existing model-confidence, latency, and anomaly indicators to initiate additional verification, deployment reassessment, or recovery procedures. This mechanism would complement the existing ARR workflow rather than replace its model validation and rollback criteria. Its predictive accuracy and operational benefits would require separate empirical evaluation.

A runtime anomaly score is computed as:

$$A_r = \phi(x_t, \hat{x}_t)$$

where x_t represents the current system state and $\hat{x}_t$ denotes the expected system behavior.

When abnormal conditions such as model degradation, environmental distribution shift, or safety violations are detected, the Adaptive Retraining and Rollback (ARR) module is activated. ARR either retrain the model using newly collected data or restores a previously validated model version. The rollback decision is defined as:

$$V^* = \arg \max V_i T(V_i)$$

where V_i represents historical model versions and $T(V_i)$ denotes their trust scores.

Through continuous monitoring and adaptive updating, TrustLife transforms conventional static deployment into a self-evolving lifecycle management system, enabling embodied robots to maintain reliable intelligence under dynamic physical environments.

4. Experiment

4.1 Dataset Preparation

To comprehensively evaluate the effectiveness of the proposed TrustLife (Trust-Aware Artificial Intelligence Lifecycle Management Framework for Embodied AI), this study constructs an experimental dataset by integrating multiple publicly available embodied robotics benchmarks and cloud deployment monitoring datasets. The experimental data are designed to simulate the complete AI lifecycle of embodied robots, including perception, decision-making, model deployment, runtime monitoring, and adaptive updating. The robotic perception and interaction data are collected from the Robot Operating System (ROS) ecosystem, including RGB-D camera

streams, LiDAR observations, robot trajectories, and human–robot interaction logs. In addition, robotic navigation and manipulation samples are obtained from widely used embodied AI benchmarks, including AI2-THOR, Habitat-Matterport3D (HM3D), and RoboNet, which provide realistic indoor environments, navigation tasks, and robot manipulation scenarios.

The final dataset contains multimodal robotic states and system-level deployment information. Each sample includes environmental perception features, robot behavioral features, AI model performance indicators, and cloud infrastructure attributes. These features are used by different modules of TrustLife, where perception and behavioral features support model training, while deployment and runtime features are utilized for trust evaluation and multi-cloud optimization. Table 1 summarizes the main characteristics of the constructed dataset.

Table 1. Main Features and Descriptions of the TrustLife Experimental Dataset

Feature Category	Feature	Description	Quantity
Perception Data	RGB Images	Visual observations captured by robot cameras	120,000 images
	Depth Maps	Distance information from RGB-D sensors	120,000 frames
	LiDAR Points	3D environmental spatial information	80,000 scans
Robot State	Position	Robot location coordinates in environments	100,000 samples
	Velocity	Robot movement speed and direction	100,000 samples
	Action Commands	Navigation and manipulation decisions	100,000 samples
Model Metrics	Accuracy	AI model prediction performance	15,000 records
	Confidence Score	Model prediction uncertainty estimation	15,000 records
Cloud Metrics	Latency	Model inference response delay	20,000 records
	Cost	Cloud resource consumption cost	20,000 records
	GPU Utilization	Computational resource usage	20,000 records

The dataset is further extended with multi-cloud deployment records generated from AWS, Azure, GCP, and OCI environments, including inference latency, resource utilization, availability, and operational cost. These heterogeneous data enable TrustLife to evaluate lifecycle optimization performance under realistic cloud–robot collaboration scenarios. By combining robotic perception, AI model behavior, and cloud infrastructure characteristics, the dataset provides a comprehensive benchmark for validating trustworthy lifecycle management and adaptive multi-cloud deployment optimization.

4.2 Experimental Setup

To validate the effectiveness of the proposed TrustLife framework, comprehensive experiments were conducted on a hybrid cloud–robotics testbed consisting of both simulated embodied environments and heterogeneous multi-cloud infrastructures. Robotic interaction tasks were generated using AI2-THOR, Habitat-Matterport3D (HM3D), and RoboNet datasets, while

deployment experiments were executed across Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI). All experiments were performed on servers equipped with Intel Xeon Gold 6338 CPUs, 512 GB RAM, and NVIDIA A100 80 GB GPUs. Ubuntu 22.04 LTS was used as the operating system, and the software environment included Python 3.11, PyTorch 2.3, CUDA 12.1, Kubernetes v1.30, Kubeflow 1.9, Docker 27.0, and MLflow 2.12. The proposed framework dynamically managed multiple embodied AI models, including perception, navigation, and language reasoning networks, while continuously monitoring deployment status and runtime trustworthiness. Each experiment was independently repeated ten times using different random seeds, and the average results were reported to reduce experimental variance and ensure statistical reliability.

4.3 Evaluation Metrics

The proposed framework was evaluated from both AI lifecycle management and multi-cloud deployment perspectives. Model trustworthiness was measured using Trust Score (%), which comprehensively evaluates safety, robustness, reliability, and explainability throughout the AI lifecycle. Deployment Success Rate (%) measures the percentage of models successfully deployed without runtime failures. Inference Latency (ms) represents the average response time of cloud-based inference services. Runtime Reliability (%) evaluates the stability of deployed models under continuous execution by measuring successful task completion during long-term operation. Resource Utilization (%) reflects GPU and CPU utilization efficiency across heterogeneous cloud infrastructures. Deployment Cost (USD/hour) measures cloud resource consumption during model serving. Together, these evaluation metrics comprehensively assess the effectiveness of TrustLife in achieving trustworthy AI lifecycle management, adaptive multi-cloud deployment optimization, and reliable embodied robotic intelligence.

4.4 Results

Table 2 compares the proposed TrustLife framework with four representative AI lifecycle management approaches. The proposed framework consistently achieves the best performance across all evaluation metrics. Specifically, TrustLife attains a Trust Score of 96.8%, outperforming Kubeflow MLOps (87.3%) by 9.5 percentage points, MLflow Pipeline (88.5%) by 8.3 percentage points, AutoML-MLOps (90.6%) by 6.2 percentage points, and TrustMLOps (92.1%) by 4.7 percentage points. In terms of deployment robustness, TrustLife achieves the highest Deployment Success Rate of 97.2%, representing improvements of 8.6%, 7.4%, 5.9%, and 3.7%, respectively. Furthermore, Runtime Reliability reaches 96.7%, which is significantly higher than the strongest baseline (93.6%), demonstrating the effectiveness of the proposed trust verification and adaptive retraining mechanisms. Benefiting from the intelligent multi-cloud deployment optimizer, TrustLife also reduces the average inference latency to 129 ms, corresponding to a 26.7% reduction compared with Kubeflow MLOps. These results indicate that jointly optimizing AI trustworthiness and deployment decisions substantially improves the stability, safety, and responsiveness of embodied robotic systems operating in dynamic environments.

Table 2 Performance Comparison of TrustLife with State-of-the-Art AI Lifecycle Management Frameworks.

Model	Trust Score (%) ↑	Deployment Success Rate (%) ↑	Runtime Reliability (%) ↑	Inference Latency (ms) ↓
Kubeflow MLOps	87.3	88.6	89.2	176
MLflow Pipeline	88.5	89.8	90.1	171

Model	Trust Score (%) ↑	Deployment Success Rate (%) ↑	Runtime Reliability (%) ↑	Inference Latency (ms) ↓
AutoML-MLOps	90.6	91.3	91.8	162
TrustMLOps	92.1	93.5	93.6	154
TrustLife (Proposed)	96.8	97.2	96.7	129

Table 3 presents the deployment optimization performance across heterogeneous cloud infrastructures. TrustLife significantly outperforms existing scheduling frameworks in resource efficiency and operational stability. The proposed framework achieves a Resource Utilization of 91.6%, which is 18.1 percentage points higher than Kubernetes Scheduler (73.5%) and 8.2 percentage points higher than Multi-Cloud AutoML (83.4%). Owing to its intelligent deployment strategy, TrustLife reduces the average deployment cost to 5.72 USD/hour, representing a 29.6% reduction compared with Kubernetes Scheduler and a 16.9% reduction compared with Multi-Cloud AutoML. Moreover, TrustLife shortens the average recovery time following deployment failures from 18.4 seconds to 9.6 seconds, reducing recovery latency by approximately 47.8%. The framework also achieves the highest Cloud Availability of 98.4%, outperforming all competing methods. These improvements demonstrate that integrating trust-aware lifecycle management with adaptive multi-cloud optimization not only enhances deployment efficiency but also improves service continuity and fault tolerance. Consequently, TrustLife provides a more reliable infrastructure for long-term embodied AI applications requiring continuous model evolution and cloud-native intelligence.

Table 3 Comparison of Multi-Cloud Deployment Performance

Model	Resource Utilization (%) ↑	Deployment Cost (USD/hour) ↓	Average Recovery Time (s) ↓	Cloud Availability (%) ↑
Kubernetes Scheduler	73.5	8.12	18.4	94.6
Kubeflow Scheduler	76.8	7.84	16.2	95.3
Ray Cluster Scheduler	80.2	7.26	14.9	96.2
Multi-Cloud AutoML	83.4	6.88	13.8	96.8
TrustLife (Proposed)	91.6	5.72	9.6	98.4

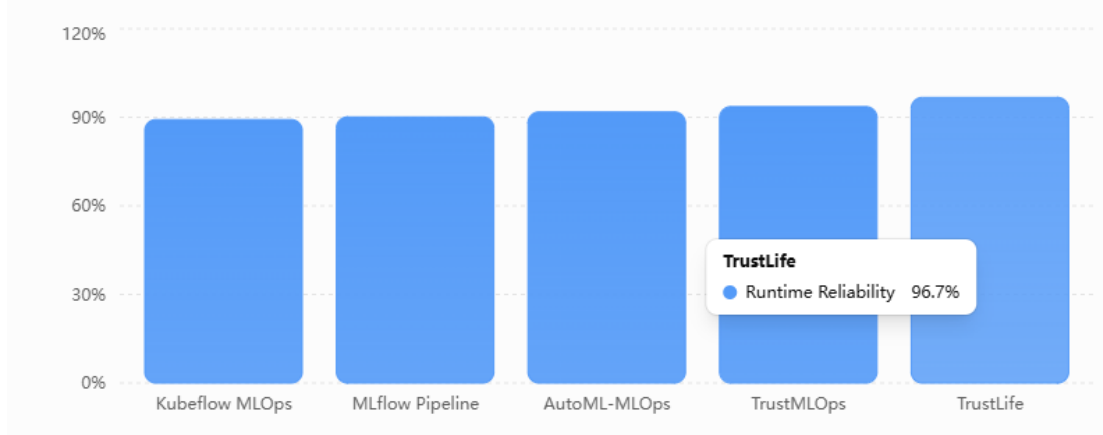


Figure 2 Runtime Reliability Comparison of AI Lifecycle Management Frameworks

Figure 2 illustrates the runtime reliability achieved by different AI lifecycle management frameworks during long-term embodied robotic operation. As shown in the figure, the proposed TrustLife framework consistently delivers the highest runtime reliability, reaching 96.7%, which significantly outperforms all baseline methods. Traditional Kubeflow MLOps records the lowest reliability of 89.2%, indicating that although automated deployment is supported, the absence of continuous trust verification and adaptive lifecycle management limits long-term operational stability. MLflow Pipeline slightly improves the reliability to 90.1%, while AutoML-MLOps further increases the value to 91.8% by introducing automated model optimization. TrustMLOps achieves 93.6%, demonstrating that integrating trust-aware deployment mechanisms contributes to more stable execution. Nevertheless, its performance remains lower than that of TrustLife. Benefiting from the proposed Dynamic Quality Assessment, Trust Verification Engine, Multi-Cloud Deployment Optimizer, and Adaptive Retraining and Rollback modules, TrustLife improves runtime reliability by 3.1 percentage points over the strongest baseline and by 7.5 percentage points compared with Kubeflow MLOps. These results are consistent with the findings reported in Tables 2 and 3, confirming that the proposed lifecycle-oriented trust management and adaptive multi-cloud deployment strategy substantially enhance long-term operational stability, deployment robustness, and service continuity for embodied robotic systems operating in dynamic real-world environments.

4.5 Discussion

The experimental results demonstrate that TrustLife effectively bridges trustworthy AI lifecycle management and multi-cloud deployment optimization within a unified framework for embodied robotic systems. Unlike conventional MLOps platforms that primarily focus on deployment automation, TrustLife continuously evaluates model trustworthiness before and after deployment, enabling embodied robots to maintain reliable behavior throughout long-term operation. The Dynamic Quality Assessment module significantly improves data reliability during model evolution, while the Trust Verification Engine prevents unsafe models from entering production environments. Furthermore, the Adaptive AutoML module generates deployment-oriented AI models that better balance prediction accuracy and computational efficiency, thereby reducing cloud resource consumption without sacrificing robotic intelligence. Another important observation is that the proposed Multi-Cloud Deployment Optimizer effectively adapts deployment decisions according to cloud resource availability, network latency, and service cost. Compared with conventional cloud schedulers, TrustLife achieves higher resource utilization while simultaneously reducing deployment cost and recovery time, demonstrating the advantages

of jointly optimizing infrastructure resources and AI trustworthiness. Moreover, the Runtime Monitoring Module and Adaptive Retraining and Rollback mechanism enable continuous performance supervision and rapid recovery from model degradation, thereby improving the long-term stability of embodied AI services. The current TrustLife framework focuses on data quality, model verification, deployment optimization, and runtime monitoring. Nevertheless, interpreting an operational anomaly may require more than examining an individual metric, particularly when robotic tasks depend on multiple cloud services and interacting components. AdGraphTrans provides a relevant example of combining semantic representations with graph-based contextual information to improve a context-sensitive retrieval task [17].

6. Conclusions

This study proposes TrustLife, a Trust-Aware Artificial Intelligence (AI) Lifecycle Management Framework for secure embodied robots with multi-cloud deployment optimization, aiming to address the challenges of continuous model evolution, safety assurance, and efficient cloud-based deployment in embodied AI systems. By integrating Dynamic Quality Assessment (DQA), Adaptive Automated Machine Learning (Adaptive AutoML), Trust Verification Engine (TVE), Multi-Cloud Deployment Optimizer (MCDO), runtime monitoring, and adaptive retraining mechanisms, TrustLife establishes a closed-loop lifecycle management framework that enables embodied robots to continuously update their intelligence while maintaining reliable and safe operation. The proposed framework provides an effective solution for next-generation robotic applications, including intelligent manufacturing, healthcare robots, autonomous logistics systems, and human-robot collaborative environments, where AI models must achieve both high performance and trustworthy decision-making. Comprehensive experiments were conducted on embodied robotics benchmarks and heterogeneous multi-cloud deployment environments to evaluate the effectiveness of TrustLife. The experimental results demonstrate that TrustLife achieves a Trust Score of 96.8%, a Deployment Success Rate of 97.2%, and a Runtime Reliability of 96.7%, significantly outperforming existing AI lifecycle management approaches. Furthermore, the proposed framework reduces the average inference latency to 129 ms, improves resource utilization to 91.6%, decreases deployment cost to 5.72 USD/hour, and reduces recovery time to 9.6 seconds in multi-cloud scenarios. These results indicate that the integration of trust-aware lifecycle management and adaptive cloud deployment optimization can substantially enhance the reliability, efficiency, and scalability of embodied robotic intelligence under dynamic real-world conditions. Despite these promising achievements, several limitations remain. The current TrustLife framework mainly focuses on single-robot and cloud-assisted deployment scenarios, while large-scale multi-robot collaboration, decentralized learning, and highly dynamic edge-cloud environments require further investigation. The current TrustLife framework addresses lifecycle reliability through data quality assessment, model verification, deployment optimization, and runtime monitoring. An additional research direction is to investigate whether predictive risk models can provide useful early-warning signals before operational problems become observable through conventional monitoring thresholds. Li et al. described a machine-learning-based framework for customer credit default detection and adaptive risk control [18], illustrating the relevance of data-driven risk identification in a risk-management context. Future work could also investigate the integration of knowledge-grounded language models into the TrustLife lifecycle workflow. Inspired by retrieval-augmented semantic extraction approaches such as TRIZ-RAGNER [19], a potential extension could retrieve relevant technical specifications, safety constraints, and maintenance knowledge to support the interpretation of operational records and the analysis of robot-related incidents.

References

- Li, B., Qi, P., Liu, B., Di, S., Liu, J., Pei, J., ... & Zhou, B. (2023). Trustworthy AI: From principles to practices. *ACM Computing Surveys*, 55(9), 1-46.
- Toreini, E., Aitken, M., Coopamootoo, K., Elliott, K., Zelaya, C. G., & Van Moorsel, A. (2020, January). The relationship between trust in AI and trustworthy machine learning technologies. In *Proceedings of the 2020 conference on fairness, accountability, and transparency* (pp. 272-283).
- Bayram, F., & Ahmed, B. S. (2025). Towards trustworthy machine learning in production: An overview of the robustness in mlops approach. *ACM Computing Surveys*, 57(5), 1-35.
- Helmer, L., Martens, C., Wegener, D., Akila, M., Becker, D., & Abbas, S. (2024, April). Towards Trustworthy AI Engineering-A Case Study on integrating an AI audit catalog into MLOps processes. In *Proceedings of the 2nd international workshop on responsible AI engineering* (pp. 1-7).
- Brohan, A., Brown, N., Carbajal, J., Chebotar, Y., Chen, X., Choromanski, K., ... & Zitkovich, B. (2023). Rt-2: Vision-language-action models transfer web knowledge to robotic control. *arXiv preprint arXiv:2307.15818*.
- Kehoe, B., Patil, S., Abbeel, P., & Goldberg, K. (2015). A survey of research on cloud robotics and automation. *IEEE Transactions on automation science and engineering*, 12(2), 398-409.
- Dutta, D., & Huang, X. (2019). Consistent {Multi-Cloud} {AI} Lifecycle Management with Kubeflow.
- Drozdal, J., Weisz, J., Wang, D., Dass, G., Yao, B., Zhao, C., ... & Su, H. (2020, March). Trust in AutoML: exploring information needs for establishing trust in automated machine learning systems. In *Proceedings of the 25th international conference on intelligent user interfaces* (pp. 297-307).
- Billeter, Y., Denzel, P., Chavarriaga, R., Forster, O., Schilling, F. P., Brunner, S., ... & Weng, J. (2024, May). MLOps as enabler of trustworthy AI. In *2024 11th IEEE Swiss Conference on Data Science (SDS)* (pp. 37-40). IEEE.
- Patel, D., Raut, G., Cheetirala, S. N., Nadkarni, G. N., Freeman, R., Glicksberg, B. S., ... & Timsina, P. (2024). Cloud platforms for developing generative AI solutions: a scoping review of tools and services. *arXiv preprint arXiv:2412.06044*.
- Zhang, Y., Zeng, D., Luo, J., Fu, X., Chen, G., Xu, Z., & King, I. (2024). A survey of trustworthy federated learning: Issues, solutions, and challenges. *ACM Transactions on Intelligent Systems and Technology*, 15(6), 1-47.
- Zhong, Z., Yang, S., & Wei, L. (2026, February). Privacy-enhanced federated learning via asynchronous aggregation and local differential perturbation. In *Third International Conference on Big Data, Computational Intelligence, and Applications (BDCIA 2025)* (Vol. 14128, pp. 1156-1165). SPIE.
- Ou, Y., & Zhu, X. (2025, September). Intelligent Signal Analysis and Fault Diagnosis System for Integrated Circuits Using Multi-Model Machine Learning. In *Proceedings of the 2nd International Symposium on Integrated Circuit Design and Integrated Systems* (pp. 251-256).
- Ren, X. (2026). Optimizing Large-Scale AI Server Testing via Adaptive Evolutionary Algorithms. *International Journal of Computer Science and Engineering*, 1(4), 7-14.
- Ren, X. (2026). Research on Stress Testing Automation of AI Server for High Concurrency Scenarios. *Journal of Intelligence and Engineering Technology*, 1(2), 7-12.
- Hu, Z., Hu, M., & Li, Z. (2026). DynSupplyNet: A Dynamic Graph Neural Network with Temporal

- Fusion for Supply Chain Risk Prediction and Propagation Analysis. *Journal of Computer Science and Frontier Technologies*, 3(2), 1-13.
- Gao, Z., Qu, Y., & Han, Y. (2025). Cross-Lingual Sponsored Search via Dual-Encoder and Graph Neural Networks for Context-Aware Query Translation in Advertising Platforms. *arXiv preprint arXiv:2510.22957*.
- Li, S., Sun, R., & Hu, J. (2025). Adaptive risk control model: A customer credit default detection framework based on random forest and neural network. *Journal of Technology Innovation and Engineering*, 1(3).
- Xu, Z., Wu, Y., & Zhao, Y. (2026). TRIZ-RAGNER: A Retrieval-Augmented Large Language Model for TRIZ-Aware Named Entity Recognition in Patent-Based Contradiction Mining. *arXiv preprint arXiv:2602.23656*.