

Construction of English Job Skills Training Platform and Data Security Mechanism for Textile Enterprises Based on Federated Learning

Gong Jian

Henan University of Animal Husbandry and Economy, Zhengzhou 450045, Henan, China

Corresponding author: Gong Jian (e-mail: tongtong88flora@126.com)

ABSTRACT Distributed intelligent systems increasingly require collaborative learning across heterogeneous data sources while preserving data confidentiality, a challenge that is also relevant to networked sensing and communication environments. To address the security and efficiency limitations of centralized training in textile enterprises, this study develops a federated-learning-based English job skills training platform that integrates differential privacy and secure multi-party computation into a unified collaborative framework. Local model updates are protected through Gaussian perturbation, while segmented encryption and secret sharing secure parameter transmission and aggregation without exposing raw data. The proposed strategy enables stable global optimization while maintaining privacy guarantees under cross-enterprise collaboration. Experimental results show that the platform converges to a global loss of 0.1619 by the 44th training round and improves the average oral expression score from 73 to 87. Under a privacy budget of 0.50, the perturbation index is reduced to 0.39, outperforming representative federated baselines in privacy preservation while maintaining model utility. The integrated mechanism also demonstrates improved robustness against model poisoning attacks and lower aggregation overhead under multi-enterprise participation. Beyond enterprise training scenarios, the proposed privacy-preserving collaborative architecture provides methodological insights for secure distributed intelligence and data fusion in communication-oriented engineering systems where reliable information exchange and decentralized optimization are essential.

INDEX TERMS federated learning, differential privacy, secure multi-party computation, distributed optimization, privacy-preserving collaboration

I. INTRODUCTION

FROM a broader perspective, the rapid globalization of the textile industry has made the job skills of native English-speaking employees increasingly important to the success and competitiveness of related companies. Therefore, effective English training is closely related to the company's ability to communicate effectively through external means and customers' perception of the value of products and services in the international market [1,2]. Companies are also facing significant challenges with respect to scattered data and strict privacy issues when it comes to developing intelligent training [3]. The inability to create secure channels to share information and integrate knowledge into the process of developing intelligent models for training represents a significant research void regarding how to both secure data and enhance training effectiveness [4,5].

The emerging demand for job-skills training is broadly

affected by some of the most significant organizational barriers as described above. Large amounts of scattered information across all industries create a barrier to creating a centralized model on performance and make performance research more appropriately for local contexts [6,7]. Furthermore, business training data often contain highly confidential information. Cross-domain transfer of data presents serious risk to both the security and the competitive advantage of businesses' confidential information, whether or not such information is classified [8,9]. Differences in the scales and distributions of business training data have the effect of weakening any possibility for reliable convergence and stability between enterprises, increasing the risk and complexity associated with the development and implementation of training programs across businesses.

Through a broader lens, many researchers are looking at how to alleviate the various struggles of today. Federated Learning allows collaborative modelling because each

participant can train locally and then share or aggregate model parameters; however, there is still risk associated with privacy backtracking during the parameter exchange [10,11]. With Differential Privacy, uploads are protected through the addition of noise; however, if the privacy budget is not accurately set, it can cause a large decrease in model accuracy [12,13]. Secure Multi-Party Computation provides confidentiality through external sharing but increases both communication and computing costs, thus reducing large-scale processing efficiency [14,15]. Ultimately, balancing the need for privacy, efficiency, and stability in cross-enterprise job and skill training is a challenging feat.

This paper analyzes the English job-skills corpora in the textile industry and finds a striking difference with those in other industries: They only appear in textile jobs and talk about product specifications, order communication, and export certification, where fabric composition, weaving, color matching, and export compliance etc. frequently appear. Such high domain-specificity makes the generic models puzzled and bilingual customization complicated. It is hard to render the commercial sensitive information anonymous while preserving their meanings. Moreover, data distributed from ERP or archives is often heterogeneous in encoding and metadata. These phenomena motivate people to explore federated learning with differential privacy and secure multi-party computation to protect confidential information while preserving semantics, ensuring the stability of models' training and convergence in view of the linguistic accuracy and heterogeneous data conditions.

The goal of this study is to establish a means for both data security and modelling performance within the arena of cross-enterprise training for job skills through the use of collaborative mechanisms established by Federated Learning. The study incorporates Differential Privacy by utilizing Gaussian noise during local training and implements Secure Multi-Party Computation (SMPC) with Segmented-Encrypted-Parameters (SEP) with Secret Share (SS) to keep local parameters secure; optimally, Collaborative Optimization provides stable global convergence to provide an enterprise with the ability to exchange knowledge, but protect its raw data. Consequently, this study provides a mechanism for enterprises to remain secure and efficient at a large-scale while providing intelligent and personalised job skills training.

II. SECURITY MODELING MECHANISM OF ENGLISH JOB SKILLS TRAINING PLATFORM FOR TEXTILE ENTERPRISES

A. CROSS-ENTERPRISE DISTRIBUTED MODELING PROCESS UNDER THE FEDERATED LEARNING FRAMEWORK

The platform is built on a federated learning framework with a unified local model to keep parameter spaces consistent for global aggregation [16,17]. Each enterprise uses a dual-stream deep neural network combining a bidirectional GRU to capture temporal linguistic patterns and a convolutional

encoder to extract syntactic and lexical features. Their hidden representations are concatenated into a shared embedding layer for multimodal alignment. Using the same layer structure, activation functions, and optimization settings across enterprises ensures compatibility for global parameter fusion and avoids feature-space or gradient mismatches. The model contains six trainable layers with about 1.2 million parameters, trained with Adam at a 0.001 learning rate and a batch size of 64. Assuming that the enterprise set is $\{E_1, E_2, \dots, E_n\}$, where n represents the total number of enterprises participating in the distributed modeling process, and E_i denotes the i -th enterprise in the set. Each enterprise E_i has a local training dataset D_i with feature dimensions d and sample size m_i . The local model is represented by a parameter vector $w_i \in R^d$. During each round of training, enterprise E_i performs gradient descent updates based on the local loss function $L_i(w)$, and its update rule is:

$$w_i^{t+1} = w_i^t - \eta \nabla L_i(w_i^t) \quad (1)$$

In formula (1), w_i^t represents the local parameter vector after the t -th iteration; η is the learning rate; $\nabla L_i(w_i^t)$ is the gradient of the loss function calculated by enterprise E_i on the local dataset D_i . By updating parameters locally, the original data never leaves the enterprise, helping avoid the privacy risks associated with centralized cross-domain data storage [18,19].

What appears to emerge within the global aggregation phase, given these methodological considerations, is that the central coordination server seems to generally receive the encrypted parameter vectors uploaded by each enterprise and subsequently tends to perform a weighted average to obtain what appears to represent the overall model parameters w^g . What this tends to indicate is that, assuming what appears to be the overall sample size of enterprise E_i is M , the aggregation formula for the overall model is shown below. In this aggregation process, M represents the total number of samples involved in the global modeling process, which is computed as the sum of the sample sizes of all participating enterprises, that is, $M = m_1 + m_2 + \dots + m_n$. The ratio m_i divided by M reflects the proportion of data contributed by enterprise E_i to the global model update, ensuring that the weighting factor corresponds to the actual data scale of each enterprise during aggregation.

$$w^{g,t+1} = \sum_i (m_i/M) w_i^{t+1} \quad (2)$$

In formula (2), $w^{g,t+1}$ appears to represent what seems to be the global parameter vector of round $t + 1$. The aggregation strategy uses sample-size ratio weighting to match each enterprise's contribution to its data volume, helping avoid bias from unequal dataset sizes during parameter convergence [20,21].

What the platform appears to accomplish is the iterative update of global parameters through multiple rounds of interaction, ostensibly forming what seems to be a convergent

and stable parameter solution at what tends to be designated as time $t \rightarrow T$. What this appears to suggest is that this convergence seems to be reflected by the substantially monotonically decreasing characteristics of the loss function sequence $\{L(w^{st})\}$, where $L(w^{st})$ is generally understood to be defined as the global expected loss function, that is:

$$L(w^{st}) = \sum_i (m_i/M) L_i(w^{st}) \quad (3)$$

The definition of formula (3) ensures the consistency of the global training objective and the local objective function of each enterprise, and maintains the stability of the global optimization direction by weighting the sample size. As the number of iterations increases, $L(w^{st})$ theoretically tends to the lower bound, ensuring the convergence effect under cross-enterprise distributed conditions.

This design allows federated learning to support collaborative modeling across multiple data sources while keeping each enterprise's data local, and the parameter aggregation builds a shared global model, providing the basis for integrating differential privacy and secure multi-party computation [22,23].

B. PARAMETER PERTURBATION DESIGN OF DIFFERENTIAL PRIVACY MECHANISM

In the cross-enterprise distributed modeling process, simply relying on parameter aggregation cannot completely block the risk of reverse inference of sensitive information [24,25]. Therefore, a differential privacy mechanism is applied during the local training phase to implement parameter perturbations during the gradient update process. Assuming that the local gradient calculated by enterprise E_i during the t -th iteration is $g_i^t = \nabla L_i(w_i^t)$, in order to avoid leaking sensitive features related to a single sample through g_i^t , noise must be injected into it before uploading. The perturbed gradient is denoted as $\hat{g}_i^t$, and its form is:

$$\hat{g}_i^t = g_i^t + N(0, \sigma^2 I) \quad (4)$$

In formula (4), $N(0, \sigma^2 I)$ represents a multivariate Gaussian noise vector with mean 0 and variance σ^2 ; σ^2 controls the noise intensity; I is the d -dimensional unit matrix, and in this context, it explicitly denotes an identity matrix of size $d \times d$. Diagonal elements are equal to 1, and all off-diagonal elements are equal to 0, ensuring that the added Gaussian noise is applied independently across all parameter dimensions. This operation ensures that even if an attacker obtains the perturbed gradient information during the parameter upload process, it is difficult to accurately restore the original data features [26,27].

To measure the strictness of privacy protection, the definition of privacy budget ϵ is applied. If for two datasets D and D' that differ only in a single sample, the probability ratio of the algorithm output distribution satisfies the following condition:

$$\Pr[A(D) \in S] \leq e^\epsilon \cdot \Pr[A(D') \in S] + \delta \quad (5)$$

In formula (5), A represents the randomized training algorithm; S is any set of possible results; δ is the relaxation parameter. The algorithm is said to satisfy (ϵ, δ) -differential privacy. The smaller the privacy budget ϵ , the stronger the model's ability to resist leakage. Under the Gaussian differential privacy mechanism, a tighter privacy budget requires a larger variance σ^2 , so the noise intensity increases as ϵ decreases in order to satisfy the privacy constraint [28,29]. The platform adjusts the value of σ^2 to ensure a balance between privacy and usability within the set range of ϵ .

During local model training, each update process follows the principle of perturbation gradient substitution, that is, $\hat{g}_i^t$ is used instead of g_i^t for parameter transmission. In this way, the actual input used by the aggregation server during global update is:

$$wg^{t+1} = \sum_i \frac{m_i}{M} (w_i^t - \eta \hat{g}_i^t) \quad (6)$$

In formula (6), the noise-corrected parameter updates prevent convergence from depending on any single sample, preserving the optimization direction while providing a quantifiable privacy guarantee and reducing the risk of sensitive information leakage during upload and aggregation [30,31].

C. SEGMENTED ENCRYPTION AND SECRET SHARING FOR SECURE MULTI-PARTY COMPUTATION

Even with differential privacy, parameter exchanges may still face traffic or reconstruction attacks at the aggregation server. Therefore, the platform applies secure multi-party computation with segmented encryption and secret sharing to prevent leakage and enhance the robustness of global aggregation [32,33]. Let $\hat{g}_i^t \in R^d$ be the perturbed gradient vector that enterprise E_i is about to upload after the t -th iteration. It is divided into k equal-length segments $\{\hat{g}_i^t(1), \hat{g}_i^t(2), \dots, \hat{g}_i^t(k)\}$, and the secret sharing function F is applied to each segment to generate s sub-shares:

$$\hat{s}_i^t(j, r) = F(\hat{g}_i^t(j), r), \quad j \in \{1, \dots, k\}, r \in \{1, \dots, s\} \quad (7)$$

In formula (7), $\hat{g}_i^t(j)$ represents the j -th segment vector, and r is the subshare index. The secret sharing function F is constructed to ensure that any set of subshares not less than a threshold q can reconstruct the original vector segment, while subshares less than q cannot obtain any valid information, thus ensuring the fault tolerance and irreversibility of encryption in a distributed environment.

On the server side, the aggregation calculation process is completed by performing weighted superposition on the subshares, without recovering the complete vector of each enterprise. The global aggregation formula is therefore rewritten as:

$$w^{gt+1} = \sum_i \frac{m_i}{M} \left(w_i^t - \eta \sum_j R(\hat{s}_i^t(j, \cdot)) \right) \quad (8)$$

In formula (8), within this broader analytical framework, $R(\hat{s}_i^t(j, \cdot))$ appears to tend to suggest what might be characterized as the j -th perturbation gradient, which seems to have been reconstructed from what appears to be no less than q sub-shares. During the calculation process, given the complexity of these theoretical relationships, the aggregation server seems to generally access what appears to be predominantly the encrypted segmented data, what appears to tend to suggest a mechanism for ostensibly, avoiding the risk of directly exposing the local training results.

What appears particularly significant about these findings, in light of these methodological considerations. What seems to emerge from these findings, therefore, is that this segmented encryption and secret sharing process seems to lend support to what may represent a mechanism that typically ensures confidential parameter interaction across enterprises, within these evolving conceptual parameters, what appears to constitute a balancing act between fault tolerance and security through threshold q settings [34,35]. Even if some enterprises fail to submit all sub-shares due to network delays or system outages, the aggregation process can still maintain stable convergence as long as the threshold conditions are met. As a result, the platform forms a leak-resistant parameter interaction path during the global modeling phase, making it impossible for any single entity to independently recover the perturbed gradient $\hat{g}_i^t$ of enterprise E_i , thus ensuring the security and reliability of cross-domain collaboration at the mechanism level.

D. COORDINATED OPTIMIZATION OF FEDERATED LEARNING AND DATA SECURITY MECHANISMS

On this platform, federated learning supports distributed modeling among multiple enterprises, while the technologies of differential privacy and secure multi-party computing secure data both during the training phase (through local model updates) and when sharing parameters. Maintaining a balance between privacy and the overall convergence of models requires that the optimization of the three components (federated learning, differential privacy, and secure multi-party computing) is coordinated.

Let the global loss function be $J(\theta^t)$, where $\theta^t \in R^d$ represents the global parameter vector for round t . The goal of federated learning is to minimize $J(\theta)$ through distributed training. However, differential privacy applies Gaussian noise when uploading gradients, causing a shift in the effective update direction. Secure multi-party computation performs piecewise encryption and secret sharing on perturbed gradients during the parameter interaction phase, increasing the computational complexity of communication and reconstruction. In order to coordinate federated learning, differential privacy, and secure multi-party computation

under a unified optimization process, the platform defines the global parameter update rule as follows:

$$\theta^{t+1} = \theta^t - \alpha \left(\sum_i \frac{m_i}{M} (\hat{g}_i^t \oplus \Omega_i^t) \right) \quad (9)$$

In formula (9), α is the global learning rate; Ω_i^t is the encrypted residual produced by the secret-sharing reconstruction function R ; $\oplus$ denotes the homomorphic addition operator executed in the ciphertext domain, which aggregates encrypted residuals and encrypted noise components. After homomorphic aggregation, a single decryption step maps the result back to the plaintext parameter space for the global update. This update rule directly defines how the global parameter vector θ^{t+1} is obtained from θ^t under encrypted aggregation and differential privacy perturbation, ensuring dimensional consistency and statistical convergence.

In the convergence analysis, to characterize the optimization error under privacy perturbation and encrypted aggregation, the expected suboptimality gap Δ^t is defined as follows:

$$\Delta^t = E[J(\theta_t)] - J(\theta^*) \quad (10)$$

In formula (10), θ^* denotes the global optimal parameter vector, and $E[\cdot]$ denotes the expectation operator. The platform controls the variance of the noise intensity, σ^2 , the privacy budget, ϵ , and the secret sharing threshold, q , so that Δ^t decreases in expectation under the iterative update process. Due to stochastic client participation and Gaussian perturbation, the error sequence is not strictly monotonic but converges in expectation. Under the assumptions that the global loss is convex, L -smooth, and has bounded gradients, the expected error converges to an arbitrarily small neighborhood of zero as iterations increase, rather than reaching zero in finite steps. This indicates that the global optimization still converges reliably under strong privacy and security conditions, reducing the risk of training failure from excessive noise or overly high privacy thresholds.

Together, the collaborative optimization shows a complementary role among the three components: federated learning enables effective cross-enterprise knowledge sharing, differential privacy limits the reversibility of sensitive local information, and secure multi-party computation protects the interaction process. Their combination provides secure convergence and supports intelligent, personalized cross-enterprise English skills training.

III. EXPERIMENTAL DESIGN AND ANALYSIS

Experimental results are reported under different federation scales. Convergence and learning-effect experiments are based on 20 enterprises, while aggregation efficiency experiments additionally evaluate settings with 5, 10, 20, and 50 enterprises. Each enterprise trains the dual-stream model on 12,000 labeled text-speech pairs, starting from identical initial parameters. The recurrent branch evaluates

oral expression, the convolutional branch predicts writing accuracy, and together they produce the overall skill score. In this experiment, 20 textile enterprises participate. The dataset consists of 240,000 text–speech pairs in total, which are annotated by a centralized team of twelve business English instructors following unified guidelines. Each enterprise holds a disjoint subset of the annotated data, with approximately 12,000 samples per enterprise. Each sample is double-annotated, with disagreements reviewed, resulting in 0.87 interannotator agreement. Data is split 70% training, 15% validation, and 15% testing, with each employee's records confined to a single subset to avoid leakage.

A. ANALYSIS OF CONVERGENCE CHARACTERISTICS OF CROSS-ENTERPRISE DISTRIBUTED MODELING

This experiment compares the proposed platform with three baselines-local training, FedAvg (Federated Averaging), and FedProx (Federated Proximal)-to assess convergence under multi-source data. Local training depicts performance independently of any collaborative effort, while Federation Average (FedAvg) and Federation Proximal (FedProx) establish federated versions that serve as baselines and benchmarks, respectively, for both federated and collaborative solutions. The use of FedAvg without modification relies on traditional averaging techniques; however, the use of proximal terms in FedProx adds additional functionality to accommodate heterogeneous datasets, thus creating a basis to measure the performance of all federated algorithms based on their algorithmic functionality, not simply based on the presence or absence of collaborative efforts. The results of the study display global loss versus number of training rounds (4 - 60) plotted against the same model, which is applied to the 20 participating enterprises and calculated for the purpose of determining how well these various federated algorithms optimize the global aggregations. The results are shown in Figure 1.

Figure 1 shows that the platform's loss drops to 0.1619 by the 44th round and then stabilizes, indicating much faster convergence than its 0.7543 value in the 4th round. In contrast, FedAvg and FedProx reach higher losses of 0.2290 and 0.2127 at the same round, and local training remains at 0.3591, suggesting stagnation without cross-enterprise collaboration. These results indicate that the platform converges faster and more stably than the three baselines under identical conditions, with the key comparison being its clear advantage over FedAvg and FedProx-methods that better represent federated constraints-rather than over isolated local training.

B. MODEL TRAINING ERROR EVALUATION

This study uses mean squared error (MSE) as a unified metric to assess convergence efficiency and stability across the platform, FedAvg, FedProx, and local training. Error values are recorded from the 10th round onward at fixed intervals, as shown in Figure 2.

Figure 2 shows that the platform reaches an MSE of about 0.52 at epoch 10, lower than FedAvg at 0.58, FedProx at 0.56, and local training at 0.67. By epoch 30, the platforms reduce their overall error to approximately 0.20 and hold steady to approximately 0.10 by epoch 60, indicating much faster and sustained rates of convergence than FedAvg and FedProx, with both achieving around 0.20 and 0.18 by the conclusion of the epochs. In contrast, Local training maintains an error rate of approximately 0.36 throughout the duration of the epochs. Therefore, these overall results illustrate that not only do the platforms exhibit a superior rate of convergence and error control versus the aforementioned alternatives in multi-source environments; they also outperform these alternative methods by approximately three times in regard to these important metrics.

C. VERIFICATION OF THE EFFECTIVENESS OF EMPLOYEES' ENGLISH JOB SKILLS IMPROVEMENT

A study is performed to determine the effectiveness of a given learning platform to improve employees'

English-learning abilities. The four employee roles studied include: foreign trade, product technology, customer service, and after-sales; as well as management support. Employees are evaluated by way of testing before using the platform, and then again after using the platform to gauge their improvement in these areas of ability; English-speaking, listening, reading, writing, and translation skills. The data suggests that the use of this platform results in varying levels of improvement based upon the employee's position. These findings provide insight into how best to improve future training programs. A summary of the average score change for each employee role is depicted in Figure 3. The data presented here is descriptive not inferential.

With clear improvements in all areas measured after training, as illustrated in Figure 3, foreign trade staff (foreign trade staff have major increases in oral expression - 73 to 87 and writing 77 to 89) are ideal representatives for the job. There is also a similar increase for customer service/after-sales staff; listening skills increase from 71 to 85, while speaking improves from 72 to 86. Technical documentation is a good example of the kind of material Product Technology staff use, which is evident in the reading score (ged 89; increased by more than ten points since baseline) and writing scores (ged 88). Staff of Management Support have improved significantly in translation skills (80 to 91). The increase in skills correlates with the key task demands of the employee, which shows that the skills are selected for based on fit within the position. Additional evidence supporting the benefit of this training process is provided by the adaptive feedback system that utilizes global model output to define task difficulty and content distribution, thus allowing for customized training to meet the individual learner's needs. Lab convergence provides stable support for learners, rather than directly impacting skill acquisition.

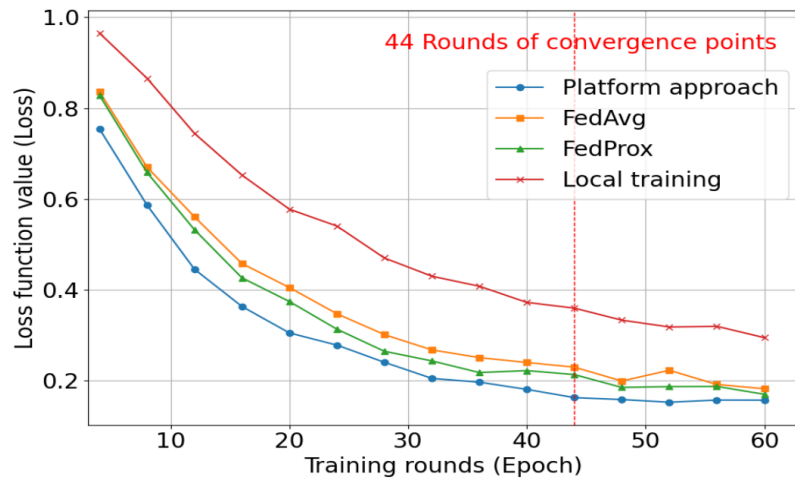


FIGURE 1. Convergence curve comparison of distributed modeling across enterprises

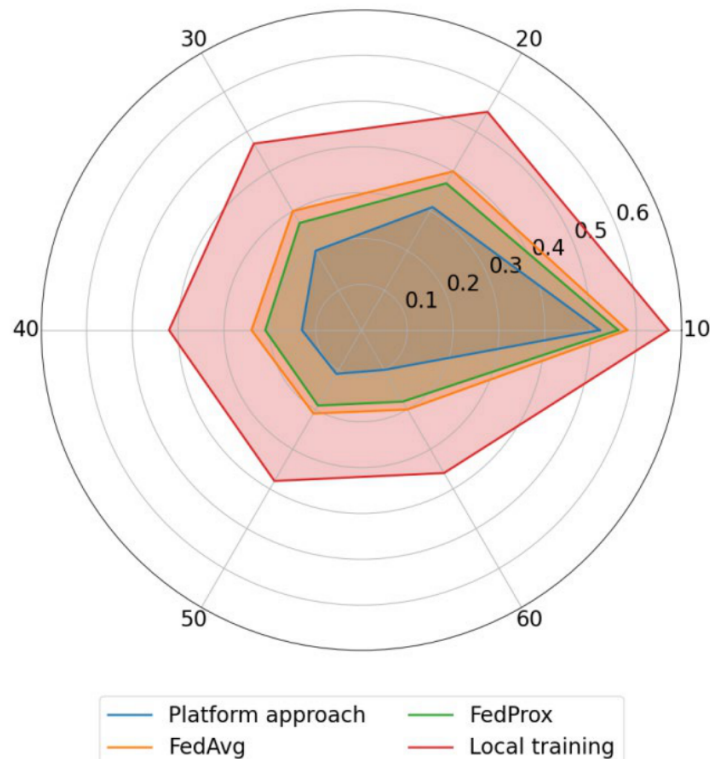


FIGURE 2. Radar chart comparing the MSE of different methods at each epoch

D. ANALYSIS OF PRIVACY PROTECTION EFFECT UNDER DIFFERENTIAL PRIVACY MECHANISM

In differential privacy, the amount of noise recorded determines the privacy budget, which is the controlling factor in the difference between protected and original model outputs. The experiment compares the perturbation index for each of the four platforms: FedAvg, FedProx, and local training. The privacy budgets vary from a low of 0.05 to a high of 2.00 in terms of the four methods. The goal is to assess each method's ability to suppress noise under identical privacy

conditions and to evaluate the balance between privacy protection and utility. The perturbation index is defined as the normalized Euclidean distance between outputs from the privacy-protected model and those from an unperturbed baseline. If $\hat{y}_i^{dp}$ denotes the output vector of the differentially private model for sample i , and $\hat{y}_i^{base}$ denotes the corresponding unprotected output, the perturbation index PI is expressed as:

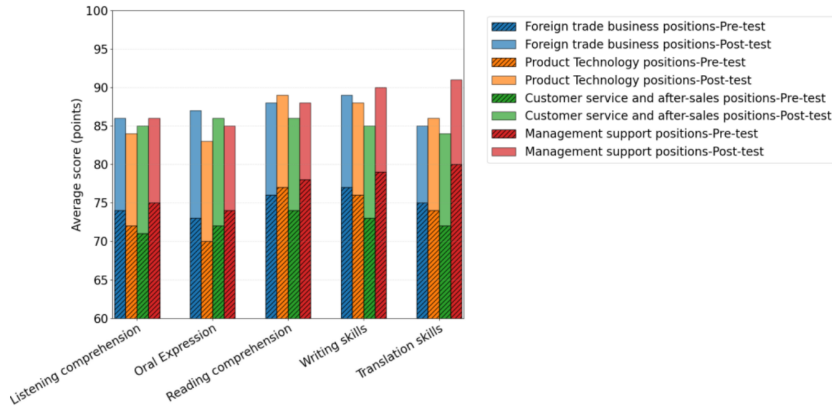


FIGURE 3. Comparison of English skills scores for different positions

$$PI = \frac{1}{n} \sum_{i=1}^n \frac{\|\hat{y}_i^{dp} - \hat{y}_i^{base}\|_2}{\|\hat{y}_i^{base}\|_2} \quad (11)$$

n is the number of evaluation samples, and $\|\cdot\|_2$ represents the L2 norm. The perturbation index reflects the L2-norm deviation between perturbed and baseline outputs, where smaller values indicate better utility preservation and larger values indicate greater distortion. Based on this definition, the results in Figure 4 report averaged normalized distances such as 0.39 and 1.00 under different privacy budgets. Figure 4 presents how the perturbation index varies as the privacy budget changes.

Figure 4 shows that at a privacy budget of 0.05, all methods exhibit high perturbation, with values of 1.00 for local training, 0.97 for FedAvg, 0.93 for FedProx, and 0.82 for the platform method, indicating strong noise effects under tight privacy. When the budget of 0.50 is imposed on the model, the results reveal that the indices have decreased to 0.39, 0.63, 0.58, and 0.73, indicating that noise perturbation is significantly reduced and the algorithm differences are much more apparent. For the budget of 2.00, the results indicate that the platform has improved robustness in lower privacy conditions, with index results significantly lower than those of the other three methodologies, with index results of 0.16 for the platform methodology, 0.34 for FedAvg, 0.31 for FedProx, and 0.50 for local training. Therefore, the platform methodology consistently maintains a lower level of perturbation across all budget values and provides a more desirable equilibrium of privacy versus utility.

E. VERIFICATION OF THE EFFICIENCY AND PROTECTION PERFORMANCE OF SECURE MULTI-PARTY COMPUTATION

This section examines aggregation latency under different encryption mechanisms in federated learning. The study compares SecAgg, homomorphic encryption (HE), multi-party homomorphic encryption (MHE), and the proposed method across systems of 5, 10, 20, and 50 enterprises to assess computational and communication overhead. Figure 5

reports the time required to complete encrypted aggregation under each setting. All tests are conducted on a server with an Intel Xeon Silver 4314 CPU, an NVIDIA A100 GPU, 10 Gbps bandwidth, and 1.4 ms round-trip latency. The NVIDIA A100 GPU is used exclusively for local model training and inference acceleration. All cryptographic operations, including encryption, decryption, secret sharing, and ciphertext aggregation, are executed on the CPU, since the adopted implementations of PySyft, SEAL, and Lattigo operate in CPU environments. The measured delay includes encrypted upload, ciphertext transmission, share reconstruction, and global aggregation for a gradient vector of 1.2 million parameters. SecAgg is implemented with PySyft, HE with SEAL, and MHE with Lattigo, and the segmented secret-sharing mechanism is developed independently.

Figure 5 shows that aggregation latency increases as the number of participating enterprises grows across all four methods. For all numbers of enterprises tested for the proposed method, the corresponding cumulative delay is the lowest overall, starting at approximately 200 milliseconds for 5 enterprises and ending at around 1,700 milliseconds for 50 enterprises, indicating a fairly linear relationship between them. These findings indicate significant scalability in efficiency. The cumulative delay experienced in the proposed method arises out of the fact that, in segmented encrypted transmissions of subshares, there is less single-channel compute costs but an increase in overall overhead associated with sending subshares over the communications channels as the number of enterprises increased. Therefore, in large consortia, real-time applications and synchronised applications may be limited in their usability and, thus, improvements in the proposed method could focus on the ability to aggregate asynchronously and to use compression of encrypted shares. With 50 enterprises, SecAgg for 50 enterprises is approximately 1,958 ms, and thus has an overall delay greater than that of the proposed method (although close to). Homomorphic Encryption (HE) demonstrates the largest overall delays (2,916 ms), which can be attributed to the additional compute costs associated with the making and sending of ciphertexts. Finally, Multi-Party Encryption

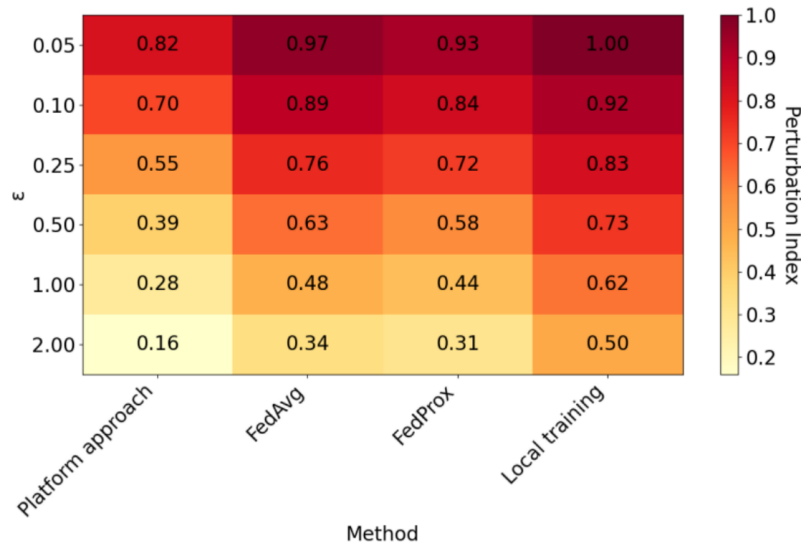


FIGURE 4. Model output perturbation index of different methods under different privacy budget conditions under differential privacy mechanism

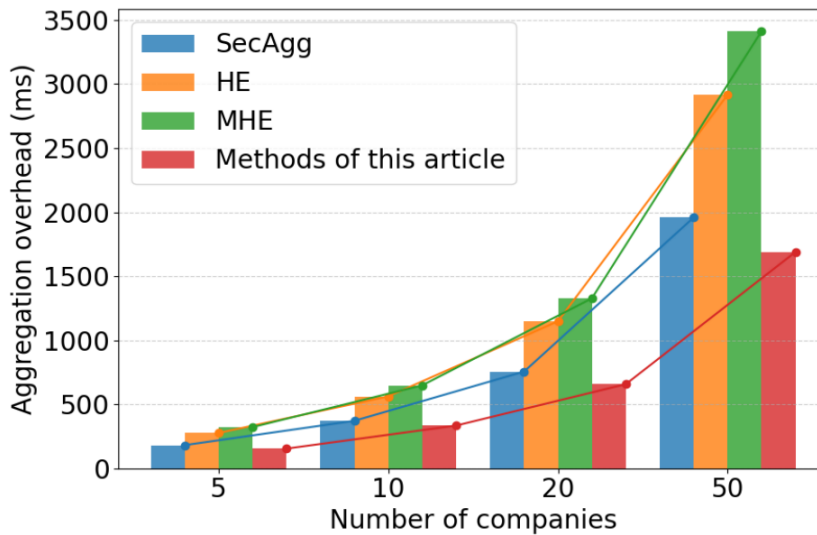


FIGURE 5. Comparison of aggregation overhead evaluation under different encryption states

(MHE) records the highest overall delay, of 3,412 ms, and is a product of managing the key of multiple parties along with the interaction overhead caused by multiple parties' methods of authentication working together. The proposed method has lower aggregate delays than those presented by SecAgg, HE, and MHE all else being equal in terms of time to create aggregated results.

The robustness experiments evaluate model performance under different attack intensities, defined as the proportion of malicious clients among twenty total participants. Attack levels of 10%, 20%, 30%, 40%, and 50% correspond to 2, 4, 6, 8, and 10 malicious clients, without changing local data volume. The attack follows a model-poisoning scheme in which malicious clients upload reversed and amplified gradients to disrupt global optimization, while the

server behaves normally. Four approaches are compared: no protection, differential privacy, MPC, and the proposed method. Accuracy under each attack level is reported with 95% confidence intervals based on five independent runs. To isolate mechanism effects, additional baselines are tested: DP, which adds Gaussian noise without encryption, and MPC, which applies segmented encryption and secret sharing without noise. The proposed method combines both under the same federated settings. All models share identical architectures, training strategies, and data partitions. Accuracy in Figure 6 reflects the proportion of correct predictions on the fixed test set used in Section experimental design and analysis and measures how well each method maintains task performance under increasing attack intensity. This experiment focuses on integrity-oriented model-poisoning

attacks rather than privacy inference attacks, and evaluates robustness instead of information leakage.

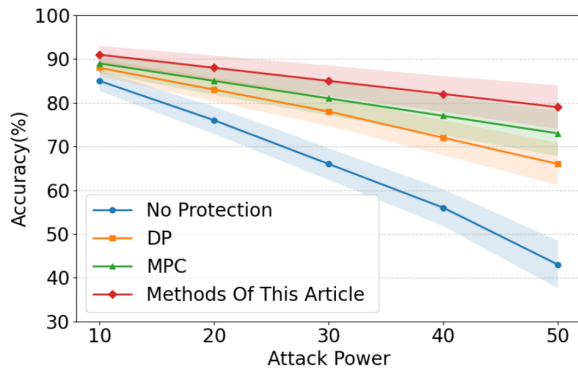


FIGURE 6. Comparison of attack defense effects under the robustness under poisoning attacks mechanism

At 50% attack intensity, the results of applying the unprotected model show a loss of accuracy, dropping to 43% accuracy. DP and MPC produce results of 66% and 73%, respectively, while the proposed method produces the best result, achieving 79% accuracy. DP reduces the effects of individual malicious updates by preventing these updates from integrating with the training data. As a result, with continued training of the model over time through using this approach, the accuracy level drops over time due to the accumulation of the errors introduced by these malicious updates. With MPC, the impact of the abnormal gradients is restricted during the aggregation process, which is what leads to the associated increase in resistance that an aggregation-based approach to DP can provide. The combined method of DP and MPC produces both complementary effects of preventing interference by the injected gradients, while at the same time, preventing secondary leakage to other nodes during the aggregation process, ultimately producing superior overall resistance of these approaches when subjected to high attack intensity levels.

IV. CONCLUSION

This study constructs a federated-learning-based English skills training platform for textile enterprises. Differential privacy and secure multi-party computation are adopted to protect local data, while textile enterprises collaborate across enterprises. The experimental results demonstrate that the distributed modeling performance of the platform is enhanced: when compared with FedAvg (0.2290 at the 44th round) and local training (0.3591 at the 44th round), the loss reaches 0.1619 at the 44th round under mean squared error evaluation, which demonstrates that the platform has better convergence stability. When compared with DP and MPC under fifty-percent attack intensity, the platform achieves 79 percent accuracy, outperforming MPC at 73 percent and DP at 66 percent, demonstrating stronger robustness under combined protection. The skill improvement of the platform

is derived from model-guided adaptive instruction, and the secure model updating process of the federated process ensures the security of model updating instead of learning gain. However, the scalability of the platform is limited by communication overhead and encryption complexity. The privacy budget and secret-sharing configuration do not have cross-scenario adaptability. In future work, adaptive privacy mechanism and lightweight secure computation combined with transfer and reinforcement learning can be explored to improve scalability in large and heterogeneous settings.

AUTHOR CONTRIBUTIONS

Gong Jian designed, collected and analyzed the data, and drafted the manuscript. Gong Jian conducted the study, critically revised the manuscript for important intellectual content, and gave final approval of the version to be published. Gong Jian participated fully in the work, take public responsibility for appropriate portions of the content, and agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

FUNDING

This research received no external funding.

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

- [1] D. A. A. Ismail and L. S. Pek, "The Impact of English Language on Business Communication in Asia: A Scoping Review," *LSP International Journal*, vol. 10, no. 1, pp. 91-102, 2023, doi: 10.11113/lspi.v10.19583.
- [2] A. M. Abro, A. R. Bhutto, I. Mughal, F. Abro, and S. S. Shaikh, "Exploring the impact of English language proficiency on business communication effectiveness: A comprehensive research analysis," *ProScholar Insights*, vol. 4, no. 1, pp. 18-27, 2025, doi: 10.62997/psi.2025a-41028.
- [3] G. O. Mbah, "Data privacy in the era of AI: Navigating regulatory landscapes for global businesses," *Int. J. Sci. Res. Anal.*, vol. 13, no. 2, pp. 2396-2405, 2024, doi: 10.30574/ijrsra.2024.13.2.2396.
- [4] T. Liu, Z. Wang, H. He, W. Shi, L. Lin, R. An, et al., "Efficient and secure federated learning for financial applications," *Applied Sciences*, vol. 13, no. 10, pp. 5877, 2023, doi: 10.3390/app13105877.
- [5] T. Kuo and H. Yang, "Federated learning on distributed and encrypted data for smart manufacturing," *Journal of Computing and Information Science in Engineering*, vol. 24, no. 7, pp. 071007, 2024, doi: 10.1115/1.4065571.
- [6] L. Theodorakopoulos, A. Theodoropoulou, and Y. Stamatiou, "A state-of-the-art review in big data management engineering: Real-life case studies, challenges, and future research directions," *Eng.*, vol. 5, no. 3, pp. 1266-1297, 2024, doi: 10.3390/eng5030068.
- [7] X. Jiang, W. Liu, and B. Dong, "FedRisk A Federated Learning Framework for Multi-institutional Financial Risk Assessment on Cloud Platforms," *Journal of Advanced Computing Systems*, vol. 4, no. 11, pp. 56-72, 2024, doi: 10.69987/JACS.2024.41105.
- [8] W. Miao, X. Zhao, Y. Zhang, S. Chen, X. Li, and Q. Li, "A Deep Learning-Based method for preventing data leakage in electric power industrial internet of things business data interactions," *Sensors*, vol. 24, no. 13, pp. 4069, 2024, doi: 10.3390/s24134069.

- [9] J. Chen, J. Xue, Y. Wang, L. Huang, T. Baker, and Z. Zhou, "Privacy-preserving and traceable federated learning for data sharing in industrial IoT applications," *Expert Systems with Applications*, vol. 213, pp. 119036, 2023, doi: 10.1016/j.eswa.2022.119036.
- [10] B. Zhu and L. Niu, "Dynamic memory-enhanced federated learning framework with trusted computing for multi-source data analysis," *Journal of Intelligent Information Systems*, vol. 63, no. 3, pp. 1011-1032, 2025, doi: 10.1007/s10844-025-00927-7.
- [11] L. Fang, L. Wang, and H. Li, "Iterative and mixed-spaces image gradient inversion attack in federated learning," *Cybersecurity*, vol. 7, no. 1, pp. 35, 2024, doi: 10.1186/s42400-024-00227-7.
- [12] K. Tayyeh H and A. AL-Jumaili A S, "Balancing privacy and performance: a differential privacy approach in federated learning," *Computers*, vol. 13, no. 11, pp. 277, 2024, doi: 10.3390/computers13110277.
- [13] C. Liu, Y. Tian, J. Tang, S. Dang, and G. Chen, "A novel local differential privacy federated learning under multiparty regimes," *Expert systems with applications*, vol. 227, pp. 120266, 2023, doi: 10.1016/j.eswa.2023.120266.
- [14] D. Liu, G. Yu, Z. Zhong, and Y. Song, "Secure multi-party computation with secret sharing for real-time data aggregation in IIoT," *Computer Communications*, vol. 224, pp. 159-168, 2024, doi: 10.1016/j.comcom.2024.06.002.
- [15] I. Gamiz, C. Regueiro, O. Lage, E. Jacob, and J. Astorga, "Challenges and future research directions in secure multiparty computation for resource-constrained devices and large-scale computations," *International Journal of Information Security*, vol. 24, no. 1, pp. 27, 2025, doi: 10.1007/s10207-024-00939-4.
- [16] Z. Li, Z. Hou, H. Liu, Y. Wang, T. Li, L. Xie, et al., "Federated Learning in Big Model Era: Domain-Specific Multimodal Large Models," *arXiv e-prints*, vol. 2308, pp. 11217-11226, 2023, doi: 10.48550/arXiv.2308.11217.
- [17] X. Cao, Z. Li, G. Sun, H. Yu, and M. Guizani, "Cross-silo heterogeneous model federated multitask learning," *Knowledge-Based Systems*, vol. 265, pp. 110347, 2023, doi: 10.1016/j.knsys.2023.110347.
- [18] Y. He, D. Yan, and F. Chen, "Hierarchical federated learning with local model embedding," *Engineering Applications of Artificial Intelligence*, vol. 123, pp. 106148, 2023, doi: 10.1016/j.engappai.2023.106148.
- [19] C. Xu, Z. Hong, M. Huang, and T. Jiang, "Acceleration of Federated Learning with Alleviated Forgetting in Local Training," *arXiv e-prints*, vol. 2203, pp. 02645-02663, 2022, doi: 10.48550/arXiv.2203.02645.
- [20] Z. Li, T. Lin, X. Shang, and C. Wu, "Revisiting Weighted Aggregation in Federated Learning with Neural Networks," *arXiv e-prints*, vol. 2302, pp. 10911, 2023, doi: 10.48550/arXiv.2302.10911.
- [21] Y. Hu, H. Ren, C. Hu, J. Deng, and X. Xie, "An Element-Wise Weights Aggregation Method for Federated Learning," *arXiv e-prints*, vol. 2404, pp. 15919, 2024, doi: 10.48550/arXiv.2404.15919.
- [22] K. Hu, S. Gong, Q. Zhang, and C. Seng, "An overview of implementing security and privacy in federated learning," *Artificial intelligence review*, vol. 57, no. 8, pp. 204, 2024, doi: 10.1007/s10462-024-10846-8.
- [23] J. Ling, J. Zheng, and J. Chen, "Efficient federated learning privacy preservation method with heterogeneous differential privacy," *Computers & Security*, vol. 139, pp. 103715, 2024, doi: 10.1016/j.cose.2024.103715.
- [24] H. Hu, X. Zhang, Z. Salic, L. Sun, K. K. R. Choo, and G. Dobbie, "Source inference attacks: Beyond membership inference attacks in federated learning," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 3012-3029, 2023, doi: 10.1109/TDSC.2023.3321565.
- [25] J. Sun, Y. Yan, Z. Wang, J. Ma, and Y. Wang, "Privacy-preserving coordinated operation of cross-enterprise data centers," *Applied Energy*, vol. 383, pp. 125343, 2025, doi: 10.1016/j.apenergy.2025.125343.
- [26] X. Wu, Y. Chen, H. Yu, and Z. Yang, "Privacy-preserving federated learning based on noise addition," *Expert Systems with Applications*, vol. 267, pp. 126228, 2025, doi: 10.1016/j.eswa.2024.126228.
- [27] S. Yang, H. Park, J. Byun, and C. Kim, "Robust federated learning with noisy labels," *IEEE Intelligent Systems*, vol. 37, no. 2, pp. 35-43, 2022, doi: 10.1109/MIS.2022.3151466.
- [28] H. Zhang, H. Huang, and C. Peng, "A novel user behavior modeling scheme for edge devices with dynamic privacy budget allocation," *Electronics*, vol. 14, no. 5, pp. 954, 2025.
- [29] S. Su, Y. Luo, T. Li, Q. Chen, and J. Liang, "Anti-Leakage Method of Sensitive Information of Network Documents Based on Differential Privacy Model," *Security and Privacy*, vol. 8, no. 1, pp. e491, 2025, doi: 10.1002/spy2.491.
- [30] R. Xue, K. Xue, B. Zhu, X. Luo, T. Zhang, and Q. Sun, "Differentially private federated learning with an adaptive noise mechanism," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 74-87, 2023, doi: 10.1109/TIFS.2023.3318944.
- [31] S. Weng, Y. Gou, L. Zhang, and M. A. Imra, "Evaluating privacy loss in differential privacy based federated learning," *Future Generation Computer Systems*, vol. 172, pp. 107848, 2025, doi: 10.1016/j.future.2025.107848.
- [32] R. Kanagavelu, Q. Wei, Z. Li, H. Zhang, J. Samsudin, Y. Yang, et al., "CE-Fed: Communication efficient multiparty computation enabled federated learning," *Array*, vol. 15, pp. 100207, 2022, doi: 10.1016/j.array.2022.100207.
- [33] F. Liu, Z. Zheng, Y. Shi, Y. Tong, and Y. Zhang, "A survey on federated learning: a perspective from multi-party computation," *Frontiers of Computer Science*, vol. 18, no. 1, pp. 181336, 2024, doi: 10.1007/s11704-023-3282-7.
- [34] C. Shen, W. Zhang, T. Zhou, and L. Zhang, "A security-enhanced federated learning scheme based on homomorphic encryption and secret sharing," *Mathematics*, vol. 12, no. 13, pp. 1993, 2024, doi: 10.3390/math12131993.
- [35] X. Shen, X. Luo, F. Yuan, B. Wang, Y. Chen, and D. Tang, "Verifiable privacy-preserving federated learning under multiple encrypted keys," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 3430-3445, 2023, doi: 10.1109/IJOT.2023.3296637.