

Differential Privacy-Enabled TextCNN for MOOCs Fake Review Detection

Caiyun Chen*

School of Information Science and Technology, Tan Kah Kee College, Xiamen University, Zhangzhou 363105, Fujian Province, China

*Corresponding author: Caiyun Chen, chency@xujc.com

Copyright: © 2025 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: The rapid development and widespread adoption of massive open online courses (MOOCs) have indeed had a significant impact on China's education curriculum. However, the problem of fake reviews and ratings on the platform has seriously affected the authenticity of course evaluations and user trust, requiring effective anomaly detection techniques for screening. The textual characteristics of MOOCs reviews, such as varying lengths and diverse emotional tendencies, have brought complexity to text analysis. Traditional rule-based analysis methods are often inadequate in dealing with such unstructured data. We propose a Differential Privacy-Enabled Text Convolutional Neural Network (DP-TextCNN) framework, aiming to achieve high-precision identification of outliers in MOOCs course reviews and ratings while protecting user privacy. This framework leverages the advantages of Convolutional Neural Networks (CNN) in text feature extraction and combines differential privacy techniques. It balances data privacy protection with model performance by introducing controlled random noise during the data preprocessing stage. By embedding differential privacy into the model training process, we ensure the privacy security of the framework when handling sensitive data, while maintaining a high recognition accuracy. Experimental results indicate that the DP-TextCNN framework achieves an exceptional accuracy of over 95% in identifying fake reviews on the dataset, this outcome not only verifies the applicability of differential privacy techniques in TextCNN but also underscores its potential in handling sensitive educational data. Additionally, we analyze the specific impact of differential privacy parameters on framework performance, offering theoretical support and empirical analysis to strike an optimal balance between privacy protection and framework efficiency.

Keywords: DP-TextCNN; Differential Privacy; Fake review; MOOCs

Online publication: February 13, 2025

1. Introduction

Massive Open Online Courses (MOOCs) have become important online platforms for learners to acquire knowledge. The evaluation of course quality has become particularly critical, not only in terms of the diversity and complexity of evaluation objectives but also in terms of the fairness and reliability of the evaluation process^[1,2].

Course reviews and ratings, as key indicators to measure teaching quality and student learning experience, play a core role in the educational evaluation system^[3]. In-depth analysis of course ratings and reviews through machine learning and natural language processing technology can more accurately reflect the course situation^[4,5]. Natural language processing technology plays an important role in analyzing student feedback, extracting keywords and topics, sentiment analysis, and evaluating teaching effectiveness^[6].

However, fake review and rating data pose challenges to the accuracy of course evaluations, which may be caused by malicious operations, system errors, or data entry errors^[7-9]. In addition, review and rating data usually contain sensitive personal information and learning preferences, which may lead to serious privacy risks if not protected^[10]. Thus, the critical issue is how to effectively detect fake reviews and ratings while ensuring privacy and security.

In recent years, Differential Privacy (DP), as a powerful privacy protection technology, has received widespread attention. It can maintain the statistical properties of data and the accuracy of analysis results while providing data privacy protection^[11]. Differential privacy effectively protects privacy by adding an appropriate amount of random noise to the data set^[12]. On the other hand, sentiment analysis and data mining based on machine learning can help detect fake reviews and ratings, identify overall evaluations and discover evaluation anomalies^[13]. In particular, Text Convolutional Neural Network (TextCNN), as an important model of deep learning in the field of text processing, has been widely used in natural language processing, sentiment analysis, etc^[14].

Given the advantages of differential privacy and Text CNN, we propose a Differential Privacy-Enabled Text Convolutional Neural Network (DP-TextCNN) model, aiming to effectively identify course fake reviews and ratings while ensuring the security of user privacy. This model introduces a differential privacy mechanism in the data processing to protect the privacy of the review data and uses the DP-TextCNN model to detect fake reviews on the processed data. Our research not only enriches the application of differential privacy in the field of deep learning but also provides a new perspective and method for detecting course fake reviews.

2. Related work

2.1. Course fake reviews detection

With the development of online education platforms, the fairness and accuracy of course reviews and rating systems have become core issues in ensuring educational quality^[15-17]. Sentiment analysis of course reviews can reflect the adaptability of teaching design, student satisfaction, and learning effectiveness^[18-20]. By integrating learning records, course reviews, and ratings, more accurate course recommendation strategies can be implemented to optimize the learning experience^[21]. Review analysis is an important factor in revealing learner preferences and course selection^[22]. Li *et al.* provided a powerful tool for deep mining course reviews through a data-driven framework^[23]. Onan's research showed that the performance of deep learning in sentiment analysis surpasses traditional methods and has great potential in educational data mining^[24]. Course reviews and rating analysis play an irreplaceable role in improving education quality and promoting educational equity.

Fake reviews and ratings significantly impact users' decision-making, distorting fair competition and eroding trust in online evaluation systems^[25]. The development of deep learning methods, especially TextCNN in the field of text processing, has brought improvements in accuracy and effectiveness to the detection of fake reviews and ratings^[26]. Jain and Pamula introduced a supervised learning framework to bolster detection capabilities^[27], while

Salminen *et al.* leveraged GPT to create fake samples and integrated them with classifiers for effective recognition [28]. The TextCNN model, with its robust feature extraction and automated processing, has excelled in identifying fake reviews and ratings [29–31]. By employing sophisticated convolutional and pooling layers, the model precisely captures key semantic content, facilitating accurate classification and identification [32].

However, despite TextCNN’s advancements in detection accuracy and efficiency, research on privacy protection in this domain remains scant. When handling reviews and ratings containing sensitive user data, such as preferences and learning habits, many detection methods overlook the risks of information leakage, posing severe threats to user privacy and security. Consequently, ensuring detection accuracy while strengthening privacy protection has emerged as a pivotal challenge requiring urgent resolution.

2.2. Differential Privacy protection and deep learning models

Differential Privacy (DP) is a privacy-preserving framework that ensures that the output of a data analysis is insensitive to small changes in the input dataset. This is achieved by adding carefully calibrated random noise to the results of queries or computations performed on the dataset [33,34]. The integration of Differential Privacy protection technology with deep learning models has become increasingly popular, especially in scenarios where user privacy is a concern. By incorporating Differential Privacy into the training process of deep learning models, it is possible to add noise to the gradients or other parameters in a way that preserves the overall utility of the model while providing strong privacy guarantees [35,36].

TextCNN is a powerful text-processing model that is effective in various natural language processing tasks, including sentiment analysis, text classification, etc. By incorporating differential privacy, we can enhance the privacy protection of user data while maintaining the model’s performance [37,38]. Adding differential privacy noise to the convolutional layer, pooling layer, or fully connected layer of TextCNN can help obscure the influence of individual data on the model’s weights, thereby protecting user privacy. While there have been some studies on the combination of differential privacy and deep learning, the specific application of differential privacy to the task, of course, fake reviews and rating detection is still relatively underdeveloped [39].

We aim to design a TextCNN model combined with differential privacy protection, refining the noise addition strategy to minimize the impact on model performance while protecting user privacy. Constructing a rigorous experimental framework and conducting systematic experiments, verifying the specific impact of differential privacy protection on the performance of the TextCNN model in detecting course fake reviews and ratings. Finding the balance between privacy protection and model performance, conducting extensive experiments, and fine-tuning the noise addition strategy to achieve optimal results.

3. Differential Privacy-Enabled TextCNN model

3.1. Data preprocessing and analysis

We have conducted an extensive collection of course reviews and rating data from various MOOCs spanning multiple disciplines, including law, engineering, computer science, education and teaching, economic management, natural sciences, foreign languages, literature, history and philosophy, psychology, medicine, and health, as well as art and design. To guarantee the quality of our data, we implemented a thorough initial cleanup process, which involved eliminating duplicate, invalid, or significantly erroneous records. These records encompassed null values, extreme rating values, logically inconsistent ratings, meaningless reviews (like “666666” or “hahaha”), and

reviews that were not directly related to the course content (such as “sofa” or “reference books”).

Furthermore, we ensured the consistency between ratings and reviews by identifying and correcting any abnormal data where ratings were mismatched with the sentiment expressed in the reviews, thereby enhancing the logical rigor and accuracy of our dataset (**Figure 1**). Following the data preprocessing stage, we successfully constructed a MOOCs course reviews and ratings dataset, which comprises 10,000 positive and negative reviews along with their corresponding ratings. To enhance the dataset’s compatibility with the DP-TextCNN model, we conducted text segmentation. Utilizing the jieba Chinese word segmentation tool, we precisely divided continuous text strings into individual word sequences. This step is crucial for ensuring that the model can effectively process and understand the textual data, ultimately improving its performance in analyzing and predicting the sentiment of the course reviews.

After data preprocessing, a MOOCs course reviews and ratings dataset containing 10,000 positive and negative reviews and ratings was constructed. We performed text segmentation to improve the applicability of the data to the DP-TextCNN model. With the help of the Chinese word segmentation tool jieba, continuous text strings were accurately segmented into independent word sequences.

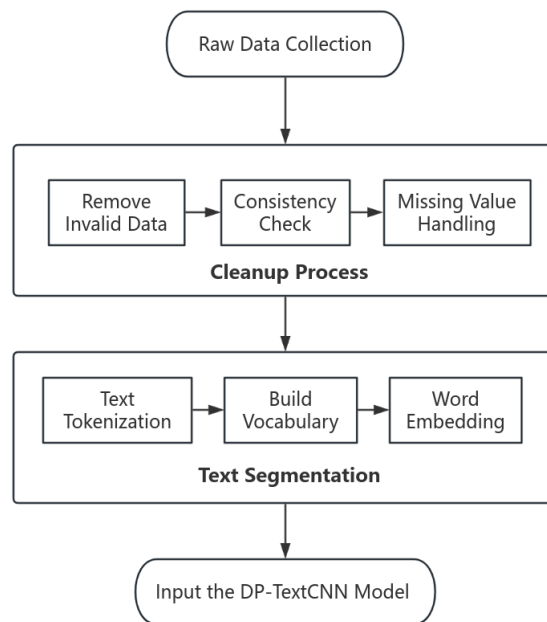


Figure 1. Data Cleaning and Transformation Process: the flowchart details the comprehensive steps involved in obtaining a high-quality dataset of reviews and ratings, starting from the raw data, through invalid record removal, consistency verification of ratings and reviews, and missing data processing

After word segmentation, we further refined the dataset by removing stop words and other invalid terms. This step significantly reduced the redundant information that the model needed to process and effectively decreased the dimensionality of the feature space. Subsequently, we established a comprehensive vocabulary and mapped each word into a fixed-dimensional vector space using word embedding techniques.

3.2. Differential Privacy protection technology

To safeguard data privacy while preserving the detection capabilities of the TextCNN model, we incorporate

differential privacy protection technology into its framework. Differential privacy minimizes the risk of information leakage from the training data by introducing noise and restricting gradient updates^[12]. By adding random noise to the data, differential privacy ensures that the model’s output remains indistinguishable regardless of whether a specific sample is present in the dataset^[40].

(1) Gradient clipping: Gradient clipping using the L2 norm involves comparing the L2 norm (the Euclidean norm or magnitude) of the gradient vector with a predefined clipping threshold. If the L2 norm of the gradient exceeds this threshold, the gradient vector is scaled down proportionally so that its L2 norm equals the clipping threshold. This step ensures that the magnitude of the gradient update does not exceed a certain limit, thereby preventing potentially destabilizing large updates during model training. By applying this clipping operation, we limit the impact of individual training samples on the model’s learning process, leading to a more stable and robust training experience. As shown in **Equation (1)**, the gradient is a vector representing the gradient calculated during model training, and `l2_norm_clip` is a scalar representing the threshold for gradient clipping. Compare the L2 norm of the gradient with a preset clipping threshold (`l2_norm_clip`). If the L2 norm of the gradient exceeds this threshold, it is scaled to be equal to the threshold.

$$\text{clipped_gradient} = \frac{\text{gradient}}{\max(1, \frac{\|\text{gradient}\|}{\text{l2_norm_clip}})} \quad (1)$$

(2) Adding noise: Adding Gaussian noise to the clipped gradient is a technique used to enhance privacy in model training, particularly in scenarios where protecting the confidentiality of training data is crucial. The noise is added to obscure the connection between gradient updates and specific training samples, thereby reducing the risk of information leakage. As shown in **Equation (2)**, where ϵ is a constant related to the privacy budget calculation, `noisy_gradient` is a vector representing the gradient with Gaussian noise added, and `noise_multiplier` is used to control the amount of noise added to the gradient. The variance of the noise is proportional to the clipping threshold of the gradient and the privacy budget parameter (`noise_multiplier`). The addition of noise blurs the connection between gradient updates and specific training samples. Modify the gradients by adding appropriate Gaussian noise to allow model training without revealing too much information about data. Adjusting the values of `noise_multiplier`, `l2_norm_clip` and ϵ can find an appropriate balance between privacy protection and model performance.

$$\text{noisy_gradient} = \text{clipped_gradient} + \text{Gaussian_noise}(0, \text{noise_multiplier} \times \text{l2_norm_clip} \times \epsilon) \quad (2)$$

3.2. DP-TextCNN model

The DP-TextCNN model is a Differential Privacy-Enabled TextCNN model designed for detecting course fake reviews and ratings^[40]. It converts the input integer index into high-dimensional dense vector representations via an embedding layer, effectively mapping the information into a vector space. Subsequently, the model employs multiple one-dimensional convolutional layers with varying convolution kernel sizes to extract local features from the input sequence. These convolutional layers are capable of capturing contextual information of different lengths, thereby enriching the model’s feature representation capabilities. To reduce the feature dimension while retaining the most crucial information, the model applies a global max pooling layer after each convolutional layer. Global maximum pooling achieves feature dimensionality reduction by selecting the maximum value on each feature map. This process not only minimizes computational complexity but also enhances the model’s generalization capabilities. During the training process, the model incorporates differential privacy technology to ensure model performance while bolstering data privacy protection. It utilizes a differential privacy-compatible optimizer,

such as DPKerasSGDOptimizer, which considers the allocation of privacy budget when adding Gaussian noise to the model gradient. By adjusting the noise intensity and the privacy budget threshold, the model can restrict information leakage, thereby providing robust privacy protection (**Figure 2**).

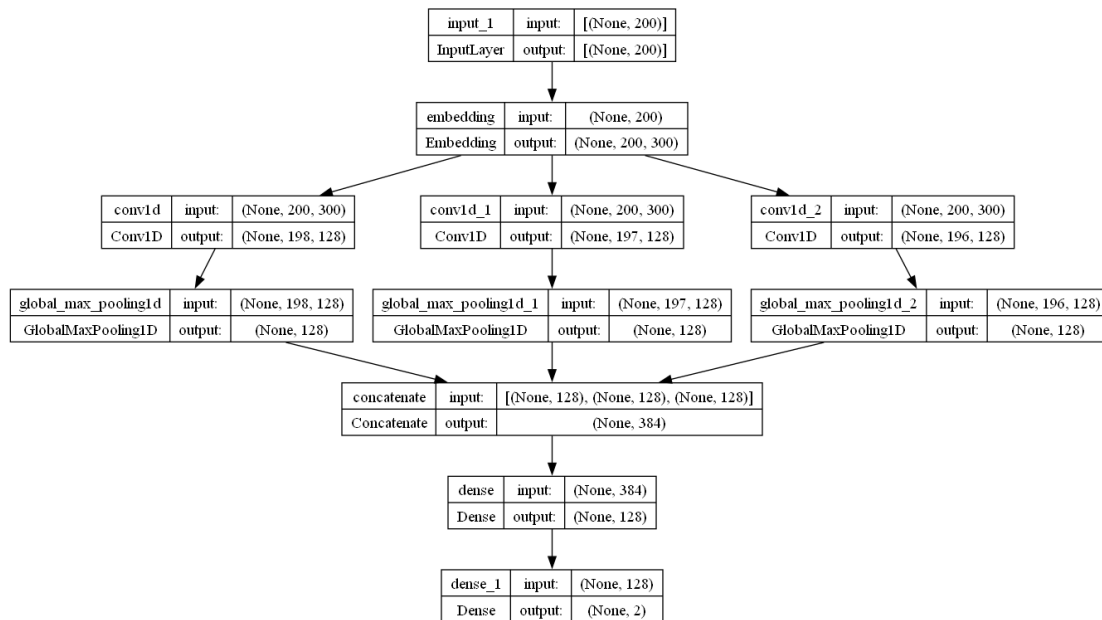


Figure 2. Structure of the DP-TextCNN Model, including the input layer, convolution layer, pooling layer, fully connected layer, as well as the connection methods and parameter settings between each layer

3.3. DP-TextCNN model

The training of the DP-textCNN model focuses on enhancing its performance in text classification tasks by iteratively adjusting its parameters. Initially, the model’s weights are randomly initialized. Subsequently, the training data is fed into the model, which undergoes a series of transformations and processing steps. To assess the model’s performance and update its parameters, a loss function is employed to quantify the discrepancy between the predicted and actual labels. The backpropagation algorithm is activated to efficiently compute the gradient of the loss function concerning the model parameters. This gradient information guides the optimization process, indicating how the model parameters should be adjusted to minimize losses and enhance performance.

The differential privacy SGD optimizer leverages gradient information to update model parameters while ensuring training efficiency and data privacy. It achieves this by incorporating gradient clipping and adding noise. The model parameters are updated in each epoch, and the training process is closely monitored to prevent overfitting. Both the training set and validation set are evaluated for loss and accuracy (**Figure 3**).

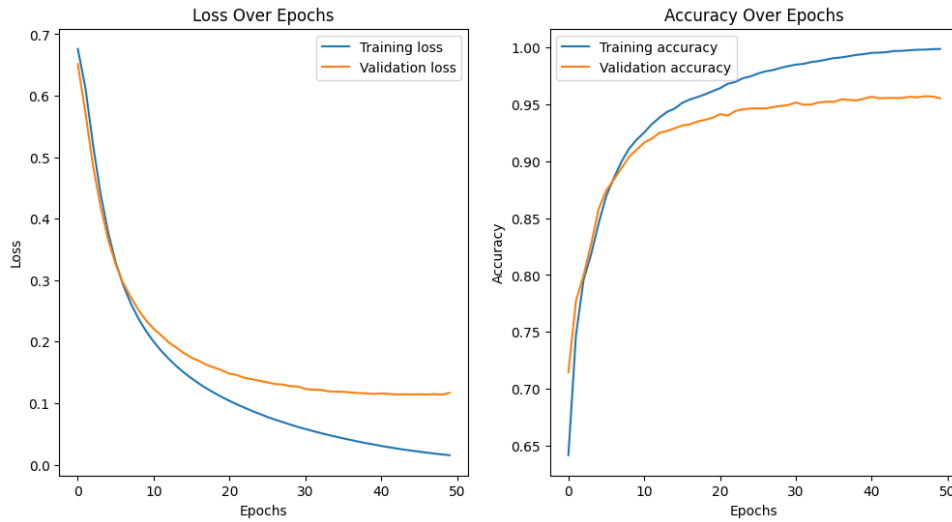


Figure 3. Loss function and recognition rate of different epochs, as the number of training epochs increases, the loss on the training set decreases, and accuracy improves until the training epoch reaches 30, which suggests that the model has begun to overfit

4. Results and analysis

We evaluated the DP-TextCNN model on a test dataset comprising fake reviews and ratings of courses across multiple disciplines on a MOOCs platform. This dataset encompasses diverse review information and is designed to assess the model’s performance in fake review classification. The results show that the DP-TextCNN model demonstrates exceptional performance on this dataset, achieving an accuracy rate for fake review classification exceeding 95% (**Figure 4**).

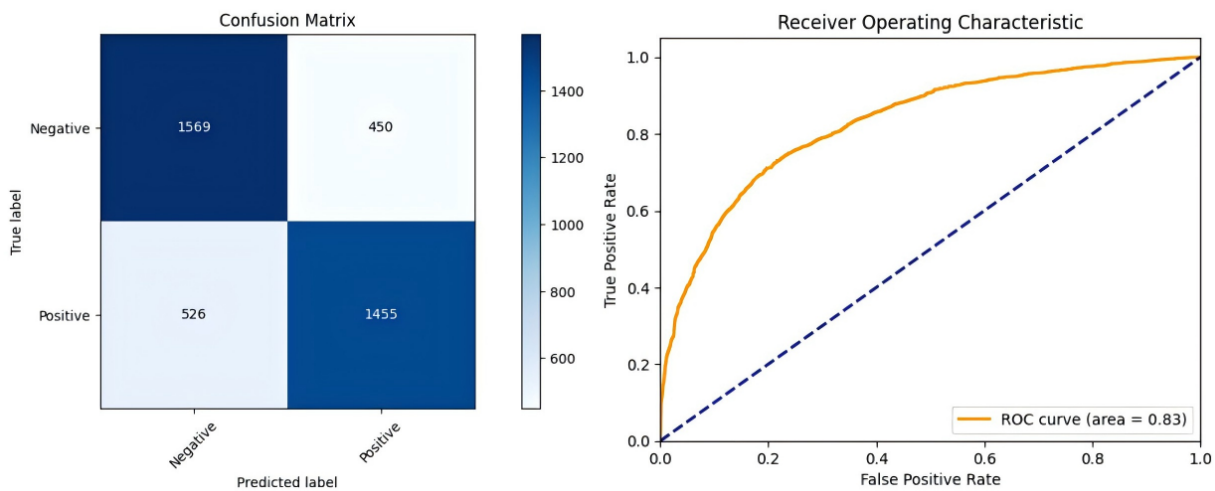


Figure 4. The Confusion Matrix and ROC of the DP-TextCNN model, the proportions of false positives (FP) and false negatives (FN) are relatively low, indicating a minimal misjudgment rate by the model. The Receiver Operating Characteristic (ROC) curve of the DP-TextCNN model closely aligns with the upper left corner, signifying high sensitivity and specificity in classifying fake reviews and ratings

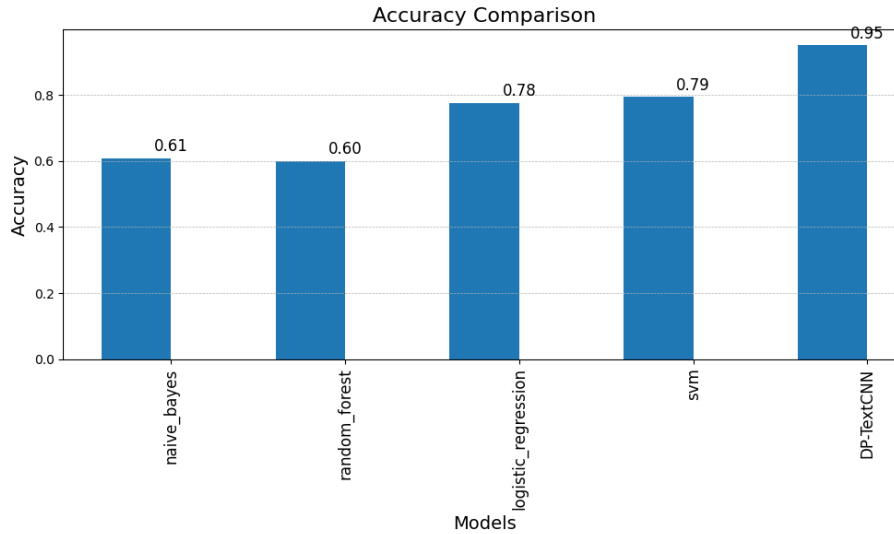


Figure 5. Comparison of accuracy among different models, including Naive Bayes, Random Forest, Logistic Regression, and Support Vector Machine (SVM).

We conducted a comparative analysis of various machine learning and deep learning models, as shown in **Figure 5**. In text classification tasks, the Random Forest’s effectiveness is limited by the quality of features and its capacity to capture interactions among complex text features. Logistic Regression exhibits relatively limited classification capabilities when dealing with text data characterized by nonlinear relationships. SVM incurs high training costs for large-scale text datasets and struggles to capture the intricate structure of text data. In contrast, DP-TextCNN excels at extracting high-level features from text data, capturing dependencies and semantic information within the text. It performs exceptionally well when processing large-scale, high-dimensional text datasets. While maintaining a high classification accuracy, DP-TextCNN incorporates differential privacy protection to safeguard the privacy of data processing. Experimental results demonstrate that DP-TextCNN achieves a classification accuracy of over 95%, surpassing other comparison models. DP-TextCNN exhibits superior classification performance and robustness in the task of identifying course fake reviews and ratings.

5. Conclusion

We proposed a DP-TextCNN model based on differential privacy protection for data privacy protection of course fake reviews and ratings classification on online MOOCs platforms. This model integrates the robust feature extraction capabilities of TextCNN with differential privacy protection, ensuring efficient classification of fake course reviews and ratings while preserving data privacy. Experimental results show that DP-TextCNN achieves a fake review classification accuracy of over 95% on a dataset comprising course reviews across multiple disciplines on the MOOCs platform, outperforming traditional methods.

Our work not only validates the application of differential privacy within the DP-TextCNN model framework but also opens up possibilities for establishing a fair evaluation system on online education platforms. Looking ahead, it is imperative to refine the implementation of differential privacy to strike an optimal balance between privacy protection and model performance. Additionally, we aim to explore the fusion of differential privacy with other privacy protection technologies and broaden the application of the DP-TextCNN model to new domains.

Disclosure statement

The author declares no conflict of interest.

References

- [1] Wei X, Saab N, Admiraal W, 2021, Assessment of Cognitive, Behavioral, and Affective Learning Outcomes in Massive Open Online Courses: A Systematic Literature Review. *Computers & Education*, 163: 104097.
- [2] Wu B, 2021, Influence of MOOC Learners Discussion Forum Social Interactions on Online Reviews of MOOC. *Education and Information Technologies*, 26: 3483–3496.
- [3] Alturkistani A, Lam C, Foley K, et al., 2020, Massive Open Online Course Evaluation Methods: Systematic Review. *Journal of Medical Internet Research*, 22: e13851.
- [4] Alger W, Doan M, Caporusso N, 2024, Student Evaluations of Teaching: Using Big Data Visualization to Explore Challenges and Opportunities. In *Proceedings of the 2024 47th MIPRO ICT and Electronics Convention (MIPRO)*, IEEE, 2024: 508–513.
- [5] Soheli A, Hossain MR, Mostofa ZB, et al., 2023, Sentiment Analysis Based on Online Course Feedback Using Textblob and Machine Learning Techniques. In *Proceedings of the 2023 26th International Conference on Computer and Information Technology (ICCIT)*, IEEE, 2023: 1–6.
- [6] Shaik T, Tao X, Li Y, et al., 2022, A Review of the Trends and Challenges in Adopting Natural Language Processing Methods for Education Feedback Analysis. *IEEE Access*, 10: 56720–56739.
- [7] Alexandron G, Ruy Pérez-Valiente JA, Lee S, et al., 2018, Evaluating the Robustness of Learning Analytics Results Against Fake Learners. In *Proceedings of the European Conference on Technology Enhanced Learning*, Springer, 2018: 74–87.
- [8] Graf P, 2024, Making Sense of Today's Use of Student Evaluations of Teaching (SET). *Human Arenas* 7: 446–450.
- [9] Paul H, Nikolaev A, 2021, Fake Review Detection on Online E-Commerce Platforms: A Systematic Literature Review. *Data Mining and Knowledge Discovery*, 35: 1830–1881.
- [10] Zigmotiros A, Casino F, Solanas A, 2020, et al., 2020, Survey on Privacy Properties for Data Publishing of Relational Data. *IEEE Access*, 8: 51071–51099.
- [11] Qin Y, Li M, Zhu J, 2023, Privacy-Preserving Federated Learning Framework in Multimedia Courses Recommendation. *Wireless Networks*, 29: 1535–1544.
- [12] Dong J, Roth A, Su WJ, 2022, Gaussian Differential Privacy. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 84: 3–37.
- [13] Shaik T, Tao X, Dann C, et al., 2023, Sentiment Analysis and Opinion Mining on Educational Data: A Survey. *Natural Language Processing Journal*, 2: 100003.
- [14] Zhang T, You F, 2021, Research on Short Text Classification Based on Textnn. In *Proceedings of the Journal of Physics: Conference Series*. IOP Publishing, 1757: 012092.
- [15] Moore RL, Blackmon SJ, 2022, From the Learner's Perspective: A Systematic Review of MOOC Learner Experiences (2008–2021). *Computers & Education*, 190: 104596.
- [16] Peng X, Xu Q, 2020, Investigating Learners' Behaviors and Discourse Content in MOOC Course Reviews. *Computers & Education*, 143: 103673.
- [17] Qi C, Liu S, 2021, Evaluating On-Line Courses via Reviews Mining. *Ieee Access*, 9: 35439–35451.
- [18] Bulusu A, Rao KR, 2021, Sentiment Analysis of Learner Reviews to Improve Efficacy of Massive Open Online Courses (MOOC's)—A survey. In *Proceedings of the 2021 Fifth International Conference on I-SMAC (IoT in Social,*

Mobile, Analytics and Cloud) (I-SMAC), IEEE, 2021: 933–941.

- [19] Kastrati Z, Imran AS, Kurti A, 2020, Weakly Supervised Framework for Aspect-Based Sentiment Analysis on Students' Reviews of MOOCs. *IEEE Access*, 8: 106799–106810.
- [20] Yang P, Liu Y, Luo Y, et al., 2024, Text Mining and Multi-Attribute Decision-Making-Based Course Improvement in Massive Open Online Courses. *Applied Sciences*, 14: 3654.
- [21] Fan J, Jiang Y, Liu Y, et al., 2022, Interpretable MOOC Recommendation: A Multi-Attention Network for Personalized Learning Behavior Analysis. *Internet Research*, 32: 588–605.
- [22] Gomez MJ, Calderón M, Sánchez V, et al., 2022, Large Scale Analysis of Open MOOC Reviews to Support Learners' Course Selection. *Expert Systems with Applications*, 210: 118400.
- [23] Li H, Gu H, Hao X, et al., 2024, Data-Driven Analytics for Student Reviews in China's Higher Vocational Education MOOCs: A Quality Improvement Perspective. *Plos One*, 19: e0298675.
- [24] Onan A, 2021, Sentiment Analysis on Massive Open Online Course Evaluations: A Text Mining and Deep Learning Approach. *Computer Applications in Engineering Education*, 29: 572–589.
- [25] Wu Y, Ngai EW, Wu P, et al., 2020, Fake Online Reviews: Literature Review, Synthesis, and Directions for Future Research. *Decision Support Systems*, 132: 113280.
- [26] Mohawesh R, Xu S, Tran SN, et al., 2021, Fake Reviews Detection: A Survey. *Ieee Access*, 9: 65771–65802.
- [27] Jain PK, Pamula R, Srivastava G, 2021, A Systematic Literature Review on Machine Learning Applications for Consumer Sentiment Analysis Using Online Reviews. *Computer Science Review*, 41: 100413.
- [28] Salminen J, Kandpal C, Kamel AM, et al., 2022, Creating and Detecting Fake Reviews of Online Products. *Journal of Retailing and Consumer Services*, 64: 102771.
- [29] Chen X, Li Z, Zou D, et al., 2024, Leveraging Deep Learning for Classifying Learner-Generated Course Evaluation Texts. In *Proceedings of the International Conference on Blended Learning*. Springer, 2024: 311–321.
- [30] Wang J, Xie H, Au OTS, et al., 2020, Attention-Based CNN for Personalized Course Recommendations for MOOC Learners. In *Proceedings of the 2020 International Symposium on Educational Technology (ISET)*. IEEE, 2020: 180–184.
- [31] Liu T, Hu W, Liu F, et al., 2021, Sentiment Analysis for MOOC Course Reviews. In *Proceedings of the Data Science: 7th International Conference of Pioneering Computer Scientists, Engineers and Educators, ICPCSEE 2021*, Springer, 2021: 78–87.
- [32] Liu J, Yan Z, Chen S, et al., 2023, Channel Attention TextCNN with Feature Word Extraction for Chinese Sentiment Analysis. *ACM Transactions on Asian and Low-Resource Language Information Processing*, 22: 1–23.
- [33] Bu Z, Dong J, Long Q, et al., 2020, Deep Learning with Gaussian Differential Privacy. *Harvard Data Science Review*, 2(3).
- [34] Ha T, Dang TK, Le H, 2020, Security and Privacy Issues in Deep Learning: A Brief Review. *SN Computer Science*, 1: 253.
- [35] Boulemtafes A, Derhab A, Challal Y, 2020, A Review of Privacy-Preserving Techniques for Deep Learning. *Neurocomputing*, 384: 21–45.
- [36] Doleck T, Lemay DJ, Basnet RB, et al., 2020, Predictive Analytics in Education: A Comparison of Deep Learning Frameworks. *Education and Information Technologies*, 25: 1951–1963.
- [37] Ghazi B, Golowich N, Kumar R, et al., 2021, Deep Learning with Label Differential Privacy. *Advances in Neural Information Processing Systems*, 34: 27131–27145.
- [38] Vasa J, Thakkar A, 2023, Deep Learning: Differential Privacy Preservation in the Era of Big Data. *Journal of*

Computer Information Systems, 63: 608–631.

- [39] Liu G, Sun X, Li Y, et al., 2023, An Automatic Privacy-Aware Framework for Text Data in Online Social Network Based on a Multi-Deep Learning Model. *International Journal of Intelligent Systems*, 2023: 1727285.
- [40] Dong M, Li Y, Tang X, et al., 2020, Variable Convolution and Pooling Convolutional Neural Network for Text Sentiment Classification. *IEEE access*, 8: 16174–16186.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.