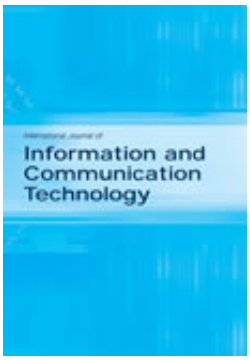


International Journal of Information and Communication Technology

ISSN online: 1741-8070 - ISSN print: 1466-6642
https://www.inderscience.com/ijict

Analysis of social English learning behaviour based on federated knowledge graph and privacy preservation

Gang Shen, Tao Feng

DOI: 10.1504/IJICT.2025.10071990

Article History:

Received:	14 May 2025
Last revised:	25 May 2025
Accepted:	25 May 2025
Published online:	16 July 2025

Analysis of social English learning behaviour based on federated knowledge graph and privacy preservation

Gang Shen* and Tao Feng

School of Foreign Studies,
Suqian University,
Suqian 223800, China
Email: sqshen2025@126.com
Email: fengtaosq2025@126.com
*Corresponding author

Abstract: Social learning platforms provide a dynamic interactive and individualised learning experience as artificial intelligence in education is increasingly used. Though they have data privacy and AI security issues, these services gather a great amount user data. Releasing user data such as voice calls, text messages, social connections, and learning preferences could cause privacy issues. This paper presents FL-KGPrivacyEdu, a federated knowledge graph model combining federated learning (FL) and knowledge graph (KG) to address the problem of behavioural modelling and privacy preservation in social English learning. The methodology examines social learning across platforms and terminals while safeguarding data. Experimental validation demonstrates that the model is successful and superior in social English learning behaviour analysis in accuracy, recall, and F1 score. This study also looks at how model convergence, a major model training reference, is affected by learning rate modification in worldwide rounds.

Keywords: federated learning; FL; knowledge graph; KG; federated knowledge graph; data privacy protection; AI security.

Reference to this paper should be made as follows: Shen, G. and Feng, T. (2025) 'Analysis of social English learning behaviour based on federated knowledge graph and privacy preservation', *Int. J. Information and Communication Technology*, Vol. 26, No. 26, pp.68–86.

Biographical notes: Gang Shen obtained his PhD in English Linguistics from the University of Laissem in the Philippines in 2023. He is currently an Associate Professor at the School of Foreign Languages, Suqian University. His research interests include English applied linguistics and college English.

Tao Feng obtained her Master's in Linguistics and Applied Linguistics from the Henan University in 2009. She is currently an Associate Professor at the School of Foreign Languages, Suqian University. Her research interests include second language acquisition and English education.

1 Introduction

Social learning systems like WeChat Group Classroom, Learning Social APP, and Xiaohongshu Learning Circle offer students a rich interactive and tailored learning experience in line with the growing use of artificial intelligence technology in education. By combining several interaction techniques like voice, video, discussion groups, and shared materials, these platforms have significantly enhanced the learning experience of students (Dahlan et al., 2023). But, even as they gather a lot of user data, these systems struggle greatly with artificial intelligence security and data privacy. User data includes sensitive material like voice exchanges, text conversations, social ties, and learning preferences; leaking this information could cause major privacy concerns. There are also risks to the integrity and dependability of artificial intelligence models from hostile client attacks, data poisoning, etc. which could compromise their accuracy and credibility (Aljanabi, 2023).

AI security is the safeguarding of AI systems against several attacks and hazards to guarantee their correct functioning and data privacy (Binhammad et al., 2024). Two fundamental concerns in AI-driven systems are data privacy and model security. While model security is more about stopping AI models from being hostilely attacked or altered, data privacy is about safeguarding user data from disclosure or misuse. Data privacy and artificial intelligence security in the education industry have come under more scrutiny in recent years as data privacy rules like the European Union's General Data Protection Regulation (GDPR) have grown more severe (Bharti and Aryal, 2023). The question of how to effectively model learning behaviours while guaranteeing privacy has become hot in the area of smart education (Alexuta et al., 2025). Furthermore, the security of artificial intelligence systems not only influences the user experience but also might significantly effect societal trust and educational equity (Balas et al., 2013).

FL, a distributed machine learning framework, successfully protects the privacy of user data by training models and distributing updated model parameters on local devices, therefore avoiding centralised data storage (Liu et al., 2022). This solution not only improves the security of artificial intelligence but also satisfies the needs of data protection laws. Still, even with FL's notable advancements in privacy protection, certain possible security concerns remain, including data poisoning and hostile client attacks.

As a strong semantic modelling tool, KG can efficiently express and examine social relationships and complex learning patterns. Constructing KG allows for systematic representation of information such social ties, resources, and learner behaviours to assist individualised recommendation and learning behaviour analysis (Lv et al., 2021). Most of the conventional KG building techniques, therefore, depend on centralised data processing, which struggles with data sharing and privacy protection in cross-platform and multi-source heterogeneous data settings.

This paper presents a federated knowledge graph (KG) combining federated learning (FL) and KG to address the issue of behaviour modelling and privacy protection in social English learning, which not only ensures data privacy but also efficiently analyses social learning behaviours across several platforms and terminals.

2 Related work

Social English learning has slowly become a key component of language learning in recent years as online education has developed quickly. By including voice, video, discussion groups, shared resources and other interaction techniques, social learning platforms have significantly enhanced the learning experience of students. These platforms have gathered a great deal of user behaviour data, and using this data for smart analysis has attracted much interest among researchers. These data, however, include a great deal of private information, such as voice exchanges, text conversations, social contacts, and learning preferences, which creates major data protection issues and AI security concerns (Winter and Davidson, 2019).

Traditional behavioural analytics techniques mostly depend on manually engineered features to conduct analysis and modelling (e.g., K-means clustering, support vector machines, and decision trees). These techniques are challenging to manage complicated unstructured data, such as video material, social interactions, and speech data since they mostly depend on manual feature engineering, which demands clear extraction of user behaviours (Adnan and Akbar, 2019). Furthermore, conventional algorithms find it challenging to fit to many learning modes as learner behaviour becomes more varied, and they cannot thoroughly examine the individual requirements of students or the influence of social learning interactions.

Deep learning techniques are being progressively integrated into the domain of social learning behaviour analysis to surpass the constraints of conventional approaches. Processing time-series data has been dominated in recent years by recurrent neural networks (RNN) and long short-term memory networks (LSTM). LSTM, in particular, is able to capture long-term temporal relationships via the memory mechanism when examining learners' learning paths, learning progress and behavioural feedback, hence, offering a more strong modelling capability than conventional machine learning techniques (Ahmed et al., 2023). Though deep learning offers significant promise in learning behaviour analysis, it still has certain issues. First, deep learning models often need a lot of data for training, which presents a major difficulty for the education sector because data silos are significant. Second, social learning behaviour data usually includes several platforms and endpoints; how to properly combine user behaviour data from several sources is still an unsolved issue.

The question of privacy protection has always been a major difficulty in educational data analytics. A commonly used privacy-preserving technique, differential privacy (DP), prevents the revelation of any individual user's information by means of data noise addition (Gong et al., 2020). DP often affects the accuracy of the analytic findings, particularly with little data volume; adding noise could cause the loss of important information. Encrypted computation, such as homomorphic encryption (HE) and secure multi-party computation (SMC), is another method that lets encrypted data run calculations, hence, preventing direct disclosure of user data. These encryption techniques, on the other hand, frequently have significant computational overhead and poor efficiency, which makes their effective use in practical applications problematic (Thavamani and Rengarajan, 2024).

By training models and distributing updated model parameters on local devices, FL, an AI privacy-preserving approach, can efficiently prevent centralised data storage and hence, safeguard user privacy. Though FL has produced outstanding outcomes in many domains, its use in social learning behaviour analysis is still in its early stages,

particularly with regard to building high-quality learning behaviour models in dispersed settings, which currently requires adequate study. Meanwhile, as a means of expressing entities and their interactions, KG has been used in education, particularly in customised recommendation and learning behaviour analysis. Most of the current KG building techniques, therefore, depend on centralised data processing, which complicates the issues of data sharing and privacy protection when used in cross-platform and multi-source heterogeneous data settings.

This work offers a federated KG model built on the combination of FL and KG to solve these problems, hence, safeguarding students' privacy and security in social English learning practices. In particular, the developments of this work are as follows:

1 Combination of FL and KG: the paper offers a novel model that both examines social learning patterns and safeguards user privacy by use of FL and KG technologies. This combination uses the dispersed character of FL to prevent centralised data storage, hence, efficiently safeguarding user AI data security.

2 Model evaluation and security safeguards: proposed is a model evaluation framework to assess model performance with measures including accuracy, recall and F1 score. Security measures like SMPC are being added to guarantee that user data is safely exchanged across several ends.

3 Research on the effect of learning rate adjustment on model convergence in global rounds: the impact of changing learning rate on model convergence in global rounds is investigated, hence, offering a significant reference for model training. This study not only offers a fresh approach for AI security but also helps to maximise the model training process.

3 Theoretical foundation

3.1 FL and privacy preserving technologies

As a developing distributed machine learning technique, FL can efficiently safeguard data privacy by means of multi-party cooperation for model training without disclosing raw data. FL framework allows each device to keep local data exclusively; training and model updates are also done locally; finally, global model optimisation is accomplished by aggregating model parameters (Zhang et al., 2022). This method assures the privacy of user data and hence, eliminates centralised storage and processing of data.

Assuming there are N clients, (e.g., user devices) and each client i has a local dataset D_i, D_i can be written as follows by setting the model parameter as θ:

$$D_i = \left\{\left(x_i^{(j)}, y_i^{(j)}\right)\right\}_{j=1}^{n_i} \tag{1}$$

where the j^{th} data point's input features and labels are $x_i^{(j)}$ and $y_i^{(j)}$ respectively. Based on the local data D_i, each client trains a local model and minimises the loss using the following objective function:

$$L_i(\theta) = \frac{1}{n_i}\sum_{j=1}^{n_i} \ell\left(f\left(x_i^{(j)}, \theta\right) y_i^{(j)}\right) \tag{2}$$

where $\ell(\cdot)$ is the loss function and $f(\cdot, \theta)$ is the prediction function of the model.

FL prevents privacy leakage by trading model parameters rather than raw data. In particular, client i calculates the local gradient and transmits its modified model parameters θ_i^{new} to the server for aggregation. Using the next update formula, the server compiles each client's changes to produce the global model θ_{global}:

$$\theta_{\text{global}} = \sum_{i=1}^{N} \frac{n_i}{n_{total}} \theta_i^{\text{new}} \tag{3}$$

$$n_{\text{total}} = \sum_{i=1}^{N} n_i \tag{4}$$

where n_{total} is the total data from all clients and $\frac{n_i}{n_{\text{total}}}$ is the weight of client i.

A simulation experiment run via a straightforward linear regression model helps to more intuitively demonstrate the changes of model parameters during the FL process (Hassan et al., 2023). During 50 rounds of FL, Figure 1 depicts the evolution of the model parameters θ.

Figure 1 Variation of the model parameter θ during the FL process (see online version for colours)

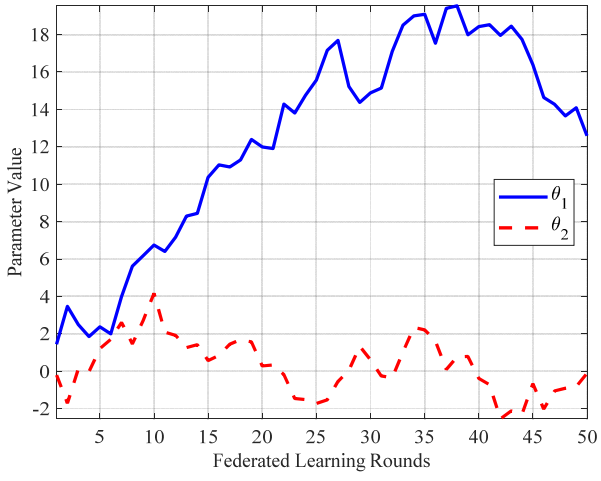


Figure 1 show that the model parameters θ_1 and θ_2 progressively tend to stabilise after undergoing early oscillations as FL rounds rise. Specifically, the values of the parameter θ_1 exhibit a distinct rising trend; those of the parameter θ_2 vary within a narrow range. Though the parameters in the first stage vary greatly, the model eventually converges as learning progresses, demonstrating the efficacy and resilience of FL in handling scattered data.

Though FL efficiently safeguards data privacy, especially during the transfer of model parameters and gradient information, there is still some danger of privacy leakage. Many methods, like DP and HE, are added into FL to help more privacy protection.

By adding noise, DP is a mathematical protective tool that renders the private data of one person unguessable from query results. By disturbing the gradient, DP generates

more noise and hence, lowers the danger of disclosing sensitive information (Tsou et al., 2019). In particular, the change following noise addition can be stated as:

$$\tilde{\theta}_i^{\text{new}} = \theta_i^{\text{new}} + N\left(0, \sigma^2\right) \tag{5}$$

where $N(0, \sigma^2)$ indicates the noise extracted from a Gaussian distribution with mean 0 and variance σ^2.

HE is an encryption technique that may run calculations in a ciphertext state without decrypting the data, hence, providing better privacy protection (Yang et al., 2020). Setting the ciphertext $c(\theta)$ as the encrypted value of the model parameter θ and the encrypted gradient update can be stated as follows:

$$c\left(\tilde{g}(\theta)\right) = \varepsilon(g(\theta)) \circ \varepsilon\left(g'(\theta)\right) \tag{6}$$

where $\varepsilon(\cdot)$ is the encryption function and $\circ$ indicates the operation under encryption.

Many elements also influence FL's efficiency and model quality. For instance, client diversity could cause data imbalance throughout the training phase, therefore influencing the performance of the global model (Thabtah et al., 2020). Therefore, the researchers suggested the weighted average approach to offset the contributions of several customers to the global model by giving each one varying weight. Assuming client i's weight is α_i and the weighted average update formula is:

$$\theta_{\text{global}} = \sum_{i=1}^{N} \alpha_i \theta_i^{\text{new}} \tag{7}$$

$$\sum\nolimits_{i=1}^{N} \alpha_i = 1 \quad \alpha_i \geq 0 \tag{8}$$

FL additionally faces significant difficulty from the communication overhead as well. The researchers suggest model compression strategies to lower the number of model parameters uploaded in every training round, therefore lessening the communication strain. Model compression aims to show the updated compressed model by the next compression function $C(\theta)$:

$$\hat{\theta}_i = C\left(\theta_i\right) \tag{9}$$

where $\hat{\theta}_i$ is the compressed model parameters; $C(\cdot)$ the compression function.

FL is able to better fit the needs in the investigation of social English learning behaviours by constantly optimising the model update and communication tactics, thereby preserving anonymity.

3.2 KGs and social learning behaviour modelling

KG can assist in structuring the depiction of students and their behaviours, resources, social connections and other data in modelling social learning behaviours see Figure 2.

Specifically, triples which denoted as (h, r, t), where h is the head entity, r is the relationship, and t is the tail entity are the fundamental building blocks of KG (Ji et al., 2021). Building these triples helps to properly capture the links between learning behaviours and learner interactions. For students of English, these organisations might be the students themselves, learning materials, social groups, interactive behaviours, etc.

relationships could include engagement in learning, sharing resources, learning preferences, etc.

The learner behaviour dataset D can be stated as follows:

$$D = \left\{ h^{(i)}, r^{(i)}, t^{(i)} \right\}_{i=1}^{n} \tag{10}$$

where n is the complete triad count in the dataset. Every learner's learning behaviour will be shaped into various triples depending on their social interactions and learning process during the construction of KG. For instance, a student h might have shared a particular learning resource via his interactions with other students, hence, creating the triad (h, shared resource, r), where r is the particular material of that resource from which a complete learner behaviour network could be built.

The variability and complexity of the data, however, is one of the main difficulties KG in modelling social learning activities. Data about learning behaviour from social learning platforms originates from many learning endpoints and platforms, which could have varied formats, dimensions, and characteristics. Thus, a key question in present study is how to properly combine these various data into a single KG framework (Garousi Mokhtarzadeh et al., 2020). A frequent approach is to use KG alignment method to map and align the data from several platforms so they may coexist in a single graph structure. For instance, by matching the mapping function f such that the triples (h_1, r_1, t_1) of platform 1 correspond to the triples (h_2, r_2, t_2) of platform 2, two datasets D_1 and D_2 with different platforms are configured to attain consistency in the global mapping. Mapping may be described as follows:

$$f\left(h_1, r_1, t_1\right) = \left(h_2, r_2, t_2\right) \tag{11}$$

Furthermore, the building and maintenance of KG gets increasingly difficult as the volume of data on social learning behaviours keeps rising. The researchers suggested a graph building technique using dynamic updating and incremental learning to address this issue. Keeping the graph updated and correct, incremental updating allows the graph to be constantly optimised and enlarged with the inclusion of new data. The dynamic updating approach allows for the following inclusion of new learner behaviours into the atlas:

$$KG_{\text{new}} = KG_{\text{old}} \cup \left\{ \left(h_{\text{new}}, r_{\text{new}}, t_{\text{new}} \right) \right\} \tag{12}$$

where KG_{new} is the modified graph with the new behaviour and KG_{old} is the old KG.

In social learning behaviour modelling, KG not only represents learners' behavioural links but also helps individualised recommendation systems (Zhang et al., 2021). For instance, by determining the similarity between students, learning materials fitting their interests could be suggested for students. Let the similarity metrics of learner h_1 and learner h_2 in KG be:

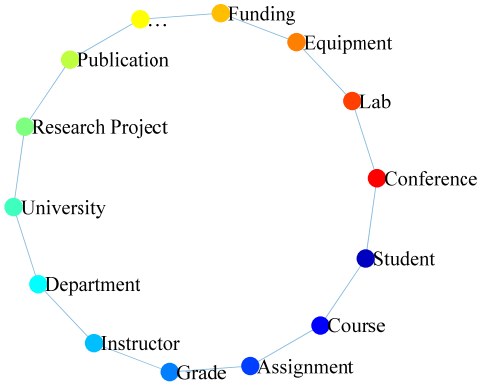
$$\text{Sim}\left(h_1, h_2\right) = \frac{1}{1 + d\left(h_1, h_2\right)} \tag{13}$$

where $d(h_1, h_2)$ is a measure of the distance between learners h_1 and h_2 in KG.

All things considered, the use of KG in social learning behaviour modelling can offer significant assistance for learner behaviour analysis and tailored recommendation. A better knowledge of students' learning process and social interaction patterns is made

possible by the systematic depiction of their activities, hence, offering efficient data support for customised instruction and resource recommendation on educational platforms.

Figure 2 Example of the structure of KG (see online version for colours)



4 A model for analysing social English learning behaviour: FL-KGPrivacyEdu

This chapter will cover in depth the design and execution of the FL-KGPrivacyEdu based paradigm. The approach guarantees the privacy and security of user data by increasing the AI security mechanism and combines FL; KG and privacy protection technologies to overcome the constraints of the conventional centralised data model see Figure 3.

The FL-KGPrivacyEdu model is meant to have the following fundamental components:

4.1 Federated KG module

Combining FL with KG, the federated KG module creates an AI-secure system that safeguards learner privacy and maximises learning behaviour analysis in a social English learning context. Specifically, the loss function may be stated as follows assuming the local model training of the i^{th} learner is based on learning behaviour data:

$$L_i(\theta_i) = \sum_{j=1}^{M_i} \left(y_j - f(x_j, \theta_i)\right)^2 \tag{14}$$

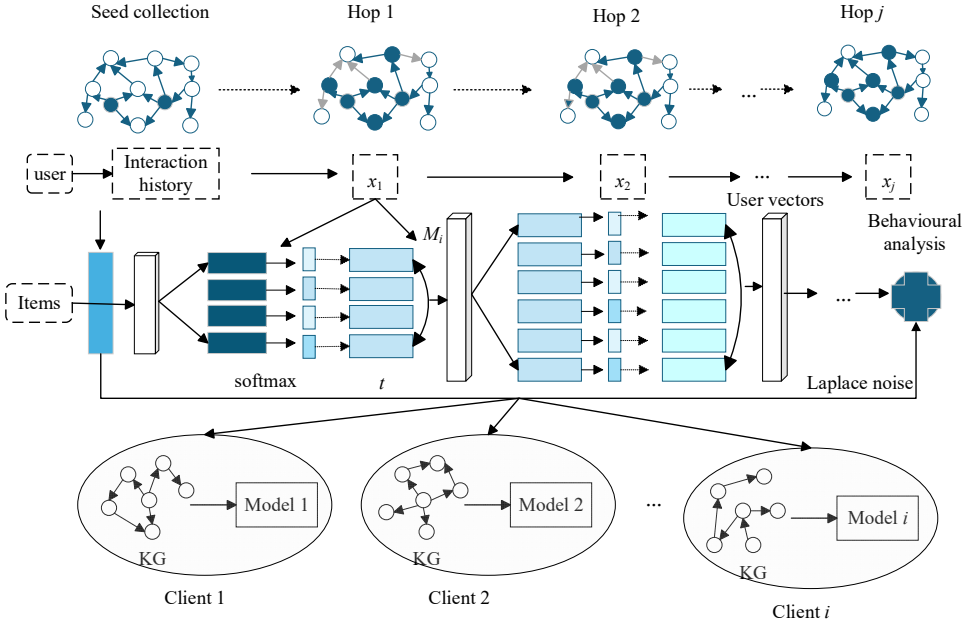
where x_j is the feature data, (e.g., word memory, grammar correction, etc.) gathered by the i^{th} learner in the j^{th} learning, y_j is the true value, θ_i is the local model parameter, and M_i is the number of data points of the i^{th} learner.

The local model parameters are obtained by each learner optimising the loss function at the local terminal (Chen et al., 2021). The model parameter updating formula is:

$$\theta_i^{t+1} = \theta_i^t - \eta \nabla L_i\left(\theta_i^t\right) \tag{15}$$

where $\nabla L_i(\theta_i^t)$ is the gradient of the local loss function and η is the learning rate.

Figure 3 FL-KGPrivacyEdu model architecture (see online version for colours)



Apart from changing the learner's model, the local terminal builds a personal KG using the learning behaviour data. Every learner's KG is made up of nodes V_i and edges E_i; nodes represent the learning material, for example, words, sentence patterns, grammar rules, etc. edges represent the links between nodes, for example, mastery, erroneous use, or correction. The local KG will be updated following the learning behaviour data after each learning; the KG update formula is as follows:

$$G_i^{t+1} = G_i^t \cup \Delta G_i \tag{16}$$

where ΔG_i indicates the knowledge points added or changed throughout this learning. Reflecting their knowledge of English learning material and social interactions with other students, each learning session will gradually increase and optimise learners' KG. By means of this technique, the student progressively improves his or her learning model and guarantees confidentiality.

The global model and global KG will be updated by weighted average of the local model parameters and KG of all endpoints gathered via the federated KG. One way to show the updating of the global KG is as follows:

$$G_i^{t+1} = \sum_{i=1}^{N} w_i G_i^t \tag{17}$$

where G_i^t is the local graph of the i^{th} terminal and w_i is the weight of the i^{th} terminal, often proportionate to its data capacity. Ultimately, the learning behaviour data in the

complete social English learning environment will create a global KG, which offers strong support for behaviour analysis and tailored learning advice.

4.2 Privacy protection module

Privacy protection in the FL-KGPrivacyEdu concept permeates the building and maintenance of the federated KG. Privacy-preserving strategies are required to guarantee data security in social English learning situations since learners' behavioural data typically include sensitive material (Viberg et al., 2022).

First, students' local data is processed and updated on their devices and uploaded via encryption to safeguard the privacy of the original data; the encrypted graph is updated as:

$$Enc\left(G_i^{t+1}\right) = \varepsilon\left(G_i^{t+1}\right) \tag{18}$$

where ε is the encryption process. The original data cannot be retrieved immediately post encryption.

The server then compiles all devices' encrypted updates next. The server simply aggregates the encrypted data throughout the aggregation process; it does not include the original information. Global mapping update is the process of

$$G^{t+1} = \sum_{i=1}^{N} w_i D\left(Enc\left(G_i^{t+1}\right)\right) \tag{19}$$

where D being the decryption process, w_i the weight of every student, and N the number of learning devices engaged. The server just calculates the encrypted data.

Second, the DP approach is used to the KG updating process to help ensure privacy even further. When the learner locally builds the graph, noise is added to the graph update, hence, preventing revealing personal information. The update following noise addition is:

$$\hat{G}_i^{t+1} = G_i^{t+1} + N\left(\mu, \sigma^2\right) \tag{20}$$

where $N(\mu, \sigma^2)$ indicates additive noise to guarantee data protection.

DP is also used, finally, in the aggregation of worldwide KG. The global graph's updating formula is:

$$\hat{G}^{t+1} = \sum_{i=1}^{N} w_i \left(G_i^{t+1} + N\left(\mu, \sigma^2\right)\right) \tag{21}$$

The FL-KGPrivacyEdu approach can create high-quality maps of social English learning behaviours and offer precise support for individualised learning while guaranteeing privacy with these privacy measures.

4.3 Learning behaviour analysis and recommendation module

By examining students' behavioural data and merging it with the built federated knowledge network, this module offers tailored learning material suggestion. To produce

personal behavioural vectors B_i, the learner's behavioural data is gathered and analysed on the local device:

$$B_i = \{b_1, b_2, ..., b_k\} \tag{22}$$

These behavioural data can fully represent the learner's learning habits and preferences since they include multi-dimensional information such as learning length, interaction frequency, question-answer scenario, etc. (Pérez-Paredes and Mark, 2024). The model builds the learner's behavioural model M_i from the behavioural data:

$$M_i = f(B_i, KG_i) \tag{23}$$

where f is a synthesis function capable of producing the user's behavioural feature models by combining the behavioural data with the semantic KG information. These behavioural models are updated locally and then sent to the server for global aggregate. The FL framework's global model update formula is:

$$M^{global} = \sum_{i=1}^{N} w_i \cdot M_i \tag{24}$$

Every learner's behavioural model M_i is weighted and updated throughout the global aggregation phase depending on their local device learning behaviour, therefore producing a worldwide shared learning behavioural model M^{global}. As the learner's personal data is not sent directly to the server but rather exchanged via encrypted model parameters, this method efficiently safeguards user privacy.

4.4 Model evaluation and safety assurance module

First, standard assessment metrics are used in model performance evaluation to gauge the efficacy of the model in social English learning behaviour analysis. The major measures are accuracy, recall and F1 value, which can indicate the predictive power of the recommendation system on learner behaviour (Cui et al., 2024). Assuming T is the test set, P_i the prediction result and G_i the actual label, thus the evaluation formula is as follows:

$$\text{Accuracy} = \frac{1}{|T|} \sum_{i \in T} 1(P_i = G_i) \tag{25}$$

$$\text{Recall} = \frac{\sum_{i \in T} 1(P_i = 1 \cap G_i = 1)}{\sum_{i \in T} 1(G_i = 1)} \tag{26}$$

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{27}$$

where $1(\cdot)$ is the indicator function, which shows whether the prediction is true or not, and precision is the accuracy, defined as the fraction of samples where the prediction is positive that are actually positive. These metrics can evaluate the accuracy of social learning behaviour prediction, therefore maximising the individualised recommendation impact of the model.

Second, social English learning behaviour analysis particularly benefits from artificial intelligence security guarantee (Liang et al., 2021). DP protects users' learning behaviour data by introducing noise to the uploaded model parameters with the following formula:

$$\epsilon\text{-}DP:\Pr[A(D)\in S]\le e^{\epsilon}\cdot\Pr[A(D')\in S] \tag{28}$$

This approach may efficiently stop the reverse inference of single user data, hence, ensuring the privacy of social learning activities.

SMPC guarantees data security by allowing several learning ends to work together to train models without revealing personal data (Zhao et al., 2019). SMPC's computational procedure is as follows:

$$\text{SecureComputation}\left(\{P_1, P_2, ..., P_n\}\right)\to R \tag{29}$$

This system guarantees that the data on the user's AI learning behaviour can be safely transmitted across several endpoints without revealing sensitive information.

By means of four modules, the FL-KGPrivacyEdu model guarantees artificial intelligence security and allows social English learning behaviour study. The federated KG module creates a learner behavioural graph; the privacy protection module guarantees data security using methods including DP; the learning behaviour analysis and recommendation module offers tailored recommendations; and the model evaluation and safety assurance module enhances security. Working together, the four components provide the intelligence and privacy protection of learning analytics.

5 Experiments and results

5.1 Experimental data

This work used the KT3 dataset from the EdNet dataset as experimental data. The KT3 dataset's specifics are shown in Table 1.

Table 1 Details of the EdNet KT3 dataset

Field name	*Data type*	*Description*	*Example values*
action_type	String	Type of interaction, e.g., 'enter', 'respond', 'submit'	'enter', 'respond', 'submit'
item_id	String	ID of the item involved in the interaction	'b790', 'l540', 'q878'
source	String	Source of the interaction, e.g., 'diagnosis', 'sprint'	'diagnosis', 'sprint', 'todays_recommendation'
user_answer	Character	Student's submitted answer	'a', 'b', 'c', 'd'
platform	String	Platform where the interaction occurred	'mobile', 'web'
cursor_time	Timestamp	The moment the student interacted with media	0, 8,000, 10,000
elapsed_time	Timestamp	Time spent on each question in milliseconds	47,000, 54,000, 67,000

5.2 Experimental setup

The following hardware and software setups are suggested for this investigation to guarantee the seamless operation of the trials. Hardware-wise, a processor with Intel Core i7 or above is advised to enable effective data processing and model training. Processing large-scale datasets calls for at least 16 GB of RAM to guarantee smooth operation; an SSD 256 GB or bigger capacity will be useful for keeping model files and datasets. Furthermore, particularly in a dispersed learning context, the stability and speed of data flow depend on a high-speed Ethernet connection.

Regarding software setup, the experimental environment must operate on Windows 10 or macOS Catalina, which offer stable support. To guarantee that the MATLAB software contains the most up-to-date function libraries and toolboxes, it should be chosen as R2020b or higher. Data processing and model implementation in the studies will be done mostly using MATLAB scripts and functions. If more model training or data processing is done, Python 3.7 is also a helpful addition.

5.3 Ablation experiment: assessing the impact of key components in the FL-KGPrivacyEdu model

Ablation experiments are used in this part of the study to evaluate in depth the particular influence of each important element of the FL-KGPrivacyEdu model on the general performance. A commonly utilised research technique called ablation studies methodically deletes or alters particular model components to see how these modifications affect the model's performance (Younis et al., 2024). This method may clarify the function and significance of every model component as well as their interaction to influence the ultimate outcome.

The trials methodically eliminated or changed various parts of the model to see their particular effect on the model performance. In particular, four ablation versions were developed:

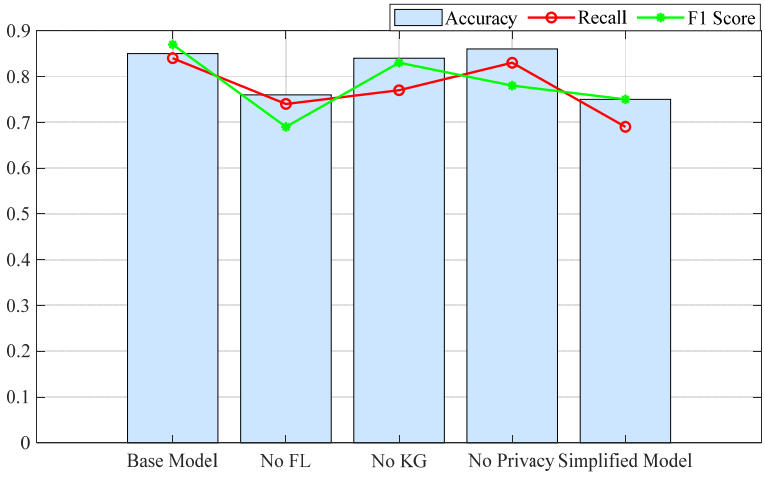
- No FL: the FL mechanism was eliminated to evaluate how a centralised learning strategy affected model performance.
- No KG: the KG construction module is deleted in order to see how the KG affects the analytical capacity of the model.
- No privacy: mechanisms preserving privacy are eliminated to evaluate how privacy preservation affects model security and performance.
- Simplified model: simplified the model architecture to evaluate the influence of model complexity on performance.

The experimental findings are displayed in Figure 4; each version was assessed and trained using the same starting learning rate and the same number of training cycles.

Base model shows the greatest performance in the accuracy evaluation with a score of 0.85, indicating its superiority in properly classifying the data as seen from the image. Following no privacy, which suggests the model's accuracy rises without the privacy-preserving mechanism, no privacy model has an accuracy of 0.86, somewhat better than base model. No KG model has an accuracy of 0.84, which is marginally lower than base model and no privacy, suggesting that the lack of KG may somewhat influence

the accuracy of the model. No FL model's accuracy drops to 0.76, indicating that FL is rather significant in raising the accuracy of the model. With 0.75, simplified model has the lowest accuracy, which could result from the loss of critical features during the model simplification process.

Figure 4 Results of ablation experiments (see online version for colours)



Base model also leads in recall with a score of 0.84, which suggests it is best at spotting all positive samples. Slightly lower than base model, no KG model has a recall of 0.77, which could suggest that KG helps to raise the recall rate. No FL model's recall drops to 0.74, which could be ascribed to the lack of the FL mechanism affecting the model's recognition capacity in scattered data settings. With a recall of 0.83, the no privacy model is near the base model, indicating that the privacy-preserving method has less effect on the recall. With a recall of 0.69, the simplified model confirms even more that model simplification could cause a major performance drop.

Base model once more scores 0.87 in the F1 score measure, indicating its better performance in balancing precision and recall. Though still good, no KG model has a somewhat lower F1 score of 0.83 than base model. No FL model has an F1 score of 0.69, which could be ascribed to the lack of the FL mechanism causing a notable performance drop of the model in processing the distributed data. Though its high accuracy, the no privacy model's F1 score of 0.78 shows it underperforms the base model and no KG in recall. With an F1 score of 0.75, the simplified model is consistent with the findings for accuracy and recall, suggesting that model simplification is detrimental.

Overall, the FL-KGPrivacyEdu model was the best across all three assessment criteria; the simplified model was the worst. These findings underline how crucial the federated KG and privacy-preserving techniques are in enhancing model AI security performance.

5.4 *Effect of learning rate adjustment on model convergence in global rounds*

This experiment aimed to evaluate how changing learning rate affected model convergence in global rounds of the social English learning behaviour analysis model FL-KGPrivacyEdu. To thoroughly evaluate the influence of learning rate on the model training dynamics, three distinct beginning learning rate values (0.01, 0.001 and 0.0001) were chosen to span the spectrum from quite large to modest learning rates (Hsu et al., 2022). Figures 5, 6, and 7 demonstrate the experimental outcomes, accordingly.

Figure 5 Variation of accuracy at different learning rates (see online version for colours)

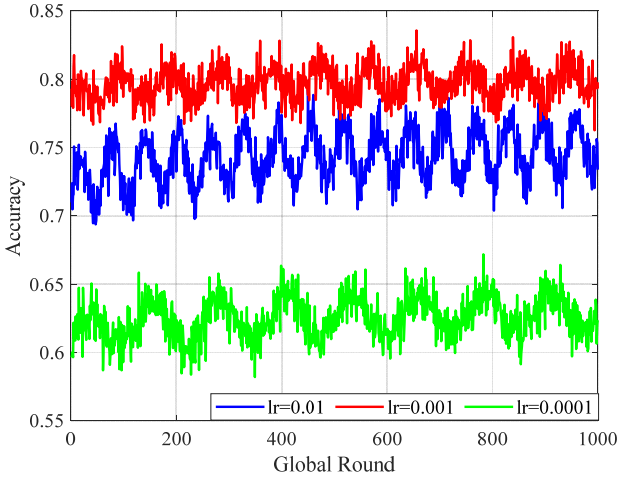
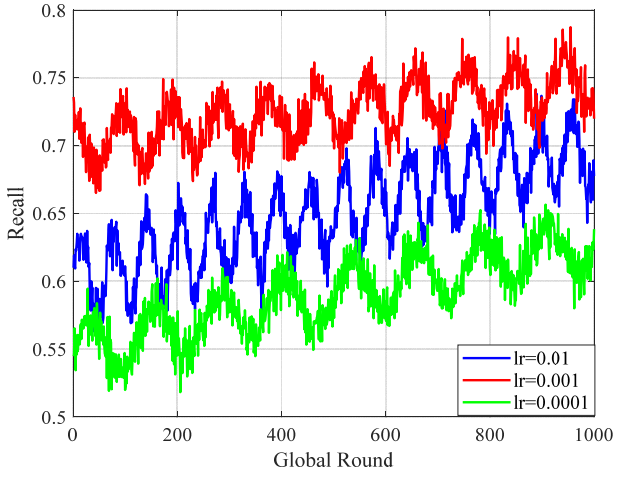


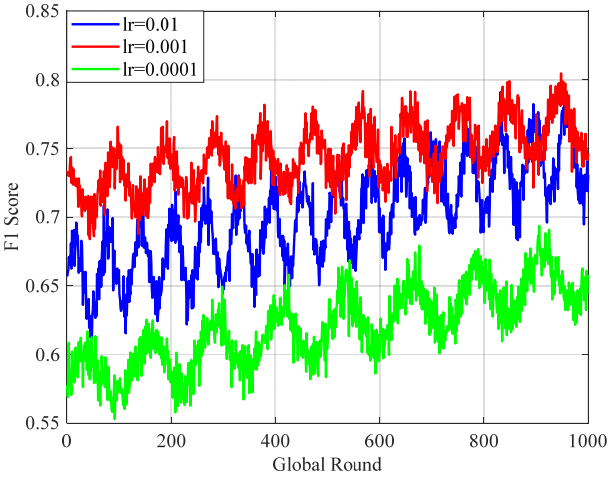
Figure 6 Variation of recall at different learning rates (see online version for colours)



The pattern of the accuracy rate in the worldwide rounds reveals the notable influence of various learning rates on the training impact of the model. The chart demonstrates that while the learning rate is 0.01, the accuracy rate of the model shows significant variations over the training period but usually shows an increasing trend and finally stabilises. By

comparison, the model's accuracy varies less and stabilises in earlier rounds when the learning rate is 0.001 and 0.0001, indicating stronger convergence. The accuracy of the model overall shows a better balance when the learning rate is 0.001.

Figure 7 Variation of F1 score at different learning rates (see online version for colours)



The trend of the recall rate confirms even more the impact of the learning rate on the model training effect. The figure reveals that although the recall rate of the model exhibits significant variability during the training process when the learning rate is 0.01, it also displays a general upward trend and finally stabilises. This corresponds to the pattern of the accuracy rate, implying that a bigger learning rate could cause model instability during the training phase. Learning rates of 0.001 and 0.0001 cause the model's recall to vary less and stabilise in earlier rounds, indicating stronger convergence. This implies that lower learning rates enable the model to perform better more consistently. The model's recall generally shows a better balance at a learning rate of 0.001.

The F1 score trend shows the overall impact of learning rate on model accuracy and recall. The figure reveals that when the learning rate is 0.01, the F1 score of the model exhibits significant variability across the training period but usually trends upward and finally stabilises. This corresponds to the pattern of accuracy and recall, suggesting that the model can become unstable during training at a larger learning rate. The F1 scores of the model varied less and stabilised in earlier rounds with learning rates of 0.001 and 0.0001, indicating stronger convergence. This implies that lower learning rates enable the model to perform better more consistently. The F1 score of the model overall shows a better balance with a learning rate of 0.001.

The experimental findings, therefore, reveal that the learning rate notably influences the convergence and final performance of the model. Though the convergence could be slower, a smaller learning rate, (e.g., 0.001) enables the model to continuously achieve superior performance. On the other hand, bigger learning rates could cause model instability during training. These results offer a significant guide for the training of the FL-KGPrivacyEdu model, particularly for selecting the starting learning rate and planning the learning rate decay approach.

Running these two tests one after the other will not only permit a thorough evaluation of the FL-KGPrivacyEdu model's component parts but also offer information on the particular consequences of learning rate change on the model training process. In the examination of social English learning behaviours, this integrated analytical technique will offer a complete viewpoint to maximise the model design and guarantee its validity and safety.

6 Conclusions

This research presents FL-KGPrivacyEdu, a behavioural analytic model for social English learning combining FL, KG and privacy-preserving technologies. The model seeks to address the behavioural modelling and privacy-preserving issues in social English learning, and efficiently preserves the privacy of users' data by training the model without disclosing the original data. The methodology, meanwhile, can assist customised learning suggestion and AI security by means of a federated KG. The experimental findings indicate that the FL-KGPrivacyEdu model excels in assessment criteria including accuracy, recall, and F1 score, thereby confirming its efficacy and superiority in social English learning behaviour analysis. Furthermore, this work investigated how global round learning rate modification affects model convergence and discovered that a lower learning rate enables the model to perform more consistently better.

Though the FL-KGPrivacyEdu model excels in the tests, it has certain drawbacks. First, the great complexity of the model calls for significant communication and processing among several clients and servers, which could increase computational expenses and communication overheads. Client heterogeneity might secondarily influence the performance of the model; the quality and amount of data from several clients may thereby influence the performance of the global model. Furthermore, while able to safeguard user privacy, privacy-preserving methods like DP could affect model accuracy.

Future studies might concentrate on the following elements:

1 Optimising model efficiency: look into more effective model update and communication techniques to lower the computational cost and communication overhead of the FL-KGPrivacyEdu model and make it more appropriate for resource-constrained settings.

2 In-depth analysis of user behaviour: further study and analysis of user activity patterns on social learning platforms to better understand user wants and enhance AI security (Olabanji et al., 2024).

3 Cross-domain application: use the FL-KGPrivacyEdu framework in other fields, such as healthcare and financial analysis, to investigate its relevance and efficacy in various contexts. Use the FL-KGPrivacyEdu framework in other fields, such as healthcare and financial analysis, to investigate its relevance and efficacy in various contexts.

Acknowledgements

This work is supported by the Jiangsu Higher Education Association Key Programme: Research on College English Teaching Methods under High-quality Development (No. 2022WYZD015).

Declarations

All authors declare that they have no conflicts of interest.

References

Adnan, K. and Akbar, R. (2019) 'An analytical study of information extraction from unstructured and multidimensional big data', *Journal of Big Data*, Vol. 6, No. 1, pp.1–38.

Ahmed, S.F., Alam, M.S.B., Hassan, M., Rozbu, M.R., Ishtiak, T., Rafa, N., Mofijur, M., Shawkat Ali, A. and Gandomi, A.H. (2023) 'Deep learning modelling techniques: current progress, applications, advantages, and challenges', *Artificial Intelligence Review*, Vol. 56, No. 11, pp.13521–13617.

Alexuta, D., Balas, V.E. and Balas, M.M. (2025) 'On the three-tank aquaponic configuration', *International Journal of Computers Communications & Control*, Vol. 20, No. 2, p.7032.

Aljanabi, M. (2023) 'Safeguarding connected health: leveraging trustworthy AI techniques to harden intrusion detection systems against data poisoning threats in IoMT environments', *Babylonian Journal of Internet of Things*, Vol. 2023, pp.31–37.

Balas, V.E., Motoc, I.M. and Barbulescu, A. (2013) 'Combined Haar-Hilbert and Log-Gabor based iris encoders', in Balas, V.E., Fodor, J. and Várkonyi-Kóczy, A.R. (Eds.): *New Concepts and Applications in Soft Computing*, pp.1–26, Springer Berlin Heidelberg, Berlin, Heidelberg.

Bharti, S.S. and Aryal, S.K. (2023) 'The right to privacy and an implication of the EU General Data Protection Regulation (GDPR) in Europe: challenges to the companies', *Journal of Contemporary European Studies*, Vol. 31, No. 4, pp.1391–1402.

Binhammad, M., Alqaydi, S., Othman, A. and Abuljadayel, L.H. (2024) 'The role of AI in cyber security: safeguarding digital identity', *Journal of Information Security*, Vol. 15, No. 2, pp.245–278.

Chen, N., Qiu, T., Zhao, L., Zhou, X. and Ning, H. (2021) 'Edge intelligent networking optimization for internet of things in smart city', *IEEE Wireless Communications*, Vol. 28, No. 2, pp.26–31.

Cui, F., Gu, J., Wang, H., Ni, M. and Zhou, T. (2024) 'Research on end-to-end computing power network architecture based on SDN and MIH technology', *International Journal of Computational Systems Engineering*, Vol. 8, No. 7, pp.1–13.

Dahlan, M.M., Halim, N.S.A., Kamarudin, N.S. and Ahmad, F.S.Z. (2023) 'Exploring interactive video learning: techniques, applications, and pedagogical insights', *International Journal of Advanced and Applied Sciences*, Vol. 10, No. 12, pp.220–230.

Garousi Mokhtarzadeh, N., Amoozad Mahdiraji, H., Jafarpanah, I., Jafari-Sadeghi, V. and Cardinali, S. (2020) 'Investigating the impact of networking capability on firm innovation performance: using the resource-action-performance framework', *Journal of Intellectual Capital*, Vol. 21, No. 6, pp.1009–1034.

Gong, M., Pan, K., Xie, Y., Qin, A.K. and Tang, Z. (2020) 'Preserving differential privacy in deep neural networks with relevance-based adaptive noise imposition', *Neural Networks*, Vol. 125, pp.131–141.

Hassan, E., Shams, M.Y., Hikal, N.A. and Elmougy, S. (2023) 'The effect of choosing optimizer algorithms to improve computer vision tasks: a comparative study', *Multimedia Tools and Applications*, Vol. 82, No. 11, pp.16591–16633.

Hsu, C., Nisonoff, H., Fannjiang, C. and Listgarten, J. (2022) 'Learning protein fitness models from evolutionary and assay-labeled data', *Nature Biotechnology*, Vol. 40, No. 7, pp.1114–1122.

Ji, S., Pan, S., Cambria, E., Marttinen, P. and Yu, P.S. (2021) 'A survey on knowledge graphs: representation, acquisition, and applications', *IEEE Transactions on Neural Networks and Learning Systems*, Vol. 33, No. 2, pp.494–514.

Liang, X., Haiping, L., Liu, J. and Lin, L. (2021) 'Reform of English interactive teaching mode based on cloud computing artificial intelligence – a practice analysis', *Journal of Intelligent & Fuzzy Systems*, Vol. 40, No. 2, pp.3617–3629.

Liu, J., Huang, J., Zhou, Y., Li, X., Ji, S., Xiong, H. and Dou, D. (2022) 'From distributed machine learning to federated learning: a survey', *Knowledge and Information Systems*, Vol. 64, No. 4, pp.885–917.

Lv, P., Wang, X., Xu, J. and Wang, J. (2021) 'Intelligent personalised exercise recommendation: a weighted knowledge graph-based approach', *Computer Applications in Engineering Education*, Vol. 29, No. 5, pp.1403–1419.

Olabanji, S.O., Marquis, Y., Adigwe, C.S., Ajayi, S.A., Oladoyinbo, T.O. and Olaniyi, O.O. (2024) 'AI-driven cloud security: examining the impact of user behavior analysis on threat detection', *Asian Journal of Research in Computer Science*, Vol. 17, No. 3, pp.57–74.

Pérez-Paredes, P. and Mark, G. (2024) 'Rethinking interviews as representations of spoken language in learner corpora', *Research in Corpus Linguistics*, Vol. 12, No. 2, pp.111–145.

Thabtah, F., Hammoud, S., Kamalov, F. and Gonsalves, A. (2020) 'Data imbalance in classification: experimental evaluation', *Information Sciences*, Vol. 513, pp.429–441.

Thavamani, C. and Rengarajan, A. (2024) 'Clustering related behaviour of users by the use of partitioning and parallel transaction reduction algorithm', *International Journal of Advanced Intelligence Paradigms*, Vol. 29, Nos. 2/3, pp.122–132.

Tsou, Y-T., Chen, H-L. and Chen, J-Y. (2019) 'RoD: evaluating the risk of data disclosure using noise estimation for differential privacy', *IEEE Transactions on Big Data*, Vol. 7, No. 1, pp.214–226.

Viberg, O., Mutimukwe, C. and Grönlund, Å. (2022) 'Privacy in LA research: understanding the field to improve the practice', *Journal of Learning Analytics*, Vol. 9, No. 3, pp.169–182.

Winter, J.S. and Davidson, E. (2019) 'Big data governance of personal health information and challenges to contextual integrity', *The Information Society*, Vol. 35, No. 1, pp.36–51.

Yang, P., Xiong, N. and Ren, J. (2020) 'Data security and privacy protection for cloud storage: a survey', *IEEE Access*, Vol. 8, pp.131723–131740.

Younis, E.M., Mohsen, S., Houssein, E.H. and Ibrahim, O.A.S. (2024) 'Machine learning for human emotion recognition: a comprehensive review', *Neural Computing and Applications*, Vol. 36, No. 16, pp.8901–8947.

Zhang, L., Li, X., Li, W., Zhou, H. and Bai, Q. (2021) 'Context-aware recommendation system using graph-based behaviours analysis', *Journal of Systems Science and Systems Engineering*, Vol. 30, pp.482–494.

Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B. and Avestimehr, A.S. (2022) 'Federated learning for the internet of things: applications, challenges, and opportunities', *IEEE Internet of Things Magazine*, Vol. 5, No. 1, pp.24–29.

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C-Z., Li, H. and Tan, Y-A. (2019) 'Secure multi-party computation: theory, practice and applications', *Information Sciences*, Vol. 476, pp.357–372.