JCSE Journal of Computing Science and Engineering

Regular Paper

Journal of Computing Science and Engineering,
Vol. 16, No. 2, June 2022, pp. 88-96

Application of Speech Recognition Interaction and Internet of Things in Data Mining

Kan Wang*
College of Computer Engineering, Henan Institute of Economics and Trade, Zhengzhou, China
wong_kvor@163.com

Abstract

The current data mining technology cannot attain the database of voice retrieval, and the data mining process has a high risk of interference. Therefore, the application of speech recognition interaction and Internet of Things (IoT) technology in data mining has been investigated. Using a speech recognition engine to recognize a user's intention, a database retrieval model based on speech recognition interaction has been constructed. To enhance the security of data mining, the IoT data were classified by differential privacy clustering, and the false data features of IoT were detected efficiently. Finally, data mining was completed by combining data fusion and a Bayesian classifier. Experimental results demonstrated that the accuracy of the proposed method is over 90%, the time of data fusion is shorter, the time of data mining is shorter, the precision is higher, and the false alarm rate is lower than 5%.

Category: Databases / Data Mining

Keywords: Speech recognition interaction; Internet of Things technology; Data mining; Speech recognition engine; False data characteristics

I. INTRODUCTION

With the rapid development of computer technology, human beings are getting more and more information on various topics. But sometimes the efficiency of obtaining information is not high because of the combination of effective and invalid information. In this context, one of the aims of information retrieval is to improve efficiency. The idea of a database is to manage immense information by DBMS conveniently and efficiently [1]. To enable ordinary users to share the development results of information technology, it is of great application value and expanded significance to provide a natural language interface for database information retrieval. After nearly 30 years of research, the related theories in the field of natural language processing have matured, and the application of database information retrieval in specific fields has passed the historical test and been recognized in the market [2].

At present, the natural language interface of the database is mainly in the form of text, and it still needs the user to input the interrogative sentence into the computer in the form of the text string, if this process is optimized to change the text input into direct speech input to realize the information retrieval of the database in the form of spoken Chinese using speech interaction technology, to completely change the human-machine interaction mode. Furthermore, I believe that it can provide users with higher quality services and accelerate the popularization of information technology in the

Open Access http://dx.doi.org/10.5626/JCSE.2022.16.2.88 http://jcse.kiise.org

Received 19 January 2022; **Accepted** 25 May 2022
*Corresponding Author

 pISSN: 1976-4677 eISSN: 2093-8020

public field. With the rapid development of the Internet of Things (IoT), the data stored in cloud terminals has shown explosive growth, and the data volume has jumped from petabyte (PB) to zettabyte (ZB), thereby indicating the arrival of the IoT data era. The emergence of the IoT has brought about the development and utilization of corresponding Internet forums, shopping, navigation, payment, and other technologies, thereby not only changing people's way of life but also improving people's quality of life. Thus, it is hypothesized that the application of IoT data can not only enhance the information service capacity but also promote the enlightenment and development of emerging technologies [3]. Although the IoT data has brought a very convenient service to people's lives, it is associated with information security challenges concerning people's personal data. Thus, the ways to deal with the IoT data is an urgent problem to be solved, and also the basic premise of information security.

Reference [4] proposed a big data mining algorithm based on multi-MapReduce job collaboration. The item-based algorithm based on distributedcache uses distributedcache to cache the I/O data between multiple MapReduce jobs, breaking the defect of independence between jobs, reducing the waiting delay between maps, and reducing tasks. The experimental results show that the distributedcache can improve the data reading speed of MapReduce jobs. The reconstructed algorithm of distributedcache greatly reduces the waiting delay between map and reduce tasks, and improves the resource efficiency by more than three times. Yang et al. [5] proposed a multi-source log security data mining method based on time series, which marks the strength of signals at different times in the multi-source log, calculates the process time and moving speed of label data in the multi-source log according to the signal strength, and removes the dirty data and redundant data in the multi-source log according to the calculation results. The time-series data in multi-source logs are processed in blocks, and the features in the sub-matrix are extracted by combining the two-dimensional singular value decomposition method and the principal component analysis method. According to the extracted features, the data classifier is established by the minimum distance method, and the data classifier is used to classify the security data in multi-source logs to complete the mining of multi-source log security data.

However, the above methods realize the voice retrieval of the database, and there is a high risk of interference in the data mining process. Therefore, the application of speech recognition interaction and IoT technology in the process of data mining has been studied in the present work.

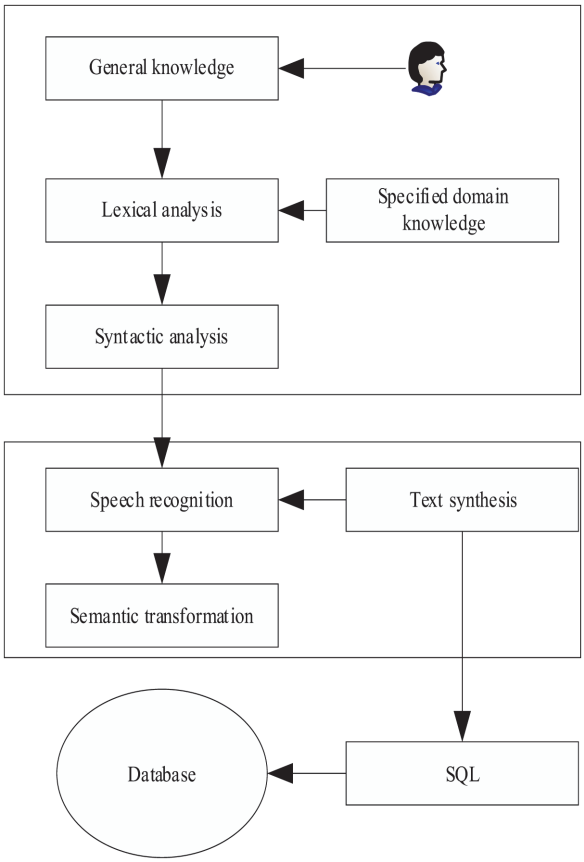

Fig. 1. Model framework.

II. APPLICATION OF VOICE RECOGNITION INTERACTION AND IOT TECHNOLOGY IN THE PROCESS OF DATA MINING

A. Application of Speech Recognition Interaction in Data Mining

1) Construction of Database Retrieval Model based on Speech Recognition Interaction

The structure of the information retrieval system in the form of database voice is shown in Fig. 1. Users interact with the system in Chinese. The query sentences are identified by the voice recognition engine according to the query patterns designed in the knowledge base, and then the semantic conversion module converts the user's real intention into the SQL commands of the database, which drives the database to carry out the retrieval, and finally generate the query results [6]. The system mainly includes a speech recognition module, knowledge base module, semantic conversion module, database communication module, text synthesis module, and user interface.

To realize the voice query, we must analyze the user's query intention in the speech recognition module. The recognition grammar of the speech recognition engine establishes the query pattern according to the user's requirement provided by the knowledge base. If the user's speech query pattern matches the recognition pattern, the key information needed in the semantic translation module is extracted from the pattern, including

the pattern needed for constructing the SQL statement, the query parameter information, and so on.

2) Speech Data Feature Fusion

The speech data recognition method integrates the characteristics of speech data based on association rule reorganization. When the multi-dimensional scale analysis method is used to decompose the background noise intensity of speech data, the component is fixed, and the decomposition result can be described by the following formula [7-9]:

$$\begin{cases} A = \sqrt{U^2(t) + X^2(t)} \\ \Psi = arctan\dfrac{X(t)}{U(t)} \end{cases} \tag{1}$$

where, A represents the detection amplitude corresponding to the voice data; $U(t)$ represents the phase rotation constraint amount corresponding to the voice data; Ψ represents the phase distribution data corresponding to the data block in the voice data.

The carrier frequency corresponding to the first array element must be calculated to obtain the frequency increment $\Re$ corresponding to the voice data:

$$\Re = A\,exp\{[f'\,ln(t - t_0) - f''\,ln\,\phi\,(t)]\} \tag{2}$$

where f' and f'' represent the initial frequency and cut-off frequency corresponding to the voice data.

Let $\aleph$ represent the low-frequency component in the voice data, and its expression is as follows:

$$\aleph = \Re + W(U, X) \tag{3}$$

where, $W(U, X)$ represents the spectral characteristic quantity corresponding to the voice data.

Calculate the interference variance h based on the separation results of spectral features of speech data:

$$e = t_0(\frac{1}{\aleph} - A)t_{MAX} + \Im \tag{4}$$

where, $\Im$ represents time delay parameter; t_{MAX} represents the peak value corresponding to each segment of data.

Under scale control, the filtered output ω of the speech data is obtained according to the time scale decomposition result:

$$\omega = \sqrt{|E|}\int_{-\infty}^{+\infty} U(t)[(t - \Im)]\,dt \tag{5}$$

The multi-dimensional feature quantity corresponding to the complete speech data is obtained by the data fusion tracking detection method.

3) Speech Recognition Interaction:

The sampling balance points of each data block in the human-computer interaction system are equally spaced. Let F represent the amplitude corresponding to the sampling interference data, and its expression is as follows:

$$F = M \cdot \psi - \frac{\omega}{2} \tag{6}$$

where M represents the mode corresponding to the modulation data.

Let's build a data classifier Q:

$$Q = F \cdot \sum_{\kappa=1} F(\kappa) - \frac{\omega}{2} \tag{7}$$

In the expression, $F(\kappa)$ represents the feature classification function, and the feature classification function is weighted and summed to obtain the speech data.

For speech data in human-computer interaction systems, feature classification is conducted by an improved neural network method, and classification state detection χ is calculated as [10]:

$$\chi = M\sum_{\kappa=1} F(\kappa) + Q(\int_{-\infty}^{+\infty} U(t)]) \tag{8}$$

According to the features of speech data, the neural network classification parameters are analyzed under fuzzy classification constraints, and the speech data recognition model is constructed by an improved neural network:

$$x_M(t) = \frac{\sum_{\kappa=1} F(\kappa)\sum_{t=1}[\frac{M-1}{s}\theta(t)]}{g(t)} \tag{9}$$

where, $g(t)$ represents part of the transmission sequence corresponding to voice data; s represents data fusion output; M represents the number of phonetic mapping symbols; and $\theta(t)$ stands for the fuzzy control function.

B. Differential Privacy Clustering of Internet of Things Data

The key to implementing differential privacy protection is to add noise to the location information so that the real location information is distorted and the similarity attack is resisted. The amount of noise added is determined by the privacy parameter, which represents the degree of privacy protection. If the amount of noise added is too small to meet the privacy needs of the location information [10-12] and if the amount of noise added is too high, the availability of the location information data will be lost. Therefore, a reasonable allocation of differential privacy parameters is needed to achieve the best privacy protection effect.

The given user information data is shown in Table 1.

Based on Table 1, the position information data is partitioned by kd-tree, and the noisy information is

Table 1. User location information datasheet

Data number	x	y
1	0.9→0	1.8→1
2	1.0→1	0.7→0
3	1.6→1	1.5→1
4	0.5→0	1.2→1
5	1.3→1	1.8→1

processed to satisfy the ε-differential privacy protection. The steps for differential privacy assignment based on the kd-tree partition are as follows:

Step 1: Calculate the number of kd-tree cells using the following formula:

$$m_1 = max\left(10, \left\lceil \frac{N}{c} \right\rceil\right) \tag{10}$$

Of these, N represents the size of the location information dataset and c represents a constant. based on t

Step 2: Divide the location information dataset into coarse-grained $m_1 \times m_1$, add noise to each cell, and get the disturbed location information D';

Step 3: Count the new kd-tree cells, using the

$$m_2 = \left\lceil \frac{\sqrt{N'(1-\alpha)\varepsilon}}{c_2} \right\rceil \tag{11}$$

where, N' represents the amount of noise added for the first division and c_2 represents a constant.

Step 4: Divide D' into fine-grained $m_2 \times m_2$ levels, add noise to each cell, and get the disturbing position information D''.

Step 5: Repeat Step 3 and Step 4 to get the undistributed position information dataset satisfying the difference factor.

Step 6: Reconcile Step 2 and Step 4 to get the final result.

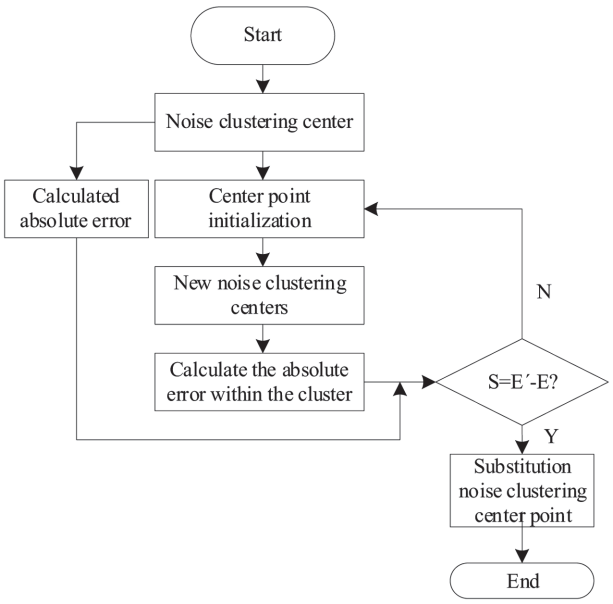

Fig. 2. Flow chart of differential privacy clustering algorithm.

Based on the results of dimensionality reduction clustering, a differential privacy clustering algorithm is proposed. The flow chart is shown in Fig. 2.

Through the above process, the launch and operation of the location-based data differential privacy clustering algorithm of the IoT are realized, which provides a more effective guarantee for data security and helps in the development of the IoT.

C. Efficient False Data Feature Detection of IoT

Based on the above results of feature extraction of false data in the IoT, the support vector machine theory shall be fused to screen and cluster the true and false information of the features of the IoT data. Within the threshold of the authenticity of the IoT data and the feature information of the false data, the probability of the existence and the similarity threshold of the false data shall be used as the evaluation rules, and the feature information of the false data in the IoT shall be identified. At the same time, the feature space of the overall false data in the IoT shall be detected and reduced in dimension by incremental learning in the adjacent areas [13, 14]. The general flow is as follows:

Assuming that the IoT data sequence is composed of a certain dataset D, and its training is decomposed into the feature vectors $\{x|x_1, x_2, ..., x_n\}$ and decision vectors $\{c|c_1, c_2, ..., c_n\}$ of the IoT data, and at the same time assuming the relative independence of all components of the feature vectors of the IoT data, the IoT data sequence can be divided into two categories (c_1, c_2): the false information and the real IoT information. When detecting a new IOT dataset, the probability that the dataset X belongs to the real data information and the false information of the physical network can be estimated using formula (12):

$$p(c_j|x) = \frac{p(x|c_j)p(c_j)}{p(x)} \tag{12}$$

Assuming that $\{P|P_1, P_2, ..., P_n\}$ is a known template vector of false data information through training and classification and can estimate the probability of obtaining false data information by estimating its amount of information for data feature x, the similarity between it and false data information for any IoT data information volume x_1 can be estimated using formula (13):

$$Sim(x_i, P_j) = \frac{\sum_{i=1,j=1}^{n} \|\Upsilon \cdot p(s_2|x)\| \cdot \|P_j\|}{\|\Upsilon \cdot p(s_2|x)\|} \tag{13}$$

where, γ is the camouflage loss function of false data of the IoT, $p(s_1|x_i)$ is the amount of real data information of the IoT, and $p(s_2|x_i)$ is the amount of false data information of the IoT. If γ is the threshold of false data information evaluation of the IoT, there are:

$$\begin{cases} sim(x_i, P_j) \geq \gamma, \text{False data} \\ sim(x_i, P_j) < \gamma, \text{Other data} \end{cases} \tag{14}$$

When detecting the characteristics of the false data of the IoT, the true and false information function of the data information quantity of the IoT shall be estimated, and the occupancy ratio of the false information in the false data features shall be estimated by relying on the probability of the occurrence of the false information quantity in the false data features. At the same time, the similarity degree of the false data information shall be estimated by using the feature template of the false data of the IoT, and the characteristics of the false data in the IoT shall be detected through comparison thresholds.

D. Data Fusion Method

Data fusion belongs to the lowest level of data fusion, and the requirements for data sources are low. Usually, only the data of the same type of nodes can be processed. For example, the fusion of homogeneous radar data is directly combined with multiple source images. Due to the complexity of the IoT environment, data preprocessing is required [15]. When the data is fused, there will be no loss or omission of data, which improves the accuracy of the fusion. The data fusion diagram is shown in Fig. 3.

The core of fusion technology is to transform the initial data using the relevant rules of the settings and to fuse the data according to the deviation of data records. The data can be fused directly to the data in the node. After fusion, the original data can be repaired by inverse operation. Incremental fusion is a lossless fusion algorithm.

Suppose the data sequence is represented as $S = \{s_1, s_2, ..., s_M\}$, and a time interval of equal size t_p is set, in the same time interval t_p, the data formed by the IoT nodes is

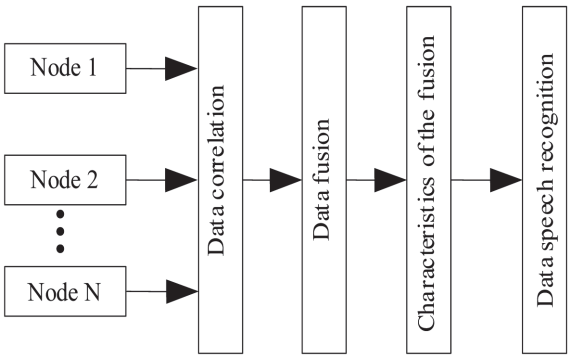

Fig. 3. Schematic diagram of data fusion.

N and S is divided into $[M/N]$ groups, namely $S = \{S_1, S_2, ..., S_{[M/N]}\}$, whose function expression is as follows:

$$F_s = \begin{cases} S_i & i \bmod N = 1 \\ S_i - S_{[i/N]} & i \bmod N \neq 1 \end{cases} \tag{15}$$

The data of the IoT shall be partitioned by time interval, the original data of time shall be selected as the basic data, and the increment of other data shall be recorded. The operation process is as follows:

Step 1: Select the best time interval and initialize it;

Step 2: When the data processing is complete, stop the fusion, otherwise if the time interval is less than the time slice, return to continue processing, greater than the time slice to continue;

Step 3: Process the sliced data in Step 2 with the first data in the new time-slicing as the baseline data.

After the repeated operation of the above steps, data fusion is finally obtained.

E. Data Mining

Based on data fusion, a Bayesian data classifier is used to mine data.

In general, $P = (A/B)$ represents the probability that an event A may occur under the premise that the event B is known, and the solution is the following:

$$P(A|B) = \frac{P(AB)}{P(B)} \tag{16}$$

However, in the naive Bayes classification, we pay more attention to $P = (A/B)$, so we can get the following formula by transforming the conditional probability formula:

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)} \tag{17}$$

Bayesian data classification uses a n dimension attribute vector sample $L = \{L_1, L_2, ..., L_N\}$ to represent each data. Bayesian classification gives the attribute value $a_1, a_2, ..., a_n$ of each data and measures the attribute value of each data. The classification set is: $B = \{b_0, b_1, b_2, ..., b_n\}$.

The Bayesian data classifier is used to distinguish whether a single data in a dataset belongs to b_i or not when it belongs to and only meets the following conditions:

$$P(B_t|L) > P(B_j|L) \tag{18}$$

Thus, the maximum a posteriori assumes that the maximum value of $P(B_i|L)$ is B_i. According to the obtained formula (18), we can know the following formula:

$$P(B_i|L) = \frac{P(B|L_i)P(L_i)}{P(x)} \quad (19)$$

Among them, $P(B_i|L)$ is the probability that the classification set B_i may appear in a particular state $L = \{l_1, l_2, ..., l_N\}$, while $P(B_i)$ is the probability that will occur in the selected state of B_i.

Because it is necessary to solve $P(L|B_i)$ under the condition that there are too many attributes given by conditions and categories, and the computation is required to be done in a large number, a simple algorithm is carried out under the condition that the Bayesian data classification set L is relatively independent of each other. In the process, the dependencies do not belong to the attributes of each condition, and the process is as follows:

$$P(L|B_i) = \prod_{j=1}^{n} P(L_j|B_i) \quad (20)$$

The final purpose of the Bayesian data classifier is to divide the selected data into corresponding item sets (the item set is the item set with the maximum a posteriori probability) for calculation. The process is as follows:

$$\zeta = \underset{j\neq 0}{argmax} P(L_j|B_i) \quad (21)$$

The extracted features are input into the classification model to realize data mining.

III. EXPERIMENTAL DESIGN AND RESULT ANALYSIS

A. Experimental Environment

To verify the performance of the proposed data mining method based on speech recognition interaction and IoT technology, a simulation comparison experiment is designed. The experiment is implemented in Java language, and the basic experimental environment configuration is shown in Table 2.

Table 2. Experimental environment configuration

Configuration item	Configuration parameter
Function	Spark2.1.0
Pattern	2.6.0
Hadoop version	1.8.0
JDK	2.80GHz
Operation	Microsoft Windows ws 7×64
System	8 GB DDR4 2400 MHz
Memory	Intel i5-6402P
CPU	Java 1.8.0_101-b13

Table 3. Basic description of experimental dataset structure

Dataset	Gewara	GeoLife	Amazon
Data type	Multivariate	Multivariate	Multivariate
Number of samples	13,875,935	228,690	517,584
Number of attributes	18	9	13
Number of clusters	18	19	15

B. Experimental Dataset Description

To meet the demand for real IoT location datasets in simulation experiments, three location datasets, Gewara, GeoLife, and Amazon were downloaded from the IoT database GeoLife GPS Trajectories. Among them, the Gewara location dataset includes a user's social network check-in time and location based on transactions; the GeoLife location dataset contains road, location, and user footprint; and the Amazon location dataset contains the user's text location information. The three location datasets mentioned above contain not only all kinds of location information, but also user's non-location information, which meets the needs of simulation and contrast experiments. The basic description of the experimental dataset structure is shown in Table 3.

C. Accuracy Analysis of Data Fusion with Different Methods

To verify the reliability of this method, the data fusion accuracy of this method, the data mining method based on MapReduce job collaboration proposed in reference [4], and the multi-source data mining method based on the time series proposed in reference [5] are experimentally analyzed. The experimental results are shown in Fig. 4.

By analyzing Fig. 4, it can be seen that the accuracy of

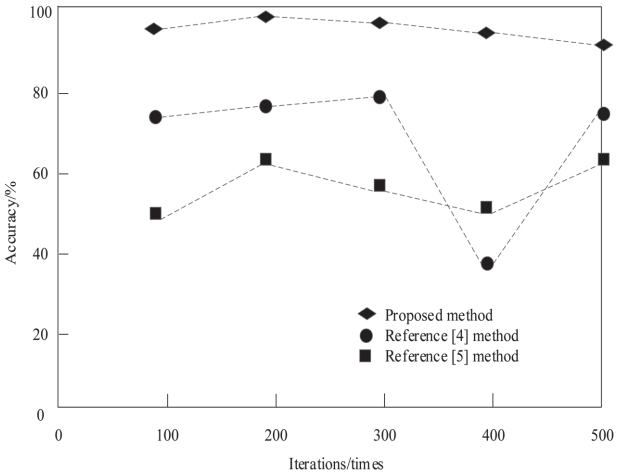

Fig. 4. Comparison of data fusion accuracy of different methods.

data fusion of the three methods varies with the number of iterations. When the number of iterations is 2, the data fusion accuracy of this method is higher than 90%, the fusion accuracy of Liao et al.'s method [4] is about 68%, and the data fusion accuracy of Yang et al.'s method [5] is about 64%. When the number of iterations is 5, the fusion accuracy of this method is about 97%, that of [4] is about 75%, and that of [5] is about 84%. Through comparison, it can be found that the data fusion method in this paper has higher accuracy and certain reliability.

D. Time Analysis of Data Fusion with Different Methods

To further verify the effectiveness of this method, the reported experiments compared the time-consuming data fusion of this method, the data mining method based on MapReduce job collaboration proposed in [4], and the multi-source data mining method based on the time series proposed in [5]. The experimental results are shown in Table 4.

By analyzing the data in Table 4, it can be seen that the fusion time of the three methods is different. When the fused data points are 2000, the time of this method is 3.6 seconds, the time of Liao et al.'s method [4] is 8.6 seconds, and the time of Yang et al.'s method [5] is 6.2 seconds. When the fused data points are 5000, the time of this method is 3.5 seconds, that of [4] is 10.3 seconds, and that of [5] is 9.6 seconds. The analysis shows that the maximum time of data fusion of this method is 3.6 seconds, while the maximum time of [4] and [5] method is 10.3 and 9.6 seconds, respectively, which is much higher than that of this method, which verifies that the work efficiency of this method is high.

E. Performance Test of Different Data Mining Methods

The proposed method, the data mining method based on MapReduce job collaboration proposed in [4], and the multi-source data mining method based on time series proposed in [5] were comparatively analyzed, and the data mining rates of different methods are compared. The test results are shown in Fig. 5.

Table 4. Comparison of data fusion time of different methods

Node data per piece	Proposed method	Liao et al. [4]	Yang et al. [5]
1000	3.2	7.1	6.6
2000	3.6	8.6	6.2
3000	3.3	9.1	7.3
4000	3.3	9.4	8.4
5000	3.5	10.3	9.6

By analyzing the data in Fig. 5, it can be seen that the mining rate obtained by the proposed method when mining data is more than 93%. The highest value of the mining rate obtained by the data mining method based on MapReduce job collaboration proposed in [4] and the multi-source data mining method based on time series proposed in [5] is 90% and the lowest value is 66%.

The proposed method, the data mining method based on MapReduce job collaboration proposed in [4], and the multi-source data mining method based on time series proposed in [5] are used to mine data, respectively. The time used by different methods to mine data is compared. The test results are described in Fig. 6.

By analyzing the data in Fig. 6, we can see that with the increase in the amount of data, the mining time used by the proposed method, the data mining method based on MapReduce job collaboration proposed in [4], and the multi-source data mining method based on time series proposed in [5] show an increasing trend. However, in the case of the same amount of data, the mining time of the proposed method is lower than that of the reference method.

Taking the mining accuracy as the test index, the proposed method, the data mining method based on MapReduce job collaboration proposed in [4], and the

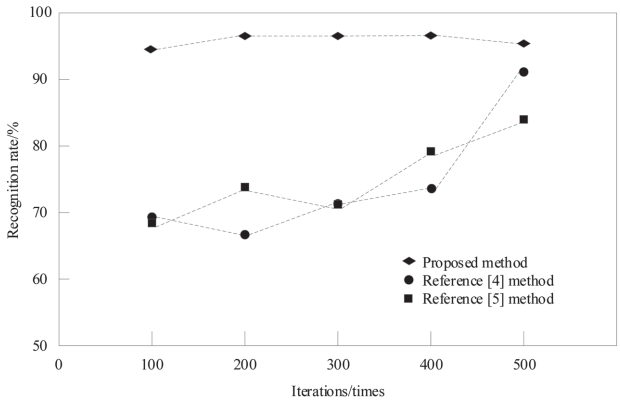

Fig. 5. Data mining rate test results.

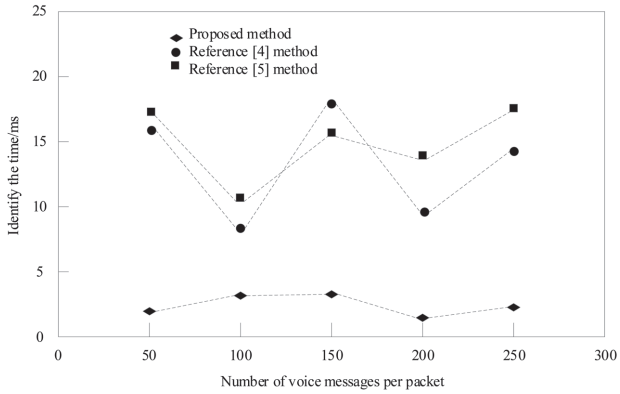

Fig. 6. Data mining time test results.

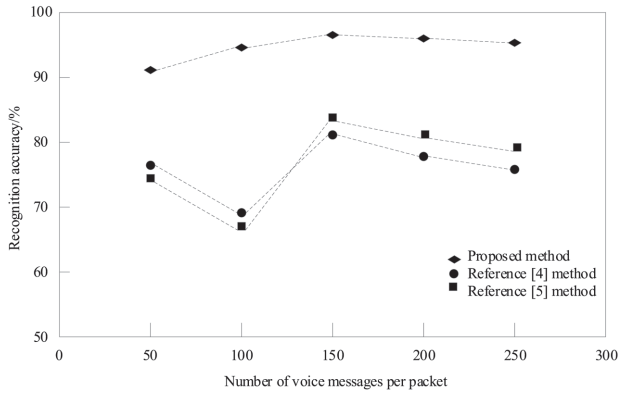

Fig. 7. Mining accuracy test results.

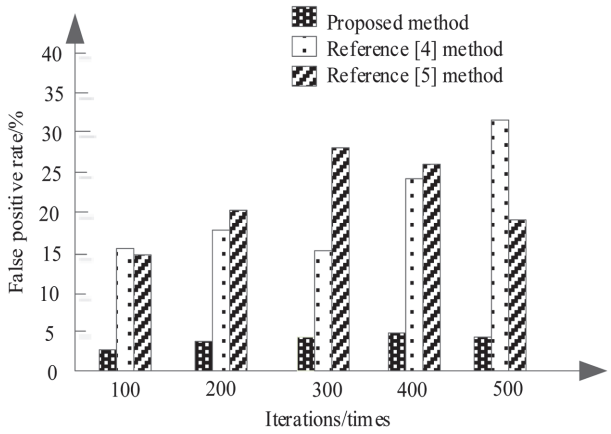

Fig. 8. Test results of mining false alarm rate.

multi-source data mining method based on the time series proposed in [5] are tested. The test results are shown in Fig. 7.

According to Fig. 7, the rate of the three methods decreases with the increase in the amount of data, but the mining accuracy of the proposed methods remains above 90% during the test. Because the proposed method uses the speech recognition engine to recognize the user's intention, and then the semantic translation module transforms the user's real intention into SQL commands of the database. To resist the similarity attack and optimize the environment of data mining, the interactive processing of speech recognition is carried out to improve the accuracy of data mining.

After testing the detection time and detection rate of network data mining, the feasibility of the network data mining method based on the improved Apriori algorithm is further tested by testing the false alarm rate of the proposed method, Liao et al.'s method [4], and Yang et al.'s method [5]. The test results are shown in Fig. 8.

By analyzing Fig. 8, it can be seen that the false positive rate of the proposed method, Liao et al.'s method [4], and Yang et al.'s method [5] increases relatively under multiple tests, but the false-positive rate of the proposed method is significantly lower. This is because the proposed method introduces a differential privacy protection method to add noise to the location information, distort the real location information, and resist the similarity attack. It avoids most of the interference and shortens the time of data mining.

IV. CONCLUSION

To solve the problem that the current data mining technology cannot realize the speech retrieval of database and avoid the interference factors affecting the accuracy of data mining, the application of speech recognition interaction and the IoT in the process of data mining is studied. Using the speech recognition engine to recognize the user's intention, the semantic transformation module transforms the user's real intention into SQL command of the database to drive the database to search. The features of speech data are fused and the process of speech recognition is processed interactively. The key to implementing differential privacy protection is to add noise to the location information so that the real location information is distorted and the similarity attack is resisted. To enhance the security of data mining, the IoT data are classified by differential privacy clustering, and the false data features of IoT are detected efficiently. Finally, data mining is completed by data fusion and a Bayesian classifier. Experimental results show that the proposed method has higher accuracy and lower time consumption, which proves that the proposed method has better application performance and higher application reliability.

REFERENCES

1. S. Marcos-Pablos and F. J. Garcia-Penalvo, "Information retrieval methodology for aiding scientific database search," *Soft Computing*, vol. 24, no. 8, pp. 5551-5560, 2020.
2. R. R. Yager, N. Alajlan, and Y. Bazi, "Uncertain database retrieval with measure-based belief function attribute values," *Information Sciences*, vol. 501, pp. 761-770, 2019.
3. Z. Du, "Energy analysis of Internet of things data mining algorithm for smart green communication networks," *Computer Communications*, vol. 152, pp. 223-231, 2020.
4. B. Liao, T. Zhang, J. Yu, J. L. Huang, B. L. Guo, and Y. Liu, "Resource efficiency optimization for big data mining algorithm with multi MapReduce collaboration scenario," *Application Research of Computers*, vol. 37, no. 5, 1321-1325, 2020.
5. Q. X. Yang, G. N. Wang, and T. Wang, "Simulation of multi-source log security data mining based on time series," *Computer Simulation*, vol. 36, no. 2, pp. 297-301, 2019.
6. M. Miao, Y. Wang, J. Wang, and X. Huang, "Verifiable database supporting keyword searches with forward security,"

Computer Standards & Interfaces, vol. 77, article no. 103491, 2021. https://doi.org/10.1016/j.csi.2020.103491
7. K. A. Arano, P. Gloor, C. Orsenigo, and C. Vercellis, "When old meets new: emotion recognition from speech signals," *Cognitive Computation*, vol. 13, pp. 771-783, 2021.
8. P. Heracleous and A. Yoneyama, "A comprehensive study on bilingual and multilingual speech emotion recognition using a two-pass classification scheme," *PLoS One*, vol. 14, no. 8, article no. e0220386, 2019. https://doi.org/10.1371/journal.pone.0220386
9. V. Tiwari, M. F. Hashmi, A. Keskar, and N. C. Shivaprakash, "Speaker identification using multi-modal i-vector approach for varying length speech in voice interactive systems," *Cognitive Systems Research*, vol. 57, pp. 66-77, 2019.
10. Y. Jung and C. M. Jeong, "Deep neural network-based automatic unknown protocol classification system using histogram feature," *The Journal of Supercomputing*, vol. 76, no. 7, pp. 5425-5441, 2020.
11. S. Li, K. Dong, Z. Liu, and Z. Li, "Dynamic network data protection algorithm using differential privacy in Internet of Things," in *Proceedings of 2019 IEEE International Conference on Smart Internet of Things (SmartIoT)*, Tianjin, China, 2019, pp. 306-313.
12. K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial Internet-of-Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4156-4165, 2020.
13. X. Wang, J. Du, R. Zou, and Z. Zhou, "Key node identification of wireless sensor networks based on cascade failure," *Modern Physics Letters B*, vol. 34, no. 34, article no. 2050394, 2020. https://doi.org/10.1142/S0217984920503947
14. G. Qing, H. Wang, L. Guo, and J. Yang, "Device type identification via network traffic and lightweight convolutional neural network for Internet of Things," *IEEE Access*, vol. 8, pp. 200219-200228, 2020.
15. D. Chen, Y. Xu, and S. Luo, "Mining and construction of information opportunity cooperation mode based on big data fusion Internet of Things," *IEEE Access*, vol. 9, pp. 29401-29415, 2021.

Kan Wang

Kan Wang, born in April 1974, is an associate professor. In June 1996, he graduated from Heilongjiang Institute of Business majoring in commodity inspection and maintenance, and in December 2004, he graduated from Huazhong University of science and technology. He currently works in Henan Institute of Economics and Trade, Zhengzhou, China (e-mail: wong_kvor@163.com). His main research interests are computer application and vocational education.