Privacy-Preserving Attribute-Based Educational Service Recommendation in Online Education System

Lijuan Huan*[1], Xueyan Liu[2], Ruirui Sun[2], Linpeng Li[2]

[1]College of Mathematics and Statistics, Northwest Normal University, Lanzhou, 730070, China;
[2]College of Computer Science and Engineering, Northwest Normal University, Lanzhou, 730070, China.

Email: Lijuan HUAN, *hh041230@163.com
Xueyan LIU, liuxy@nwnu.edu.cn
Ruirui SUN, srr6694@163.com
Linpeng LI, llp2017160401210@163.com

Abstract. Educational service recommendation has attracted considerable attention since it can solve complicated educational tasks by gathering the wisdom of a crowd of teachers in recent years. In the education service recommendation system, parent (student) can send requirements to the education platform, and get a suitable teacher recommended. In the existing education service recommendation schemes, although parent (student) can send the basic requirements to get education service recommendations, they cannot set personalized requirements to obtain personalized education services. In addition, teacher' ability or credibility has not been concerned, and the privacy-preserving of tasks and task recipients have also been ignored. To address the above problems, this article proposes a privacy-preserving attribute-based education service recommendation scheme, which realizes fine-grained access control and keywords search for education services by using attribute-based searchable encryption (ABKS). Then, the anonymous key generation method is adopted, in which the attribute authority and the teacher interact to generate the key to ensure the security of the teacher's key. Besides, education platform can choose the best teacher to accept the task by evaluation mechanism. The security proof and performance analysis show that the scheme has strong security and practicality in the online education system.

Keywords: ABKS, education services, anonymity, policy hiding, credibility evaluation.

1 Introduction

With the continuous development of informatization and 5G technology, many online learning platforms have been widely used, and people's learning is no longer limited especially by time, space, and geographical location in recent years. Teacher can leverage these potential mobile devices to carry out some special tasks in his spare time. In

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 826–838, 2022.
https://doi.org/10.2991/978-94-6463-108-1_92

the education service recommendation system, parent (student) can send his requirements to the education platform, and then the education platform recommends appropriate teacher according to the requirements of parent (student). Therefore, helping student find educational resources, helping student find and fill gaps, and cultivating student' knowledge systems have become the key research contents of educational resource service recommendations [1].

In the educational service recommendation system, task allocation is a very key service and determines the quality of tasks accomplished. To achieve accurate task allocation, parent (student) needs to mark his tasks with a few proprietary keywords and uploads them to the education platform, and the education platform distributes the corresponding tasks to the teacher by matching the task's proprietary keywords with the interest keywords designated by teacher. If these keywords are given in plaintext format, the education platform will possess full knowledge of keywords of the task content and the teacher's interests, in which sensitive information about task content and the teacher are usually involved. In addition, the education platform is not fully trusted. For its benefit, it may inevitably disclose sensitive information related to task content and teacher profiles. Therefore, it is a huge challenge how to enable efficient task distribution of education platform without sacrificing the privacy of teacher.

At a first glance, attribute-based searchable encryption (ABKS) [4] [5] [6] [7], which combines attribute-based encryption (ABE) [2] and searchable encryption (SE) [3] may be the best solution in the current education service recommendation system. It enables the education platform to match keywords with teacher' interests. Specifically, parent (student) uses attribute-based encryption to encrypt ciphertext and extracts keywords before uploading educational requirements, while teacher subscribes to his educational tasks by sending requirements to the education platform without knowing the basic content of tasks and interests. Among the existing ABKS schemes [8] [9] [17], they only support single keyword search, which greatly reduces the flexibility and practicality in practical applications.

In addition to privacy and effective implementation of fine-grained access control, some teacher' keys may be maliciously tampered with, disclosed, or attacked. In ABKS schemes, key generation depends on trusted attribute authority. To ensure the security of the key, scholars have successively proposed some solutions, such as key-free regeneration [10], without key escrow [11] [12] [13], and multi-attribute authority [14] [15] [16]. However, they cannot guarantee the anonymity of the key in the key generation.

Therefore, we propose a privacy-preserving attribute-based education service recommendation scheme in online education system. First of all, we introduce the linear secret sharing mechanism [18] to encrypt educational service requirements, and the keywords extracted from his requirements are encrypted. Secondly, teacher extracts keywords according to his hobbies to generate token and sends them to the education platform to receive tasks. After the education platform matches, only qualified teacher can decrypt. Finally, the teacher with the best credibility can get the task. The contribution of this paper is summarized in the following three aspects:

- ABKS is used to achieve the task access control of fine-grained education services and the precise search of keywords.
- The anonymous key generation method is adopted, in which the attribute authority and teacher interact to generate the key to ensure the security of the teacher' key. So, teacher chooses appropriate education tasks anonymously according to his interests.
- We have designed an evaluation mechanism for teacher' credibility, and the education platform can choose the best teacher to accept the task, to prevent greedy teacher from grabbing the education task maliciously to obtain high remuneration.

2 Preliminaries

2.1 Decisional parallel DIFFIE-HELLMAN (BDHE)assumption

Definition 1: The decisional $q-$ parallel bilinear Diffie–Hellman exponent (BDHE) problem is that for any probabilistic polynomial time (PPT) algorithm, given $\vec{y}=g,$ $g^{s},g^{a},\cdots g^{a^{q}},g^{a^{q+2}},\cdots,g^{a^{2q}}$, $\forall 1\le j\le q,g^{s\cdot b_j},g^{\frac{a}{b_j}},\cdots,g^{\frac{a^{q}}{b_j}},g^{\frac{a^{q+2}}{b_j}},\cdots,g^{\frac{a^{2q}}{b_j}}$, $\forall 1\le j,k\le q,k\ne j,g^{\frac{a\cdot s\cdot b_k}{b_j}},\cdots,g^{\frac{a^{q}\cdot s\cdot b_k}{b_j}}$. It is difficult to distinguish $\left(\vec{y},e(g,g)^{a^{q+1}\cdot s}\right)$ from $\left(\vec{y},z\right)$, where $g\in G,z\in G,a,s,b_1,\cdots,b_q\in Z_p$ are chosen independently and uniformly at random.

2.2 Access structure

Definition 2: Let $P=\{P_1,P_2,\cdots,P_n\}$ be a set of parties. A collection $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}$ is monotone if $\forall B,C,B\in A$ and $B\subseteq C$, then $C\in A$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of $P_1,P_2,\cdots,P_n$, i.e., $A\subseteq 2^{\{P_1,P_2,\cdots,P_n\}}/\{\varnothing\}$. The sets in A are called the authorized sets.

3 System model and security analysis

3.1 System model

As shown in Figure. 1, our system consists of four entities: Parent (Student), Teacher, Education Platform (EP), and Attribute Authority (AA).

Parent (Student): Parent (Student) encrypts his own requirements, and extracts keywords to generate index. He uploads the task and index to the EP and recruits teacher who satisfies his requirements to accomplish the tasks.

Teacher: Teacher extracts keywords to generate token according to his interests and hobbies, and uploads the token to the EP to look for tasks whose requirements are satisfied by his attributes.

Education Platform (EP): EP is assumed with abundant computing and storage resources. It is responsible for provide education services to parent (student) according to his requirements and recommending educational tasks to teacher.

Attribute Authority (AA): AA is a trusted third party and distributes public key to parent (student) and anonymous private key to teacher.

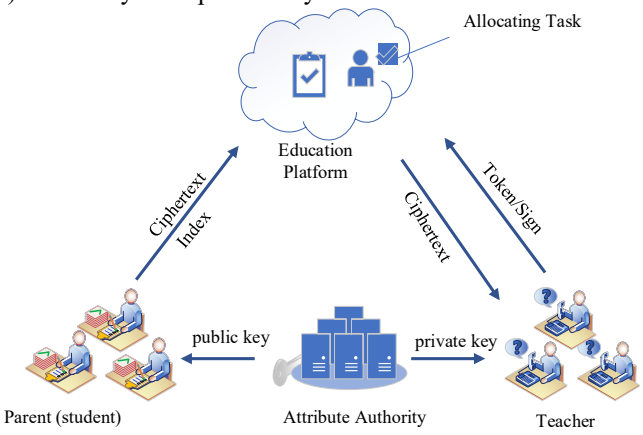

Fig. 1. System Model.

3.2 Security goals

Assume that the education platform is "honest but curious". It will not modify or destroy the specific information of the files stored on it, but will be curious about the encrypted files (including indexes) of parent (student) and queries generated by teacher. The education platform knows outsourced ciphertext, indexes, and some backgrounds on file sets. Based on the above possible threats, the security goals of the scheme are as follows:

Confidentiality: Unauthorized teacher cannot obtain data and related content.

Anonymity: AA and a teacher interact to generate the key, so, the teacher can choose appropriate education tasks anonymously according to his interests.

4 Our construction

4.1 Specific scheme

Phase 1: System Setup

On input the security parameter λ and the system attributes $U=\{U_1,U_2,\cdots U_n\}$, AA randomly selects $v_x \in Z_P^*$, $\forall x \in U$, and calculates $\left\{g^{v_x}\right\}_{x\in U}$. G and G_T are

two groups of prime order p and g,h are generator of G. $e:G\times G\to G_T$ is the bilinear map, H,H_0 and H' are anti-collision hash functions $H:\{0,1\}^*\to Z_P^*$, $H_0:\{0,1\}^*\to G_0, H':G_0\to Z_P^*$. Finally, AA randomly selects $\alpha\in {Z_P}^*$, and outputs public key and master key:

$$PK=\left(p,g,h,G,G_T,e,H,H_0,H',g^{\alpha},\left\{g^{v_x}\right\}_{x\in U},e(g,g)^{\alpha}\right),\ MSK=(\alpha,v_x).$$

Phase 2: key generation

AA runs the interactive operation with the teacher. Input teacher' attribute set $Att=\{att_1,att_2,\cdots,att_n\}$ and master key MSK, and output private key SK.

(1) First, a teacher with global identifier GID randomly selects $R_u\in Z_P$, and calculates $x_u=H\left(GID\|R_u\right)$, $Y_u=g^{\alpha x_u}$, and then sends Y_u to AA.

(2) AA selects $t\in Z_p^*$ randomly, and calculates $k_{1,i}{}'=Y_u g^{v_x t},k_2{}'=g^t,k_{3,i}{}'=h^{tH_0(att_i)}$, $k_{4,i}{}'=H_0\left(att_i\right)^{\alpha}$, then can return $\left(k_{1,i}{}',k_2{}',k_{3,i}{}',k_{4,i}{}'\right)$ to the teacher.

(3) Then, the teacher uses x_u to recover private key, $k_{1,i}=\left(k_{1,i}{}'\right)^{\frac{1}{x_u}}=g^{\alpha}g^{\frac{v_x t}{x_u}}$, $k_2=\left(k_2{}'\right)^{\frac{1}{x_u}}=g^{\frac{t}{x_u}},k_{3,i}=\left(k_{3,i}{}'\right)^{\frac{1}{x_u}}=h^{\frac{tH_0(att_i)}{x_u}},k_{4,i}=k_{4,i}{}'=H_0\left(att_i\right)^{\alpha}$, where the private key $k_{4,i}$ is used for attribute hiding.

(4) Finally, output private key: $SK=\left(k_2,\{k_{1,i},k_{3,i},k_{4,i}\}_{i\in[1,n]}\right)$.

Phase 3: Task encryption

For the educational requirements $m\in F$, parent (student) first encrypts m with a symmetric key $K\in G_T$ as $C_m=Enc_K(m)$. Then the parent (student) encrypts the symmetric key K with ABE. D is a matrix of $l\times n$, a function ρ maps each row D of D_i to each attribute. Parent (Student) selects a column vector $\vec{v}=(s,r_2,r_3,\cdots r_l)\in {}_R{Z_P}^l$ and $s\in Z_P$, where s is a secret value, computes $\lambda_i=\vec{D}_i\vec{v},i=1,2\cdots l$. Set ciphertext:

$$C=Ke(g,g)^{\alpha s},C_1=g^s,C_{2,i}=g^{v_x\lambda_i},C_3=g^{H'(K)},C_{4,i}=h^{H_0(\rho(i))}.$$

Next, the parent (student) will calculate $q_i=\left(H_0\left(\rho(i)\right),g^{\alpha}\right)$ for each i in the access policy (D,ρ), and the hid access policy is $\left(\bar{D},\bar{\rho}\right)$. The set of keywords is $\{kw_k\}_{k\in W_{\varphi}}$, the parent (student) randomly selects $r_i\in Z_P$, and calculates $r=\sum_{i=1}^{n}r_i$. Set

index $I_1 = g^{\alpha r \sum_{k \in W_\varphi} H(kw_k)}, I_2 = h^{\sum_{i \in [1,n]} r_i H_0(\rho(i))}$. Finally, upload the ciphertext C_m, $CT = \left\{C, C_1, C_3, \left\{C_{2,i}, C_{4,i}, q_i\right\}_{i \in [1,l]}\right\}$ and the index $I = \{I_1, I_2\}$ to EP.

Phase 4: Interest encryption

The teacher extracts the keywords $\{kw_k'\}_{k \in W_\varphi}$ according to his abilities and interests to encrypt them. Teacher first selects $\tau_i \in Z_P$, and computes token $T_{l,k} = g^{\alpha \tau_i H(kw_k')}, T_{2,i} = h^{\tau_i}$. For each attribute $i \in Att$, the teacher calculates $q_i' = \left(g, H_0(i)^\alpha\right)$, to replace each attribute $Att(i)$ with q_i' and the attribute set is converted into $\overline{Att}$.

Finally, the teacher sends the token $Tok = \left\{\left\{T_{1,k}\right\}_{k \in W_\varphi}, \left\{T_{2,i}, q_i'\right\}_{i \in [1,n]}\right\}$ to EP.

Phase 5: Task assignment

In order to accurately complete the push task, EP will test whether the keywords related to the task satisfy the requirements of parent (student). Input the index, token, and teacher' attribute set. EP first checks the teacher' attribute set, and whether $\overline{Att}$ satisfies the task's access policy through $q_i = q_i'$. If the access policy is satisfied, EP will continue to check the equation $e\left(I_1, \prod_{i \in [1,n]} T_{2,i}^{H_0(att(i))}\right) = e\left(I_{2,i}, \prod_{k \in W_\varphi} T_{1,k}\right)$. If it holds, it means that the attributes of the teacher satisfy the requirements of parent (student).

Phase 6: Decryption phase

Before assigning tasks to the matching teacher, EP calculates $V = g^a$ with a random number $a \in Z_P$, and sends (CT, V) to the matching teacher. If the teacher's attributes satisfy the requirements, an authorization set $I = \{l : \rho(l) \in S\} \subset (1, 2, \cdots, l)$ is obtained. There exists a set of constants ω_i such that, $\sum_{l \in I} \omega_i \vec{M}_i = (1, 0, \cdots, 0)$ and $\sum_{l \in I} \omega_i \lambda_i = s$. Then the teacher calculates

$$K = \frac{C \cdot e\left(k_{3,i}, g^{-1}\right) e\left(\prod C_{2,i}^{\omega_i} \cdot C_4, k_2\right)}{e\left(k_{1,i}, C_1\right)}.$$

Then, the teacher signs V with the symmetric key K, i.e., $P = V^{H'(K)}$, and sends it back to EP as the proof. After verifying $P = (C_3)^a$, EP selects the teacher with the highest credibility, and sends C_m to the selected teacher, the teacher can get m by $m = Dec_K(C_m)$ lastly.

4.2 Correctness:

$$K=\frac{C\cdot e\left(k_{3,i},g^{-1}\right)e\left(\prod C_{2,i}{}^{\omega_i}\cdot C_4,k_2\right)}{e\left(k_{1,i},C_1\right)}=\frac{Ke(g,g)^{\alpha s}\,e\left(h^{\frac{tH_0(att_i)}{x_u}},g^{-1}\right)e\left(\prod_{i\in I}\left(g^{v_x\lambda_i}\right)^{\omega_i}\cdot h^{H_0(\rho(i))},g^{\frac{t}{x_u}}\right)}{e\left(g^{\alpha}g^{\frac{v_x t}{x_u}},g^{s}\right)}$$

$$=\frac{Ke(g,g)^{\alpha s}\,e(h,g)^{\frac{-tH_0(att_i)}{x_u}}\,e(g,g)^{\frac{v_x st}{x_u}}\,e(h,g)^{\frac{tH_0(\rho(i))}{x_u}}}{(g,g)^{\alpha s}\,e(g,g)^{\frac{sv_x t}{x_u}}}=K\,.$$

4.3 Credibility evaluation

EP establishes an evaluation mechanism to generate the corresponding credibility value according to the factors such as each teacher's successful acceptance of the task and the parents' evaluation. See Figure 2 for details.

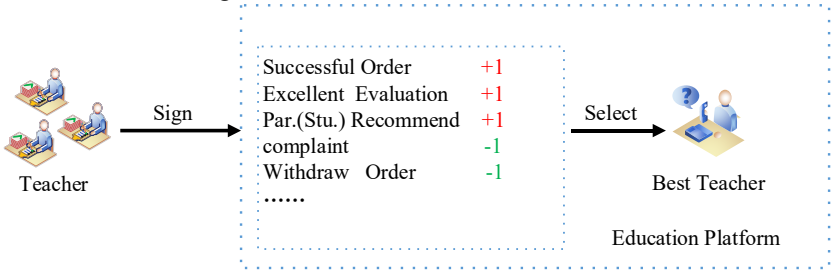

Fig. 2. Credibility evaluation system.

5 Security analysis

Theorem 1: Under the assumption of $q-$Parallel BDHE, the attribute-based educational service recommendation encryption scheme is secure against indistinguish-able chosen-plaintext attacks.

Proof: Assume that there is a PPT adversary A who can win the ciphertext indistinguishability security game with a non-negligible advantage ε.

Set Up: C runs the Setup algorithm according to the system attribute set, outputs public key PK to A and retains the master secret key MSK.

Query Phase 1: A queries the key to the challenger C. The key generated by the interaction between the attribute authority and the teacher is secure and will not disclose private information. A submits attribute set Att with identity GID to C, C randomly selects $R_u' \in Z_P$ and interacts with the attribute authority to calculate the private key. Finally, sends the private key to A.

Challenge: A submits two messages K_0^* and K_1^* with the same length with access policy to C. C randomly chooses a bit $b \in (0,1)$ and sets $C = K_b^* e(g,g)^{\alpha s}$, and randomly selects vectors $\vec{v} = (s, r_2', r_3', \cdots, r_l') \in {}_R Z_p^l$ that are calculated by sharing secret value s, computes $C_{2,i}{}^* = g^{v_x \lambda_i}, C_{4,i}{}^* = h^{H_0(\rho(i))}$. Finally, C sends the challenge ciphertext CT^* to A.

Query Phase 2: A makes queries adaptively as in Query Phase 1.

Guess: A outputs a guess $b' \in (0,1)$ for b and if $b' = b$, A wins the game. In other words, it is effective to CT^* under the assumption of $q-$ Parallel BDHE. The advantage of A for winning the confidentiality game is defined as $Adv_A = \left| \Pr[b' = b] - \frac{1}{2} \right|$. Then the scheme is proved to achieve selective plaintext security.

Theorem 2: The scheme can resist the collusion attack of teachers.

Proof: When a teacher initiates a private key request, AA interacts with the teacher to perform the following operations: firstly, the teacher randomly selects a number $R_u \in Z_P$, and calculates $x_u = H(GID \| R_u)$ under unilaterality of Hash Function, where GID is the global identifier. Secondly, AA selects $t \in Z_p^*$ randomly and calculates $(k_{1,i}', k_2', k_{3,i}', k_{4,i}')$ to the teacher under the discrete logarithm. To sum up, the user's real identity and the random number selected by AA are embedded in the user's private key, so multiple teachers cannot conspire to obtain a group of private keys that can pass the verification. Therefore, our scheme is to resist the collusive attack of teachers.

6 Performance analysis

6.1 Theoretical analysis

Function comparison

Table 1. Function Comparison

	Access Policy	Multi-Keywords	Anonymous Key	Hidden Policy
19	AND-gate	×	×	×
20	LSSS	×	×	×
22	AND-gate	×	×	√
21	Access tree	×	×	×
Ours	LSSS	√	√	√

Table 1 shows the comparison between our scheme and related schemes [19 [20] [21] [22] in terms of access policy, multiple keywords search, anonymous key and hidden access policy. As can be seen from the table, our scheme and scheme [20] introduce the linear secret sharing. Next, our scheme realizes multiple keywords search, while other schemes do not support multiple keywords search, which is more suitable for the

promotion of education service recommendation system. Moreover, only our scheme and scheme [22] support access policy hiding. In addition, our scheme uses an anonymous key distribution protocol to generate teacher' keys, which can well prevent AA from using teacher' identity to obtain the content of task. However, other schemes do not consider key security issues. Therefore, our scheme has higher feasibility in the aspect of the educational service recommendation system.

The computational cost

Let $|U|$ represent the number of system attributes. $|G|/|G_T|$ represents the size of the element in the G/G_T, n indicates the number of user attributes. n_s represents the number of keywords used in token generation, and l represents the number of attributes in the access policy, $E_G/E_{G_T}, E_p$ represent the exponential operation in G/G_T and pairing operation respectively.

Table 2. Computational Cost

	Decryption	Index	Token	Search
20	$3E_P$	$(2n+n_s+3)E_G$	$n_s(n++7)E_G$	$6E_P$
21	$4E_P$	$2n_sE_G+E_P$	$(2n+n_s+3)E_G$	$6E_P$
23	$(2n+2)E_P$	$5n_sE_G+E_P$	$(4n_s+3)E_G$	$(5n+1)E_P$
Ours	$3E_P$	$(n_s+1)E_G$	$(n_s+1)E_G$	$2E_P$

In this subsection, a computation cost comparison between our scheme and related schemes [20] [21] [23] are presented in terms of the Decryption, Index, Token and Search computation size, as shown in Table 2. The decryption computation cost of our scheme and schemes [20] [21] is constant. In addition, in terms of index and token computing costs, the scheme [20] is not only related to the number of attributes, but to the number of keywords, so the cost is high. However, our scheme and scheme [23] are only related to the number of keywords, and our scheme is less than schemes [21] [23]. Finally, both our scheme and the schemes [21] [23] are constant in search phase, and the search cost in our scheme is far less than that schemes [20] [21]. Therefore, our scheme is efficient.

6.2 Experimental simulation

To further evaluate the performance of our scheme, we conducted a series of simulation experiments. Experiments are implemented on a platform window 10 with 2.70 GHz Intel (R) core (TM) i5-7200u CPU, 8GB RAM by using Paring-Based Cryptography (PBC) [24] with large prime 512 bits.

Figure 3 shows the time cost of index and token generation, when the number of fixed attributes is $n=5$, our scheme and the schemes [20] [21] [23] in the index and token generation stage with the increase of the number of keywords are compared. It

can be seen from Figure 3 (a) that the index generation time increases linearly with the increase of the number of keywords. Scheme [23] spends more time in the index generation phase, but our scheme increases more slowly. Figure 3 (b) introduces the comparison of computational cost in token generation with the increase of the number of keywords. Compared with the other three schemes, our scheme increases slowly, which reflects the superiority of the time efficiency of our scheme in the token generation phase.

Figure 4 (a) shows the search time, scheme [23] increases linearly with the number of attributes during the search phase. Although our scheme and schemes [20] [21] are constant, the time cost in our scheme is lower. Figure 4 (b) shows that the decryption time of our scheme and schemes [20] [21] are constant, but our scheme is less than the two schemes. Only scheme [23] increases linearly with the number of attributes and is fast. So, our scheme is higher than other schemes in the search and decryption phase.

According to the comprehensive analysis, our scheme has highlight computing advantages and is more suitable for current education service recommendation system.

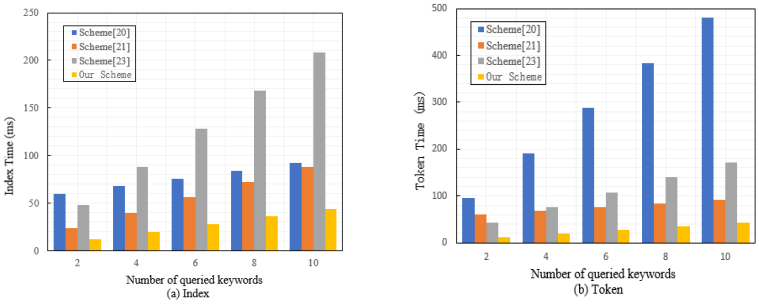

Fig. 3. Time costs of index/token generation phase.

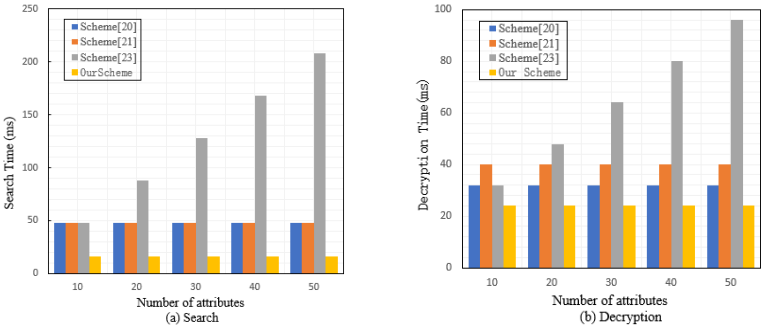

Fig. 4. Time costs of search/decryption phase.

7 Conclusion

For the education service recommendation system, we propose a privacy-preserving attribute-based education service recommendation scheme. First of all, parent (student) uses linear secret sharing to encrypt educational requirements, and hides access policy

to ensure the confidentiality of sensitive educational requirements. Secondly, we use the anonymous key generation method, in which the attribute authority and the teacher interact to generate the key to ensure the security of the teacher's key. So, teacher can choose appropriate education tasks anonymously according to his interests. In addition, in order to satisfy the educational requirements of parent (student) to a greater extent and quickly, multiple keywords technology is used to achieve fast search. Finally, we design an evaluation mechanism for teacher' credibility, and the education platform can choose the best teacher to accept the task, which not only satisfies the educational requirements but enables student to obtain the best educational services. Theoretical analysis and experimental simulation show that the scheme is effective and practical in the education recommendation system.

As a part of our future work, we will continue to explore the update of keywords and the deletion and addition of education resources in the education service recommendation system.

Acknowledgements

The work was supported by Foundation Items: The National Natural Science Foundation of China (No. 62262060, 61662071); Industrial support plan project of Gansu Provincial Department of Education (2022CYZC-17); Gansu Science and Technology Program (22JR5RA158).

References

1. D. Q. Wang, H. Y. Yin. "Research on design of personalized exercise recommendation system based on knowledge map," *Chinese Journal of ICT in Education*, vol. 2019, no.17, pp. 81-86, 2019.
2. V. Goyal, O. Pandey, A. Sahai, et al. "Attribute-based encryption for fine-grained access control of encrypted data," *Proceedings of the 13th ACM conference on Computer and communications security*. New York: ACM, pp. 89-98, 2006.
3. H. Li, D. Liu, Y. Dai, et al. "Personalized search over encrypted data with efficient and secure updates in mobile clouds," *IEEE Transactions on Emerging Topics in Computing*, vol.6, no. 1, pp. 97-109, 2018.
4. Q. J. Zheng, S. H. Xu, and G. Ateniese. "VABKS: Verifiable attribute-based keyword search over outsourced encrypted data," in Proc, *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications,* pp. 522–530, 2014.
5. Y. B. Miao, X. M. Liu, K. K. R. Choo, et al. "Privacy-preserving attribute-based keyword search in shared multi-owner setting," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1080-1094, 2019.
6. J. G. Li, M. Wang, et al. "ABKS-SKGA: Attribute-based keyword search secure against keyword guessing attack," *Computer Standards and Interfaces*, vol. 74, pp. 103471. 2021.
7. Y. Yang, X. M. Liu, et al. "Efficient trace able authorization search system for secure cloud storage," *IEEE Transactions on Cloud Computing*, vol. 8, no. 3, pp. 819–832, 2020.

8. S. F. Niu, Y. Y. Xie, P. P. Yang, et al. “Cloud-Assisted Attribute-Based Searchable Encryption Scheme on Blockchain,” *Journal of Computer Research and Devlopment*, vol. 58, no. 04, pp. 811-821, 2021.
9. S.H. Liu, J.G. Yu, Y. H. Xiao, et al. “BC-SABE: Blockchain-aided searchable attribute-based encryption for cloud-IoT, ” *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7851-7867, 2020.
10. H. Cui, R. H. Deng, B.D. Qin, et al. “Key regeneration-free ciphertext-policy attribute-based encryption and its application,” *Information Sciences*, vol. 517, pp. 217-229, 2020.
11. K. Sowjanya, D. Mou, S. Ray. “A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems,” *Journal of Systems Architecture*, 2021.
12. S. Song, X. L. Zhang. “Attribute-based Encryption Scheme without Key Escrow Supporting Attribute Revocation in Cloud Environment,” *Netinfo Security*, vol. 20, no. 8, pp. 62-70, 2020.
13. R. Y. Zhang, J. G. Li, Y. Lu, et al. “Key escrow-free attribute-based encryption with user revocation,” *Information Sciences*, vol. 600, pp. 59-72, 2022.
14. S. Banerjee, S. Roy, V. Odelu, et al. “Multi-Authority CP-ABE-Based user access control scheme with constant-size key and ciphertext for IoT deployment,” *Journal of Information Security and Applications*, vol. 53, pp. 102503, 2020.
15. K. C. Chandan, R. Sarma, A. B, Ferdous. “RMA-CPABE: A multi-authority CPABE scheme with reduced ciphertext size for IoT devices,” *Future Generation Computer Systems*, vol. 138, pp. 226-242, 2022.
16. X. B. Zhou, J. Rui. “Multi-authority threshold attribute-based encryption from R-LWE in fog and cloud computing environments,” *International Conference on Cyber Security, Artificial Intelligence, and Digital Economy* (CSAIDE 2022). SPIE, vol. 12330, pp. 112-119, 2022.
17. J. G. Li, M. Wang, Y. Lu, et al. “ABKS-SKGA: Attribute-based keyword search secure against keyword guessing attack,” *Computer Standards and Interfaces*, vol. 74: pp. 103471, 2021.
18. B. Waters. “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” International workshop on public key cryptography. Springer, Berlin, Heidelberg, pp. 53-70, 2011.
19. H. J. Wang. X. L. Dong, Z. F. Cao, et al. “Secure and efficient attribute-based encryption with keyword search,” The Computer Journal, vol. 61, no. 8, pp. 1133-1142, 2018.
20. M. S. Cao, L. H. Wang, Z. G. Qin, et al. “A lightweight fine-grained search scheme over encrypted data in cloud-assisted wireless body area networks，” Wireless communications and mobile computing, vol. 2019, 2019.
21. F. Meng, L. X. Cheng, M. Q. Wang. “ABDKS: attribute-based encryption with dynamic keyword search in fog computing,” *Frontiers of Computer Science*, vol. 15, no. 5, pp. 1-9, 2021.
22. C. Payal, L. D. Manik. “Keysea: Keyword-based search with receiver anonymity in attribute-based searchable encryption,” *IEEE Transactions on Services Computing*, vol. 15, no. 2, pp. 1036 – 1044, 2020.
23. S. Y. Gao, Y. L. Chen, Y. L. Xu. “Expressive Attribute-based Searchable Encryption Scheme in Cloud Computing,” *Computer Science*, vol. 49, no. 3, pp. 313-321, 2021.
24. https://crypto.stanford.edu/pbc/manual/