Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 18 No. 18 (2024) | OPEN ACCESS

https://doi.org/10.3991/ijim.v18i18.51493

PAPER

Application of Mobile Technology in Enterprise Management: From Mobile Office to Intelligent Decision Support

Fan Yang(✉)

Shijiazhuang College of Applied Technology, Shijiazhuang, China

2018000872@sjzpt.edu.cn

ABSTRACT

With the rapid advancement of information technology, the application of mobile technology in enterprise management has become increasingly widespread. From mobile office solutions to intelligent decision support systems, the proliferation of mobile technology has not only enhanced operational efficiency but also provided more flexible and convenient management methods. Existing research indicates that the adoption of mobile office solutions enables enterprises to overcome limitations of time and space, improving work efficiency and employee satisfaction. Additionally, the implementation of intelligent decision support systems allows enterprises to make faster and more accurate business decisions. However, current studies often focus on individual mobile technologies or application scenarios, lacking a systematic exploration of mobile office data sharing and intelligent decision-making collaboration. Moreover, most research overlooks privacy protection issues in the enterprise management decision-making process. To address these gaps, this paper proposes a scheme for mobile office data sharing and intelligent decision-making collaboration and examines the integration of privacy protection in the decision-making process. The findings not only enrich the theoretical framework of management studies but also provide enterprises with a systematic and practical solution for mobile technology applications, enhancing management efficiency and intelligence while effectively safeguarding data privacy and security.

KEYWORDS

mobile technology, enterprise management, mobile office, intelligent decision support, data sharing, privacy protection

1 INTRODUCTION

With the rapid development of information technology, the application of mobile technology in enterprise management has become increasingly widespread [1–3]. From mobile office solutions to intelligent decision support, the proliferation of

Yang, F. (2024). Application of Mobile Technology in Enterprise Management: From Mobile Office to Intelligent Decision Support. *International Journal of Interactive Mobile Technologies (iJIM)*, 18(18), pp. 4–18. https://doi.org/10.3991/ijim.v18i18.51493

Article submitted 2024-06-13. Revision uploaded 2024-07-28. Final acceptance 2024-07-31.

mobile technology has not only improved operational efficiency but also provided enterprises with more flexible and convenient management methods [4, 5]. With the popularity of mobile devices such as smartphones and tablets, employees can access and process work information anytime and anywhere, greatly altering traditional office models [6–9]. At the same time, advancements in mobile technology have also driven the development of data analysis and decision support systems, making enterprise management more intelligent and data-driven.

Research on the application of mobile technology in enterprise management has significant theoretical and practical implications. Firstly, the widespread adoption of mobile office solutions allows enterprises to overcome time and space limitations, enhancing work efficiency and employee satisfaction [10, 11]. Secondly, the application of intelligent decision support systems enables enterprises to make faster and more accurate business decisions, increasing their competitiveness. By studying the application of mobile technology in these areas, new management ideas and methods can be provided to enterprises, enriching the theoretical framework of management studies and advancing academic research [12–15].

Although a large number of studies have explored the application of mobile technology in enterprise management, there are still some shortcomings and deficiencies [16]. Firstly, existing research often focuses on individual mobile technologies or application scenarios, lacking systematic research on mobile office data sharing and intelligent decision-making collaboration. Secondly, most studies overlook privacy protection issues in the enterprise management decision-making process and fail to effectively address the conflict between data security and privacy protection [17–19]. Therefore, it is necessary to conduct in-depth research on these issues to address the shortcomings of existing research.

This paper mainly studies two major applications of mobile technology in enterprise management: mobile office data sharing and intelligent decision-making collaboration solutions, as well as privacy integration in the enterprise management decision-making process. Through an in-depth exploration of these two aspects, this paper aims to provide enterprises with a systematic and practical solution for mobile technology applications, which can enhance management efficiency and intelligence while effectively protecting data privacy and security. The research results not only have significant theoretical value but also provide guidance and reference for practical application in enterprises.

2 MOBILE OFFICE DATA SHARING AND INTELLIGENT DECISION-MAKING COLLABORATION SOLUTIONS

2.1 Data preparation

In the application scenario of mobile office data sharing, the credibility and security of the data are crucial. To ensure the reliability of data during sharing and usage, this paper adopts a consortium blockchain-based data preparation method. Mobile office participants will use the SHA256 hashing function to generate the hash value A for local data. To further ensure data security and tamper-proofing, mobile office participants will use a pre-set key value, which is the edge server's ID, RT_u. Participants will concatenate this key value with the current hash generation time S, so the generated hash value has timestamp characteristics, preventing replay attacks and tampering. Then, mobile office participants will query the corresponding hash value B from the blockchain at the given time point and compare it with the locally

generated hash value *A*. If hash values *A* and *B* are consistent, it indicates that the local data has not been tampered with and matches the record on the blockchain, confirming data credibility. After confirming the data's credibility, mobile office participants can use this data to train intelligent control models. The training process is conducted locally to ensure data privacy is not compromised. If hash values *A* and *B* are inconsistent, it indicates that the local data may have been tampered with or does not match the blockchain record. In this case, mobile office participants will reject using this batch of data for model training. Figure 1 shows the overall framework of the mobile office consortium blockchain network.

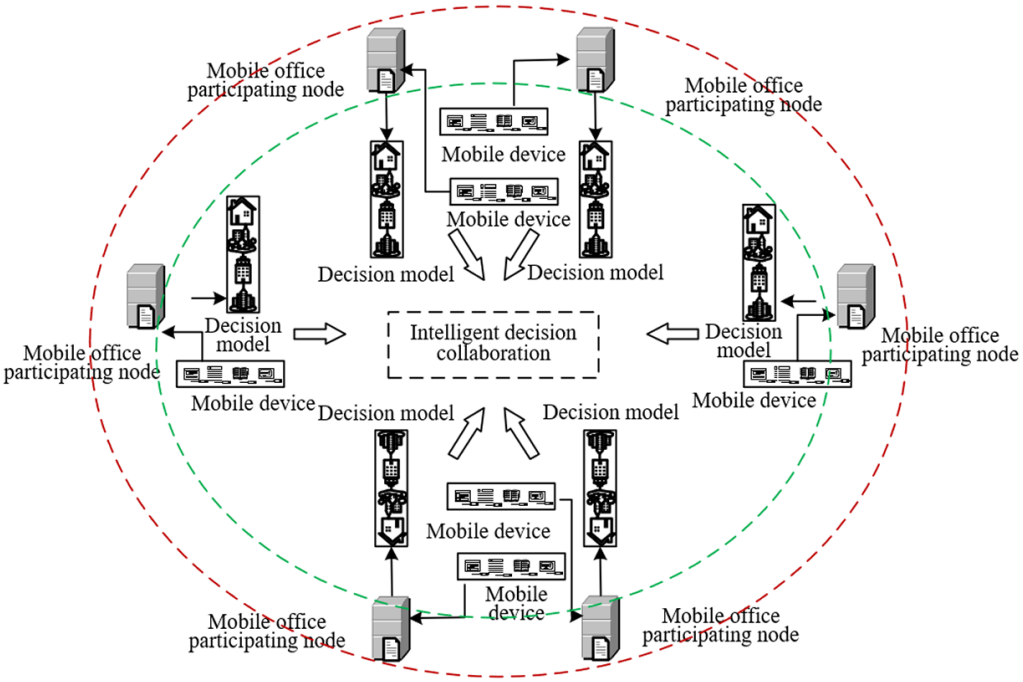

Fig. 1. Overall framework of the mobile office consortium blockchain network

2.2 Decision model

In the application scenarios of mobile office and enterprise management, the effectiveness and accuracy of decisions are crucial. The consortium blockchain-based enterprise management decision model can enhance the reliability of the decision-making process by ensuring data credibility and transparency. This paper proposes a consortium blockchain-based enterprise management decision model that utilizes artificial neural networks to support intelligent decision-making in mobile office environments.

Specifically, in the model construction phase, this paper uses two artificial neural networks to handle different decision tasks. The input layer parameters of the two networks are the same, using basic enterprise management data and historical decision results as input parameters. The input layer is set to eight nodes, reflecting the main data dimensions required for decision-making. The first artificial neural network is used to predict decision types in enterprise management, such as resource allocation and project priority setting. Based on the model's needs, the output layer is set to six nodes, corresponding to different decision types. The number of hidden layer nodes is determined empirically to be 11, ensuring the model has sufficient

learning and generalization capabilities. The second artificial neural network is used to predict specific execution actions, such as the approval or rejection of processes and budget adjustments. The output layer is set to four nodes, corresponding to key action types in the work, such as approval, rejection, increase, and decrease. The number of hidden layer nodes is set to six, ensuring accurate prediction of execution actions without increasing model complexity. The collaboration of these two neural network models can help enterprises achieve rapid and accurate decision support in a mobile office environment. By deeply learning from basic data and historical decision results, the model can anticipate future management needs and provide corresponding operational recommendations.

Assuming the elements of the hidden layer output vector G are represented by g_k, the elements of the output layer output vector P are represented by p_u, the weights and thresholds between the input layer and the hidden layer are represented by q_{uk} and n_k, and the weights and thresholds between the hidden layer and the output layer are represented by q_{kj} and n_j, where the number of input layer nodes is represented by u and j, the number of hidden layer nodes is represented by k, and the sigmoid activation function is represented by d. The signal propagation process of the constructed artificial neural network can be characterized by the following equation:

$$\begin{cases} g_k = d\left(\sum_{u=1}^{8} q_{uk} \cdot a_u + n_k\right), k = 1,2,\ldots,11 \\ p_k = d\left(\sum_{u=1}^{11} q_{kj} \cdot g_k + n_j\right), j = 1,2,\ldots,8 \end{cases} \tag{1}$$

Assuming the number of input layer nodes is represented by v, the number of output layer nodes is represented by m, and the number of hidden layer nodes is represented by l, the calculation formula for the number of hidden layer nodes is:

$$l = \sqrt{vm} \tag{2}$$

2.3 Data upload to the blockchain

In mobile office scenarios, the reliability and transparency of data sharing and intelligent decision-making are crucial. The principle of data upload to the consortium blockchain in mobile office applications enhances collaborative efficiency and decision-making reliability through the immutability and transparency of data. Before data is uploaded to the blockchain, the unique identifier key formed during the data preparation phase, combined with the summary value of the decision data and execution results, will be stored on the consortium blockchain. The value includes specific details of decisions such as approval results, project priorities, descriptions of execution actions like approval, rejection, or delay, and the hash values of this data to ensure data integrity and tamper-proofing.

When these decision data summaries are stored on the consortium blockchain, the decision analysis party can query the matching decision results from the blockchain based on the server ID and data hash value. If a decision result is successfully matched, the parsed results will be sent to the relevant execution party, which will perform the actual operations based on the parsed results and return the execution results. After receiving the execution results, the decision analysis party will record the time of return and the ID of the execution device and store this data on the blockchain again.

This means that the decision return time and the execution device ID are used as the key values, and the decision execution result is used as the value stored on the consortium blockchain. If the blockchain query fails to match the corresponding decision result, it indicates that there is no executable decision record for the current data. In this case, it is necessary to obtain the latest data for decision analysis and upload the new decision result to the blockchain. This cyclical mechanism ensures the continuous updating and effectiveness of decision data in the mobile office environment.

3 PRIVACY INTEGRATION IN THE ENTERPRISE MANAGEMENT DECISION-MAKING COLLABORATION PROCESS

3.1 Local model training

In the enterprise management decision-making collaboration process, the training mode based on multi-key homomorphic encryption and blockchain group federated learning frameworks can effectively ensure data privacy while improving decision accuracy and efficiency. This mode uses multi-key homomorphic encryption technology and blockchain technology, combined with federated learning algorithms, to achieve secure data sharing and collaborative training among various mobile office participants, thereby generating a globally optimized enterprise management decision model. Figure 2 shows the blockchain-federated learning model architecture for enterprise management decision-making collaboration.

Each enterprise management department or subsidiary, as a mobile office participant, possesses its own local business data set $F = \{f_1, f_2, ..., f_v\}$. Each node PM has local training model parameters $\mu_l = \{\mu_1, \mu_2, ..., \mu_u\}$ and local data with labels $f_l = \{(a_1, b_1), (a_2, b_2), ..., (a_u, b_u)\}$, where a_u is the input parameter and b_u is the corresponding expected output. To protect data privacy, this data is encrypted locally and is not directly shared with other nodes or the central server.

During training, each node uses the stochastic gradient descent algorithm to minimize its loss function. Specifically, each node O_l calculates the gradient of the loss function on its local data set f_l and updates the local model parameters μ_l based on this. Since multi-key homomorphic encryption technology is used, nodes can perform calculations in the encrypted state, ensuring data privacy while computing gradients and updating model parameters. Let $d_k(a_k, b_k; \mu_l)$ represent the value of the loss function on the data sample (a_k, b_k), and $|f_l|$ represent the number of samples in the data set. Then the loss function of node O_l on the training data set f_l is given by:

$$M(\mu_l) = \frac{1}{|f_l|} \sum_{k \in f_j} d_k(a_k, b_k; \mu_l) \tag{3}$$

The formula for gradient calculation is given by:

$$\nabla M(\mu_l) = \frac{\partial M(\mu_l)}{\partial \mu_l} \tag{4}$$

Assuming the learning rate is denoted by λ, the gradient of the loss function for parameter $\mu_l(s-1)$ is denoted by $\lambda \cdot \nabla M(\mu_l(s-1))$. For node O_j during the s-th iteration, the formula for updating model parameters is given by:

$$l_j(s) = \mu_l(s-1) - \lambda \cdot \nabla M\left(\mu_l(s-1)\right) \tag{5}$$

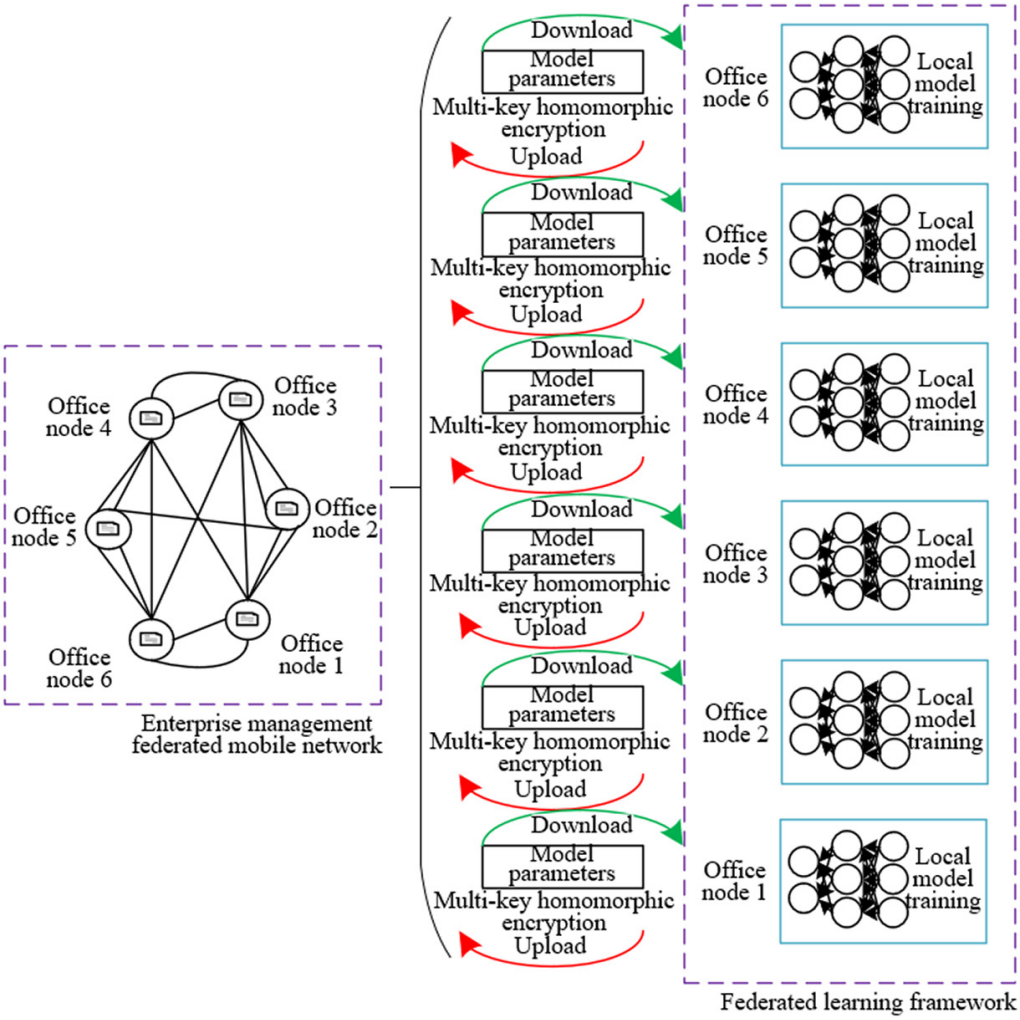

Fig. 2. The blockchain-federated learning model architecture for enterprise management decision-making collaboration

3.2 Privacy integration mechanism

In the enterprise management decision-making collaboration process, the privacy integration mechanism based on multi-key homomorphic encryption and the blockchain group federated learning framework ensure data security and decision efficiency. This mechanism achieves privacy protection and collaborative optimization among mobile office participants in 13 specific steps, as follows:

Step 1: Generate public parameters: In the enterprise management decision-making collaboration process, the public parameters of the Ring Learning with Errors (RLWE)-based homomorphic encryption scheme need to be initialized first. This step is carried out by the user certificate management organization, Fabric-CA. Specifically, Fabric-CA generates a random vector $x \leftarrow I(E_w^f)$ based on the given public parameter settings, including RLWE dimension v, ciphertext modulus w, key distribution υ, and error distribution Ω on E. These parameters constitute the public parameters of RLWE and are returned to the mobile office participants, forming the public parameter set $oo^{ELQR} = (v, w, \upsilon, \Omega, x)$. Through Fabric-CA's management, mobile office participants can obtain certified and verified public parameters, ensuring the security and reliability of the parameter generation process.

Step 2: Obtain public parameters: After generating the public parameters, different departments or subsidiaries in the enterprise management system can obtain these public parameters through the blockchain network. Each node uses these public parameters to generate its key pair, preparing it for use in subsequent model training and data sharing processes. This step ensures that all mobile office participants can securely obtain and use the same public parameters, enabling collaborative operations under the same encryption framework.

Step 3: Generate a private key, a public key, and an evaluation key: In the enterprise management decision-making collaboration process, each mobile office participant needs to independently generate its encryption key pair and evaluation key to ensure effective encryption and secure processing of data during collaborative decision-making. First, each node uses the public parameters to generate a private key and a public key. Specifically, mobile office participants sample the private key t_u from distribution υ and sample the error vector $r \leftarrow \Omega^f$ from E_w^f, then calculate the public key $y_u = -t_u \cdot x + r$ $(MOD\ w)$. Next, the node generates the evaluation key F_u. The specific steps are: sampling a random number e from υ, sampling error vectors $r_1 \leftarrow \Omega^f$, $f_1 \leftarrow I(E_w^f)$, and $r_2 \leftarrow \Omega^f$, and calculating $f_0 = -t_u \cdot f_1 + r_1 + e \cdot h$ $(MOD\ w)$ and $f_2 = e \cdot x + r_2 + t_u \cdot h$ $(MOD\ w)$, finally obtaining the evaluation key $F_u = \left[f_0 \middle| f_1 \middle| f_2 \right] \in E_w^{fx3}$. These keys will be used for subsequent homomorphic encryption and decryption operations, ensuring data privacy during transmission and processing.

Step 4: Upload public key: After generating the public key, mobile office participants need to upload their public key to the blockchain network. Each node uploads its generated public key y_u to the blockchain, where these public keys are stored for other nodes to query and use. This step ensures that other nodes can use these public keys for homomorphic encryption and computation, enabling secure data sharing and collaborative computation.

Step 5: Generate local model parameters: In the enterprise management decision-making collaboration process, each mobile office participant first trains the model locally to generate the model parameters for the current training round. During this process, nodes independently conduct model training without sharing plaintext model parameters to ensure data privacy. Nodes train the model locally based on their own data sets and compute the model parameters for the current round. These model parameters contain the characteristics and training results of the node's data, but to protect data privacy, these parameters will not be shared in plaintext with other nodes.

Step 6: Encrypt gradient information: After generating the local model parameters, mobile office participants need to encrypt the model parameters using their public keys to protect the privacy of gradient information. The encryption process is as follows: Each node encrypts the plaintext model parameters ω. First, a random number n is sampled from distribution υ, and error vectors r_0 and r_1 are sampled from Ω. Then, the two parts of the ciphertext are calculated: $z_0 = n \cdot y + \omega + r_0$ $(MOD\ w)$ and $z_1 = n \cdot x + r_1$ $(MOD\ w)$. The final generated ciphertext is $z_s = (z_0, z_1)$. This process ensures the security of the parameters during transmission and sharing, preventing sensitive information leakage.

Step 7: Upload ciphertext: In the enterprise management decision-making collaboration process, mobile office participants store the encrypted parameter information on the blockchain after encrypting the local model parameters. By storing the ciphertext on the blockchain, nodes can ensure that sensitive information remains encrypted even in the public distributed ledger, thereby protecting data privacy. At the same time, the distributed nature of the blockchain enhances the system's

reliability and resistance to attacks, further improving the security of the entire collaborative decision-making process.

Step 8: Obtain an encrypted gradient: After the ciphertext is uploaded to the blockchain, the distributed ledger stores the gradient information of each node under encryption conditions. Mobile office participants can autonomously obtain the required gradient information from the blockchain and perform homomorphic operations in encrypted form. To decrypt and proceed with further collaboration, all selected mobile office participants must participate in the decryption process. The decryption process is achieved through a multi-key mechanism, requiring multi-party cooperation to complete, further enhancing security and preventing the risk of single-point leakage.

Step 9: Homomorphic operations: In the enterprise management decision-making collaboration process, mobile office participants can perform homomorphic operations, including addition and multiplication, on local data after obtaining the gradient information of other nodes. Specifically, nodes can first use the addition operation in the multi-key homomorphic encryption scheme to perform addition calculations on two ciphertexts at the same level, with the formula $zs^{-\prime} = zs_1^{-} + zs_2^{-}(MOD\ wm)$. Secondly, nodes can perform multiplication operations, that is, multiplying two ciphertexts at the same level and returning the relinearized ciphertext $zs^{-\prime}$. After the multiplication operation, to ensure that the ciphertext modulus does not exceed the decryption capacity, rescaling is performed. This operation reduces the ciphertext modulus to a decryptable range, specifically calculated as $z'_u = \left[o_m^{-1} \cdot z_u\right]$, and returns the new ciphertext $zs^{-\prime}$. Through these homomorphic operations, nodes can perform necessary mathematical operations without decrypting the data, thereby ensuring data privacy and computational accuracy.

Step 10: Partial decryption: Multi-key homomorphic encryption requires all mobile office participants to participate in the decryption process to ensure data security and privacy. For the homomorphic computation results within the group, each mobile office participant first uses its private key to perform partial decryption of the results. The specific step is that nodes use their private key z_u to decrypt the ciphertext t_u, perform partial decryption operations, and calculate the partially decrypted ciphertext $\omega_u = z_u \cdot t_u + r_u\,(MOD\ w)$ by sampling the error r_u. In this way, each node independently calculates the partial decryption result, and only after aggregating the partial decryption results of all nodes can the complete decryption information be obtained.

Step 11: Share partially decrypted ciphertext: In the enterprise management decision-making collaboration process, mobile office participants store their partially decrypted ciphertext on the blockchain after completing partial decryption. The partially decrypted ciphertext stored on the blockchain can be accessed by other mobile office participants within the group. This sharing mechanism leverages the transparency and immutability of the blockchain, ensuring the secure transmission and storage of partially decrypted ciphertext, further enhancing data credibility and security.

Step 12: Decryption by other nodes: Other mobile office participants within the group can obtain these partially decrypted ciphertexts from the blockchain and continue the decryption process according to the method in step 10. Each node independently obtains the partially decrypted ciphertext from the blockchain and continues decryption using its private key until all mobile office participants within the group complete their partial decryption tasks. This ensures a distributed and secure decryption process, preventing single-point failures and potential data leakage risks.

Step 13: Update parameters: After all mobile office participants complete partial decryption, the mobile office participants within the group will obtain the partial decryption results of other nodes from the blockchain and perform local decryption merge operations. By combining all partial decryption results and the initial ciphertext, nodes can obtain the final plaintext $\omega = z_0 + \sum_{u=1}^{j} \omega_u (MOD\ w)$. After obtaining the plaintext, mobile office participants will share the global parameters through the blockchain with other nodes. Other nodes obtain the plaintext global parameters from the blockchain and calculate the global fusion parameters locally, then update their local training parameters.

3.3 Federated fusion process

In the enterprise management decision-making collaboration process, the federated fusion process based on multi-key homomorphic encryption and the blockchain group federated learning framework aim to ensure data privacy while achieving efficient decision collaboration.

Specifically, each enterprise management node sets the necessary parameters for federated learning, including learning rate λ, local batch size Y, number of iterations R, etc. Then, the initial global model parameters are released so that all mobile office participants can obtain these initial values from the blockchain, preparing for the upcoming local training. Each mobile office participant updates its local model parameters based on the global model parameters obtained from the blockchain. Next, nodes conduct model training on their local datasets, and the training process proceeds according to the predetermined number of iterations. When the number of iterations meets the set requirements, nodes generate their local model parameters, μ_u^s.

Nodes encrypt the generated μ_u^s using the multi-key homomorphic encryption algorithm, obtaining the encrypted model parameters $R_{J\text{-}ZJJT}\left[\mu_u^s\right]$. These encrypted parameters are stored on the blockchain, leveraging the blockchain's distributed storage and immutability to ensure the security and transparency of the parameters. On the blockchain, the encrypted model parameters $R_{J\text{-}ZJJT}\left[\mu_u^s\right]$ of all mobile office participants are retrieved and homomorphically summed to obtain the fused encrypted parameters $R_{J\text{-}ZJJT}[SUM(\mu^s)]$. The advantage of homomorphic computation is that it operates directly on the encrypted data without needing decryption, ensuring data privacy during the computation process.

After homomorphic computation is completed, the mobile office participants jointly decrypt the encrypted fusion results $R_{J\text{-}ZJJT}[SUM(\mu^s)]$, obtaining the decrypted fusion parameters $SUM(\mu^s)$. This process requires the collaboration of all nodes within the group to ensure the accuracy of the decryption results and the security of the data. The decrypted fusion parameters $SUM(\mu^s)$ are obtained by each node, and the global model parameters μ^s for this round of fusion are calculated based on the number of mobile office participants. The method for calculating the global parameters is to divide $SUM(\mu^s)$ by the number of mobile office participants, thereby obtaining the averaged global model parameters.

The finally calculated global model parameters (μ^s) are released on the blockchain, providing new initial parameters for the next round of local training. Each mobile office participant obtains the latest global parameters from the blockchain, updates the local model again, and enters the next round of model training and parameter fusion. Assuming the global model after the s-th round of fusion is represented by μ^s, the model of the u-th participant updated locally after the $s + 1$ round

is represented by M_u^{s+1}, and the global model after the $s+1$ round of fusion is represented by μ^{s+1}. The global model update formula is given by the following equation:

$$\mu^{s+1} = \mu^s + \frac{1}{J}\sum_{u=1}^{l}\left(M_u^{s+1} - \mu_u^s\right) \tag{6}$$

4 EXPERIMENTAL RESULTS AND ANALYSIS

From the length-time charts shown in Figures 3 and 4, the data characteristics of the mobile office email service and the mobile office online storage service under the mobile office mode can be deduced. The experimental results show that the number of uplink and downlink data packets for the mobile office email service is relatively small and scattered. Specifically, data transmission in the mobile office network mainly occurs during upload and download operations, while reading emails does not significantly consume traffic. Observing the curve, it can be found that more than 50% of the data packet sizes are below 200 bytes, and about 40% of the data packet sizes are distributed between 200 and 1500 bytes. Additionally, the ultra-large uplink data packet appearing around 110 seconds in the experiment is due to attachment uploads. The above data characteristics reveal that in the mobile office environment, the network bandwidth demand is mainly concentrated in the attachment processing stage. Therefore, when designing mobile technology application solutions, the efficiency of data transmission can be optimized for this situation to improve the user experience.

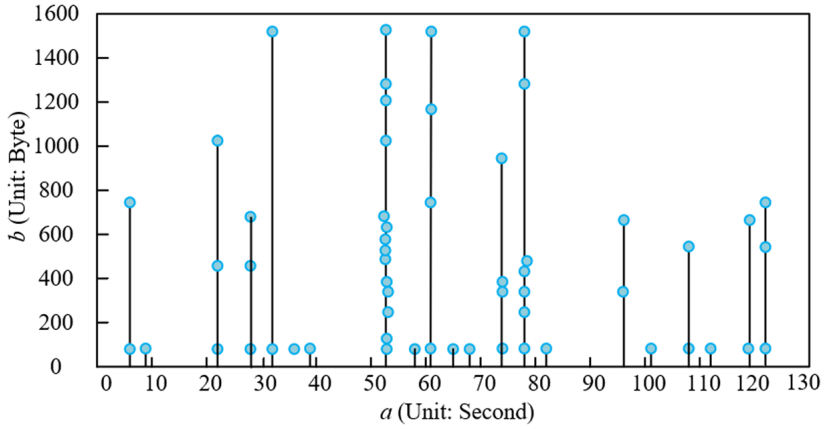

Fig. 3. Length-time segment of mobile office email service data packets

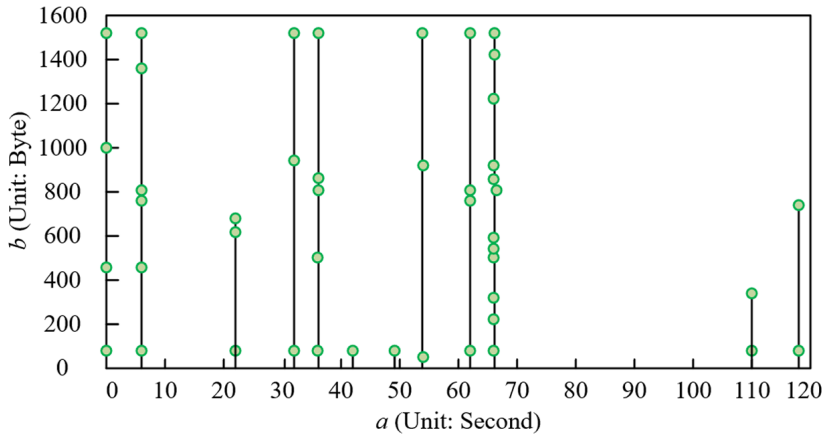

Fig. 4. Length-time segment of mobile office online storage service data packets

By analyzing the length-time charts of the online storage service, the experimental results show significant differences in the lengths of uplink and downlink data packets. Specifically, the data shows that more than 50% of the uplink data packets are over 2000 bytes, with the maximum data packet length reaching 16512 bytes; in contrast, over 96% of the downlink data packets are 60 bytes in length. Throughout the experiment, 95% of the data transmission was caused by the operation of uploading two songs. During the upload process, a large number of ultra-large uplink data packets are generated, accompanied by a large number of 60-byte downlink acknowledgment packets. The data transmission is generally sparse, but there are several dense clusters of data, which account for about 90% of the total data volume. The experimental results reveal that the data transmission characteristics of the online storage service in a mobile office environment are mainly concentrated in the process of uploading large data packets, especially when dealing with large files, where the number and size of uplink data packets significantly increase. This indicates that the online storage service in a mobile office environment has high demands on uplink bandwidth, while downlink bandwidth is mainly used for transmitting small acknowledgment packets. Enterprises should focus on optimizing and managing uplink bandwidth to ensure effective handling of peak data traffic during large file uploads while further improving overall data transmission stability and efficiency by optimizing the transmission efficiency of downlink acknowledgment packets. Additionally, the presence of these dense data clusters suggests periodic peaks in data transmission, allowing enterprises to optimize network resource allocation to enhance data transmission reliability and user experience.

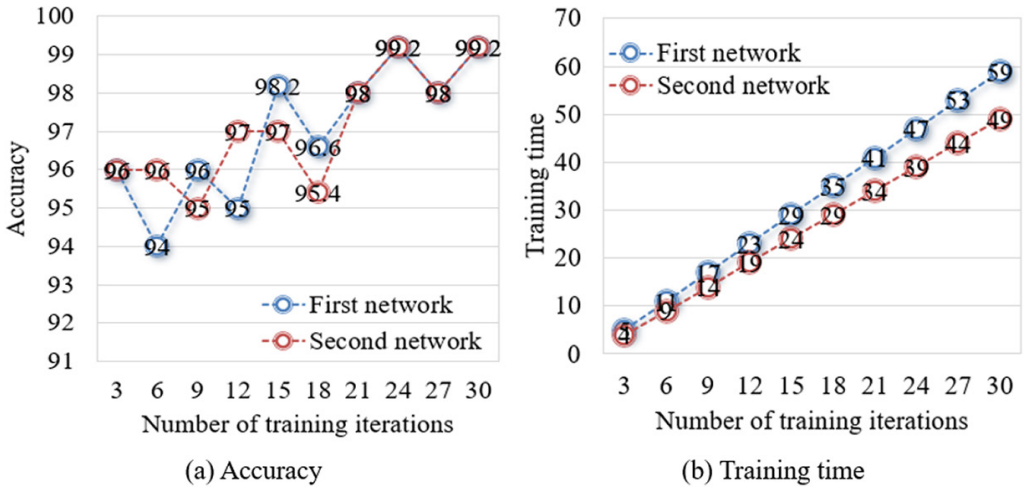

Fig. 5. Training performance of the constructed decision model

From the training performance data shown in Figure 5, it can be seen that the two artificial neural networks exhibit certain differences in accuracy and training time. For the first network, the accuracy reaches 98.2% after 15 training iterations, then fluctuates slightly, reaching 99.2% again after 30 iterations. The second network's accuracy reaches 96% after 6 training iterations, then improves to 97% after 12 iterations, reaching 99.2% after 30 iterations. In terms of training time, the training time of the first network gradually increases with the number of training iterations, from five minutes at three iterations to 59 minutes at 30 iterations; in contrast, the training time of the second network is shorter, increasing from four minutes to 49 minutes. Combining the experimental results, it is evident that the first network exhibits significant changes in accuracy and training time. Despite the longer training time,

its accuracy improvement is significant with increased training iterations, demonstrating strong learning ability and stability. The second network performs more efficiently in training time, with accuracy gradually improving with the number of training iterations, ultimately reaching the same accuracy level as the first network. Overall, the performance of both networks in different decision tasks meets the high accuracy requirements in enterprise management. The first network is suitable for decision tasks requiring deeper analysis and higher accuracy, while the second network has an advantage in time efficiency, making it suitable for business scenarios requiring quick responses. By combining these two artificial neural networks, enterprises can achieve efficient and precise management in mobile office data sharing and intelligent decision-making collaboration solutions, while further enhancing overall management efficiency and intelligence through optimization of training time and accuracy.

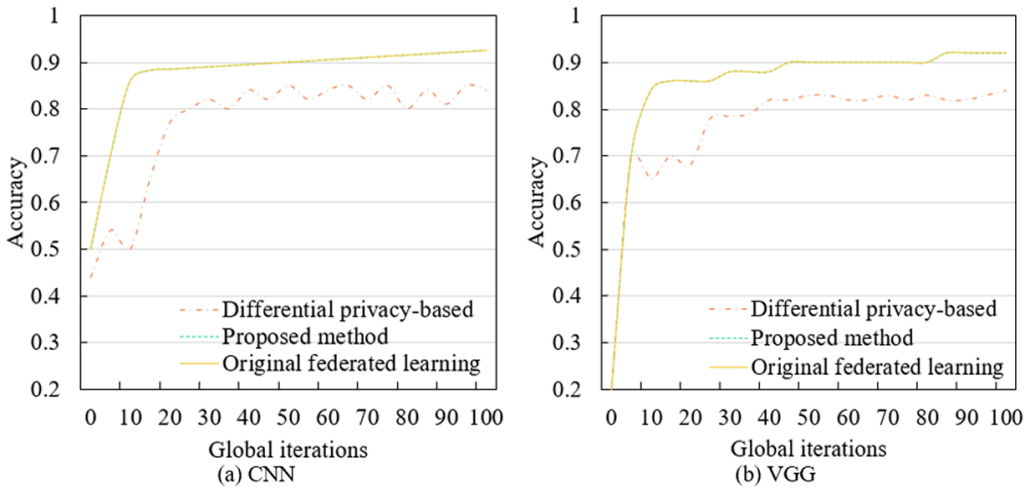

Fig. 6. Training performance of the constructed decision model

From the experimental results of the CNN model shown in Figure 6, it can be seen that during the global iterations from 0 to 100, the accuracy of the proposed method and the original federated learning consistently remained high, with both achieving an accuracy of 92.5% at each iteration point. In comparison, the method based on differential privacy exhibits stable performance in the early iterations, with accuracy gradually increasing from an initial 0.44 to 0.85, but shows some fluctuations in the later iterations, failing to exceed 0.85. For the VGG model, both the proposed method and the original federated learning show a consistent accuracy growth trend during the global iterations from 0 to 100, ultimately reaching 92% at 100 iterations. The method based on differential privacy performs well in the early iterations, with accuracy increasing from 0.2 to 0.84, but in the later iterations, the accuracy remains between 0.83 and 0.84, slightly lower than that of the proposed method and the original federated learning. Combining the experimental results, the following conclusions can be drawn: the proposed method and the original federated learning show almost consistent performance in both the CNN and VGG models, and they significantly outperform the method based on differential privacy in all global iterations. This indicates that the proposed multi-key homomorphic encryption and blockchain group federated learning framework can effectively ensure data privacy without sacrificing model accuracy and, in some cases, can further enhance performance. The method based on differential privacy performs well initially but slightly

lags in the later stages, suggesting that its privacy protection mechanism may negatively impact model accuracy under higher iterations. Therefore, the efficiency and stability of the proposed method make it more suitable for application scenarios in enterprise management decision collaboration that require high data privacy and model accuracy. By combining multi-key homomorphic encryption and blockchain technology, the proposed method not only improves the accuracy and efficiency of decision-making but also provides a more reliable solution for intelligent enterprise management and data security protection.

5 CONCLUSION

This paper primarily studied two major applications of mobile technology in enterprise management: mobile office data sharing and intelligent decision-making collaboration solutions, and privacy fusion in the enterprise management decision-making collaboration process. Through an in-depth discussion of these two aspects, this paper aims to provide enterprises with a systematic and feasible mobile technology application solution that can both improve the efficiency and intelligence level of enterprise management and effectively protect the privacy and security of enterprise data. Specifically, this paper first analyzed the data packet characteristics of email services and online storage services in a mobile office environment and described them in detail through length-time segments. Secondly, this paper constructed a decision model and evaluated its training performance, focusing on the application of multi-key homomorphic encryption and blockchain technology in the federated learning framework to ensure data privacy protection and the efficiency of the decision model. Experimental results show that in the aspect of mobile office data sharing, the analysis of the length-time segments of data packets in email services and online storage services demonstrates the characteristics of data during transmission, providing a basis for subsequent data processing and privacy protection measures. In the aspect of intelligent decision-making collaboration solutions, through the training of CNN and VGG models, the proposed method and the original federated learning method show a high consistency in accuracy during the global iterations from 0 to 100, ultimately reaching 92.5% in the CNN model and 92% in the VGG model. The method based on differential privacy performed well in the initial iterations but showed some fluctuations in the later iterations, failing to surpass the proposed method and the original federated learning.

Although this study has achieved significant results, there are still some limitations. The research is mainly based on specific datasets and experimental environments, which may not fully represent the actual application scenarios of all enterprises. Additionally, the implementation complexity and cost of multi-key homomorphic encryption and blockchain technology may pose certain limitations for some small and medium-sized enterprises. To address these limitations, future research can expand and deepen aspects such as diversifying datasets and real-world scenario validation, optimizing algorithms and reducing costs, and expanding application scenarios. By verifying with more diverse datasets and real enterprise scenarios, the applicability and universality of the proposed method can be further verified; researching more efficient encryption algorithms and blockchain technologies to reduce implementation complexity and costs, improving its acceptability for small and medium-sized enterprises; and exploring the application of the proposed method in other enterprise management fields, such as supply chain management, customer relationship management, etc., to further enhance its application value.

6 REFERENCES

[1] M. Shakir, M. J. Al Farsi, I. R. Al-Shamsi, B. Shannaq, and T.-H. Ghilan Al-Madhagy, "The influence of mobile information systems implementation on enhancing human resource performance skills: An applied study in a small organization," *International Journal of Interactive Mobile Technologies*, vol. 18, no. 13, pp. 37–68, 2024. https://doi.org/10.3991/ijim.v18i13.47027

[2] P. K. Choudhary, S. Routray, P. Upadhyay, and A. K. Pani, "Adoption of enterprise mobile systems – An alternative theoretical perspective," *International Journal of Information Management*, vol. 67, p. 102539, 2022. https://doi.org/10.1016/j.ijinfomgt.2022.102539

[3] I. M. Ali, M. N. Mohd Nawi, M. Y. Hamid, F. I. A Jalil, and B. Hussain, "Integration of IoT, data analytics and mobile application towards digitisation facilities management: A case study," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 22, pp. 154–164, 2021. https://doi.org/10.3991/ijim.v15i22.24115

[4] M. T. Hamid and M. Abid, "Decision support system for mobile phone selection utilizing fuzzy hypersoft sets and machine learning," *Journal of Intelligent Management Decision*, vol. 3, no. 2, pp. 104–115, 2024. https://doi.org/10.56578/jimd030204

[5] A. I. Suroso, I. Fahmi, and H. Tandra, "Adoption of mobile internet and the implication on palm oil productivity: Case study in Siak Regency," *International Journal of Sustainable Development and Planning*, vol. 18, no. 1, pp. 335–342, 2023. https://doi.org/10.18280/ijsdp.180135

[6] A. El Mettiti and M. Oumsis, "A survey on 6G networks: Vision, requirements, architecture, technologies and challenges," *Ingénierie des Systèmes d'Information*, vol. 27, no. 1, pp. 1–10, 2022. https://doi.org/10.18280/isi.270101

[7] A. Elmorshidy, "M-commerce security: Assessing the value of mobile applications used in controlling internet security cameras at home and office – An empirical study," *International Journal of Information Security and Privacy*, vol. 15, no. 4, pp. 79–97, 2021. https://doi.org/10.4018/IJISP.2021100105

[8] M. R. Rahman and M. M. Rahman, "Impact of digital financial services on customers' choice of financial institutions: A modified UTAUT study in Bangladesh," *International Journal of Safety and Security Engineering*, vol. 13, no. 3, pp. 409–421, 2023. https://doi.org/10.18280/ijsse.130304

[9] M. R. Ahmad and A. Awang, "Wi-Fi offloading on mobile data communication in the office, the measurement study," *Przeglad Elektrotechniczny*, vol. 10, 2023. https://doi.org/10.15199/48.2023.10.32

[10] I. Al-Surmi, B. Raddwan, and I. Al-Baltah, "Next generation mobile core resource orchestration: Comprehensive survey, challenges and perspectives," *Wireless Personal Communications*, vol. 120, pp. 1341–1415, 2021. https://doi.org/10.1007/s11277-021-08517-w

[11] J. Ding, Y. Li, P. Zhang, and D. Jin, "Time dependent pricing for large-scale mobile networks of urban environment: Feasibility and adaptability," *IEEE Transactions on Services Computing*, vol. 13, no. 3, pp. 559–571, 2017. https://doi.org/10.1109/TSC.2017.2713779

[12] T. D. Jayarathne, N. De Silva, and W. K. U. R. M. K. P. K. Samarakoon, "Adopting smart retrofits: A decision-making model and benchmarking criteria," *Built Environment Project and Asset Management*, vol. 14, no. 3, pp. 366–383, 2024. https://doi.org/10.1108/BEPAM-02-2023-0034

[13] S. Leem, J. Oh, D. So, and J. Moon, "Towards data-driven decision-making in the Korean film industry: An XAI model for box office analysis using dimension reduction, clustering, and classification," *Entropy*, vol. 25, no. 4, p. 571, 2023. https://doi.org/10.3390/e25040571

[14] G. Schneider, N. Segadlo, and M. Leue, "Forty-eight shades of Germany: Positive and negative discrimination in federal asylum decision making," *German Politics*, vol. 29, no. 4, pp. 564–581, 2020. https://doi.org/10.1080/09644008.2019.1707810

[15] L. Furman, R. Gornowicz, A. Kozuch, and K. Adamowicz, "Optimising the decision-making process in the management of forest building infrastructure," *Sylwan*, vol. 167, no. 9, pp. 606–616, 2023. http://doi.org/10.26202/sylwan.2023074

[16] Y. Xie and Y. Liu, "Tripartite evolutionary game analysis of stakeholder decision-making behavior in energy-efficient retrofitting of office buildings," *Sustainability*, vol. 14, no. 18, p. 11697, 2022. https://doi.org/10.3390/su141811697

[17] J. Weinberg, "Feelings of trust, distrust and risky decision-making in political office. An experimental study with national politicians in three democracies," *Comparative Political Studies*, vol. 56, no. 7, pp. 935–967, 2023. https://doi.org/10.1177/00104140221139376

[18] J. S. Kim and B. K. Kim, "Examining different technology transfer capabilities and their counterpart works from two different positions," *Technology in Society*, vol. 68, p. 101856, 2022. https://doi.org/10.1016/j.techsoc.2021.101856

[19] T. Guimaraes and K. Paranjape, "Assessing the overall impact of data analytics on company decision making and innovation," *International Journal of Business Analytics*, vol. 8, no. 4, pp. 34–51, 2021. https://doi.org/10.4018/IJBAN.2021100103

7 AUTHOR

Fan Yang graduated from Hebei University of Business and Economics with a master's degree in Management. He works in the Economics and Trade Department of Shijiazhuang College of Applied Technology. His main research direction is enterprise management and e-commerce (E-mail: 2018000872@sjzpt.edu.cn).