Hindawi
Mobile Information Systems
Volume 2022, Article ID 5124707, 9 pages
https://doi.org/10.1155/2022/5124707

Research Article

Cloud Computing Database and Travel Smart Platform Design Based on LSTM Algorithm

Dongfeng Chen

Graduate School Hotel Tourism Department, Tongmyong University, Busan 48520, Republic of Korea

Correspondence should be addressed to Dongfeng Chen; 2007048@muc.edu.cn

Received 2 July 2022; Revised 27 July 2022; Accepted 8 August 2022; Published 26 August 2022

Academic Editor: Shadi Aljawarneh

Information technology has played a key role in the development of the tourism planning service industry and has now become an important foundation for the survival and rapid development of the industry. In this context, due to the fast updating and popularization of information technology, it has greatly promoted the development of the tourism industry. In order to meet the current public demand for tourism information, this paper integrates cloud computing, VR technology, and big data analysis technology to build a smart platform for intelligent perception tourism information services. The system can obtain tourism information through mobile Internet terminals. Among them, the database of the smart tourism planning platform is the most important module. Aiming at the many difficulties in adapting data encryption in cloud storage applications, this article designs an adaptive CloudCrypt data encryption system based on cloud computing technology and proposes dynamic JavaScript dynamic analysis and automatic identification of data technology, through adaptive different cloud applications to obtain data encryption protection. CloudCrypt is suitable for typical cloud applications, such as mail and storage. The entry cost of the system is extremely low; it can fully guarantee the security of the tourism information platform database and can integrate wireless sensor networks into the tourism information platform. The network system composed of sensor nodes activates detection, calculation, and communication modules through wireless communication and has the advantages of low cost, low power consumption, and fast networking speed. In this paper, through the construction of integrated wireless sensor technology and cloud computing database, it is applied to the construction of a tourism smart platform, thereby promoting the development of smart travel technology.

1. Introduction

Smart tourism concept has not yet had a clear unified view of the industry. Generally speaking, smart tourism is often regarded as a new type of information technology, such as cloud platforms and the Internet, which can connect to each other and exchange data through the Internet [1]. The use of Internet terminals can enable the public to quickly and conveniently obtain travel information, so as to realize the planning and modification of travel plans and conduct intelligent perception processing of travel information [2]. With the further development of the Internet, personalized tourism and multipolar tourism technology have been promoted as never before, enabling more and more tourists to learn about tourism information around the world in this relatively simple way [3].

At present, the development potential of China's tourism industry is based on the gradual expansion of the supply market, and the development of personalized tourism is more obvious. On the one hand, the number of tourists continues to increase; on the other hand, the proportion of tourists and individual tourists has also continued to increase [4]. Therefore, higher requirements are put forward for the design and practical application of the tourism planning service platform. This article first conducts a detailed investigation of the technical characteristics and theoretical knowledge of smart tourism construction and elaborates on the feasibility of cloud computing construction mode and cloud computing resource library design [5]. Subsequently, based on the actual situation of a certain scenic spot, the demand analysis is carried out from multiple perspectives of users, such as tourists, tourism targets in the scenic spot, service providers, and tourism management agencies, so as to clarify customer needs and examine their overall demand trends [6]. Subsequently, the article carried out general planning and detailed planning for the implementation of smart tourism construction, explained in detail

the construction content, construction plan, technical approach, and other details, and provided necessary data support and ideas for construction. Therefore, based on China's smart tourism service, the current construction status has created a tourism smart platform [7]. Among them, database security is the top priority of researchers. In view of its difficulty in balancing data encryption and storage functions, this paper designs a cloud ciphertext retrieval system EncBox for analysis and proposes a security gateway-based model [8].

In addition, the ciphertext retrieval method of cross-gateway data security sharing does not require the cooperation of cloud providers to achieve this solution and only needs to obtain data encryption protection to preserve the original search function of the cloud service to the maximum extent [9]. Experiments show that EncBox can not only transparently encrypt and protect data, but also retain the original search function, thereby minimizing the introduction of production costs and completely solving the database security problem [10]. Finally, this article investigates wireless sensor network technology, compares the advantages and disadvantages of a variety of commonly used wireless sensor technologies, and finally chooses ZigBee communication technology to create a type of wireless sensor network installation positioning system, so as to provide users with better scenic location positioning function.

2. Related Work

The research background and importance of the wireless sensor network positioning system compatible with the ZigBee protocol were introduced. By studying the status quo of various nonsatellite positioning technologies, comparing and evaluating their advantages and disadvantages, the sensor network based on the ZigBee protocol is finally selected [11]. CloudDLP, a cloud computing-oriented sensitive data recognition and desensitization system, was designed; an improved end-to-end CTPN-MASK text recognition model and a sensitive BERT-CRF data recognition model were proposed, which can effectively solve sensitive content recognition and insensitive scene recognition poor ability and other issues [12, 13]. Experiments show that the accuracy of intelligent desensitization recognition of photos and documents can reach 93.5% and 97.98%, respectively.

An adaptive data encryption system for cloud browser storage applications was proposed, which can automatically identify and adapt different cloud applications to ensure the encryption and protection of sensitive data in different cloud applications [14]. CloudCrypt uses dynamic JavaScript analysis technology to monitor the upload behavior of each client program in cloud applications and encrypts file content by identifying file operation requests. This technology can safely isolate sensitive data and fundamentally solve the problem of cloud application adaptation [15, 16].

A new cloud data platform login and identity verification system was proposed, which is equipped with a fingerprint authentication and identification module, which has the advantages of high information security and strong antiattack ability [17]. After testing, this technology improves the security and validity of the connection and access to the cloud data platform without affecting the user experience [18]. The security performance requirements of the cloud data platform application in the communication process authentication were analyzed. The article designs the platform access framework based on fingerprint authentication by realizing the security of the multidomain access identity authentication in the cloud data platform [19, 20]. And, for the fingerprint feature extraction of the platform fingerprint authentication module, it lays the foundation for connecting the cloud data platform and interdomain access, so as to realize the design of anonymous account encryption and decryption.

3. Database Security Design Based on Cloud Computing

3.1. Technical Principles of Database Security Based on Cloud Computing. LSTM. Long short-term memory (LSTM) networks are different from repetitive neural networks (RNN). The structure of the LSTM network can merge long and short memories by adding thresholds, thereby solving the problem of only short-term memory due to gradient loss in RNN. The calculation is as follows:

$$f_t = \sigma\left(W_f\left[h_{t-1}, x_t\right] + b_f\right). \tag{1}$$

The input gate first clarifies what information can be stored and then creates a new candidate vector value according to the tan$h$ function. The calculation is as follows:

$$\begin{aligned} i_t &= \sigma\left(W_i\left[h_{t-1}, x_t\right] + b_i\right), \\ \widehat{C}_t &= \tanh\left(W_C\left[h_{t-1,x_t} + b_C\right]\right). \end{aligned} \tag{2}$$

The output gate decides which part of the unit state is output according to the unit state information and then multiplies the output of the output layer with the tan$h$ layer to extract the specified part of the output. The calculation is as follows:

$$\begin{aligned} o_t &= \sigma\left(W_o\left[h_{t-1}, x_t\right] + b_o\right), \\ h_t &= o_t \tanh\left(C_t\right). \end{aligned} \tag{3}$$

Given the input x and the tag order, the sum of all probability paths that can be mapped to l in the mapping of relationship B is the probability of appearing in the tag sequence, and the final result is the most likely path annotation.

$$\begin{aligned} p(\pi|x) &= \prod_{t=1}^{T} y_{\pi_t}^t, \forall \pi \in L^T, \\ p(l|x) &= \sum_{\pi \in B^{-1}} p(\pi|x), h(x) = \operatorname{argmax}_{l \in L^{\leq T}} p(l|x). \end{aligned} \tag{4}$$

According to the threshold scheme of cryptography, the idea of "secret sharing" is adopted, which is a threshold scheme algorithm based on Lagrangian polynomial interpolation. The shared threshold scheme has the advantage of

risk sharing. The specific calculation of the threshold (t, k) is as follows:

$$f(x) = key + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}. \quad (5)$$

Set the identification ID and subkey of the known user t and use the Lagrangian difference formula to reconstruct the polynomial method, as shown in the following equation:

$$f(x) = \sum_{i=1}^{t} \left(f(x_i) \prod_{j=1 j \neq i}^{t} \frac{x - x_i}{x_i - x_j} \right). \quad (6)$$

Assuming that the scheme of Shamir threshold (t, k) divides the key into k parts, the division of information x is denoted by $\text{key}|_x$ key$x$ and the key of the distribution process is shown in the following equation:

$$\text{Shamir}(t,k)\{\text{key}\} = \text{key}|_x. \quad (7)$$

Then, the key recovery process is shown in the following formula:

$$\{\text{key}|_x\}\text{Shamir}(t,k) = \text{key}. \quad (8)$$

The purpose of digital signature is to prevent the signer from rejecting his signature. The digital signature is based on a password, and the digital signature information is generated based on the key that only the signer knows and the information waiting to be signed. The digital signature consists of a signature algorithm and a verification algorithm. The algorithm and signature key are private information of the signer, and the algorithm and verification key are public information, so that it is convenient for others to verify the result of the user's digital signature.

When the system is turned on, each user has unique identification information I. After the user identification information is changed through the hash function $H()$, the hash value $J = H(I)$ is obtained. Assuming that the user identity information in A is IA, and the corresponding hash value is JA, a third-party TTP trusted by all users can choose the RSA algorithm to generate secret SA parameters for user A. The specific process is as follows: select multiple secret prime numbers p and q, calculate $n = pxq$ accordingly, and then select e according to

$$\gcd(e, (p-1) \times (q-1)) = 1. \quad (9)$$

Generate the public key (e, n) and private key (d, n) of user A, where

$$d = e \bmod ((p-1) \times (q-1)). \quad (10)$$

Based on this, the secret parameter SA of A is generated:

$$S_A = J_A^d \bmod n. \quad (11)$$

Here,

$$\begin{aligned} &1 < J_A < n, \\ &\gcd(J_A, (p-1) \times (q-1) = 1). \end{aligned} \quad (12)$$

3.2. Analysis of Desensitization Effect of Cloud Computing Database. The text recognition experiment data is divided into two parts: the first part mainly comes from the ICDAR2017 Chinese text analysis competition data, of which the total data values of 20,000 pictures are used as training samples; the second part of the data uses artificially annotated sensitive data desensitization scene graphs. The total amount of data is about 1600 pieces, the total number of data in the image training set is 1000 pieces, and the total number of data entered in the test image data is 600 pieces.

The text recognition data is mainly composed of synthetic pictures. About 30 M Chinese and English texts were searched in the set corpus. Most of these libraries are computer-related, and there are 20 Chinese and English fonts in total, of which there are about 10,000 background images; one is randomly selected as the background wallpaper. A piece of randomly generated text and font, size, color, etc., is combined with the background image, and the text image thus generated can be used as a sample.

The text detection analysis index 110S is composed of the accuracy rate P (precision), the recall rate R (recall), and the average harmonic score F (F-score) of the two. Among them, the accuracy rate P is the ratio of the correct value of the text recognition box to the value of the number of all text recognition boxes; the recall rate R is the ratio of the value to the correct number when recognizing the text. F-score can be comprehensively evaluated by accuracy rate P and recall rate R. The calculation formula is as follows, where G represents the actual marked text recognition box, D represents the text recognition box to be predicted, and Best M is the best match (BestMatch) in text recognition. The actual mark in the box and Best Mp are the best match in the actual text recognition box:

$$\begin{aligned} R &= \frac{\sum_{i=1}^{|G|} Best\, M_G(G_i)}{|G|}, \\ P &= \frac{\sum_{j=1}^{|D|} Best\, M_D(D_j)}{|D|}, \\ F - score &= \frac{2^* P^* R}{P + R}. \end{aligned} \quad (13)$$

The character recognition evaluation index adopts the single character recognition accuracy rate Prec to measure the character recognition algorithm, among which

$$P_{rec} = \frac{N_{rec}}{N_{total}}. \quad (14)$$

The text analysis training data is composed of a text recognition competition data set and a manual labeling part of the data set. First, the first group of data is trained, and then the second group of data is used to improve and fine-tune the network foundation. Finally, 600 photos of data-sensitive desensitization scenes were tested, and the 600 pieces of test data were further divided into three groups of test data.

The text recognition test results of CTPN-MASK model and CTPN model are shown in Table 1. The measurement accuracy of the CTPN-MASK text detection model is 77.3%, the recall rate is 75.9%, and the F-score score is 76.6%. It can

Table 1: Comparison of CTPN-MASK and CTPN overall test results.

Model	Accuracy rate P	Recall rate R	F-score
CTPN	0.551	0.568	0.559
CTPN-MASK	0.773	0.759	0.766

Table 2: Test data set 1-CTPN-MASK and CTPN test results comparison.

Model	Accuracy rate P	Recall rate R	F-score
CTPN	0.628	0.624	0.627
CTPN-MASK	0.762	0.731	0.746

Table 3: Test data set 2-CTPN-MASK and CTPN test results comparison.

Model	Accuracy rate P	Recall rate R	F-score
CTPN	0.481	0.512	0.496
CTPN-MASK	0.768	0.758	0.763

Table 4: Test data set 3-CTPN-MASK and CTPN test results comparison.

Model	Accuracy rate P	Recall rate R	F-score
CTPN	0.484	0.518	0.502
CTPN-MASK	0.793	0.806	0.798

Table 5: CRNN-MASK and CRNN overall test results comparison.

Model	Accuracy
CRNN	0.905
CRNN-MASK	0.925

be seen that the three data items of this model are all higher than those of the CTPN model.

Tables 2–4 are the comparison of CTPN-MASK and CTPN text recognition test results in the three sets of test data. Experiments have confirmed that the CTPN-MASK model proposed in this section has certain advantages in the accuracy of text recognition.

The test data set 2-CTPN-MASK and CTPN test results are shown in Table 3.

The test data set 3-CTPN-MASK and CTPN test results are shown in Table 4.

The overall test results of CRNN-MASK and CRNN are shown in Table 5.

Table 6 shows the comparison of the test results of CRNN-MASK and CRNN on the three test data sets.

The comparison of the overall test results of CTPN-MASK + CRNN-MASK and CTPN + CRNN is shown in Table 7.

Table 8 shows the comparison of the test results of CTPN-MASK + CRNN-MASK and CTPN + CRNN on the three test data sets.

3.3. Test Method of Cloud Computing Database Security. The cloud service platform user enters the user name and password on the login page to complete the login. In order to avoid affecting the initial authentication process, you only need to edit the authentication page, add a fingerprint connection module and related registration modules, and add them to the authentication page to confirm cross-domain fingerprint recognition. In this way, the authentication system can be transformed on the basis of preserving the functions of the original connected website.

Table 6: Comparison of test results between CRNN-MASK and CRNN on three test data sets.

Model	Test data set 1	Test data set 2	Test data set 3
CRNN	0.885	0.942	0.829
CRNN-MASK	0.892	0.941	0.926

Table 7: Comparison of overall test results of CTPN-MASK + CRNN-MASK and CTPN + CRNN.

Model	Accuracy
CTPN + CRNN	0.807
CTPN-MASK + CRNN-MASK	0.917

The test platform provides two authentication interfaces, one for intradomain authentication and the other for cross-domain authentication. The platform verifies the identity verification information between internal users and domains through different interfaces accessed by users. If the verification is passed, it will automatically enter the homepage of the test platform. If the verification fails, go to the failed verification page. The home page of the test platform can display all verified user account records. Table 9 shows the main files related to the test platform.

This feature uses a temporary account registered on the cloud platform to enable intradomain and cross-domain authentication on the test platform and analyzes the authentication impact of the cross-domain authentication system based on the authentication results.

Create an anonymous account: enter the cloud platform login page, use the cloud user test to register a personal domain name, and retrieve 10 account information.

Identity verification test: the test platform continuously uses 10 temporary accounts for intradomain and cross-domain identity verification and calculates the result of each identity verification and the total identity verification time. After the authentication is successful, the page will display the login information of the successfully authenticated domain and display the previous authentication records, authentication parameters, and certificates used.

3.4. Test Results and Analysis of Cloud Computing Database Security. Figure 1 shows the statistical information of the test platform results after using 10 temporary accounts for intradomain authentication.

Figure 2 shows the use of 10 temporary accounts for intradomain authentication and the statistical information of the results of the test platform.

The results of intradomain authentication and cross-domain authentication are shown in Figure 2. In addition to modifying the intradomain authentication parameters of

Table 8: Comparison of the test results of CTPN-MASK + CRNN-MASK and CTPN + CRNN on three test data sets.

Model	Test data set 1	Test data set 2	Test data set 3
CTPN + CRNN	0.802	0.867	0.672
CTPN-MASK + CRNN-MASK	0.897	0.928	0.926

Table 9: Class files mainly included in the test platform.

Class file name	Class belonging to package	Class function description	Owned functional module
Action.java	Controller	Intradomain authentication	Intradomain authentication module
CrossAction.java	Controller	Cross-domain authentication	Cross-domain authentication module
ShowRecordList.java	Controller	Get data list	Data display module
RecordListDAO.java	DAO	Perform data list database operations	Database operation module
CertiRecordList.java	Model	Certification record list management	Register module

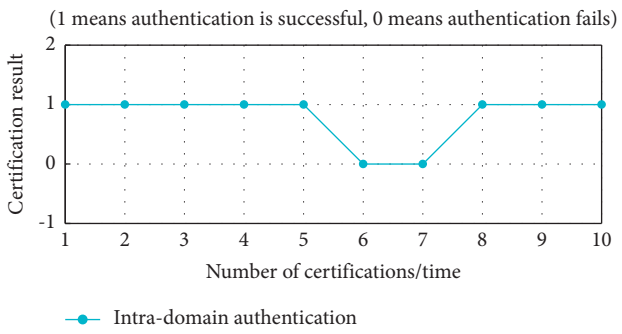

Figure 1: Intradomain authentication result statistics.

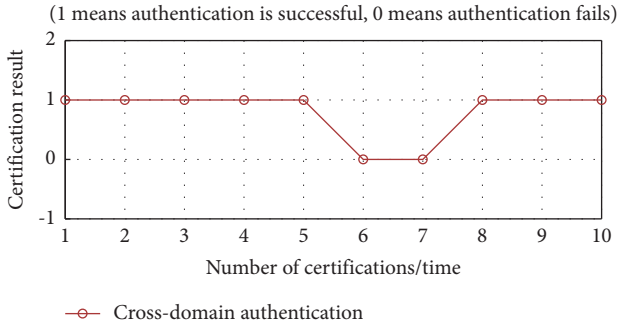

Figure 2: Statistics of cross-domain authentication results.

accounts 6 and 7, other temporary accounts can successfully verify their identity through participating in the test. The results show that the cross-domain authentication system can effectively identify the identity. Comparing the intradomain authentication time and the cross-domain authentication time, it can be concluded that the time spent in each cross-domain authentication exceeds the time spent in the intradomain authentication. This is because a large number of encryption operations are performed during the cross-domain authentication process, which makes the verification time longer. As the authentication time accumulates, the time difference between the two authentication processes will gradually increase, thereby reducing the time required for the interdomain authentication process. Therefore, it is necessary to improve encryption and decryption algorithms and improve the efficiency of identity

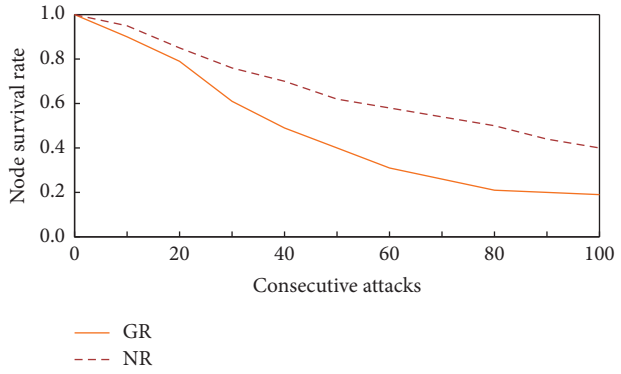

Figure 3: System vulnerability comparison.

verification. Such problems will become the focus of future research.

For information security under attack mode, test how to stably access the system. Robustness refers to the stability of the system. Whether the system can provide services normally under abnormal conditions depends more on the stability of the system itself.

According to statistics, 10,000 pieces of user registration data were sent to the user registration function in the system, and the number of abnormalities in the user registration function was 102 times. It can be seen that if the system is attacked, the abnormal rate of the system is 1.02%, which is generally kept at a low level.

In order to better measure the stability of the attacked system, a system vulnerability index is introduced here for analysis and measurement. System vulnerability refers to the degree to which system performance is impaired when the system is attacked. The vulnerability measurement formula is

$$R_n = \frac{M'}{M}. \tag{15}$$

Figure 3 shows the comparison of the vulnerability analysis of the general system (GR) and this system (NR) when they are attacked, which shows that the robustness of this system is better.

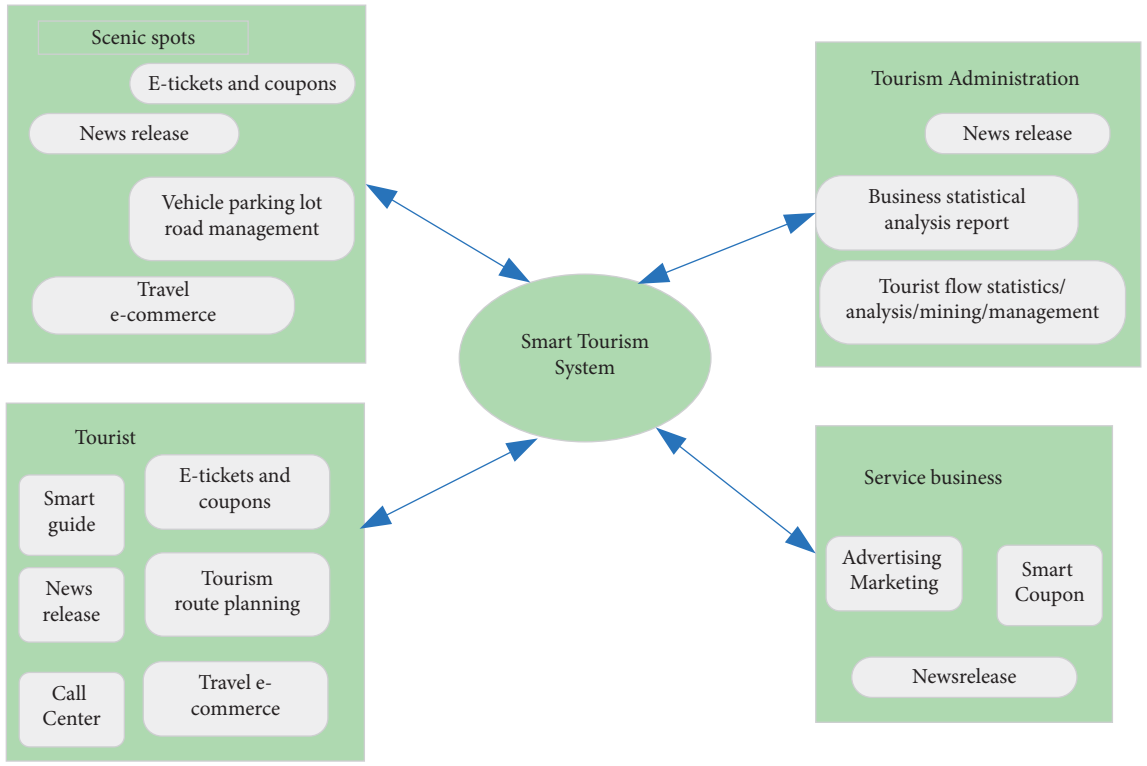

Figure 4: Smart tourism demand relationship.

4. Design and Application of the Sensor-Based Tourism Smart Platform

4.1. Demand Analysis of The Tourism Smart Platform. Smart tourism takes the integration of service resources as the core, focuses on user travel needs, and integrates data sources with the e-government tourism system as the basis. Through demand analysis, it adopts the analysis method facing the user. Smart tourism has four types of objects: tourists, scenic spots, service companies, and tourism management agencies, as shown in Figure 4.

To make a good product, we must not only fully meet the specific requirements of customers for system functions, but also continuously optimize the nonfunctional modules in the system, so that users have a better experience. According to the characteristics of SNS itself, combined with some specific requirements for the operation of mobile social systems, this article will discuss the nonfunctional requirements of the system from the aspects of compatibility, reliability, ease of use, ease of maintenance, and adaptability.

Because different tourists will use different Android client mobile phones, different mobile phones will be different in terms of brand, operating system version, screen resolution, etc. Therefore, the system that we created needs to ensure better compatibility, so that visitors from different Android customers can quickly get started using the system.

Maintainability focuses on a set of attributes related to the work required to make clear changes, including stability, ease of analysis, ease of testability, and ease of change. The application program created with this system should have the above characteristics to ensure that the subsequent maintenance work is simpler and the maintenance cost is lower.

Technological progress in the modern world is changing with each passing day, especially in the fast-updated software industry. Therefore, when designing the system, we need to ensure that it can meet the user's requirements for new technologies in a certain period of time in the future. In the process of designing the system, we need to introduce hierarchy and modularity in order to expand it in the future.

4.2. Model Design of the Sensor-Based Network Positioning System. The positioning system uses a mesh network topology to build a ZigBee wireless sensor network. The ZigBee wireless sensor network has a coordinator, router, and terminal equipment and connects the network to the computer through the coordinator. According to the received signal strength principle realized by RSSI, the router is designed as a fixed reference node, and the PC configures the coordinates of each recommended node through the coordinator; the terminal device is designed as an anonymous node, and the anonymous node uses the RSSI configuration algorithm to calculate the coordinates and transmits the ZigBee wireless network to the computer.

The wireless sensor network positioning system model based on ZigBee protocol designed in this paper is shown in Figure 5.

4.3. System Architecture Design. The Android client of this system adopts C/S structure. However, the Android client of this system first transmits the data to the Web side and then

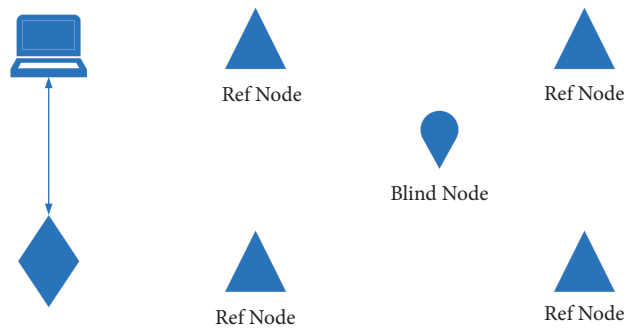

Figure 5: Wireless sensor network positioning system model based on the ZigBee protocol.

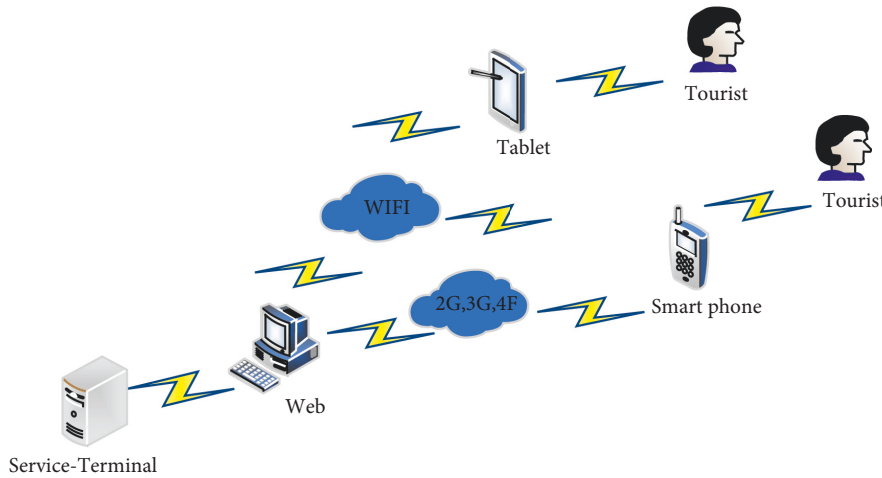

Figure 6: Physical architecture diagram of the Android client.

accesses the server side based on the Web side. The physical architecture diagram of the Android client of this system is shown in Figure 6.

Users, namely, tourists, communicate with the Web terminal through Android smart mobile terminal devices such as smart phones or tablet computers, and the Web terminal interacts with the server for data processing and operations. Finally, the results are delivered through a return form specific to the Android client user.

4.4. Realization of the Functions of the Tourism Smart Platform. Unregistered Android client users must register before they can continue to log in to access the Android client. Android users need to fill in some relevant registration information on the signup.xml page, including user name, password, nickname, e-mail, and birthday information. The user name and password are required information, and a unique password must be filled in during registration to ensure that the user does not enter wrong information when entering the password for the first time. After completing all the information, the user can click the registration button. After completing the registration information, the information will be taken to the background activity. In the background activity, people first obtain the relevant reference of the registration button and add a listener for the registration button, so as to ensure that the correct information jump is recorded. Then, they prepare the URL for receiving server-side information. The URL for receiving information in this application is Register.action. Open the connection website and send the relevant record information to the registered users on the server. Then, the RegisterAction server reads the corresponding parameter information from the HttpServletRequest. Then, call the corresponding UserDao method to manipulate the database data and verify whether the registration information has been registered. The log function is implemented using the POST method of the HTTP protocol.

In the realization of the travel service module, related functions are involved in searching for nearby locations. Searching for neighborhood locations obviously means searching for specific locations around the user based on the user's specific location. This method has many implementations. One of the most easily considered methods is to directly search the entire database on a certain scale; that is, we search the entire database according to specific requirements, and if the appropriate conditions are met, it will be regarded as a pair, but this method is the yield that is relatively poor, and the effectiveness is very low. Therefore, we made the following idea: whether we can divide the search area into several small areas first, that is, search the small areas first and then combine these results to get more

search results, in this case, the search efficiency will be higher. The answer is yes. R-tree two-dimensional search can solve such problems, but the structure of R-tree is very complicated. If the map is very large, many new ones will appear (complicated question). Moreover, the fragmentation and integration of R-tree are also an annoying problem. Therefore, the production cost of this method is not very high.

There are two formulas for calculating the distance between any two interior points according to the latitude and longitude coordinate information, namely, the Great-circle distance formula and the Haversine formula. There are obvious differences between the two formulas. The former is composed of several cosine formulas, while the latter has multiple sine formulas. If the distance between the two interior points that we want to calculate is too small, then the Great-circle distance formula will give a large error, while the Haversine formular formula will not produce this situation. This is the reason why the Haversine formular is used here in this article, which is defined as

$$\text{haver sin}\left(\frac{d}{R}\right) = \text{haver sin}\left(\phi_2 - \phi_1\right) + \cos\left(\phi_1\right)\cos\left(\phi_2\right) \text{haver sin}\left(\varnothing_2 - \varnothing_1\right). \tag{16}$$

Here,

$$\text{haver sin}\left(\theta\right) = \sin^2\left(\frac{\theta}{2}\right) = \frac{\left(1 - \cos\left(\theta\right)\right)}{2}. \tag{17}$$

Let us first calculate the range between the longitudes on the east and west sides. In the Haversine formula, letting $\varphi 1 = \varphi 2$, we can get

$$\Delta\varnothing = 2\arcsin\left(\frac{\sin\left(d/2R\right)}{\cos\left(\phi_1\right]}\right). \tag{18}$$

Then, we come to find the boundary of the range of latitudes on both sides of the north and south. In the Haversine formula, letting $\varphi 1 = \varphi 2$, we can get

$$\Delta\phi = \frac{d}{R}. \tag{19}$$

In this way, we can get the coordinates of the four points in the rectangular area according to the coordinates of the current point, thereby obtaining the search range. In addition, establishing proper indexes in the longitude and latitude columns can improve the order of queries for effective measurement.

The function of the information of the surrounding scenic spots is that, after obtaining and locating the specific location of the tourist, the status of the surrounding scenic area of the tourist can be displayed according to the specific location of the tourist, thereby facilitating the arrangement of the travel itinerary. In the process of realizing this function, you must first know the longitude and latitude coordinates of the user's location on the Android client, and then the system searches the surrounding locations through algorithms, finds relevant information about the surrounding scenic spots, and combines the information according to the longitude and latitude information of the tourist location and returns it to the Android client user. The details of the specific implementation process are as follows: first, the customer uses a certain map software to find the latitude and longitude coordinates of the current Android customer's location. Then, the latitude and longitude information is sent to the back-end server, and then the server calls the relevant redirection layer method to query the content of the database and finally returns the query result to the Android client to display to the relevant user.

5. Conclusion

In recent years, the tourism industry has received more and more attention from the national and local authorities. The Director of the China National Tourism Administration has repeatedly suggested that the construction of localized smart tourism in China should be realized as soon as possible. The National Tourism Administration has also implemented the determination of the "Smart Tourism Year." It can be seen that smart tourism is developing in an extremely rapid manner in China. Based on this, in the Internet, with the continuous advancement of information technology such as multiple data analysis, cloud computing, and mobile communications, the public's demand for tourism information services has become more vigorous, which has provided technical support and motivation for the flourishing development of the tourism industry. Smart tourism uses modern information technology to create a smart tourism service construction plan. By analyzing the status quo and customer needs, it gathers relevant elements of the tourism industry to promote the in-depth integration of modern information technology and the tourism industry. This article takes a certain scenic spot in China as an example, starts from the perspective of smart tourism, examines the correlation between smart tourism and the development of traditional tourism, considers the role of smart tourism in promoting the development and innovation of traditional tourism, and establishes the basis of this research. The smart tourism system was developed, and the construction plan, system operation mechanism, and technical realization were comprehensively analyzed and explained in depth.

Data Availability

The data used to support the findings of this study are available from the author upon request.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] C. Li, Y. Fang, and B. Sukoco, "Value proposition as a catalyst for innovative service experience: the case of smart-tourism destinations," *Service Business*, vol. 15, no. 2, pp. 281–308, 2021.

[2] Z. Ghaderi, P. Hatamifar, and L. Ghahramani, "How smartphones enhance local tourism experiences?" *Asia Pacific Journal of Tourism Research*, vol. 24, no. 8, pp. 778–788, 2019.
[3] A. Caldeira and E. Kastenholz, "Spatiotemporal tourist behaviour in urban destinations: a framework of analysis," *Tourism Geographies*, vol. 22, no. 1, pp. 22–50, 2020.
[4] S. Mandal, "Exploring the influence of big data analytics management capabilities on sustainable tourism supply chain performance: the moderating role of technology orientation," *Journal of Travel & Tourism Marketing*, vol. 35, no. 8, pp. 1104–1118, 2018.
[5] G Nikoli and A Lazakidou, "The impact of information and communication technology on the tourism sector," *Almatourism - Journal of Tourism, Culture and Territorial Development*, vol. 10, no. 19, pp. 45–68, 2019.
[6] F. Fusté-Forné and T. Jamal, "Co-creating new directions for service robots in hospitality and tourism," *Tourism and Hospitality*, vol. 2, no. 1, pp. 43–61, 2021.
[7] J. Lemley, S. Bazrafkan, and P. Corcoran, "Deep learning for consumer devices and services: pushing the limits for machine learning, artificial intelligence, and computer vision," *IEEE Consumer Electronics Magazine*, vol. 6, no. 2, pp. 48–56, 2017.
[8] Y. Zhang, J. Ren, J. Liu, C. Xu, H. Guo, and Y. Liu, "A survey on emerging computing paradigms for big data," *Chinese Journal of Electronics*, vol. 26, no. 1, pp. 1–12, 2017.
[9] S. Toapanta, O. Escalante Quimis, L. Gallegos, and M. Maciel Arellano, "Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks," *IEEE Access*, vol. 8, pp. 169367–169384, 2020.
[10] P. Casas, F. Soro, J. Vanerio, G. Settanni, and A. D'Alconzo, "Network security and anomaly detection with Big-DAMA, a big data analytics framework," in *Proceedings of the 2017 IEEE 6th International Conference on Cloud Networking (CloudNet)*, pp. 1–7, Prague, Czech, September 2017.
[11] E. Nadimi, H. Søgaard, T. Bak, and F. Oudshoorn, "ZigBee-based wireless sensor networks for monitoring animal presence and pasture time in a strip of new grass," *Computers and Electronics in Agriculture*, vol. 61, no. 2, pp. 79–87, 2008.
[12] C. Yang, Y. Liu, and X. Tao, "Assure deletion supporting dynamic insertion for outsourced data in cloud computing," *International Journal of Distributed Sensor Networks*, vol. 16, no. 9, Article ID 1550147720958294, 2020.
[13] J. Zhao and S. Hu, "A new adaptive weighted fusion algorithm for multi-sensor tracking," in *Proceedings of the 1st International Conference on Machine Learning and Cybernetics*, pp. 285–287, Beijing, China, November 2002.
[14] G. Bian and J. Chang, "Certificateless provable data possession protocol for the multiple copies and clouds case," *IEEE Access*, vol. 8, pp. 102958–102970, 2020.
[15] C. Cervellera, D. Macciò, and M. Muselli, "Deterministic learning for maximum-likelihood estimation through neural networks," *IEEE Transactions on Neural Networks*, vol. 19, no. 8, pp. 1456–1467, 2008.
[16] S. Heidari, M. Abutalib, M. Alkhambashi, A. Farouk, and M. Naseri, "A new general model for quantum image histogram (QIH)," *Quantum Information Processing*, vol. 18, no. 6, pp. 175–220, 2019.
[17] L. Ruff, J. R. Kauffmann, R. A. Vandermeulen et al., "A unifying review of deep and shallow anomaly detection," *Proceedings of the IEEE*, vol. 109, no. 5, pp. 756–795, 2021.
[18] C. Wu, S. Shao, and C. Tunc, "An explainable and efficient deep learning framework for video anomaly detection," *Cluster Computing*, vol. 25, no. 4, 2021.
[19] M. Vadursi, A. Ceccarelli, E. Duarte, and A. Mahanti, "System and network security: anomaly detection and monitoring," *Journal of Electrical and Computer Engineering*, vol. 2016, pp. 1-2, Article ID 2093790, 2016.
[20] C. Chahla, H. Snoussi, L. Merghem, and M. Esseghir, "A deep learning approach for anomaly detection and prediction in power consumption data," *Energy Efficiency*, vol. 13, no. 8, pp. 1633–1651, 2020.