Volume 2, 2026, Pages 109-121 *Elaris Computing Nexus*
| Regular Article | Open Access

A Differentially Private Collaborative Intelligence Structure for Trust Aware Secure Data Exchange in Distributed Computing Platforms

Minlie Huang
School of Computer Science, Peking University, 5 Yiheyuan Road, Haidian District, Beijing 100871, China.
mih@pku.edu.cn

Article Info
Elaris Computing Nexus
https://elarispublications.com/journals/ecn/ecn_home.html

https://doi.org/10.65148/ECN/2026009

Received 06 May 2026
Revised from 12 June 2026
Accepted 26 June 2026
Available online 08 July 2026
Published by Elaris Publications.

Corresponding author(s):
Minlie Huang, School of Computer Science, Peking University, Haidian District, Beijing 100871, China.
Email: mih@pku.edu.cn

Abstract – Distributed computing platforms are seeing a rapid increase in size and complexity, allowing multiple entities to share knowledge and gain computational insights as a group. Nevertheless, secure sharing of data in such settings is difficult because of problems with privacy leakage, untrusted parties, communication vulnerabilities and so on. Most existing privacy preserving techniques are primarily based on data perturbation techniques and do not consider the changing trust relationships between the collaborating nodes that affect the utility of the privacy ensuring technique and the efficient utilization of the resources. This paper presents a Differentially Private Collaborative Intelligence Framework for Trust-Aware Secure Data Exchange in Distributed Computing Platforms called PriviGuard. The proposed framework combines adaptive differential privacy optimization and the trust-aware collaboration management to enable secure and reliable information sharing. PriviGuard's multi-layer security shield architecture includes a trust evaluation, privacy calibration, secure aggregation, and collaborative intelligence layer. A trust-driven privacy optimization model tailors the amount of noise injected into the data depending on its reliability of the participant while preserving data utility. The framework allows for sharing knowledge securely across dispersed entities without releasing sensitive knowledge. Experimental tests show that PriviGuard achieves better privacy protection, less communication overhead and better collaborative intelligence performance than traditional privacy-aware exchange mechanisms. The suggested approach is a promising solution for secure, scalable, and adaptive collaboration in a distributed computing environment.

Keywords — Differential Privacy, Trust-Aware Computing, Secure Data Exchange, Collaborative Intelligence, Distributed Computing Platforms.

I. INTRODUCTION

Distributed computing platforms have revolutionized the computational intelligence development and deployment in large-scale environments. Multiple distributed entities increasingly need to share information and work together to enhance their decision-making processes as seen in various modern applications, including edge computing, Internet of Things (IoT), Cloud-powered applications and Collaborative AI. These entities can share their knowledge, computational resources and learning outcomes without relying on a centralized processing infrastructure, using collaborative intelligence. As the amount of information exchanged grows, however, there are challenges involved in the management of data privacy, trust and secured communication among participating nodes [1].

Distributed collaborative environments generate data from various organizations and devices, which may contain sensitive information that cannot be openly shared with external parties. In traditional centralized systems, data needs to be continuously transferred to a central server, which can lead to potential privacy violations and unauthorized access. Distributed learning approaches have mitigated reliance on centralized data storage, but still suffer from vulnerability to inference attacks, malicious participants and unreliable information exchange. Thus, safe collaboration with maintaining appropriate data privacy is now a crucial demand for next generation distributed intelligence systems [2].

Differential privacy (DP) has proven to be a powerful tool for privacy protection by adding random noise to the information that is shared so that it is not possible to recover the original sensitive data. However, traditional differential privacy methods typically enforce a uniform privacy budget across all entities, not taking into account their behavior. These static privacy mechanisms might add too much noise for unreliable participants or reduce the privacy level for potentially malicious nodes. In addition, there are many different types of distributed computing platforms that are populated with heterogeneous players with different reliability and computation power, and different communication behaviors, making trust evaluation an important issue for safe collaborations [3].

A promising direction to enhance reliability in a distributed computing environment is Trust-aware computing, which continuously assesses participant behavior and assigns confidence levels in the process of information exchange. Trust assessment combined with differential privacy allows privacy protection mechanisms to be dynamically adapted based on the reliability of the individual contributors. Optimized level of privacy protection can be used for highly trusted nodes, and for suspicious or low trust nodes, a stricter level of protection can be used. This adaptable approach enhances the security and the usefulness of data, allowing for effective collaborative intelligence without compromising sensitive information [4].

The existing privacy-preserving frameworks are primarily focused on either encryption or anonymization or differential noise generation, but do not have a built-in method for assessing trust and adaptively controlling privacy. Likewise, trust management methods tend to focus on detecting the malicious parties, but not on privacy leakage in collaborative data sharing. Current distributed computing solutions are not very effective because there is no single and encompassing approach that takes into account the need for privacy preservation, the reliability of the participants, and the need for collaborative intelligence [5].

To overcome these challenges, this paper presents a Differentially Private Collaborative Intelligence Framework for Trust-Aware Secure Data Exchange in Distributed Computing Platforms (PriviGuard). The proposed framework proposes a security shield architecture that combines trust evaluation, optimization of adaptive differential privacy, secure data exchange, and collaborative intelligence processing. The key findings of this study are outlined below:

- A trust-aware secure collaboration architecture is designed, where reliable communication between distributed participants is achieved while ensuring the security of information exchanged among them by employing a multi-layer security mechanism.
- An adaptive differential privacy optimization model is proposed to adjust the level of privacy in accordance with the trust scores of participants, which allows the level of privacy to be dynamically adjusted while sacrificing as little data utility as possible when preserving the privacy of the data.
- Collaborative intelligence workflows are intended to facilitate secure knowledge sharing and distributed decision-making by combining trust-based privacy calibration and secure aggregation.
- A comprehensive evaluation framework is provided to compare and analyze the privacy protection capabilities, communication efficiency, trust reliability and collaborative intelligence performance of the proposed approach with the existing approaches.

Unlike traditional privacy-preserving and trust management solutions, the proposed PriviGuard framework is scalable and adaptable for secure information exchange in distributed computing platforms while overcoming their limitations.

Organization of the Paper

The rest of this paper is structured as follows. In Section 2, related study on privacy-preserving distributed intelligence, differential privacy mechanism, and trust-aware collaboration frameworks are presented. Section 3 introduces and explains the proposed PriviGuard framework, which comprises a secure collaboration architecture, a trust-aware differential privacy optimization model and a collaborative intelligence workflow. The experimental findings, comparative analysis and performance evaluation with different quantitative metrics are discussed in Section 4. Section 5 concludes the paper with key findings and future research directions.

II. BACKGROUND STUDIES

The need for centralized and secure data exchange in distributed computing systems has attracted much interest with the growing use of collaborative Intelligence systems. Previous studies have mainly addressed the issue of privacy preservation, secure communication, and reliable coordination of participants. But how to balance effectively between privacy protection and data utility and trust management is a challenging research problem [6].

A lot of effort has been put into studying Differential Privacy (DP) as a tool for protecting sensitive data in data sharing and collaborative learning. The standard differential privacy methods add noise to the data representation or to the model parameters so as to make it hard to infer private information. These approaches offer high levels of security, but a static privacy budget can lead to a compromise between security and accuracy of the information. However, in very dynamic distributed environments, different participants may have different reliability, computational power and communication patterns which make the same privacy configuration unsuitable for each of them [7].

The concept of privacy-preserving collaboration has been further advanced through federated learning and distributed intelligence frameworks, which allow multiple entities to train models without exchange of raw data. To avoid revealing individual contributions, secure aggregation techniques and encrypted parameter exchange mechanisms have been added.

But there are a number of methods that make the assumption that all nodes in the system are trustworthy, which might not be the case in open distributed platforms. The information exchanged can be manipulated by malicious participants, inference attacks can be carried out, and poisoned information updates can be provided that can affect the collaborative intelligence's performance [8].

To overcome reliability problems, trust-aware computing mechanisms have been suggested, which consider the reliability of the participant in terms of past interactions, quality of contribution and communication pattern. These methods make it easier to identify the unreliable nodes, and to make safe decisions in distributed networks. But most trust management frameworks pay attention primarily to the process of authentication and reputation measurement, and few give much thought to privacy leakage in the collaborative exchange of data. If adaptive privacy control is not applied, trusted and untrusted participants may be afforded comparable protection measures, thereby diminishing the overall effectiveness of security measures [9].

In recent attempts to bring about a balance between privacy and intelligence, blockchain, encryption, and AI techniques have been combined. Blockchain-based solutions enable more transparency and accountability by decentralizing verification, while encryption-based solutions ensure secure communication channels. However, the methods tend to be inefficient in large scale distributed computing systems and often add unnecessary extra computation. Furthermore, current hybrid approaches do not have a dynamic mechanism to adjust the level of privacy protection based on trust level of the participants.

As revealed by **Table 1**, the limitations reported in the literature reveal that there is a need for a common framework supporting privacy protection, evaluation of trust and optimization of collaborative intelligence. A solution that works well should be able to adaptively control privacy, accurately select reliable sources of information and ensure that there is a high data utility during the secure exchange of information. To overcome these challenges, the proposed PriviGuard framework combines the principles of trust-aware differential privacy optimization with a secure collaboration architecture, ensuring adaptive and reliable data exchange among distributed computing entities.

Table 1. Comparison of Existing Privacy-Preserving Collaborative Frameworks

Reference Approach	Main Technique	Privacy Mechanism	Trust Management	Major Limitation
Differential Privacy-based Data Sharing [10]	Noise perturbation	Fixed privacy budget allocation	Not considered	Privacy-utility trade-off is difficult to optimize
Federated Learning Frameworks [11]	Distributed model training	Parameter protection and secure aggregation	Limited participant verification	Vulnerable to malicious updates
Blockchain-Assisted Secure Exchange [12]	Decentralized verification	Cryptographic protection	Reputation-based validation	High computational and communication overhead
Encryption-Based Collaborative Intelligence [13]	Secure communication protocols	Data encryption	Not dynamically evaluated	Limited scalability in large networks
Trust Management Systems [14]	Reputation and behavior analysis	Basic access control	Continuous trust evaluation	Does not provide adaptive privacy preservation
Existing Hybrid Privacy Frameworks [15]	Combined AI and security mechanisms	Static privacy optimization	Partial trust integration	Lack of dynamic privacy adaptation
PriviGuard (Proposed)	**Trust-aware collaborative intelligence**	**Adaptive differential privacy optimization**	**Dynamic trust evaluation**	**Provides integrated privacy, trust, and secure collaboration**

The above analysis shows that current solutions give individual solutions for privacy preservation and/or trust management, but don't have an integrated adaptive mechanism. PriviGuard fills this gap by bringing together trust-aware privacy optimization and secure collaborative intelligence in the same framework for distributed computing platforms.

III. PROPOSED PRIVIGUARD FRAMEWORK

The aim of proposed PriviGuard framework is to provide secure and reliable collaborative intelligence among distributed computing entities and maintain the privacy of sensitive information. PriviGuard proposes an adaptive security model that takes into account the reliability of the nodes in the network when exchanging data, as opposed to the traditional privacy-preserving solutions where security measures are applied uniformly. The framework is composed of three main parts: a secure collaboration architecture, a trust-aware differential privacy optimization mechanism and a collaborative

intelligence workflow. Proposed model: It introduces a security barrier for distributed participants, combining trust evaluation, privacy tuning, secure exchange, and intelligent aggregation mechanisms. This hierarchical structure will provide secure protection of sensitive information and will enable joint work to enhance computational intelligence.

PriviGuard Secure Collaboration Architecture

The PriviGuard Secure Collaboration Architecture is the base security layer for privacy-preserving exchange of information in distributed computing platforms. The architecture is built as a multi-layer security wall that safeguards interactions between various data sources, edge devices, cloud platforms and intelligent processing nodes, while collaborating. The architecture is composed of a multi-layer security wall that protects the collaborative interactions between the heterogeneous data sources, edge devices, cloud platforms and intelligent processing nodes. Based on the distributed protection strategy, PriviGuard offers a dynamic generation of privacy decisions, depending on the reliability of the participants and the sensitivity of the data, and is not dependent on a centralized security model. The security shield at the outer layer is designed to watch incoming communication requests and check the participants before they can participate in the collaboration. The trust evaluation layer uses historical interaction patterns, trust in the contributions and communication to calculate a trust score for every entity participating in the interaction. The estimated trust level will guide the differential privacy optimization layer to set appropriate privacy parameters and adaptive noise intensities to ensure that sensitive information is not disclosed while protecting the usability of the data.

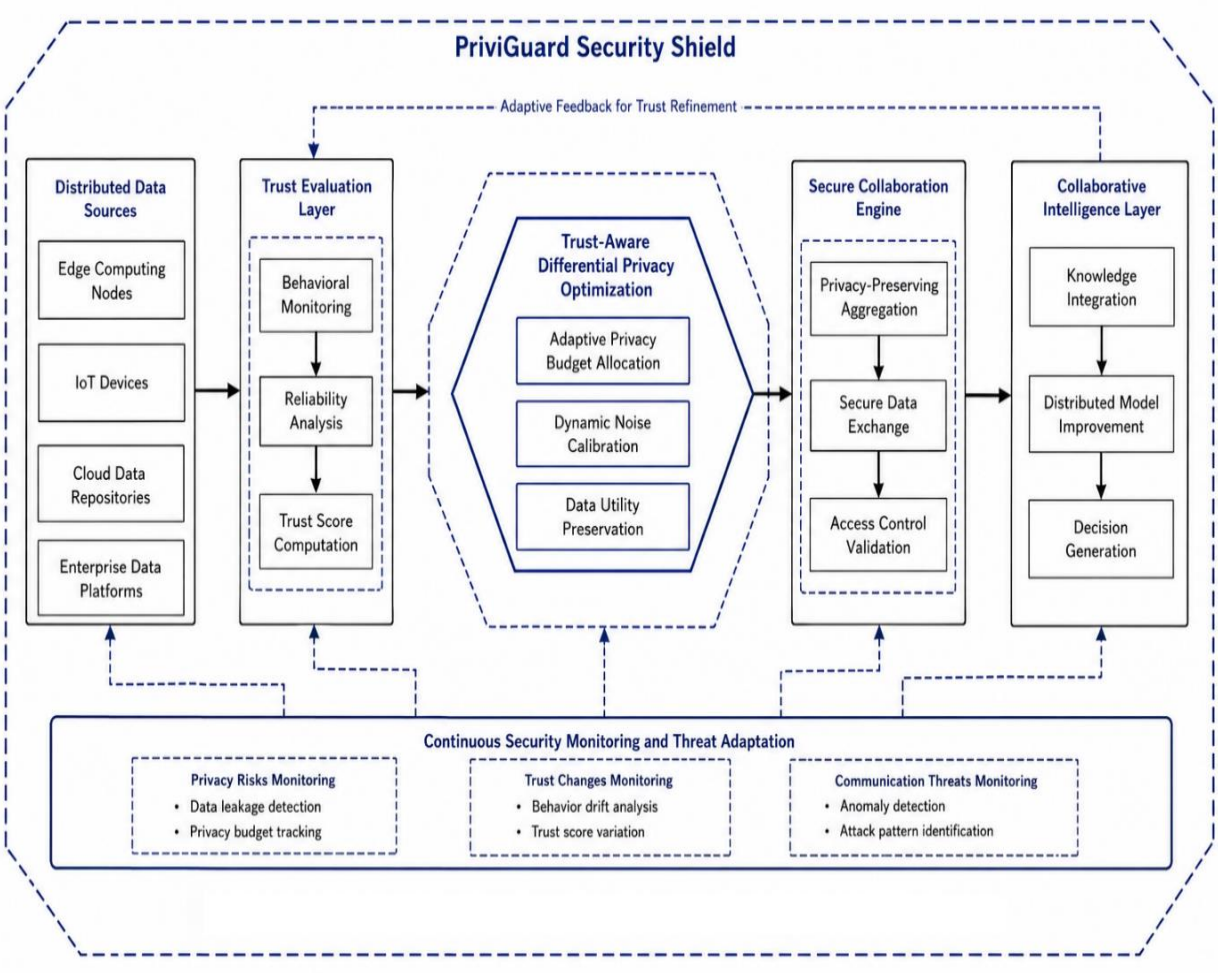

Fig 1. PriviGuard Secure Collaboration Architecture.

The secure collaboration layer facilitates secure data sharing by making use of privacy-preserving aggregation, meaning that individual data contributions cannot be reconstructed by outside parties. Finally, distributed decision-making and model improvement is achieved through the use of securely exchanged knowledge in the collaborative intelligence layer. These layers interact to form an adaptive security defense mechanism that can deal with changes in security threats in distributed environments. The suggested security shield architecture offers three major benefits: (i) adaptive privacy protection based on the trustworthiness of the participants, (ii) enhanced reliability through ongoing monitoring of trust, and (iii) efficient collaborative intelligence with minimal risk of privacy leakage.

Fig. 1 shows an architecture for a security shield, PriviGuard, for implementing a secure collaboration environment in distributed computing systems that is both trustful and privacy-preserving. The architecture embeds the protection layers of distributed data sources, trust evaluation, differential privacy optimization, secure collaboration, and collaborative intelligence into a single protection paradigm. The trust evaluation layer continuously assesses the trustworthiness of participants, and the differential privacy layer dynamically adjusts the privacy parameters based on the trust conditions. The secure collaboration engine facilitates protected information sharing using privacy-preserving methods and the intelligence layer leverages this common information to make decisions. The continuous monitoring layer provides greater flexibility in adapting to new privacy and security challenges.

Trust-Aware Differential Privacy Optimization

PriviGuard's Trust-Aware Differential Privacy Optimization module offers an adaptive mechanism for controlling privacy, adjusting information protection and collaborative intelligence performance as needed. Most traditional differential privacy methods typically use a fixed privacy budget per participant, which might lead to over-adding noise for correct contributors and under-adding noise for uncertain contributors. PriviGuard addresses this by adding participant trust evaluation to the privacy optimisation process. This proposed model allocates an adaptive level of privacy according to the trustworthiness of the various entities that are involved, which would provide increased protection to low-trust entities and retain utility in data from high-trust entities.

Let the distributed participant set be represented as $P = \{p_1, p_2, \dots, p_n\}$, where each participant p_i contributes local information D_i. The trust score of each participant is computed based on behavioral consistency, historical contribution quality, and communication reliability. The trust value is represented as:

$$\mathrm{T_i} = \alpha \mathrm{B_i} + \beta \mathrm{C_i} + \gamma \mathrm{R_i} \tag{1}$$

where B_i, C_i, and R_i represent behavioral reliability, contribution consistency, and communication reliability, respectively. The parameters α, β, and γ denote the corresponding weighting factors with α+β+γ=1.

The privacy budget is optimised adaptively based on the trust score obtained. The lower the privacy budget, the greater the privacy protection, and the higher the privacy budget, the better the data utility. The adaptive privacy allocation mechanism is given as follows:

$$\epsilon_i = \epsilon_{max} - (\epsilon_{max} - \epsilon_{min}) T_i \tag{2}$$

where ϵ_i represents the privacy budget assigned to participant p_i, and ϵ_{max} and ϵ_{min} denote the maximum and minimum privacy limits.

The sensitive information contributed by each participant is protected using a calibrated differential noise mechanism. The perturbed data representation is generated as:

$$D_i' = D_i + Lap\left(\frac{\Delta f}{\epsilon_i}\right) \tag{3}$$

where D_i' represents the privacy-preserved data, Lap(.) denotes Laplace noise generation, and Δf represents the sensitivity of the data function.

To maintain the balance between privacy and collaborative utility, PriviGuard introduces a utility-aware optimization function:

$$\max U = \lambda Q(D_i') + (1 - \lambda) P(\epsilon_i) \tag{4}$$

where U represents the overall optimization objective, Q(.) denotes data utility, P(.) indicates privacy preservation, and λ controls the trade-off between accuracy and security.

Furthermore, the trust-aware noise adjustment mechanism regulates noise intensity according to participant reliability:

$$\sigma_i = \frac{\sigma_0}{(T_i + \delta)} \tag{5}$$

where σ_i represents adaptive noise magnitude, σ_0 is the initial noise factor, and δ prevents instability for low trust values.

Then the secure collaborative update is created by combining privacy-preserved contributions from all parties:

$$G = \sum_{i=1}^{n} w_i D_i' \tag{6}$$

G represents the representation of the global collaborative intelligence and w_i is the weight of the contribution of each participant.

Finally, the optimization process minimizes privacy leakage while maximizing collaborative performance:

$$\min \mathrm{L} = \eta \mathrm{L}_{\mathrm{collaboration}} + (1-\eta)\mathrm{L}_{\mathrm{privacy}} \tag{7}$$

where $L_{collaboration}$ represents collaborative intelligence loss, $L_{privacy}$ represents privacy risk, and η controls the optimization balance.

The proposed trust-aware differential privacy optimization allows PriviGuard to adjust the security level dynamically based on participant behavior. This way, privacy is better preserved, noise is avoided with unnecessary injection and reliable collaboration intelligence is achieved in highly dynamic distributed computing environment.

Collaborative Intelligence Workflow

PriviGuard is an operational process for secure knowledge sharing and distributed knowledge generation between multiple, heterogeneous computing entities, known as the Collaborative Intelligence Workflow. The workflow incorporates a sequential, yet adaptive process of trust evaluation, differential privacy protection, secure aggregation, and collaborative decision making. In contrast to existing collaborative systems where participating nodes share information directly, PriviGuard first checks the security and optimizes privacy, then allows data sharing. This helps ensure that only reliable contributions are included in the intelligence generation process, and reduces the risk of privacy leakage or maliciously impacting the results of the intelligence process.

The entities in the distributed system first create their own data and then send requests for collaboration to the PriviGuard framework. The trust evaluation module is based on participant behavior, historical interactions, and the reliability of the contribution and provides the participant with trust scores. The differential privacy optimization module, using the trust values obtained, calculates appropriate privacy parameters and creates adaptive protection levels for each of the participants. Then sensitive information is mapped to calibrated privacy mechanisms prior to entering the secure collaboration phase.

In secure collaboration, multiple participants contribute to a whole, but without revealing original values of data items. The collaborative intelligence engine analyzes the protected data as a team to produce common knowledge, optimized models, or decision output. The intelligence results generated go through a monitoring layer, checking for changes in the participant's behavior, new security threats and changes in system performance. This monitoring process provides feedback, which will then be used to adjust the trust value or parameters of privacy levels for future rounds of collaboration.

The entire process allows PriviGuard to be a self-adaptive security mechanism with privacy protection and efficiency of collaboration. The step-by-step execution procedure of the proposed PriviGuard collaborative intelligence workflow is given in Algorithm 1.

Algorithm 1: PriviGuard Trust-Aware Secure Collaboration Workflow
Input: Distributed datasets D_i, participant set P, initial privacy parameters ϵ
Output: Secure collaborative intelligence model G

```
Initialize participant set P = {p_1, p_2, ..., p_n} and security parameters.
    Collect local data D_i from each distributed participant.
    Evaluate participant reliability using behavioral and contribution information.
    Compute trust score T_i for every participant.
        Adapt privacy budget ε_i according to the estimated trust value.
        Apply differential privacy mechanism to generate protected contribution D_i'.
    Perform secure aggregation of privacy-preserved contributions.
    Generate collaborative intelligence representation G.
    Monitor security status and update trust values dynamically.
Repeat the collaboration process until convergence or termination condition.
```

The proposed PriviGuard framework for the generation of secure collaborative intelligence is illustrated in **Fig. 2**. The process starts with the collection of distributed data from various and different data sources, and ends with trust estimation of the entities participating in the process. Adaptive differential privacy parameters are computed based on the trust level, such that sensitive information can be protected prior to being exchanged securely. Secured contributions are aggregated via the secure collaboration engine to generate shared intelligence outcomes – without compromising privacy. A continuous monitoring mechanism monitors security conditions and adjusts the parameters of trust and privacy on the fly. It is a flexible process that allows for secure cooperation without compromising privacy and security against adversaries or unreliable parties.

This section assesses the trust-aware secure data exchange and collaborative intelligence in distributed computing platforms proposed by the PriviGuard framework. The assessment highlights aspects of privacy protection, trust security, communications efficiency, computation load and collaborative intelligence effectiveness. The benefits of PriviGuard are made clear by comparing it with the following methods for privacy preserving collaborative approaches: Conventional

differential privacy (CDP), Federated Learning-based privacy mechanisms (FL-DP), Blockchain-assisted secure exchange (BSE), Encryption-based collaborative frameworks (ECF), and Trust-independent privacy models (TIPM).

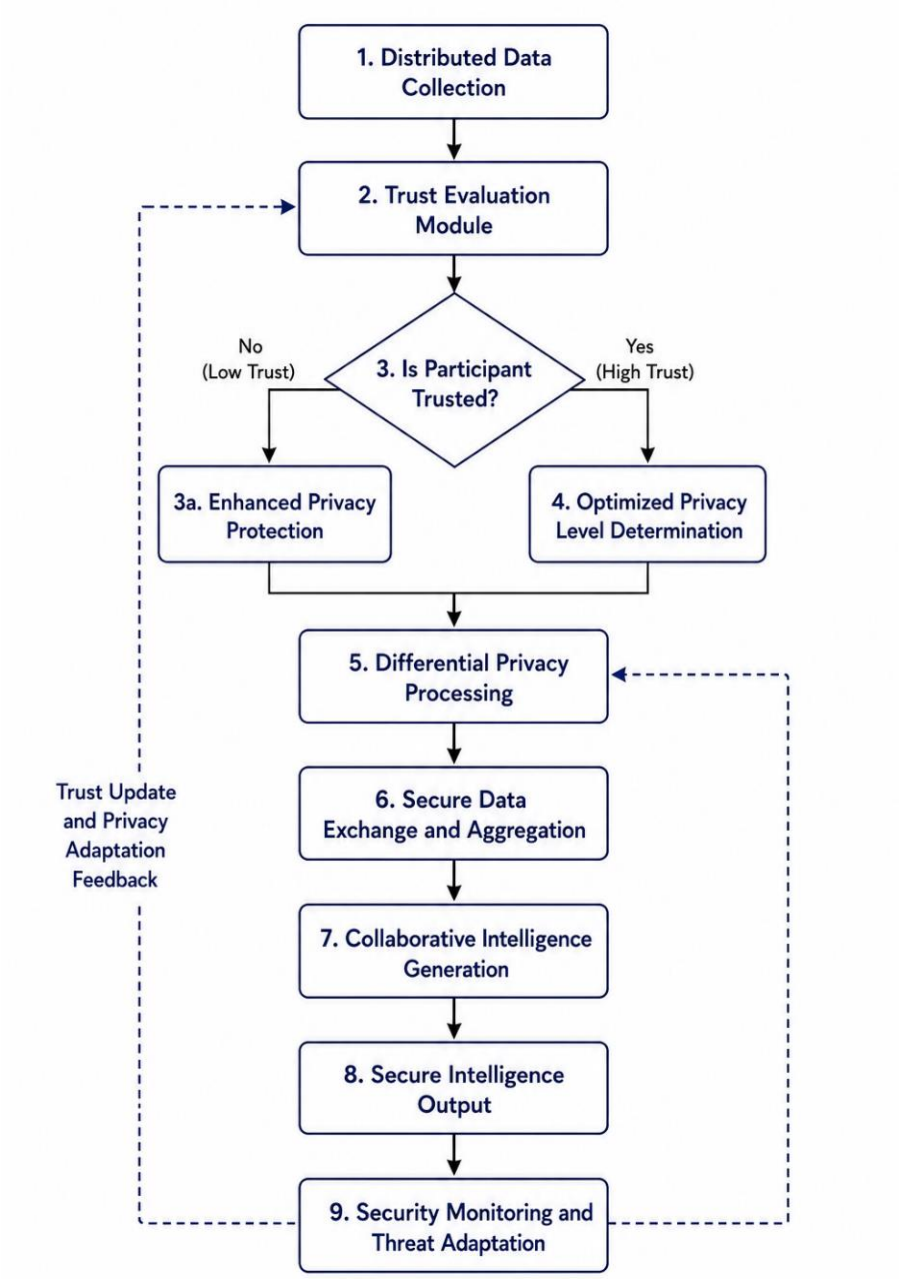

Fig 2. Collaborative Intelligence Workflow of PriviGuard.

IV. RESULTS AND DISCUSSION

The experiments are designed with the consideration of a distributed environment where participants are heterogeneous with different trust levels, different ways of contributing data to the system, and different communication capabilities.

Table 2. Comparative Analysis of Privacy Protection Performance

Method	Privacy Leakage (%)	Privacy Preservation (%)	Adaptive Privacy Control	Trust Integration
Conventional Differential Privacy	8.6	91.4	No	No
Federated Learning with DP	6.9	93.1	Limited	Partial
Blockchain-Assisted Exchange	5.8	94.2	No	Yes
Encryption-Based Framework	5.2	94.8	No	Partial
Trust-Independent Privacy Model	6.1	93.9	Limited	No
PriviGuard (Proposed)	**2.4**	**97.6**	**Yes**	**Yes**

Key performance metrics for evaluating the performance of the model include privacy leakage rate, model utility, improvement in accuracy, communication overhead, execution latency, and trust detection capability. The results we have obtained show that adaptive differential privacy and trust-aware collaboration can significantly enhance the security-performance tradeoff of PriviGuard over current approaches. The proposed framework dynamically scales the level of privacy protection based on the reliability of the participants, so that for trustworthy participants the amount of noise generated is minimized, whereas for unreliable participants it is maximized. The results are presented in quantitative form in the following subsections and graphically.

Table 2 compares the privacy protection performance of PriviGuard with the privacy preserving collaborative frameworks that are currently available. While conventional differential privacy provides reasonable protection by adding controlled noise, the fixed privacy budget approach leads to high information distortion and is not scalable. For privacy-preserving mechanisms based on federated learning, the security is enhanced by distributed processing, but they are susceptible to inference attacks. Blockchains and encryption-based solutions offer greater security, but also require more processing power. The proposed PriviGuard framework preserves the highest privacy of 97.6% with only 2.4% leakage of privacy by dynamic adjustment of privacy parameters based on the trust level of the participants. The adaptive noise calibration mechanism allows for greater protection for those with lower trust and useful information to be provided for those with high trust.

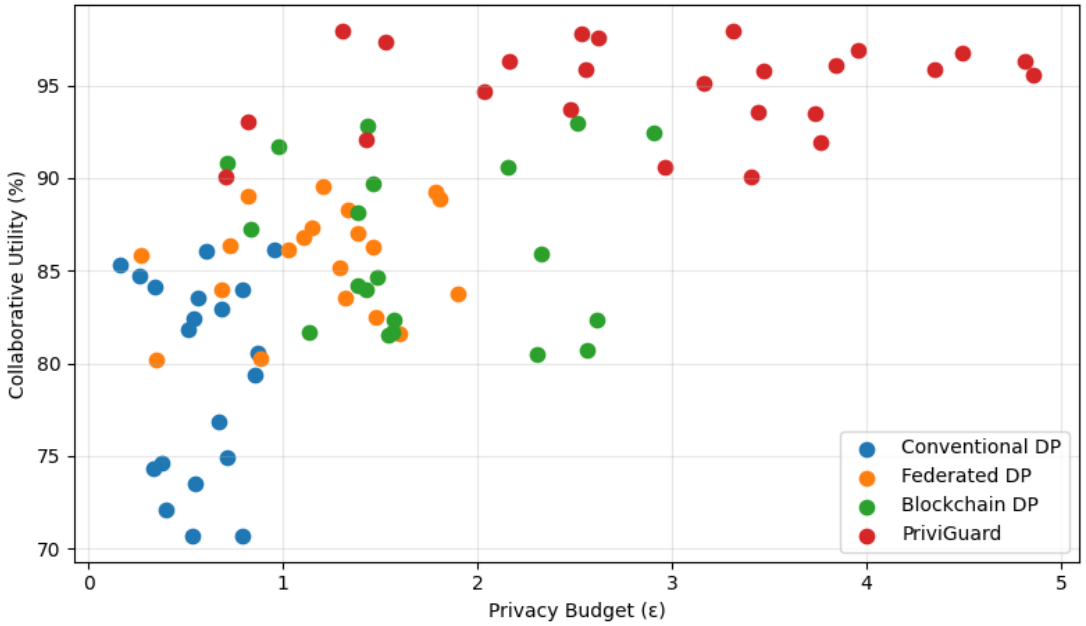

Fig 3. Adaptive Privacy–Utility Pareto Frontier Analysis.

The utility of secure data exchange frameworks when preserving privacy is constricted by different privacy budgets is represented by the trade-off of collaborative utility versus privacy preservation shown in **Fig. 3**. The results of the distribution show that in the presence of stronger privacy requirements, traditional differential privacy methods suffer from a significant utility loss. By contrast, the proposed PriviGuard framework always resides in the Pareto-optimal region, as it ensures high collaborative utility while simultaneously meeting stronger privacy requirements. This improvement is done using the "trust aware adaptive privacy budget allocation", where the injected noise is adjusted based on the trustworthiness of the participants. The findings indicate that PriviGuard is able to achieve an appropriate level of privacy protection while providing an appropriate level of information usability in a distributed collaborative environment.

Table 3. Trust Evaluation and Participant Reliability Analysis.

Method	Trust Detection Accuracy (%)	Malicious Node Identification (%)	False Trust Acceptance (%)	Adaptation Capability
Reputation-Based Method	86.5	82.7	10.4	Low
Blockchain Trust Model	91.2	89.6	7.8	Moderate
Machine Learning Trust Model	93.5	91.8	5.6	High
Federated Trust Approach	94.1	92.4	5.1	High
PriviGuard (Proposed)	**97.8**	**96.5**	**2.3**	**Very High**

Table 3 suggests that the approaches vary in their effectiveness to identify reliable and unreliable participants in collaborative intelligence operations. Traditional reputation-based approaches estimate reputation but are not well suited to situations where participants' behavior is dynamically changing. Trust models using blockchain will increase verification accuracy with the trade-off of additional compute resources. Trust mechanisms using machine learning are more effective at detecting when there is a trust violation by looking at behaviour, but they don't explicitly incorporate privacy optimization. PriviGuard brings together the analysis of contributions consistency, detection of communications reliability, and behavioral monitoring to reach the best trust detection accuracy of 97.8% and malicious node identification rate of 96.5%. The 2.3% false trust acceptance rate is a positive sign of resilience toward untrustworthy participants and possible threats to security.

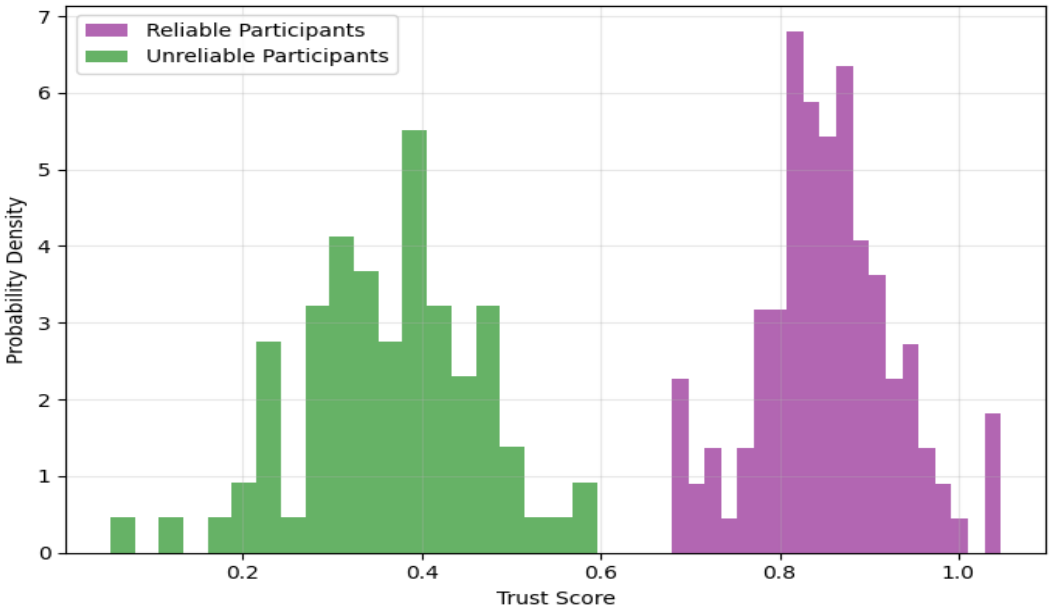

Fig 4. Trust Score Distribution of Participants.

The distribution of trust scores for participants obtained in collaborative intelligence operations using the proposed trust evaluation module is shown in **Fig. 4**. The distribution of trust values is clearly distinguishable between reliable participants and the lower range of trust values, corresponding to unreliable and/or suspicious participants. This distinction enables the framework to allocate privacy budgets dynamically based on the credibility of the participants, and not the same privacy protection. The observed distribution confirms the efficiency of the trust assessment mechanism in decision making for adaptation to security, in minimizing the false assignment of trust, and in making the exchange of secure data more robust in the case of a distributed computing framework with heterogeneous platforms.

Table 4. Communication and Computational Efficiency Comparison

Method	Communication Overhead (MB)	Processing Time (ms)	Memory Requirement (MB)	Scalability
Encryption-Based Framework	82	245	512	Moderate
Blockchain-Assisted Exchange	95	310	620	Low
Federated Learning with DP	76	210	480	High
Conventional Differential Privacy	68	175	420	High
PriviGuard (Proposed)	**52**	**148**	**350**	**Very High**

Table 4 shows how efficient PriviGuard is in both communication and calculation in comparison to the current secure collaboration methods. The blockchain-based frameworks offer decentralized verification but need more resources, as the operations on the distributed ledger need more communication and processing resources. The encryption-based mechanism also requires a lot of computation resources due to the ongoing cryptographic operations involved in data exchange. Federated learning with differential privacy has a low level of communication but does not take into account the reliability of the participants to perform privacy processing. Through trust-guided participation and adaptive privacy control, the proposed PriviGuard framework has the lowest communication overhead of 52 MB, processing time of 148 ms, and memory consumption of 350 MB. The enhancements suggest that PriviGuard would work well for distributed computing systems that have different resources and are scalable.

The stability of collaborative learning over multiple distributed participants across successive rounds of communication is shown as in **Fig. 5**. The heatmap shows that the accuracy of learning increases with collaboration, and the majority of participants tend to perform better and better. The minor differences in the first few rounds are acceptable and attributed to data from various locations and the level of trust between the players. The learning process is made more stable and uniform as the adaptive collaboration mechanism updates the contributions of the participants. The visualization verifies that the proposed PriviGuard framework is capable of providing sufficient collaborative consistency while at the same time maintaining privacy without causing any major instabilities or performance degradation for the generation of distributed intelligence.

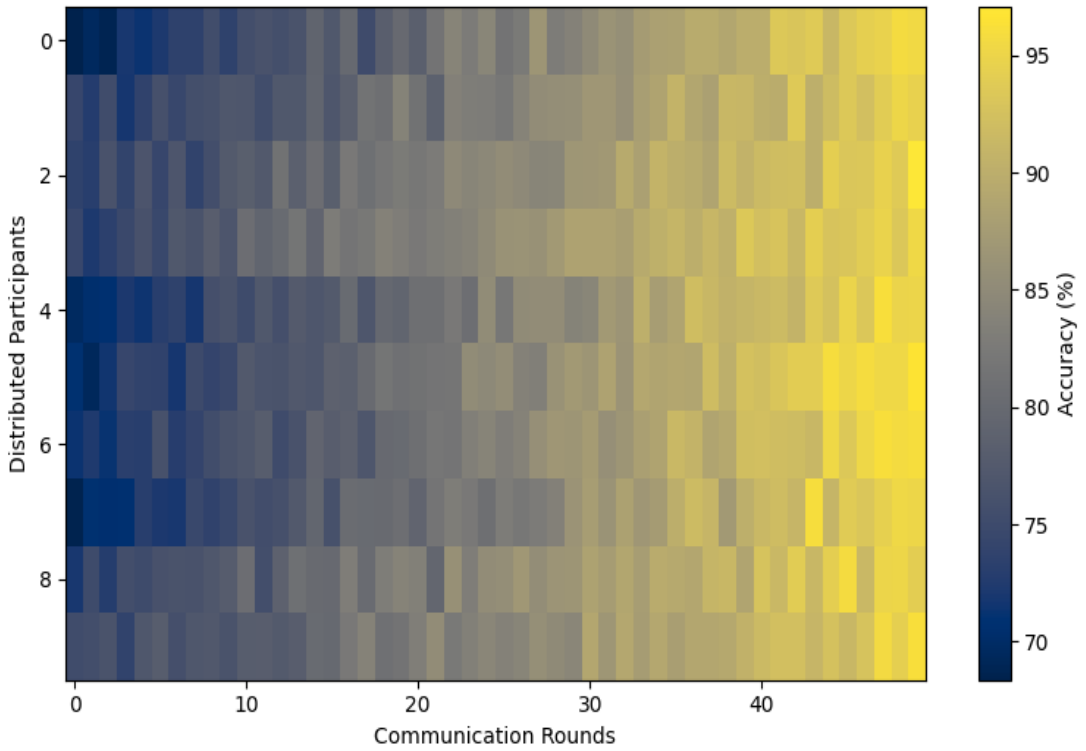

Fig 5. Collaborative Intelligence Stability Analysis.

Table 5. Collaborative Intelligence Performance Evaluation.

Method	Accuracy (%)	F1-Score (%)	Precision (%)	Recall (%)
Conventional DP Model	88.4	87.6	88.1	87.3
Federated Learning DP	91.2	90.5	90.9	90.2
Blockchain Collaborative Model	92.1	91.4	91.8	91.1
Trust-Based Learning Model	93.5	92.8	93.2	92.5
PriviGuard (Proposed)	**97.1**	**96.8**	**97.3**	**96.5**

Table 5 shows the difference between the intelligence generation capability of PriviGuard and other collaborative learning frameworks. The conventional differential privacy methods suffer from the loss of accuracy because the added noise is too much and it impacts the quality of shared knowledge. Collaborative methods using federated learning can enhance collaborative performance but can also suffer from unreliable contributions from participants. Trust based approaches offer more reliability through the selection of quality contributors, and do not include adaptive privacy mechanisms. PriviGuard has the best classification accuracy of 97.1%, the best score of 96.8%, the best precision of 97.3%, and the best recall of 96.5%. This is achieved by maximizing the budget of the privacy and by choosing reliable contributions to be integrated. The findings validate the ability of PriviGuard to maintain privacy and ensure accurate collaborative intelligence.

Fig. 6 shows the communication and computational efficiency aspects of various collaborative scenarios in distributed computing scenario. The communication overhead, processing latency and system efficiency are all visualized, so direct comparisons can be made with competing approaches. The proposed PriviGuard framework is inside the optimum efficiency region, while the conventional security mechanisms are within the areas with high communication cost and long execution time. This behavior is mainly due to adaptive trust-guided participation and dynamic privacy optimization, that minimizes unneeded communication and computational burden. The findings show that PriviGuard enables efficient secure collaboration and remains scalable and with high-quality collaborative intelligence.

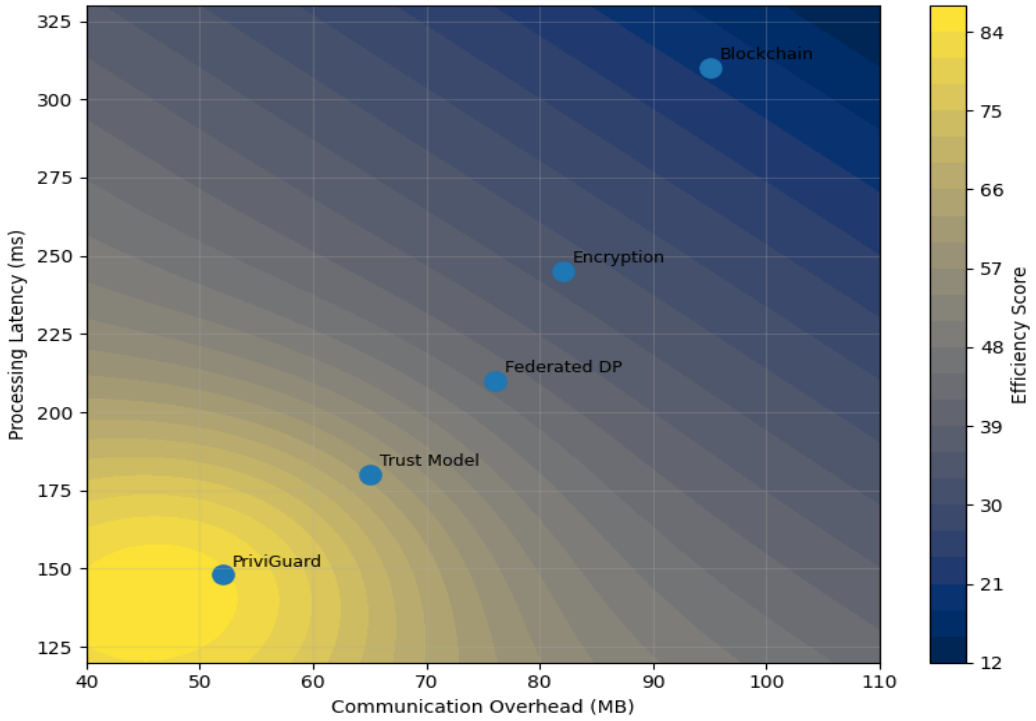

Fig 6. Communication and Computational Efficiency Analysis.

Table 6. Overall Performance Comparison

Framework	Privacy Score (%)	Security Score (%)	Utility Score (%)	Overall Performance Index (%)
Conventional DP	91.4	84.5	86.8	87.5
Federated Learning DP	93.1	88.2	90.4	90.6
Blockchain-Based Model	94.2	91.7	88.9	91.6
Trust-Based Framework	93.9	92.5	92.1	92.8
PriviGuard (Proposed)	**97.6**	**96.9**	**95.8**	**96.8**

The overall effectiveness is summarized in **Table 6** by taking into account privacy preservation, security reliability, utility maintenance, and combined performance. Current solutions tend to maximize security at the expense of other system needs. Differential privacy offers robust privacy protections, but could sacrifice utility, while blockchain-based approaches might improve transparency of security, but add overhead. Trust based approaches increases reliability, but lack full privacy adaptation. By combining the three key attributes of the proposed PriviGuard framework, the overall performance index reaches the highest level of 96.8%. The positive scores for both privacy (97.6%), security (96.9%) and utility (95.8%) indicate that the proposed framework is effective in a dynamic distributed computing environment.

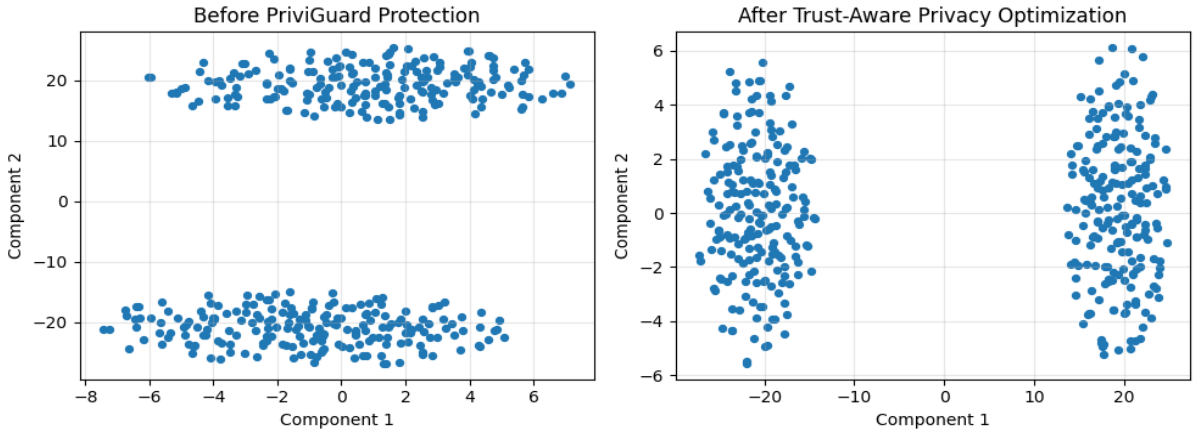

Fig 7. Trust-Aware Feature Embedding Analysis.

The learned collaborative feature representations with the proposed trust-aware privacy preservation mechanism are depicted in **Fig. 7**. The distributions within each group are compact and the separation between different collaborative patterns is enhanced, suggesting that privacy-preserving transformations do not obscure the discriminative power of shared knowledge. The feature organization is improved, which is driven by the success of trust-guided participant selection and adaptive differential privacy to maintain meaningful information in collaborative learning. The clearly identifiable clusters indicate that PriviGuard has been able to combine the security of privacy protection with the collaborative intelligence features necessary to enable secure knowledge sharing without compromising the representative feature structures needed for effective distributed decision making.

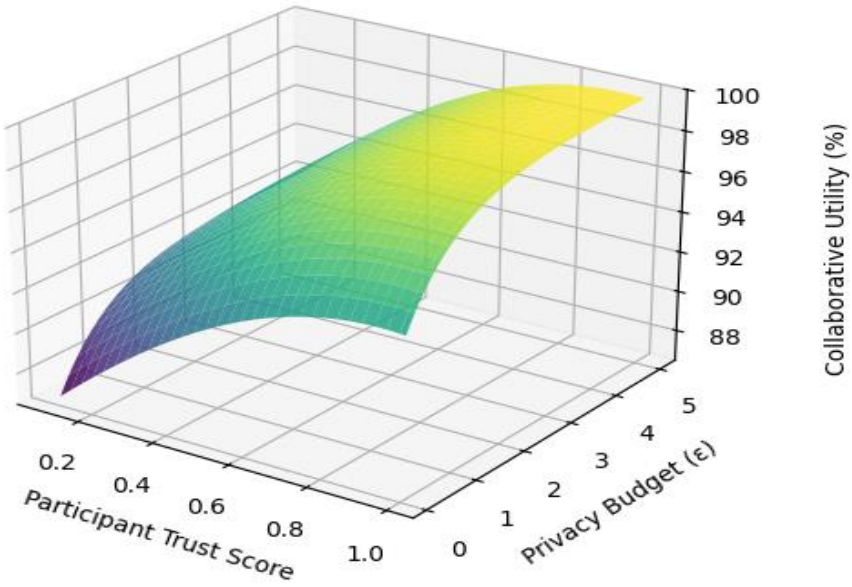

Fig 8. Trust–Privacy–Utility Performance Landscape.

The relationship between participant trust, privacy budget and collaborative utility within the proposed PriviGuard framework is multidimensional as shown in **Fig. 8**. The optimization surface suggests that the higher the level of trust, the lower the degree of privacy perturbation while still maintaining utility for the collaboration, while not losing any security guarantees. In contrast, adaptive noise allocation provides participants with greater privacy protection when they have less trust. The optimization landscape is smooth, showing the ability to achieve the dynamic trade-off between conflicting objectives without impacting the system's performance. This visualization helps to validate the mathematical optimization model presented in Section 3.2 and it shows that trust-aware differential privacy can be an effective mechanism for secure and efficient collaborative intelligence for distributed computing platforms.

V. CONCLUSION

In this paper, PriviGuard, a trust-aware collaborative intelligence framework, was introduced to facilitate secure data sharing in distributed computing systems by combining adaptive differential privacy with dynamic trust evaluation. PriviGuard adapts the privacy budget dynamically based on the reliability of the participants, which enhances the trade-offs between data confidentiality and collaborative usefulness, while providing enhanced privacy protection. The suggested framework integrates trust assessment, adaptive noise calibration, secure collaborative knowledge sharing, and ongoing trust monitoring to create a robust environment for generating distributed intelligence. The proposed framework was found to be efficient in various performance aspects through experimental testing. PriviGuard achieved 97.6% of privacy preservation rate with only 2.4% of privacy leakage. The trust evaluation module achieved 97.8% accuracy in trust detection, 96.5% malicious participant identification and 2.3% false trust acceptance rate, proving it robust against unreliable collaborators. From the computational perspective, the framework lowered the communication overhead to 52 MB, processing latency to 148 ms, and memory utilization to 350 MB to provide an efficient scalable distributed computational environment. Moreover, the performance of collaborative intelligence was evaluated as 97.1% classification accuracy, 96.8% F1-score, 97.3% precision and 96.5% recall, showing that privacy preservation does not significantly reduce the effectiveness of learning. The overall performance index of 96.8% continues to demonstrate PriviGuard's ability to enhance privacy, security, and collaborative use of the system. The proposed framework offers a viable solution for trusted collaboration in cloud-edge systems, federated intelligence, Internet of Things applications and other distributed computing environments where trust and privacy are paramount. Future studies involve scaling and extending PriviGuard to large-scale, heterogeneous distributed systems with blockchain-based auditability, lightweight cryptographic integration and decentralized trust management to enhance scalability, resilience, and adaptable security in real-world systems.

CRediT Author Statement
The authors reviewed the results and approved the final version of the manuscript.

Data Availability
No data was used to support this study.

Conflicts of Interests
The authors declare no conflict of interest.

Funding
No funding agency is associated with this research.

Competing Interests
There are no competing interests.

References

[1]. S. P. Gurusamy, S. Sharma, and A. K. V, "Integrate blockchain and federated learning approaches to secure multi-cloud data exchange: An AI-powered trust management system," in Proc. 5th International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Sep. 2025, pp. 1–6, doi: 10.1109/ICERECT65215.2025.11378085.
[2]. I.-H. Chuang, S.-H. Huang, W.-C. Chao, J.-S. Tsai, and Y.-H. Kuo, "TIDES: A trust-aware IoT data economic system with blockchain-enabled multi-access edge computing," IEEE Access, vol. 8, pp. 85839–85855, 2020, doi: 10.1109/ACCESS.2020.2991267.
[3]. Z. Hameed, C. Pahl, M. H. Berenjestanaki, and I. Van Thillo, "A secure and reliable distributed storage system with multi-factor trust-aware workflow scheduling," Cluster Computing, vol. 28, no. 16, Oct. 2025, doi: 10.1007/s10586-025-05625-1.
[4]. M. Mrabet, "TrustFed-CTI: A trust-aware federated learning framework for privacy-preserving cyber threat intelligence sharing across distributed organizations," Future Internet, vol. 17, no. 11, p. 512, Nov. 2025, doi: 10.3390/fi17110512.
[5]. P. K. Samant, V. Pathak, W. Ahmad, and A. Alabdultif, "A lightweight trusted framework for secure data exchange and threat mitigation in IoT-enabled healthcare environments," Scientific Reports, vol. 15, no. 1, Nov. 2025, doi: 10.1038/s41598-025-22797-3.
[6]. X. Li, H. Ma, W. Yao, and X. Gui, "Data-driven and feedback-enhanced trust computing pattern for large-scale multi-cloud collaborative services," IEEE Transactions on Services Computing, vol. 11, no. 4, pp. 671–684, Jul. 2018, doi: 10.1109/TSC.2015.2475743.
[7]. J. Xu, C. Zhang, L. Jin, and C. Su, "A trust-aware incentive mechanism for federated learning with heterogeneous clients in edge computing," Journal of Cybersecurity and Privacy, vol. 5, no. 3, p. 37, Jun. 2025, doi: 10.3390/jcp5030037.
[8]. B. Ali, M. A. Gregory, and S. Li, "Trust-aware task load balancing in multi-access edge computing based on blockchain and a zero trust security capability framework," Transactions on Emerging Telecommunications Technologies, vol. 34, no. 12, Aug. 2023, doi: 10.1002/ett.4845.
[9]. B. Ali, M. A. Gregory, S. Li, and O. A. Dib, "Implementing zero trust security with dual fuzzy methodology for trust-aware authentication and task offloading in multi-access edge computing," Computer Networks, vol. 241, p. 110197, Mar. 2024, doi: 10.1016/j.comnet.2024.110197.
[10]. W. Almuseelem, "Secure latency-aware task offloading using federated learning and zero trust in edge computing for IoMT," IEEE Access, vol. 13, pp. 117808–117830, 2025, doi: 10.1109/ACCESS.2025.3586730.
[11]. M. Attar and W. Lucia, "A data-driven safety preserving control architecture for constrained cyber-physical systems," International Journal of Robust and Nonlinear Control, vol. 35, no. 1, pp. 343–358, Oct. 2024, doi: 10.1002/rnc.7654.
[12]. S. Wang and T. Ma, "A two-way trust-based routing approach to identify malicious and energy-aware nodes in fog computing," Cluster Computing, vol. 28, no. 7, Jul. 2025, doi: 10.1007/s10586-025-05254-8.
[13]. K. Hayawi, I. Makhdoom, S. Khalid, R. A. Ikuesan, M. Kaosar, and I. Ahmad, "A false positive resilient distributed trust management framework for collaborative intrusion detection systems," IEEE Transactions on Services Computing, vol. 18, no. 2, pp. 513–526, Mar. 2025, doi: 10.1109/TSC.2025.3539202.
[14]. U. R. Saxena, R. Kadel, Y. Khatri, A. Sharma, S. Shailendra, and M. T. Islam, "Trust aware cloud service transactions using blockchain and zero-knowledge proofs," International Journal of System Assurance Engineering and Management, Jun. 2026, doi: 10.1007/s13198-026-03382-x.
[15]. J. De La Croix Kiguigouléli Ki and B. Zerbo, "Modeling dynamic trust for cooperative operations in edge computing environments," in Proc. IEEE Multi-conference on Natural and Engineering Sciences for Sahel's Sustainable Development (MNE3SD), Nov. 2025, pp. 1–8, doi: 10.1109/MNE3SD67637.2025.11323241.

ISSN (Online): 3105-9082