Encrypted Storage Method of Oral English Teaching Resources based on Cloud Platform

Tongsheng Si
School of Culture-Tourism and International Education, Henan Polytechnic Institute, Nanyang, China

***Abstract*—With the development of the times, the secure storage of educational resources has become one of the key security problems faced by colleges and universities. On the one hand, the cost of traditional resource storage is too expensive, on the other hand, its encryption and access efficiency are low. To solve this problem, this research takes the cloud platform serves as the main carrier for the encrypted storage of school teaching resources. On this basis, the convolutional neural network is encrypted and optimized, and the argmax algorithm is improved to improve the access efficiency of encrypted data. Finally, the effectiveness and superiority of the design method are compared and analyzed through the method of performance detection. The results show that the maximum consumption time of encryption and decryption of the encrypted storage model is no more than 20000ms, which is significantly less than that of the traditional model. The running time of the argmax output encryption module is 1.76ms and the running loss is 0.26 MB, which is less than that of the traditional model. It can be seen that the encrypted storage model has stronger encryption performance and access performance, and has a better application effect in the encrypted storage of oral English teaching resources with a large amount of access data and frequent updates.**

Keywords—Cloud platform; oral language; encryption; resource storage

I. INTRODUCTION

With the development of modern network technology, the cloud platform, as a new cloud service model, can provide more secure and efficient services for users who need computing and storage services through the deployment of a cloud machine learning model [1]. The development of cloud platform technology provides customers with services that need a high budget and high-tech support in the actual environment more conveniently and economically. Encrypted storage is one of the main types [2]. For modern colleges and universities, the security of teaching resources is one of the main security problems in the teaching process. Oral English teaching resources themselves have the characteristics of fast replacement speed and a large amount of stored data. As a network grafting service platform, the cloud platform has a stronger fit with the encrypted storage of oral English teaching resources [3]. As a special resource containing multilingual voice and text contrast materials, oral teaching resources are diversified and integrated. At the same time, the resource reserve is large and the real-time update speed is fast. Therefore, the encryption system for oral teaching resources needs higher data processing efficiency and a more robust and easy architecture. Applying cloud platform encrypted storage technology to the encrypted storage of oral English teaching resources can effectively improve the economy and quickness of the encrypted storage of school teaching resources, and provide teachers and students with better teaching and learning experience while improving security [4]. This research applies convolutional neural network, a robust deep learning model, to cloud platform encryption. On the one hand, it provides a theoretical path for the formation of an economic and practical teaching resource encryption system in colleges and universities, and on the other hand, it provides a new idea for the application research of deep learning algorithm in the field of data encryption.

II. RELATED WORKS

In recent years, the research on encrypted storage has developed more deeply from the perspective of encryption details and user experience. Li M et al. constructed an encrypted storage scheme using a searchable symmetric encryption method and used locally sensitive hash and bloom filter with high search accuracy. The results show that the encryption efficiency of this method is higher than that of the traditional method [5]. Xue K et al. proposed a method to protect encrypted cloud storage from EDOS attacks. This method reduces the resource consumption cost of cloud computing users and can comply with any access policy of cp-abe. The results show that this method has higher security and practicability [6]. Kumar G K's team proposed an encrypted storage algorithm using symmetric encryption keys for the same set of keys. The results show that the algorithm can reduce the data burden of cloud storage in the form of eliminating duplicate data, and can provide more efficient data access by using access policies [7]. Rao E et al. provided a secure data search method for encrypted user data. The results show that this method can provide users with different types of online data while ensuring users' privacy and data security [8].

On the other hand, the research based on cloud platform is gradually diversified. Farhadi H et al. used the cloud platform to quickly and automatically detect the time series image of measuring the burn area, so as to obtain the accurate information of the density and distribution of the combustion area in the large vegetation coverage area. The results show that this method has stronger dynamic real-time performance and can greatly improve the accuracy of the map of the combustion area [9]. Taking the cloud platform as the basic framework of smart education, Liu steam proposed a dual high-precision cooperation strategy to accurately perceive the needs of smart teaching and resource supply. The results show that this method not only improves the effectiveness of communication between teaching resources and learning needs, but also provides teachers and learners with a more personalized and secure data access strategy [10]. Liu P proposed an EV battery voltage evaluation strategy based on cloud platform, and used the spatial clustering method with noise to improve the calculation efficiency of outlier detection. The results show that this method not only maintains high recognition ability, but also reduces the complexity of calculation and has higher calculation efficiency [11]. Choi S et al. Built a digital twin data platform based on cloud platform to facilitate novices to build digital twin data schemes more quickly and easily. An example shows that this method is fast and effective [12]. This research applies the cloud platform, which has compatibility and diversified development direction, to the encrypted storage of teaching resources, and provides the school with a more economical and reliable security scheme of teaching resources through the encrypted storage service of cloud platform.

III. Design of Encrypted Storage Method of Oral English Teaching Resources on Cloud Platform

A. Design of Cloud platform Storage Encryption Method based on Convolutional Neural Network Algorithm

Modern teaching resource storage is divided into three main ways. One is that users graft and train the encryption storage module of teaching resources by themselves. For the school that lacks practical and technical talents in network and intelligent computing technology, the cost of designing the encryption storage system of teaching resources alone is too high, and it is technically impossible to achieve to a certain extent [13]; the second is to use it by renting a third-party encrypted storage model. Although this method can solve its own technical shortcomings, the maintenance cost is still relatively high, and the encrypted storage process is controlled by the third-party organization in the whole process, which has a certain risk; the third is to use cloud platform services for teaching resource storage [14]. For oral English teaching, which needs to constantly update a large number of oral interactive resources, cloud platform encrypted storage is a more secure, economical and real-time encrypted storage method. However, there are still some risks in cloud platform encrypted storage. This risk is mainly reflected in the infrastructure of cloud platform. The infrastructure of cloud platform encrypted storage is shown in Fig. 1.

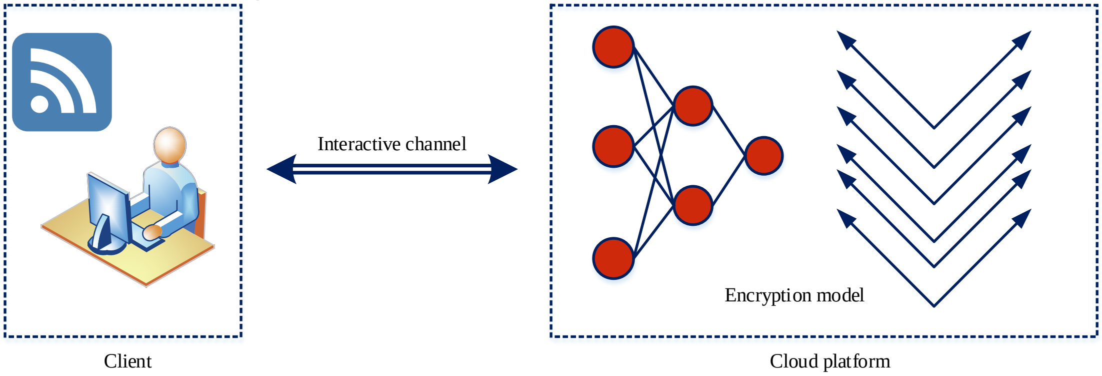


Fig. 1. Cloud platform based encrypted storage architecture

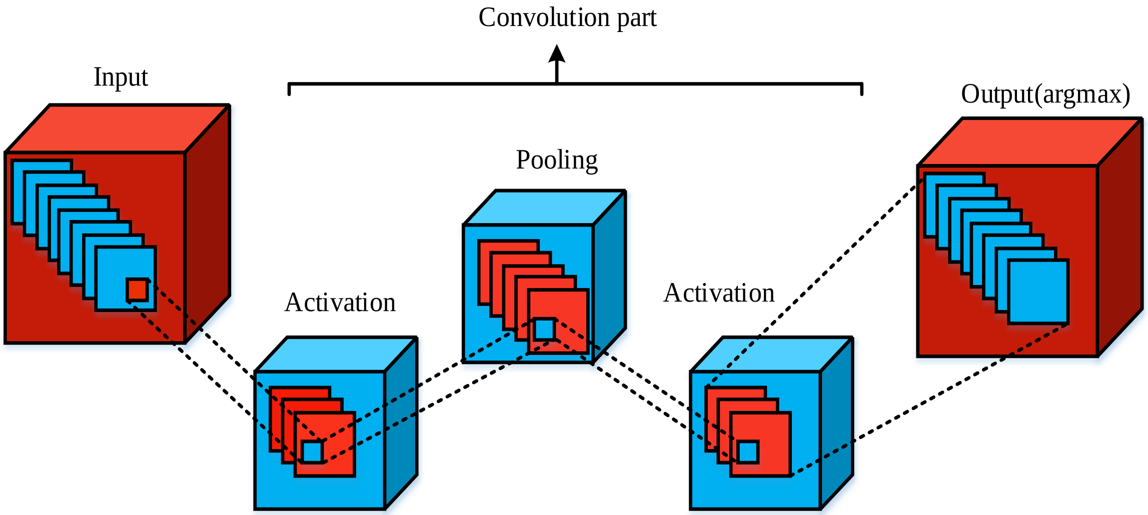


Fig. 2. Convolutional neural network

Fig. 1 shows the basic encrypted storage architecture of the cloud platform. It can be seen that users communicate with the cloud platform mainly through interactive channels. This way of user operation, channel communication, and cloud encrypted storage is easy to form the risk of resource leakage in two parts. One is the security and privacy protection of the cloud platform itself, that is, whether the encrypted storage model used by the cloud platform is reliable; the other is the data transmission security problem that may occur in the process of user interaction with the cloud platform. In this study, the two storage security issues are studied respectively. For the security and privacy protection of the cloud platform itself, this research optimizes the convolutional neural network algorithm based on the characteristics of encrypted storage of spoken English teaching resources. This is mainly because the convolutional neural network itself has strong deep learning ability and structural stability. For the college encryption application scenario, the convolutional neural network has lower application costs, is economical, and requires less maintenance consumption, Colleges and universities can implement the application without consuming a lot of technical support. The specific schematic diagram of the architecture is shown in Fig. 2.

The convolution neural network model in Fig. 2 is divided into three main parts: input part, convolution part and output part. The main input content of the input part of the optimized encrypted storage convolution neural network model in this study is to store the ciphertext used for encryption. This part of ciphertext can be divided into two specific ciphertexts, both of which are $w \times h \times c$ in size. The two ciphertexts are expressed as real part $\left[F(x)_R\right]$ and imaginary part $\left[F(x)_I\right]$ respectively. At this time, the number of plaintext slots of the system is n, and the convolution kernel parameter of plaintext of the system is k, At this time, the convolutional neural network encrypted storage model performs the operation by means of fast Fourier transform, and the real part operation result can be obtained:

$$\left[F(y)_R\right]=\left[F(x)_R\right]\otimes\left[F(f_i)_R\right]\oplus\left[F(x)_I\right]\otimes\left(-F(f_i)_I\right) \tag{1}$$

In formula (1), y represents the convolution result of the algorithm, x represents the input data, $\otimes$ represents homomorphic multiplication, and $\oplus$ represents homomorphic addition. Calculate the imaginary part of the ciphertext in the same way to obtain formula (2):

$$\left[F(y)_I\right]=\left[F(x)_R\right]\otimes\left[F(f_i)_I\right]\oplus\left[F(x)_I\right]\otimes F(f_i)_R \tag{2}$$

$F(f_i)_I$ and $F(f_i)_R$ represent the Fourier transform results of convolution kernel respectively. The cloud platform will automatically generate random variables r after calculation. The size of the random variable r is $w \times h$. On this basis, the cloud platform encrypts the results of the fast Fourier transform and sends the ciphertext to the user. The real encryption formula is shown in formula (3):

$$\left[F(y-r)_R\right]=\left[F(y)_R\right]\oplus\left[-F(r)_R\right] \tag{3}$$

In formula (3), $\left[F(y-r)_R\right]$ represents the real content of the ciphertext sent by the cloud platform to the customer, and $\left[-F(r)_R\right]$ represents the real fast Fourier transform encryption result. The imaginary part ciphertext can be obtained by adopting the same calculation method:

$$\left[F(y-r)_I\right]=\left[F(y)_I\right]\oplus\left[-F(r)_I\right] \tag{4}$$

In formula (4), $\left[F(y-r)_I\right]$ respectively represents the virtual part ciphertext content sent by the cloud platform to customers, and $\left[-F(r)_I\right]$ represents the virtual part fast Fourier transform encryption result. After the user decrypts the ciphertexts at both ends respectively, the two short ciphertexts can be combined to form a complete $F(y-r)$, and then the $(y-r)$ can be obtained by inverse fast Fourier transform. At this time, the cloud platform and the user can share the state of additivity. The common setting formula is:

$$\begin{cases} x^s = r \\ x^c = y-r \end{cases} \tag{5}$$

Where s represents the cloud platform, c represents the client, and r represents that the cloud platform will automatically generate random variables after operation. The plaintext convolution kernel parameters of the convolution neural network model are encrypted and stored. The calculation flow of the encryption process is shown in Fig. 3.

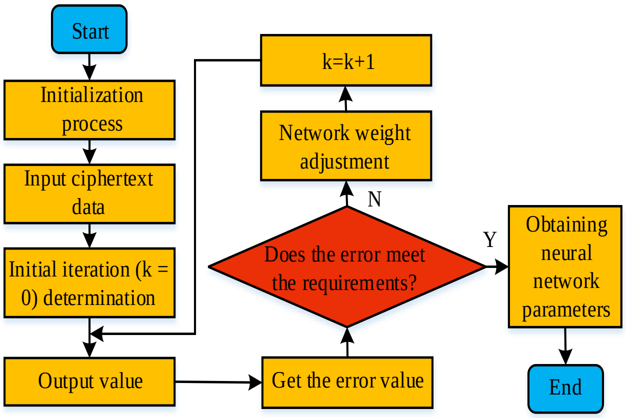
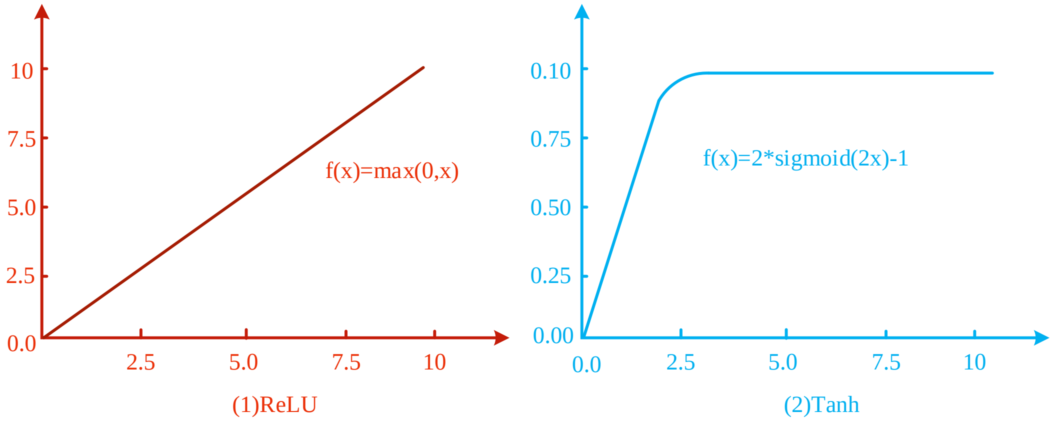

Start
Initialization process
Input ciphertext data
Initial iteration (k = 0) determination
Output value
Get the error value
Does the error meet the requirements?
N
Network weight adjustment
k=k+1
Y
Obtaining neural network parameters
End

Fig. 3. Encrypted convolutional neural network flow

In the practical application of encrypted storage of teaching resources, due to the requirements of oral English teaching storage and real-time update, more complex operations are often required. In this case, the convolution cores of the convolution layer must participate in the independent input and convolution process, so as to obtain their own convolution results. Here, it can be assumed that there are c convolution cores and the same number of data channel inputs in the convolution layer. At this time, the system needs to treat each input and filtering calculation process as a separate data operation group in the ciphertext domain, carry out parallel operation through the operation method in a simple case, obtain c ciphertext individual results at the same time, and then accumulate a large number of ciphertext individual results to form the final overall ciphertext results. In addition to the convolution layer, this study also optimizes the activation layer of the encrypted storage product neural network model. Since the encrypted storage design conducted in this study requires the convolutional neural network model to perform nonlinear calculation, it is necessary to select the nonlinear function of the activation layer. The commonly used convolutional neural network activation functions include tanh function and relu function. The comparison of the function images of the two functions is shown in Fig. 4:



(1)ReLU

(2)Tanh

Fig. 4. Function image comparison

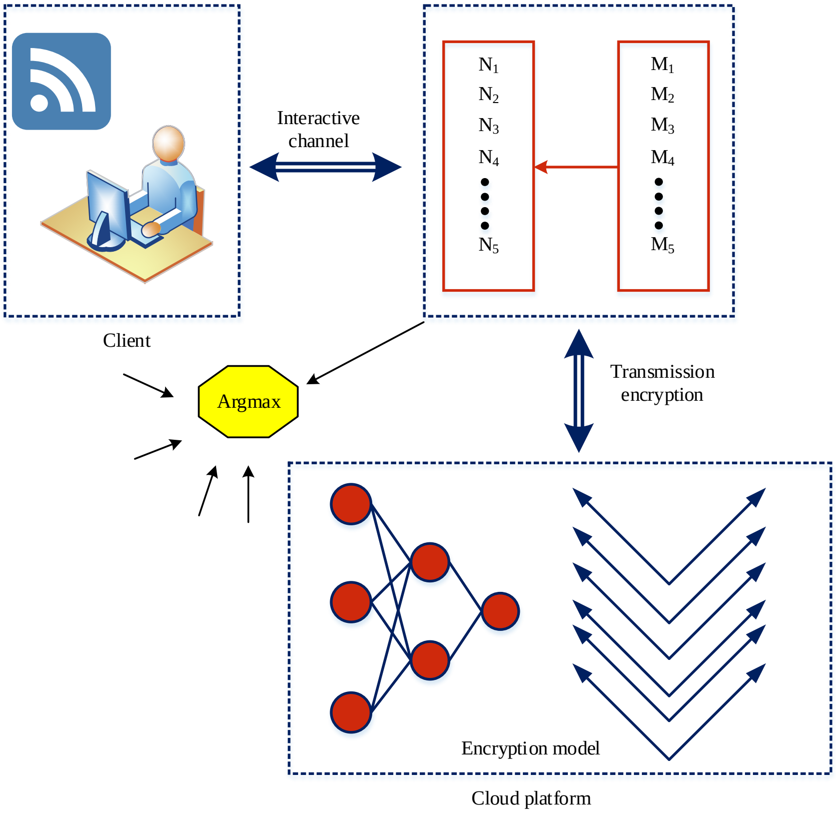


Fig. 5. Storage data transmission optimization

Tanh function formula is shown in formula (6):

$$\tanh(x) = 2 \cdot sigmoid(2x) - 1 \tag{6}$$

As shown in the calculation formula of Lu power division, it is more difficult to select and activate the Lu power division function (Reh) in the design process, so it is more difficult to activate the two kinds of operation formulas:

$$f(x) = \max(0, x) \tag{7}$$

Relu activation function can clear all nonpositive terms in the input data center, balance the size relationship between input data and output data on this basis, enable each neuron to be activated in the process of input and output, and continuously transfer this activation state downward. This method can help the model improve its input sparsity and model activity, and improve the operational performance of the model. Design of cloud platform output encryption method based on argmax algorithm

The ultimate purpose of the encrypted storage model of cloud platform oral English teaching resources designed in this study is to effectively ensure the security of teaching data in the two operations of customer storage and data transmission. Therefore, after the optimization design of the storage model, the research will also carry out the security design for the data transmission part of the cloud platform encrypted storage model, which is mainly optimized by the argmax algorithm, the overall optimization position is shown in Fig. 5:

It can be seen from Fig. 5 that the Argmax algorithm mainly acts on the transmission channel established when users communicate with the cloud platform on the channel, and improves data security by strengthening the reliability in the process of data input and output. In the cloud platform encryption storage algorithm designed in this study, cloud platform has encrypted the oral English teaching resources. When users need to take out or input data from the cloud platform storage, they need to access the data through the common protocol between the client and the cloud platform. This research mainly uses the optimized convolution neural network algorithm as the main storage encryption technology. The output of the last convolution layer in the convolution neural network is called Logits, which represents the weight difference between different categories in the input process, and the main function of the softmax layer is to convert Logits into the vector form representing the probability values of different categories. The softmax function is shown in formula (8):

$$f(x)_k = \frac{e^{x_i}}{\sum_{k=1}^{K} e^{x_k}} \tag{8}$$

Where $i = 1, 2, \ldots, K$, K represents the length of Logits vector. The final classification result can be expressed as:

$$t = \arg\max(\log its) \tag{9}$$

The model connection between softmax layer and argmax algorithm is shown in Fig. 6.

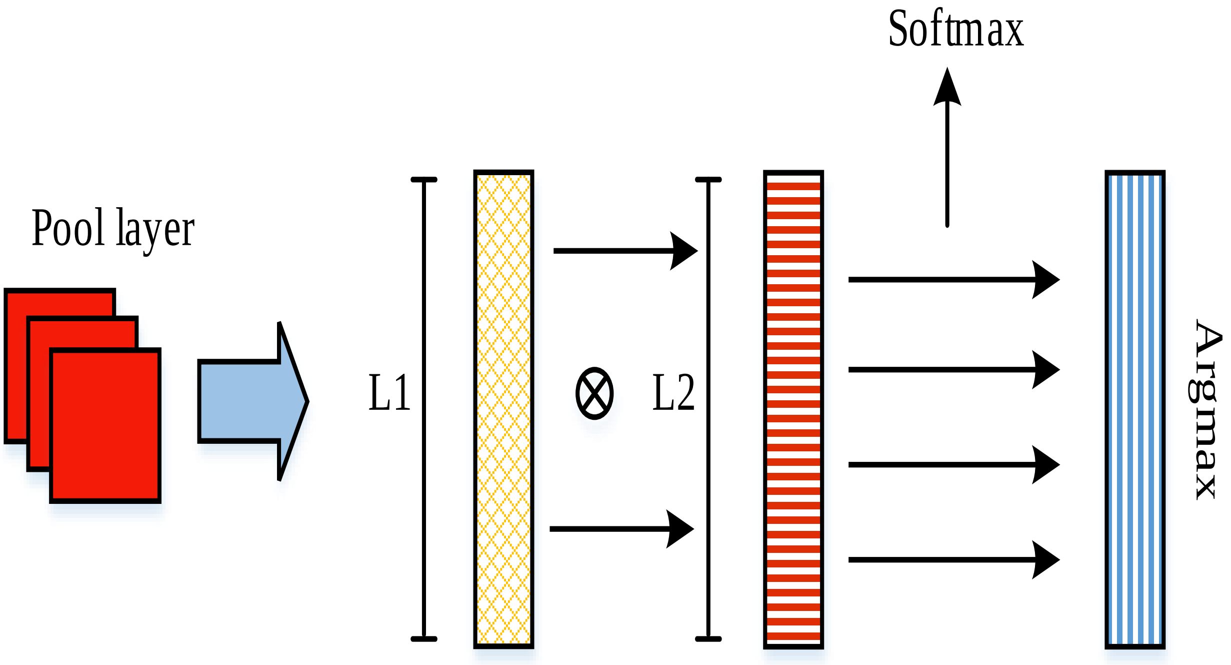


Fig. 6. Model connection

In this study, the improved argmax algorithm is used to encrypt the data access part. The Logits vector obtained from cloud platform encryption can be expressed as:

$$Enc(x)=\left(Enc(x_1),Enc(x_2),\cdots,Enc(x_n)\right) \tag{10}$$

Where x represents the generated random vector. The cloud platform extracts two ciphertexts arbitrarily from the ciphertext set and performs homomorphic subtraction calculation for the ciphertext to obtain $n\cdot(n-1)$ new ciphertexts. The specific matrix is shown in formula (11):

$$\left\{\begin{matrix} [x_1-x_2] & [x_1-x_3] & \cdots & [x_1-x_n] \\ [x_2-x_1] & [x_2-x_3] & \cdots & [x_2-x_n] \\ \cdots & \cdots & \cdots & \cdots \\ [x_n-x_1] & [x_n-x_2] & \cdots & [x_n-x_{n-1}] \end{matrix}\right\} \tag{11}$$

Since the optimized convolutional neural network encryption storage model used in this study adopts the combined encryption mode of real part ciphertext and imaginary part ciphertext, after obtaining the basic Logits vector matrix, it needs to be transformed into the form of double encryption matrix corresponding to the double ciphertext mode. The estimated size of the ciphertext matrix is n, and each individual ciphertext contains $n-1$ plaintext data different from each other, Ciphertext matrix itself has the dual commonalities of cloud platform and client. After the $n-1$ subhomomorphic subtraction, the cloud platform needs to perform random inter row conversion on the ciphertext matrix to obtain the row random matrix formed by the combination of double ciphertext matrices. The specific formula is shown in formula (12):

$$\left\{\begin{matrix} \left[\left(x_{\psi_1}-x_{\pi_{\psi1}(2)}\right)\right. & \left(x_{\psi_1}-x_{\pi_{\psi_1}(3)}\right) & \cdots & \left.\left(x_{\psi_1}-x_{\pi_{\psi1}(n)}\right)\right] \\ \left[\left(x_{\psi_2}-x_{\pi_{\psi2}(1)}\right)\right. & \left(x_{\psi_2}-x_{\pi_{\psi_2}(3)}\right) & \cdots & \left.\left(x_{\psi_2}-x_{\pi_{\psi_2}(n)}\right)\right] \\ \cdots & \cdots & \cdots & \cdots \\ \left[\left(x_{\psi_1}-x_{\pi_{\psi_n}(1)}\right)\right. & \left(x_{\psi_n}-x_{\pi_{\psi n}(2)}\right) & \cdots & \left.\left(x_{\psi_n}-x_{\pi_{\psi n}(n-1)}\right)\right] \end{matrix}\right\} \tag{12}$$

Where $(\psi_1,\ \psi_2,\ldots,\ \psi_n)$ represents a random arrangement of $(1,2,\cdots,\ n)$, and on this basis, $(\pi_{\psi1}(2),\ \pi_{\psi1}(3),\ldots,\ \pi_{\psi1}(3))$ can be obtained by removing ψ_1 from the arrangement, while $(\pi_{\psi2}(1),\ \pi_{\psi2}(3),\ldots,\ \pi_{\psi2}(n))$ represents the nonrandom arrangement after removing ψ_2 from the arrangement. After the cloud platform analogizes the matrix, it then randomizes the matrix of formula (12) with two matrices to obtain:

$$\left\{\begin{matrix} r_2^1 & r_2^1 & \cdots & r_n^1 \\ r_1^2 & r_3^2 & \cdots & r_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ r_1^n & r_2^n & \cdots & r_{n-1}^n \end{matrix}\right\},\left\{\begin{matrix} \varepsilon_2^1 & \varepsilon_2^1 & \cdots & \varepsilon_n^1 \\ \varepsilon_1^2 & \varepsilon_3^2 & \cdots & \varepsilon_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ \varepsilon_1^n & \varepsilon_2^n & \cdots & \varepsilon_{n-1}^n \end{matrix}\right\} \tag{13}$$

Formula (13) represents a random positive number r_j^i, $\varepsilon_j^i\in\left[0,r_j^i\right)$. The first ciphertext matrix and the row random matrix are multiplied by homomorphic multiplication, and then the matrix is interleaved with the second ciphertext matrix by homomorphic subtraction to obtain a fully random ciphertext matrix. The specific matrix is shown in formula (14):

$$\left\{\begin{matrix} \left[r_2^1\cdot\left(x_{\psi_1}-x_{\pi_{\psi_1}}(2)\right)-\varepsilon_2^1\right. & \cdots & \cdots & \left.r_n^1\cdot\left(x_{\psi_1}-x_{\pi_{\psi_1}}(n)\right)-\varepsilon_n^1\right] \\ \left[r_1^2\cdot\left(x_{\psi_2}-x_{\pi_{\psi_2}}(1)\right)-\varepsilon_1^2\right. & \cdots & \cdots & \left.r_n^2\cdot\left(x_{\psi_2}-x_{\pi_{\psi_2}}(n)\right)-\varepsilon_n^2\right] \\ \cdots & \cdots & \cdots & \cdots \\ \left[r_1^n\cdot\left(x_{\psi_n}-x_{\pi_{\psi_n}}(1)\right)-\varepsilon_1^n\right. & \cdots & \cdots & \left.r_{n-1}^n\cdot\left(x_{\psi_n}-x_{\pi_{\psi_n}(n-1)}\right)-\varepsilon_{n-1}^n\right] \end{matrix}\right\} \tag{14}$$

This operation process requires n sub homomorphic subtraction, homomorphic addition and homomorphic multiplication. When different types of homomorphic addition operations are carried out, it is necessary to change the setting mode in the operation process to ensure that the random number generated in the calculation process will not affect the symbol corresponding to the encrypted plaintext, that is, in the homomorphic encryption operation process, its influence on the symbol data is limited by the value range of the associated random number. After the cloud platform obtains the random ciphertext matrix, it can send the matrix information to the access user. The access user decrypts the ciphertext matrix using the common protocol to obtain the plaintext matrix. The specific matrix is shown in formula (15):

$$\left\{\begin{matrix} r_2^1\cdot\left(x_{\psi_1}-x_{\pi_{\psi_1}}(2)\right)-\varepsilon_2^1 & \cdots & \cdots & r_n^1\cdot\left(x_{\psi_1}-x_{\pi_{\psi_1}}(n)\right)-\varepsilon_n^1 \\ r_1^2\cdot\left(x_{\psi_2}-x_{\pi_{\psi_2}}(1)\right)-\varepsilon_1^2 & \cdots & \cdots & r_n^2\cdot\left(x_{\psi_2}-x_{\pi_{\psi_2}}(n)\right)-\varepsilon_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ r_1^n\cdot\left(x_{\psi_n}-x_{\pi_{\psi_n}}(1)\right)-\varepsilon_1^n & \cdots & \cdots & r_{n-1}^n\cdot\left(x_{\psi_n}-x_{\pi_{\psi_n}(n-1)}\right)-\varepsilon_{n-1}^n \end{matrix}\right\} \tag{15}$$

The access client finally counts and classifies the matrix plaintext symbols of each line, and obtains the corresponding real value at the cloud platform.

IV. Effect Analysis of Encrypted Storage Method of Oral English Teaching Resources on Cloud Platform

A. *Analysis of Storage Encryption Effect of Neural Network*

In the part of the effect analysis of the encrypted storage method of oral English teaching resources on the cloud platform, this study will be divided into two parts: cloud platform storage encryption and cloud platform storage and transmission encryption according to the cloud platform structure of oral English teaching resources. The cloud platform storage encryption part takes the optimized convolutional neural network storage encryption model as the main encryption storage tool. Therefore, this research will analyze the connection layer performance of the model, the running time and overhead of the model, and the efficiency of encryption and decryption. In order to explore the performance change of the model when the user input demand increases but the model output is stable, the performance of the model connection layer is analyzed. The performance analysis of the connection layer of the model is shown in Fig. 7.

Fig. 7 shows the operation performance changes of the connection layer under different input levels when the output level is fixed. Here, the operation performance changes are measured mainly by running time. As can be seen from Fig. 7, the operation efficiency of the model running time in the setting stage and the operation stage is significantly different. Under almost all input variables, the operation efficiency of the model connection layer in the operation stage is significantly higher than that in the setting stage. On this basis, observing the operation efficiency caused by the change of input variables, it can be found that when the value of input variables is between 2000 and 2500 and between 4000 and 4500, the operation efficiency of the connection layer has changed greatly. When the input variable value is between 2000 and 2500, the running time of the connection layer in the setting stage increases from 5.4ms to 7.8ms, while the running time of the connection layer in the setting stage increases from 2.9ms to 4.1ms, and the running efficiency decreases significantly. This is because the plaintext slot size of the model in this study is 2048, that is, a ciphertext in the model can support 2048 plaintext at the same time when it is most saturated, Therefore, when the amount of input data exceeds this amount, the operation efficiency of the model connection layer is greatly affected. In addition, in the stage where the value of the input variable is between 4000 and 4500, it is the node when the number of inputs exceeds twice the number of plaintext slots, so the impairment of operational efficiency is more obvious. To sum up, when the number of inputs does not exceed the number of plaintext slots, the performance of the connection layer of the model involved in this time is relatively reliable, but after exceeding, the performance will be affected to some extent, which is a normal phenomenon. In this study, the overall running time and running cost of the model is tested by distinguishing the storage encryption scheme from the convolution neural model. The convolution neural model selects the MNIST model and cifar-10 model respectively, and the storage encryption scheme selects minions and gazelle. The specific test results are shown in Fig. 8.

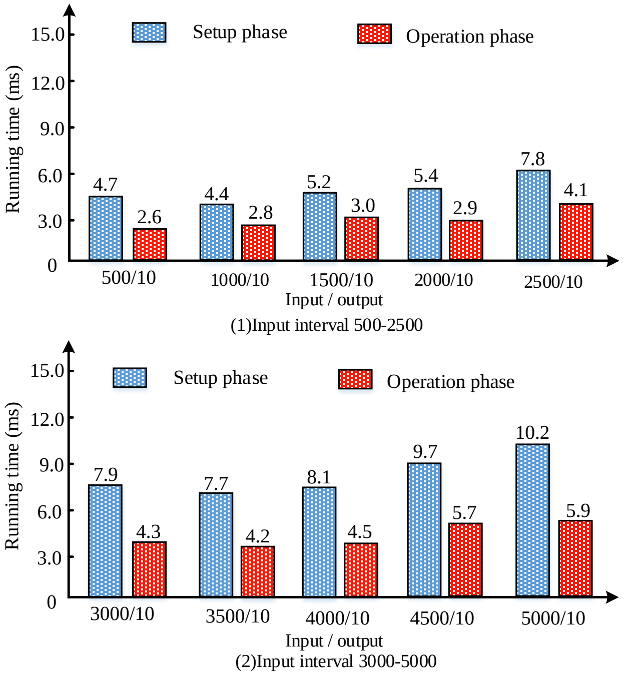
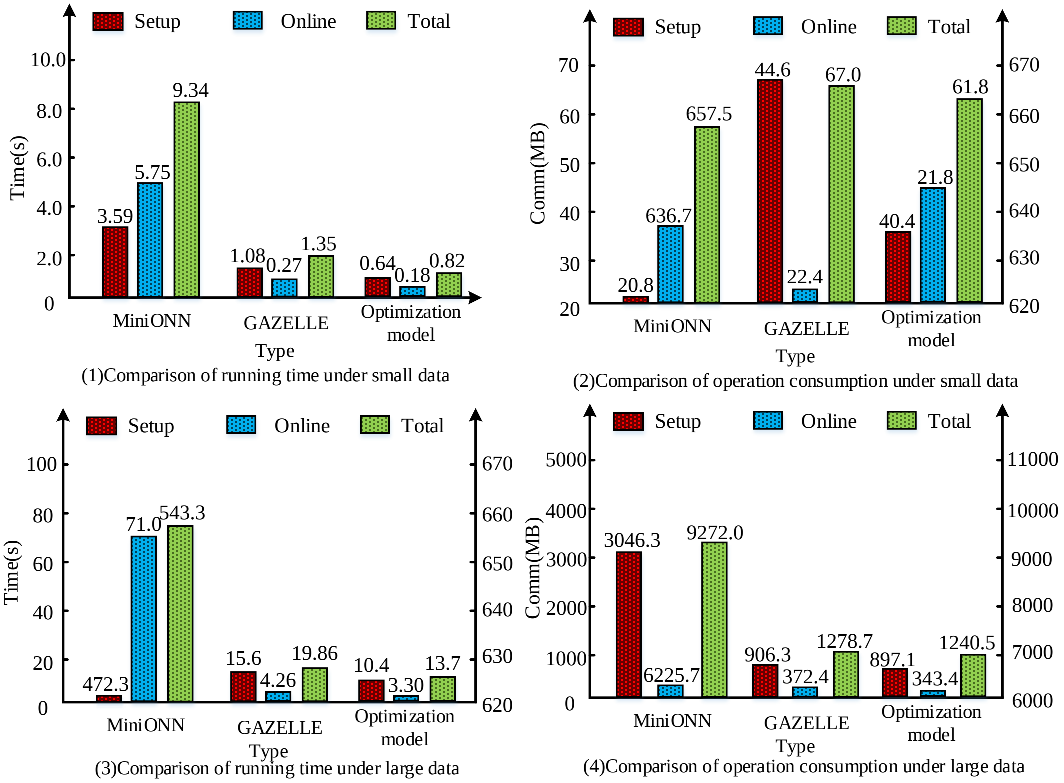


Fig. 7. Performance analysis of connection layer



(1)Comparison of running time under small data

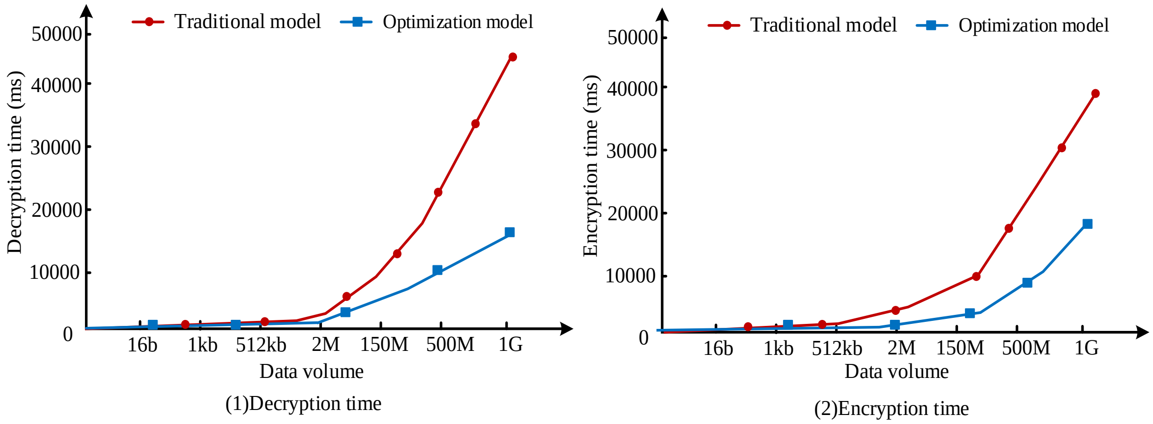
(2)Comparison of operation consumption under small data

(3)Comparison of running time under large data

(4)Comparison of operation consumption under large data

Fig. 8. Data set performance test

Fig. 8 compares and analyzes the models from the perspectives of running time and running cost. The results show that the running time of the model optimized in this study is 0.64ms under the small data set, 0.18ms online, and 0.82ms overall. The overall running time is less than 9.34ms of the minion model and 1.35ms of the gazelle model, and the running time in the setting stage and online stage is smaller; In terms of running cost, the model optimized in this study sets the running cost to 40.4 MB under the small data set, the online running cost to 21.8 MB, and the overall running cost to 61.8 MB. The overall running cost is less than 657.5 MB for the minion model and 67.0 Mb for the gazelle model, and the running cost is less in the setting stage and online stage; Under the large data set, the set running time of the model optimized in this study is 10.4ms, the online running time is 3.30ms, and the overall running time is 13.7ms. The overall running time is less than 543.3ms of the minion model and 19.86ms of the gazelle model, and shows significant advantages in the running time of the setting stage and online stage; In terms of running cost, the model optimized in this study sets the running cost as 897.1 MB under large data set, 343.4 MB on-line running cost and 1240.5 MB overall running cost. The overall running cost is less than 9272.0 MB for the minionn model and 1278.7 MB for the gazelle model, and the running cost in the setting stage and online stage is smaller. The analysis of the encryption and decryption efficiency of the model is shown in Fig. 9.



(1)Decryption time

(2)Encryption time

Fig. 9. Analysis of encryption and decryption efficiency

It can be seen that the encryption time and decryption time of the traditional model and the model optimized in this study show a positive proportional trend with the increase of the data scale. In terms of encryption time, taking the 512KB data scale as the starting point, the encryption time of the traditional model and the model designed in this study has increased significantly, but the encryption time of the model optimized in this study on each data scale node is relatively less, and the highest time point is no more than 20000ms; The decryption time of each node of the traditional research model is not less than 2m, but the decryption time of each node of the traditional design model is not less than 2m. It can be seen that the optimized models have higher operation efficiency in the process of encryption and decryption.

B. *Analysis of Output Encryption Effect of argmax Algorithm*

In the cloud platform storage and transmission encryption analysis part, this research first analyzes the running time and transmission efficiency of optimizing the traditional module of argmax. In the analysis process, the research will take the category parameters and precision values as the main distinguishing dimensions. The correlation analysis of category parameters is shown in Fig. 10.

It can be seen that the operation time and operation consumption data of the optimized argmax output encryption module under the three category parameters of 10, 100, and 1000 are 0. It can be seen that the optimized argmax output encryption module does not need to operate in the setting stage. In the online operation stage, when the category parameter is 10, the operation time of the system is 0.21ms; When the category parameter rises to 100, the running time of the system is 2.01ms; When the category parameter rises to 1000, the running time of the system is 20.01ms; It can be seen that the running time of the optimized argmax output encryption module shows an increasing trend with the increase of category parameters. In terms of system operation consumption, when the category parameter is 10, the system operation consumption data is 0.59 Mb; When the category parameter rises to 100, the consumption data of the system is 5.92 Mb; When the category parameter rises to 1000, the consumption data of the system is 59.21 Mb; It can be seen that the amount of data transmitted by the optimized argmax output encryption module shows an increasing trend with the growth of category parameters. It can also be seen from the growth law of the two indicators that with the increase of category parameters in the order of 10 times, the running time and the amount of transmitted data of the system also increase in the order of 10 times. This indicates that the operation efficiency and loss of the system are relatively stable and will not exceed the expected additional loss with the increase in operation demand, which proves that the overall system is still stable in the face of the excessive operation. As different precision operations will lead to different system operation costs, if the system has a large difference in operation costs between high precision and low precision, the overall system operation stability will be insufficient, which will easily lead to higher performance consumption and resource waste. Therefore, the research will analyze the system costs under different precision. The specific accuracy analysis results are shown in Fig. 11.

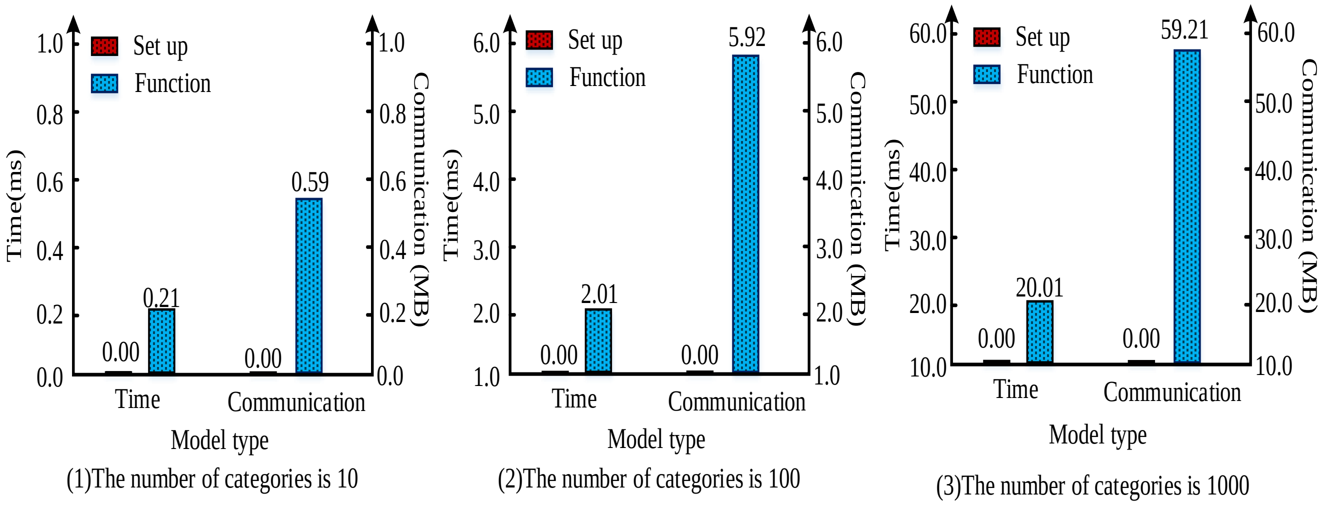
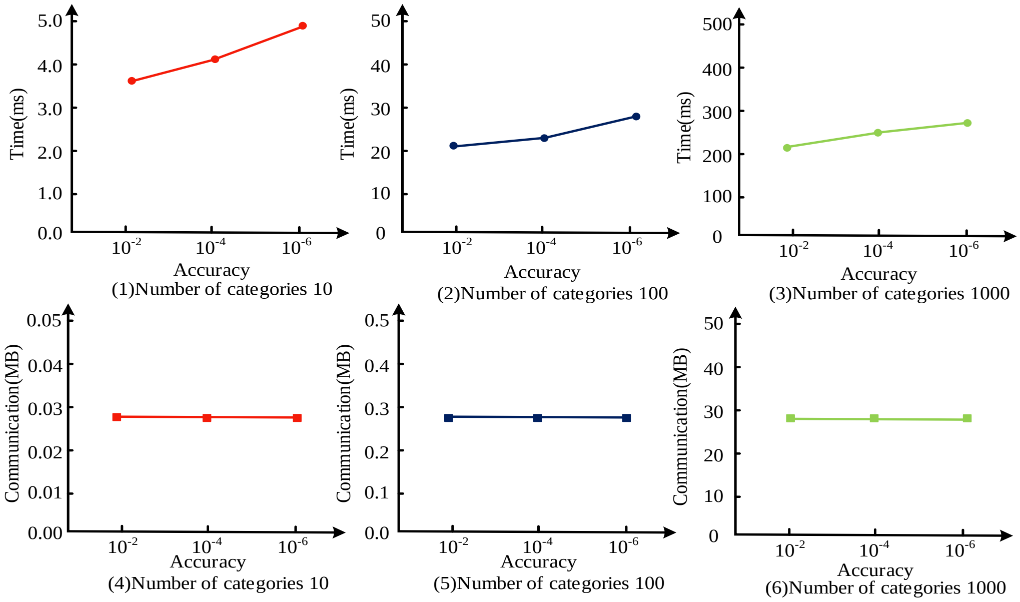


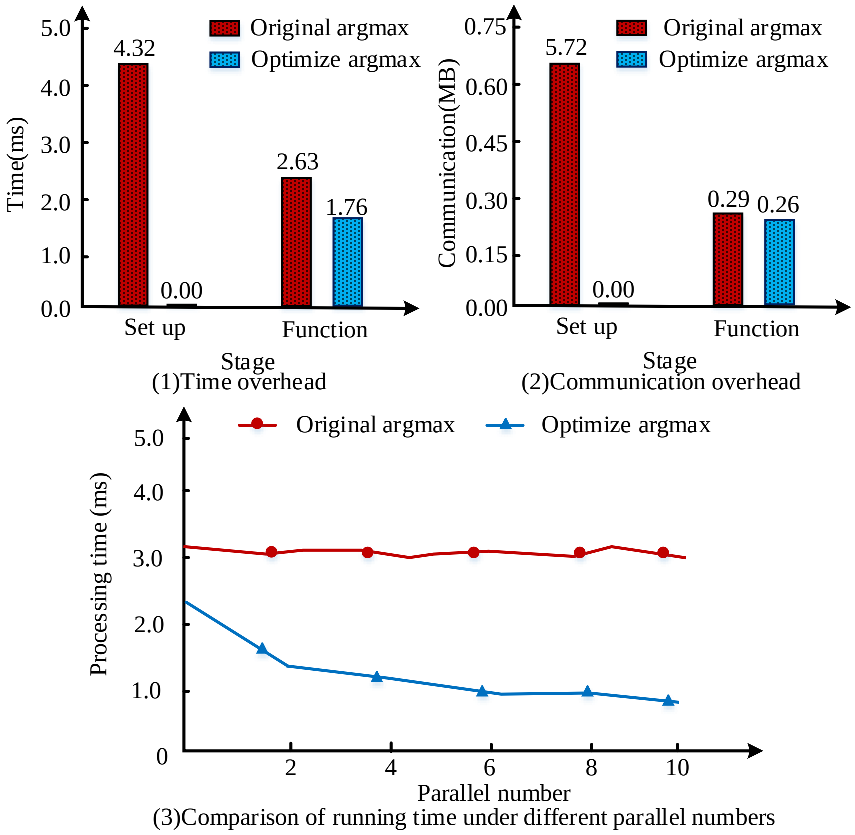
Fig. 10. Category parameter analysis



(1)Number of categories 10 (2)Number of categories 100 (3)Number of categories 1000

(4)Number of categories 10 (5)Number of categories 100 (6)Number of categories 1000

Fig. 11. Accuracy analysis



(1)Time overhead (2)Communication overhead

(3)Comparison of running time under different parallel numbers

Fig. 12. Performance comparison of overall transmission module

Fig. 11 analyzes the running time and running consumption of 10, 100, and 1000 parameters under the accuracy conditions of 10-2, 10-4, and 10-6. The results show that when the category parameter is 10, the running time of the system increases gradually with the increase of accuracy, the overall range is between 3.0 and 5.0, while the running consumption does not fluctuate, and remains at 0.028 under all accuracy; When the category parameter is 100, the running time of the system also shows a gradually increasing trend with the increase of accuracy, the overall range is between 0.2 and 0.3, while the running consumption does not fluctuate and remains at 0.28 under all accuracy; When the category parameter is 1000, the running time of the system still shows a gradually increasing trend with the increase of accuracy, the overall range is between 20 and 30, while the running consumption does not fluctuate and remains at 28 under all accuracy. It can be seen that the setting and online operation efficiency of the system increase with the increase of accuracy, but the overall operation cost does not change with the change of accuracy but maintains the overall consistency, and the overall operation resource consumption is relatively stable. The comparative analysis of the overall system performance is shown in Fig. 12.

Fig. 12 compares the optimized argmax output encryption module with the traditional argmax output encryption module. The results show that the optimized argmax output encryption module in this study will not produce running time and running consumption in the system setting stage, which is because the optimized argmax output encryption module does not need to be calculated in the setting stage. From the perspective of online operation, the running time and running loss of the optimized argmax output encryption module are relatively small. The running time of the traditional argmax output encryption module is 2.63ms, while the running time of the optimized argmax output encryption module is 1.76ms, the running loss of the traditional argmax output encryption module is 0.29mb, and the running time of the optimized argmax output encryption module is 0.26mb. In addition, from the perspective of system processing time, with the increase of parallel number, the overall system processing time of the optimized argmax output encryption module is less than that of the traditional argmax output encryption module, and with the increase of parallel number, the system processing time of the optimized argmax output encryption module shows a certain downward trend. It can be seen that the optimized argmax output encryption module has stronger encryption processing performance.

V. Conclusion

To solve the budget problems and technical difficulties caused by the localized encrypted storage of oral English teaching data, this study takes the cloud platform as the main encrypted storage platform of teaching resources, optimizes the convolutional neural network from the perspective of ciphertext encryption and decryption, and takes it as the main model of cloud platform data storage encryption. On this basis, it studies the encryption improvement of argmax algorithm, makes it more efficient in storing encrypted data, and finally tests the computing performance of the main part and transmission part of the encrypted storage model of the cloud platform. The results show that the overall running time of the encryption model is 0.82 MS under small data sets; the overall running cost is 61.8 MB, and the overall running time is 13.7ms under large data sets; the overall running cost is 1240.5 MB, which is less than other comparable models. The longest consumption time of encryption and decryption of the research and design encryption model is no more than 20000 MS, which is significantly less than that of the traditional model. In terms of encrypted data transmission, the running time of the optimized argmax output encryption module is 1.76ms and the running loss is 0.26 MB, which is less than the traditional encryption model. It can be seen that the encryption model designed in the research has higher security and higher encryption and decryption efficiency in the encrypted storage and transmission of oral English education resources. At the same time, the cloud platform itself also has strong realizability and economic advantages, which is more suitable to help the school carry out the encrypted storage of oral English education resources and improve the security and access efficiency of educational resources.

References

[1] J. Deng, W. Yang, Q. W. Li, et al. “Research and Application of Fire Power Cloud Platform,” Procedia Engineering, vol. 211, pp. 911-916, 2018.

[2] X. Feng, F. Yan, X. Y. Liu, et al. “Development of IoT Cloud Platform Based Intelligent Raising System for Rice Seedlings,” Wireless Personal Communications, vol. 122, no. 2, pp. 1695-1707, 2021.

[3] R. S. Kumar, L. Parthiban, “Privacy preservation in big data with encrypted cloud data storage using walrus,” International Journal of Pure and Applied Mathematics, vol. 119, no. 15, pp. 1833-1842, 2018.

[4] M. Uphoff, M. Wander, T. Weis, et al. “SecureCloud: An Encrypted, Scalable Storage for Cloud Forensics,” pp.1934-1941, 2018.

[5] M. Li, G. Wang, S. Liu, et al. “Multi-keyword Fuzzy Search over Encrypted Cloud Storage Data.” Procedia Computer Science, vol. 187, no. 2, pp. 365-370, 2021.

[6] K. Xue, W. Chen, W. Li, et al. “Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage,” IEEE Transactions on Information Forensics and Security, pp. 2062-2074, 2018.

[7] G. K. Kumar, E. A. Reddy, B. Mamatha, et al. “Access Policy’s Over Encrypted Cloud Storage for Secure Deduplication,” International Journal of Engineering & Technology, vol. 7, no. 3, pp. 27-31, 2018.

[8] E. Rao, “Enhanced Effective and Privacy Preserving Multi Keyword Search over Encrypted Data in Cloud Storage Using Blowfish Algorithm,” Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 2, pp. 2845-2853, 2021.

[9] H. Farhadi, M. Mokhtarzade, H. Ebadi, et al. “Rapid and automatic burned area detection using sentinel-2 time-series images in google earth engine cloud platform: a case study over the Andika and Behbahan Regions, Iran,” Environmental Monitoring and Assessment, vol. 194, no. 5, pp. 1-19, 2022.

[10] S. Liu, Y. Dai, Z. Cai, et al. “Construction of Double-Precision Wisdom Teaching Framework Based on Blockchain Technology in Cloud Platform,” IEEE Access, vol. 9, pp. 11823-11834, 2021.

[11] P. Liu, J. Wang, Z. Wang, et al. “Cloud Platform-Oriented Electrical Vehicle Abnormal Battery Cell Detection and Pack Consistency Evaluation with Big Data: Devising an Early-Warning System for Latent Risks,” IEEE Industry Applications Magazine, no. 99, pp. 2-13, 2021.

[12] S. Choi, J. Woo, H. P. Yang, et al. “User-Friendly Method of Digital Twin Application based on Cloud Platform for Smart Manufacturing,” Transactions of the Korean Society of Mechanical Engineers A, vol. 45, no. 2, pp. 175-184, 2021.

[13] Q. Yan. “Design of Teaching Video Resource Management System in Colleges and Universities based on Microtechnology,” Security and Communication Networks, no. 4, pp. 1-11, 2021.

[14] O. Kolesnyk, IP. Bubeník, J. Apek. “Cloud platform for learning factories,” Transportation Research Procedia, vol. 55, no. 23, pp. 561-567, 2021.