International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.187

PHSRS: The Privacy-preserving Healthcare Service Recommender System

Logesh Ravi
Center for Advanced Data Science,
Vellore Institute of Technology,
Chennai, Tamilnadu, India
logeshphd@gmail.com

Pyla Ratan
School of Electronics Engineering,
Vellore Institute of Technology,
Chennai, Tamilnadu, India
pyla.ratan2020@vitstudent.ac.in

Malathi D.
School of Computer Science and Engineering,
Vellore Institute of Technology,
Chennai, Tamilnadu, India
drmalathiphd@gmail.com

Sasikumar A.
Department of Data Science and Business Systems, School of Computing
SRM Institute of Science & Technology
Kattankulathur, Chennai, India
drsasikumaraphd@gmail.com

Hossam Kotb
Department of Electrical Power and Machines, Faculty of Engineering,
Alexandria University,
Alexandria 21544, Egypt
hossam.kotb@alexu.edu.eg

***Abstract*—An immense interest is shown to E-Healthcare systems as medical service recommendation increases with the advancement of technology and internet facility. It assists elderly people and other patients to discover professionals. Besides that, recommending personalized professionals and ensuring privacy remains great challenge. In an aim to increase the accuracy of the recommendation generation process, similarity between user's expectation and experts' knowledge is discovered and used along with expert's reputation score. Multiple user feedbacks are used to determine the reputation scores of doctors. On the basis of the curve-based cryptosystem and truth discovery technology, privacy-preserving recommendation method is proposed to compute reputation and similarity scores. In order to demonstrate its security proficiency, a detailed security analysis is provided.**

Keywords—Recommender system, Healthcare service, privacy preservation, curve-based cryptography

I. INTRODUCTION

Due to the rapid development of E-healthcare systems [1], online healthcare service recommendations have become fundamental part of everyday life. Here, user can submit their symptoms, doubts and necessity to a medical server, and then the server suggests most appropriate professionals in accordance with those requirements to the corresponding users. Healthcare service recommender systems are automated tools that use machine learning and artificial intelligence (AI) to make tailored healthcare suggestions to individuals. By making timely and accurate suggestions based on patient data, medical records, and other pertinent information, these systems have the potential to enhance healthcare outcomes. There are several kinds of healthcare recommender systems that can be applied in various contexts, including telemedicine platforms, patient-facing applications, and clinical decision support systems.

Algorithms are used by clinical decision support systems to offer real-time guidance on medication, diagnosis, and therapy to healthcare professionals. In order to enhance patient safety and lower medical errors, these systems can also offer alerts and reminders. Applications geared for patients are created to enable users to actively participate in their health management. They offer customized advice on food, exercise, medication adherence, and disease management based on information about the patient's medical history, lifestyle, and preferences. To assist patients in achieving their health objectives, these applications can also offer them feedback and educational resources. To offer patients remote healthcare services, telemedicine platforms employ healthcare service recommender systems. Based on patient data and symptoms, these platforms can offer personalized suggestions for a diagnosis, a course of action, and a prescription. Additionally, they can offer patients virtual follow-up care and monitoring, lowering the need for in-person visits and enhancing access to healthcare.

The capacity of healthcare recommender systems to enhance healthcare outcomes by offering personalized recommendations that are suited to specific patient needs is one of their main advantages. These systems can assist healthcare professionals in making better judgements, enhancing patient safety, and minimizing medical errors by utilizing patient data and other pertinent information. Better health outcomes can result from empowering patients to have a more active part in their own health management. Healthcare recommender systems do have several difficulties, though, including assuring data confidentiality and privacy, overcoming algorithmic biases, and guaranteeing that recommendations are founded on the most recent and correct medical knowledge. For healthcare recommender systems to be successfully implemented and adopted, several issues must be resolved.

Numerous studies were carried out to design a reliable healthcare recommendation system, some uses reputation score as basis for recommendation [2, 3], while others place greater emphasis on users interests and needs [4]. In former type, service requested users will be directed to the professionals who have high reputation score. In later type, most appropriate professionals will be suggested based on users' requirements. It is evident that the recommendation accuracy may be compromised if only the reputation or user need is considered for recommendation generation process.

In fact, reputation is derived from other user's feedback. Sometimes, it may reflect irrelevant medical services required by the target user. Since, false feedback that has been entered maliciously by them can have a negative impact on the professional's reputation [5]. Thus it is important to filtering it. Similarly, recommendation of professionals based on the similarity score of user needs may result in the recommendation of doctors who provide poor quality service

DOI: rp-9788770040723.187
[6]. Thus, it is necessary to consider both similarity score of user needs and the aggregated service feedback from multiple users to obtain high-quality medical services.

More importantly, the system should be capable enough in filtering redundant feedback received from malicious users, whether it is positive or negative. Besides the accuracy of the recommendation generation process, sensitive information of both the user and professional must be protected from disclosure. Here, a fundamental cryptographic primitive called key management can be used to ensure security [7, 8], but it alone is inadequate to achieve privacy-preserving recommendations. In addition, due to their expensive computational requirements, they are not practical for system with increasing number of users. In an attempt to address the challenges of existing recommender systems, a privacy-preserving online healthcare service recommender system (PHSRS) is proposed. The major contributions are:

- The PHSRS scheme takes both the similarity score of user needs and reputation score of the doctors as the basis for medical service recommendations.
- The PHSRS scheme not only provides accurate professional recommendations but also protects the privacy of both the doctor and user's sensitive information.
- In this scheme, users' needs and demands, and the professional's information are compared in the form of Ciphertext, not as plaintext.
- It discovers and filters feedback from malicious users, and assigns different weights dynamically.
- To demonstrate the efficiency, the proposed PHSRS scheme is compared to that of other related schemes.

The remaining sections are organized as: Section II describes the currently available literature-based solutions. Following that, Section III presents the healthcare service recommender system design goals and Section IV presents preliminary of the proposed work. Section V defines in detail about the proposed PHSRS scheme, and Section VI provides a thorough evaluation of the performance. Finally, Section VII draws the conclusion.

II. Related Works

The protection of one's privacy and anonymity has become a topic of widespread interest among the research communities of healthcare recommender system. If a user's privacy is breached, an adversary may be able to discern the victim's way of life, their routines, and even in some instances, the location of a remote user. Li et al. [6] introduced privacy-preserving online service recommendations for social communities. Here, interest-based pseudonyms were used to protect user identity from the server, but it is unfit for recommending professionals. An online friend suggestion based on user's trust relationship and social attributes has been proposed by Ma et al. [9] in a private manner. However, it cannot be used to generate doctor recommendation as there are no direct relationship between user and doctor in healthcare systems. To make accurate healthcare service recommendations, both reputation and similarity score need to be calculated.

Huang et al. [10] proposed privacy-preserving vector similarity computation model. However, this approach is not efficient as it involves users, trust authority and server to calculate similarity. A disease prediction scheme based on matrices is proposed by Zhang et al. [11]. To calculate reputation scores, Hu et al. [12] uses Dirichlet distribution and proposed a privacy-preserving communication scheme for vanets. However, due to the dynamic nature of users' feedback scores, the scheme is inaccurate. Furthermore, the server processes users' raw data and raise privacy concerns. Recently, numerous models have been introduced to protect user's privacy.

A privacy-preserving scheme for truth discovery (PPTD) was proposed by Miao et al. [13] to preserve user's sensitive data in the cloud. Unfortunately, their scheme becomes less effective as number of user increases. Zhang and colleagues [14] introduced privacy protected truth discovery (LPTD) scheme for fog-cloud platforms and they claimed that their scheme is lightweight. Kang et al. [15] used pseudonyms to preserve private information of fog computing users. An attribute-based protection scheme is proposed by Li et al. [16] to share data in cloud. However, this encryption model is not meant for truth discovery. Minding the above mentioned limitations, a new recommender solution is developed based on professional's reputation rate and user needs while filtering malicious user feedbacks. Throughout the system, the communicating participant's information should be secure and protected from malicious activities.

Various methods such as attribute-based encryption [21], differential privacy, identity-based encryption, elliptic curve cryptography, and k-anonymity or zero-knowledge proof are utilized to address privacy [22]. Hashing and cryptographic methods, primarily the SHA-256 or SHA-512 hashing algorithms, are used by blockchain technology to secure data transferred between nodes connected to a network. Due to the possibility of performance degradation, a suitable privacy preserving strategy must be carefully considered [23, 24].

The Curve-based cryptosystem [17] has attracted a lot of interest because of its lightweight operations. It's widespread because of the low cost operations, less memory requirement and low communication overhead. It offers faster processing, and also requires smaller key sizes than other public key cryptosystems. The curve-based cryptosystems have exponential complexity. At a given level of security (2^n), the key size grows as n^2 for curve-based cryptography, but it grows as n^3 for classical cryptosystems. As a consequence, curve-based cryptosystems are now advised to be used for new products where backward compatibility is not necessary. The security of ECC depends on the mathematical complexity of breaking elliptic curve discrete logarithm problem (ECDLP) [18]. For instance, the security offered by a 1024-bit RSA key is equivalent to that of a 160-bit elliptic curve key. Since then, numerous studies have been done to employ the ECC on recommender system to ensure privacy protection.

DOI: rp-9788770040723.187

III. Design Goal

The main goal is to design a secure and reliable privacy-preserving healthcare service recommender system, where the curve-based cryptosystem is used to protect sensitive information from malicious activities and unauthorized access.

A. Privacy Preserving Recommender System

The key challenge of any service oriented recommender system is the privacy preservation. As a result of the sensitive personal and medical data that healthcare service recommender systems handle, privacy-preservation plays a major concern. The information found in healthcare data can be used to determine a patient's identity, treatment history, and personal preferences. As a result, it is essential to make sure that sensitive data is shielded against misuse, disclosure, and illegal access. One of the crucial privacy-preserving strategies for healthcare service recommendations is the user anonymity. De-identifying healthcare data is taking out any personal identifiers or protected health information (PHI). Techniques like data masking, perturbation, or aggregation can be used to accomplish data anonymity. It lowers the possibility of re-identification and safeguard patient privacy.

Secure data storage is the other essential privacy-preserving measure. To avoid unwanted access or disclosure, healthcare data should be stored securely. This can be done by utilizing secure authentication methods, encrypting data in transit and at rest, and putting access control measures in place. For healthcare service recommender systems, secure data sharing mechanisms must be put into place to exchange healthcare data between healthcare service providers and seekers. These protocols should make sure that the data is sent securely and that only authorized people may access it.

The recommendation algorithm should respect user privacy while generating personalized healthcare service recommendations. Transparency and accountability are also essential for maintaining privacy in healthcare recommendation systems in addition to cryptographic mechanisms. These systems ought to be open about how they handle data and include detailed descriptions of the methods they employ for gathering, storing, and using it. In conclusion, to safeguard sensitive healthcare data from illegal access, disclosure, or misuse, healthcare recommender systems must integrate effective privacy-preserving procedures. A well-modeled healthcare service recommender system should preserve patient's privacy while offering personalized and useful healthcare suggestions by putting these precautions in place.

B. Role of Cryptosystem in Privacy Preserving Recommender Systems

To protect patient privacy, healthcare service recommender system uses various cryptosystems to safeguard the private and sensitive information from unwanted access or disclosure. Secure multi-party computation, differential privacy, homomorphic encryption, and other cryptographic methods can be utilized to ensure that private health information is shielded from illegal access and exposure while generating customized recommendations. These methods are crucial for safeguarding patient privacy and fostering confidence in healthcare recommendation systems. One of the fundamental cryptographic primitive utilized in privacy-preserving healthcare recommender system is the encryption algorithm. Sensitive data can be protected both in transit and at rest by using encryption algorithms to avoid interception or eavesdropping and to guarantee that only authorized users can access it.

Homomorphic encryption is another cryptographic method used in healthcare recommendation systems that protect patient privacy. By enabling computations on encrypted data without first decrypting it, Homomorphic encryption protects the confidentiality of the data. Using this method, it is possible to perform computations on personal healthcare information like patient records or medical histories. Another cryptographic method used in healthcare recommendation systems that protect patient privacy is secure multi-party computation. In this method, several parties can compute a result without disclosing their inputs to other. This method can be used to create collaborative recommender systems for healthcare where several healthcare professionals can work together to offer personalized recommendations without disclosing any patient-specific information.

Another crucial cryptographic method utilized in privacy-preserving healthcare recommendations is differential privacy. Differential privacy guarantees data anonymity, preventing person identity while facilitating personalized recommendations. Through the use of differential privacy, patient privacy can be protected by introducing noise or other disturbances to the data while maintaining its overall quality. Through literature analysis, it is found that among currently available public key cryptosystems, curve-based cryptosystem has shown a lot of promise in terms of both security as well as speed. This is because of its smaller key size to provide equal level of security as other cryptosystem provides which means less computation. The algorithm uses robust security based on the computational complexity, key generation, curve selection, point multiplication for encryption, and point addition for decryption. Due to its tiny key size and quick computation time, it is employed in the proposed privacy-preserving healthcare service recommender system.

IV. Preliminaries

The cryptosystem used to protect the sensitive information and the truth discovery approach used to calculate the weight of similar users are defined in this section for better understanding of readers.

C. Truth Discovery

To resolve the conflicts of noisy data, truth discovery approach is used in various applications. Once the algorithm begins, then the ground truths are randomly assigned and the weights will be updated iteratively till convergence has been achieved. The higher weight will be given to the user whose data is nearer to previously determined ground truth. The

DOI: rp-9788770040723.187
distance between the current user data and ground truth is calculated as:

$$d\left(x_o^u, x_o^*\right) = \frac{\left(x_o^u - x_o^*\right)^2}{std_o} \quad (1)$$

where o represents the object, x_o^* is the ground truth, x_o^u is user data and std_o represents the standard deviation of object o for all users u.

D. Overview of Elliptic Curve Cryptosystem

Public-key cryptography known as elliptic curve cryptography (ECC) makes use of the characteristics of elliptic curves to produce safe encryption methods. It generates the key pair as the initial stage in the ECC process. The public key is produced from the private key via a mathematical formula, whereas the private key is a secret number that is generated at random and kept hidden by the owner. While the private key is required for decryption, the public key is utilized for encryption. The curve must be carefully selected to guarantee that it possesses specific mathematical characteristics that make it appropriate for use in cryptography. Fig. 1 gives the graphical representation of an elliptic curve over the finite field F_q.

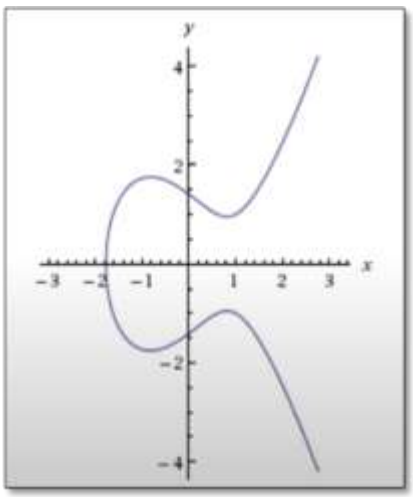

Fig. 1. Graphical Representation of Elliptic Curve

In ECC, the plaintext message that is being encrypted is represented by the scalar value. During encryption, a point on the elliptic curve is multiplied by that scalar value. A new point on the curve i.e. the Ciphertext is produced as a result of the multiplication. During decryption, the ciphertext point on the elliptic curve is added to get the original plaintext message. Due to the challenging mathematics required to calculate the private key from the public key, ECC is thought to be safe.

E. Arithemtic operations of ECC

With a smaller key size ECC offers comparable security than other public key cryptosystems like RSA. A non-singular curve with the equation $y^2 = x^3 + ax + b \bmod p$, with the discriminate $4a^3 + 27b^2 \bmod p \neq 0$, is known as an elliptic curve $E_p(a, b)$ defined over a prime field F_p. The three fundamental arithmetic operations carried out on the ECC are

- **Point multiplication:** addition of a point in k times
- **Point addition:** addition of 2 different points
- **Point doubling:** addition of same point

Assuming there are two points on the curve, then point addition is $P_3 = P_1 + P_2 \bmod p \in E\left(F_p\right)$. The same point is added twice $P_3 = P_1 + P_1 \bmod p \in E\left(F_p\right)$ in point doubling, whereas the same point is added k times $P_3 = kP_1 \bmod p \in E\left(F_p\right)$ then it is called as scalar multiplication.

F. Elliptic Curve Cryptosystem

The PHSRS scheme achieves privacy preservation using Elliptic curve cryptosystem. It comprises of key generation, encryption and decryption algorithms.

- **Key Generation:** The domain parameters that are made publicly available for key generation are the prime p, elliptic curve E, and the generator point P. Let us assume that the point P is on the curve $E(F_P)$, then the cyclic subgroup fabricated by P is given as $\langle P \rangle = \{\infty, P, 2P, 3P, \cdots, (n-1)P\}$. Now, the key pair is generated by uniformly selecting the random integer $k \in [1, n\text{-}1]$ as a private key, and its equivalent public key P_k is computed as $P_k = k \times P$. The security of an elliptic curve cryptosystem relies on the hardness of computing k from P_k though provided with P which is called the ECDLP.
- **Encryption:** The data M which is to be protected is initially converted into the point on the elliptic curve P_M. Then it is encoded into its corresponding Ciphertext C which is the pair of points (C_1, C_2) as follows:

$$C = \left(C_1, C_2\right) = \left(kP, P_M + P_k\right) \quad (2)$$

- **Decryption:** With the Ciphertext C, the following actions are performed to retrieve the plaintext P_M. Finally the point P_M is then decoded to the original data M.

$$\begin{aligned} P_M &= \left(C_2 - k \times C_1\right) = \left(\left(P_M + kP_k\right) - \left(k \times kP\right)\right) \\ &= P_M + kP_k - kP_k = P_M \end{aligned} \quad (3)$$

G. Elliptic Curve Discrete Logarithm Problem

The elliptic curve discrete logarithm problem (ECDLP), which is the problem of separating the private key from the public key, determines how secure ECC is. For an elliptic curve $E\left(F_p\right)$, determining an integer $k \in [0, n-1]$ from $Q = k \times P$ is difficult, provided a generator point $P \in E\left(F_p\right)$ and the resultant point $Q \in \langle P \rangle$. Even for large

DOI: rp-9788770040723.187
key sizes, the ECDLP is thought to be computationally infeasible.

V. Privacy-Preserving Healthcare Service Recommender System (PHSRS)

The privacy-preserving online healthcare service recommender system (PHSRS) is designed, where the user submits the service request through public network to the medical server, following that server suggests the professionals based on their requirements. After that, the user will provide feedback regarding the received service quality to compute particular professional reputation rate. The formal PHSRS model is demonstrated in the Fig. 2, which consists of User, Medical server and the Trusted Authority.

- Users are the person who needs medical advices and they must own smart device to send the request and to receive the recommendations. Following that, the user provides feedback in order to assess the quality of service they received.
- Trusted Authority is in charge of managing and distributing the key resources to users and medical servers.
- After receiving the service request, the medical server calculate the similarity score between user needs and professional's attribute, then responds to user with suitable doctor suggestion. And then collects the feedback from them to calculate the reputation scores of doctors.

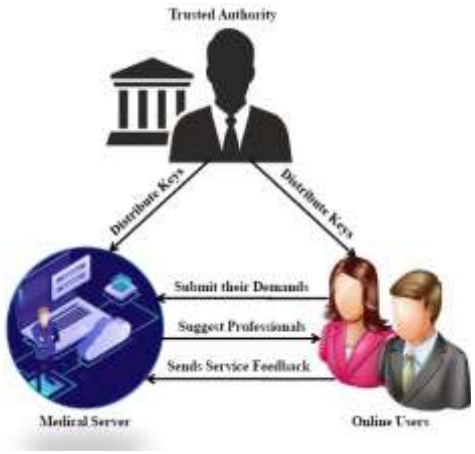

Fig. 2. The PHSRS System Architecture

The proposed privacy-preserving healthcare service recommender system (PHSRS) consists of system initialization, professional recommendation, and reputation score computation phases. These are explained in detail the following subsections.

H. System Initialization

Trusted authority (TA) is the one who is completely believed by all the participants of PHSRS scheme. Initially, TA selects the global parameters like elliptic curve, generator point and then generates the key pairs based on the security parameter. Finally, TA distributes these key pairs to the appropriate user and medical server, respectively.

I. Doctor Recommendation

The entire process can be broken down into three parts: sending the requirements, calculating the similarity, and recommending the professionals. Each participant should prove their authenticity before taking advantage of the service provided by the PHSRS system. After successful authentication, the user sends their perturbed demand vectors to the medical server through public network without expressing their identities for recommendation generation. Each user has their own demand vectors $\vec{A_i} = \{a_1, a_2, \cdots a_n\}$, includes name of the hospital, information about the department, the type of disease, and so on. Similarly, the doctor's attribute vector $\vec{B_i} = \{b_1, b_2, \cdots b_n\}$ includes information about the hospital name, the type of treatable disease, and so on. Then the distance between professionals attribute vectors and users demand vectors are calculated as follows:

$$sim = \sum_{i=1}^{n} (a_i - b_i)^2 \quad (4)$$

Finally, the doctors are selected whose similarity score is greater than the threshold value. Then the top listed professionals with highest reputation score is recommended to the user.

J. Reputation Score Computation

Following the service recommendation, the user will provide a feedback to assess the quality of the healthcare service provided by the particular professional. This feedback is then utilized to determine the doctor's overall reputation score. In this phase, the medical server will aggregate all the feedbacks received from multiple users and compute the truth value. With that truth value, the reputation score of doctor will be determined. In truth value calculation, different weights are assigned dynamically to each user feedback, and update them constantly based on multiple user feedbacks. To compute specific professional's reputation score, truth values obtained from various time periods were used.

VI. Performance Evaluation

The performance efficiency of the PHSRS scheme is evaluated in terms of the running time required to suggest relevant professionals. Here, 10 iterations are performed on the system with 2.5GHz Intel i5 processor and 8GB of RAM. The proposed PHSRS scheme is compared with other two related schemes, like PPMR [19] and FSSR [10] to demonstrate the efficiency of PHSRS. FSSR recommends a doctor based on only the user similarity. In PPMR, unlike FSSR, both user similarity and doctor reputation score are taken into account. It is observed from the Fig. 3 that the time taken for recommendation generation increases with the increasing number of professionals. This is because, the medical server needs to compute the similarity score between user's demand vectors and each professional's attribute vectors. And the time required to doctor recommendations based on reputation score is less when compared to user similarity score, because the medical server selects only the doctors with high reputation rate.

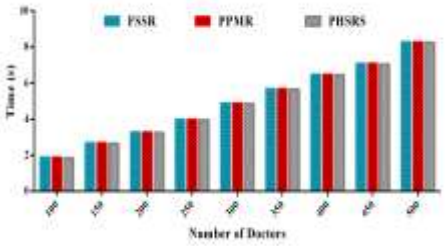

Fig. 3. Running Time Required to Recommend Doctors

Initially, the truth value of several user's feedback from various time period is obtained before computing the the reputation rate of professionals. The running time required for discovering the truth values of existing PPTD [20] and PPMR [19] schemes and the proposed PHSRS scheme is compared and depicted in the Fig. 4 with different number of users. It is clear from the Fig. 4 that the running time consumed by PHSRS is significantly less when compared to the schemes PPTD and PPMR with the increasing number of online users.

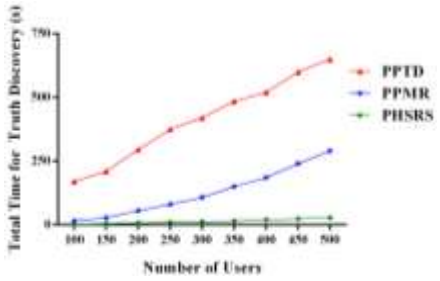

Fig. 4. Comparing the running time required to discover truth values

The running time required to discover truth values increases linearly with the increasing number of online users as seen in Fig. 4. Similarly, Fig. 5 depicts the total time required for calculating the reputation score with different number of truth values obtained from various time periods. It clearly shows that the time taken to compute the reputation rate is comparatively small when increasing the users from 100 to 500, confirming the performance effectiveness of the PHSRS scheme. As a result, as the number of service seekers grows, PHSRS becomes more proficient.

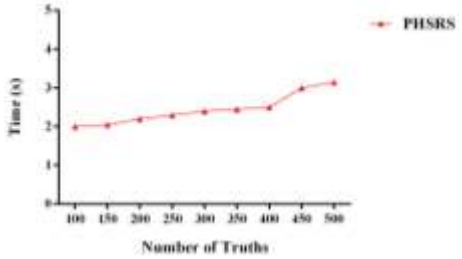

Fig. 5. Time Required to Compute Doctor's Reputation Score

VII. Conclusion

The privacy-preserving online service recommendations for E-healthcare system is proposed to assists users in discovering a appropriate doctor based on their needs, interests and reputation rate of doctors. In comparison to the existing associated online medical recommendations schemes, the proposed PHSRS scheme is more efficient and accurate. In order to achieve secure recommendation services, the privacy-preserving system were developed which prevents the unauthorized user from accessing the user's private data. A thorough performance analysis demonstrates that PHSRS is efficient and can provide reliable online service recommendations.

References

[1] K. Wang, Y. Shao, L. Shu, C. Zhu, and Y. Zhang, "Mobile big data fault-tolerant processing for ehealth networks", IEEE Network, vol. 30(1), pp. 36–42, 2016.

[2] H. Hu, R. Lu, and Z. Zhang, "TPSQ: Trust-based platoon service query via vehicular communications" Peer-to-peer Networking and Applications, vol. 10, pp. 262–277, 2017.

[3] F. G. Mármol, and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks" Journal of network and computer applications, vol. 35(3), pp. 934–941, 2012.

[4] Y. Shi, M. Larson, and A. Hanjalic, "Collaborative filtering beyond the user-item matrix: A survey of the state of the art and future challenges", ACM Computing Surveys (CSUR), vol. 47(1), pp. 1–45, 2014.

[5] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET", IEEE Transactions on Vehicular Technology, vol. 66(2), pp. 1786–1797, 2016.

[6] D. Li, Q. Lv, L. Shang, and N. Gu "Efficient privacy-preserving content recommendation for online social communities", Neurocomputing, vol. 219, pp. 440–454, 2017.

[7] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective key management scheme for heterogeneous sensor networks", Ad hoc networks, vol. 5(1), pp. 24–34, 2007.

[8] X. Du, and H. H. Chen, "Security in wireless sensor networks", IEEE Wireless Communications, vol. 15(4), pp. 60–66, 2008.

[9] X. Ma, J. Ma, H. Li, Q. Jiang, and S. Gao, "ARMOR: A trust-based privacy-preserving framework for decentralized friend recommendation in online social networks", Future Generation Computer Systems, vol. 79, pp. 82–94, 2018.

[10] C. Huang, R. Lu, H. Zhu, J. Shao, and X. Lin, "FSSR: Fine-grained EHRs sharing via similarity-based recommendation in cloud-assisted eHealthcare system", In Proceedings of the 11th ACM on Asia conference on computer and communications security (pp. 95–106), 2016.

[11] C. Zhang, L. Zhu, C. Xu, and R. Lu, "PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system", Future Generation Computer Systems, vol. 79, pp. 16–25, 2018.

[12] H. Hu, R. Lu, C. Huang, and Z. Zhang, "PTRS: A privacy-preserving trust-based relay selection scheme in VANETs", Peer-to-Peer Networking and Applications, vol. 10, pp. 1204–1218, 2017.

[13] C. Miao, W. Jiang, L. Su, Y. Li, S. Guo, Z. Qin, X. Houping, G. Jing and K. Ren, "Cloud-enabled privacy-preserving truth discovery in crowd sensing systems", In Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, pp. 183–196, 2015.

[14] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and M. Guizani, "LPTD: Achieving lightweight and privacy-preserving truth discovery in CIoT", Future Generation Computer Systems, vol. 90, pp. 175–184, 2019.

[15] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles", IEEE Transactions on Intelligent Transportation Systems, vol. 19(8), pp. 2627–2637, 2017.

[16] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing", Computers & Security, vol. 72, pp. 1–12, 2018.

[17] Dhanabalan, S. S., Sitharthan, R., Madurakavi, K., Thirumurugan, A., Rajesh, M., Avaninathan, S. R., & Carrasco, M. F. (2022). Flexible compact system for wearable health monitoring applications.Computers and Electrical Engineering, 102, 108130.

[18] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, “Handbook of applied cryptography”, CRC press, 2001.

[19] C. Xu, J. Wang, L. Zhu, C. Zhang, and K. Sharif, “PPMR: a privacy-preserving online medical service recommendation scheme in eHealthcare system”, IEEE Internet of Things Journal, vol. 6(3), pp. 5665–5673, 2019.

[20] C. Zhang, L. Zhu, C. Xu, K. Sharif, and X. Liu, “PPTDS: A privacy-preserving truth discovery scheme in crowd sensing systems”, Information Sciences, vol. 484, pp. 183–196, 2019.

[21] X. Yan, Q. Wu, and Y. Sun, “A homomorphic encryption and privacy protection method based on blockchain and edge computing”, Wireless Communications and Mobile Computing, 2020, pp. 1–9.

[22] A. Shahnaz, U. Qamar, and A. Khalid, “Using blockchain for electronic health records”, IEEE access, vol. 7, pp. 147782–147795, 2019.

[23] Gomathy, V., Janarthanan, K., Al-Turjman, F., Sitharthan, R., Rajesh, M., Vengatesan, K., &Reshma, T. P. (2021). Investigating the spread of coronavirus disease via edge-AI and air pollution correlation. ACM Transactions on Internet Technology, 21(4), 1-10.

[24] I. Boumezbeur, and K. Zarour, K. “Privacy-Preserving and Access Control for Sharing Electronic Health Record using Blockchain Technology”, Acta Informatica Pragensia, vol. 11(1), pp. 105–122, 2022.