iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IV **Month of publication:** April 2023

DOI: https://doi.org/10.22214/ijraset.2023.50398

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

A Review on new Era Medical Healthcare Services with Privacy-free Data Fusion and Integration Methods

Preeti Dagar
Management Education Research Institute, Sampla

Abstract: In this growing age of Internet of Health (IoH), with rapidly going Web and Internet services more and more organization national and world-wide transferring data and information both personal and professional on cloud, our traditional health and medical services are also migrating and transforming in a new age mod- ern healthcare system. Thus, having a large amount of available medical data regarding doctors, patients, medical infrastructures, medicine, treatment plans and procedures and so on. This information is often very help full in medical care services and in preventing many health disasters by providing right data at right time. But this comes with a very challenging task of carefully integrating the sensitive data, and making sure of user privacy in not disclosed while doing this. In these papers we are analyzing various works done on this problem and trying to come up with a suitable and possible solution, for a better health care services a multi-source data integration and mining method for medical data, named as PDFM (Privacy-free Data Fu- sion and Mining), to search for similar medical records in privacy-preserving and time-efficient manner. In this paper we are reviewing as many as research mythologies as we can, to understand the how the tech- nology is changing our healthcare services, and how IoH is being used to save patient life as well as mentining their privacy.

Keywords: Service recommendation, Internet of Health, locality-sensitive hashing, user privacy, data integra- tion, Hybrid Cloud, Multi-keyword Ranked Search, Privacy-preserving, Searchable Encryption.

I. INTRODUCTION

Various agencies and medical departments are accu- mulating the considerable amount of patients historical data (like medical record, past and current treatment record and so on). This records form main source of Big Internet of Health (IoH) data. [1]With increasing pop- ularity of information technology and the adoption if *These authors contributed equally. digital software in health and medical domain, the uti- lization of such IoH data is the main source for quantify the information for medical or health units or depart- ments.[2]. Mining and analyzing of IoH data which contain valu- able information such as past disease of a patient and past treatments, can be very important contribution to doctors' scientific and reasonable diagnosis and treat- ment making decision, as well as for disaster trend pre- diction and precaution[3]. Therefore, for high quality healthcare services suitable for any patients, it become necessity to collect, integrate, fuse and analyze IoH data from multiple source and provided on a single platform. This, IoH medical data often contain very sensitive information about patient privacy(e.g., blood pressure, temperature, some sexual disease) that a patient is not willing to let anyone know[4]. Thus, the patients or stakeholders of IoH data records would not dare to dis-close these records in public domain. Also, lack of suf-ficient incentive for IoH data records for sharing with others, become the concerns of a patients which block the utilization of historical IoH data records. Thus, even though many health or medical agencies and hospitals may have accumulated a considerable large amount of medical IoH data records, they seldom release the data due to privacy concerns of a patients. Moreover, these historical IoH data records are many a time distributed over a large number of platforms and different agencies, which further increase the privacy disclosure concerns while integration and fusion of these records.

II. MOTIVATION

The motivation of this paper is shown in figure1. Figure show the doctor-nurse medicine medical records of pa- tients are located partially in cloud platforms, cp1 and cp2, respectively. we need to fuse and integrat multi- source data for uniform data analyses and make more scientific healthcare decisions, to mine the valuable information comprehensively from the IoH data distributed across platforms cp1 and cp2. However, some privacy concerns are often raised in the above IoH data fusion and analyses process, as the data records often contain some sensitive information of patients.

It is nec- essary to develop a novel data fusion method without revealing privacy, to encourage platforms cp1 and cp2 to release their data records and alleviate the patients' privacy disclosure concerns. For better understading the details of data fusion method without revealing privacy information, we summarize the used symbols and their respective meanings in the method with TABLE 1.

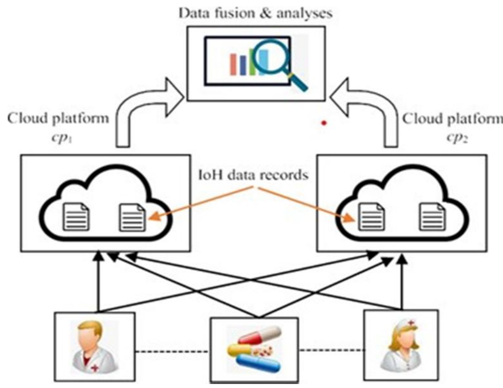


FIGURE 1. Multi-source IoH data fusion.

Symbols	Specification
$R_1, \ldots, R_n$	IoH data records
$q_1, \ldots, q_m$	Healthcare criteria
$f_1, \ldots, f_a$	Hash functions
$T_1, \ldots, T_b$	Hash tables
$cp_1, \ldots, cp_n$	Distributed cloud platform
$v_1, \ldots, v_m$	M dimensions of each hash function
$h_1(R_x), \ldots, h_a(R_x)$	Hash values of R_x based on $f_1, \ldots, f_a$
$H_1(R_x), \ldots, H_b(R_x)$	Indices of R_x in hash tables $T_1, \ldots, T_b$

Table 1. Symbol specifications.

III. RELATED WORK

Multisource big data integration and sensitive data pro-tection are some of the major problems in modern med-ical healthcare services, to many researches has been going on, we have summarize current research status asbelow:

A. Encryption

A classic and effective way to secure sensitive data is Encryption, which has been used for a long time. Peng T. [5] brought forth a multi-keywords sorting- based secure search method, which adopt the symmet-ric public key search encryption way to permit a user to make secure infor- mation retrieval in an encrypted dataset based on multiple keywords.The major advan-tage of this methos is that it provide secure service pro- tection for cloud computing with minimum resources, but with a drawback of low computational efficiency, along with the risks of the key disclosure.

Dai H. [6], introduced a new method oval curve en- cryption to realize secure data use and proved that it is method is superior to the traditional FP-based method. This method has a relatively high data security perfor- mance. But only for the simple Boolean value-basedkeyword search, which nar rows its application scope tosome extent.

Phuong T. V. X.[7], used vector space model and homomorphic encryption technique to encrypted data ranking, as well as multi-keyword file retrieval and data retrieval. This guarantee high-level quality data protec- tion but it also brings additional computational timeand communication cost which are often very high.

The Authors in[8] used a homomorphic encryption based data retrieveal methos to help the stakeholders of the data, each data item ready to be searched is homomorphic encrypted during information retrieveal process, this provide solution for sortable and multi- keyword data encryption problem. The method can solve many of the secure data processing requirements, but it cannot support fuzzy retrieval.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

B. *Differentially Privacy*

A improved collaborative filtering methos based on dif- ferentially privacy is IPriCF[9], to secure user privacy. IPriCF can eliminate the disruption caused by noises, through dividing user data and item data, which in- curred by differentially privacy. This also make a bal- ance between user privacy and accuracy of the recom- mended list.

To analyze the sparse data and provide optimal ser- vices a stakeholder-feature-item matrix[10] was built. This method guarantee the privacy preservation of dataas well as maintaining an acceptable predication accu- racy loss.

Another method named DPMF (differentially pri- vate matrix factorization) was brought forth in [11]:this method convert sensitive user data into poten- tial low-dimensional vectors using matrix factorization technique and differentially privacy technique was used to confuse the targeted object functions. But prediction accuracy is reduced as number of dimensions grows.

TrustSVD model is improved by introducing differ- entially privacy [12]: DPTrustSVD, which is said toreach a tradeoff among data privacy, data sparsity and data availability effectively. In [13] authors combined Differentially Privacy and Huffman Coding, which put forward a privacy-aware location segments publishing method and in [14] authors combined Differentially Pri-vacy, Bayes network and entropy theory, that provid protection method for high-dimensional data.

C. *Anonymization*

Anonymization is an effective method to secure the user sensitive data while doing analyses and mining on big data [15]. Anonymization can publish the non-sensitive data (i.e., data after anonymization) to the public. while hiding sensitive data (e.g., name, identity card no.) ,sothat tradeoff between data privacy and availabilitycanbe achieve [16].

To hide the most sensitive information, K-anonymity solution is adopted in [17] data-driven decision-making process. A K-anonymity-based user location protection method is suggested in [18], which helps in hidding the real location or position of the user. Even though these methods can hide sensitive user data during data-driven business analyses and applications, they still can-not balance the data privacy and data utilization, alsoanonymized data can still lose certain key information.

IV. METHODOLOGY

In this section, ourproposed data mining and fusion method is presents, whose major procedure is general- ized with following steps: First, the sensitive data areprojected based on LSH functions. Second, accordingto each data record and its corresponding hash values derived after hash projection, a set of hash tables without patient privacy is created. Third, according to the derived hash tables, we make data search and mining. In summary, the detailed three steps are listed in FIGURE 2.

Step-1: LSH-based IoH data projection. We randomly choose a group of LSH functions to project each piece of IoH data record. This way, for each piece of IoH data record, we obtain a group of hash values.

Step-2: Creation of hash tables without privacy. According to the "IoH data record-hash values" paris, we create a group of hash tables without much patient privacy. Each hash table includes the index of each IoH data record.

Step-3: Hash tables-based similar IoH data search and mining. According to the hash tables, we cluster the IoH data records into multiple groups and each group of records share the similar IoH data. Furthermore, we mine and analyze the IoH data records based on the derived multiple clusters.

Figure2. Three steps of our proposal.

1) *Step-1: LSH-based IoH data projection.*

Ri.qj are used to denote the value of dimension qj (j =1, 2,. . . , m) of IoH data record Ri (i=1,2. . , n) from a patient. As Ri.qj is sensitive to the patient, these haveto secure the private information of Ri.qj when Ri.qj ispublished to the public. Thus, LSH strategy is used to achieve

For Ri (i=1, 2, . . . , n), it has m criteria q1, . . . , qm. The healthy information of to Ri is denoted by symbolRi =(R .q , . . . , R .q). We need to make an LSH projection, when Ri is relesed to others.

For this , a new vector V = (v1, . . . , vm) is created where vj (j = 1, 2, . . . , m) is a randomly generated value from domain [1, 1]. Thus, we create an LSH function f as in equation (1).

f(Ri) = Ri • V

= (Ri.q1, . . . , Ri.qm) • (v1, . . . , vm)

= Ri.q1*v1 + . . . + Ri.qm*vm –(1)

Thus, we can get a f(Ri) which can be positiveor negative. Next, we make mapping as shown in equation (2) and V. Concrete procedure can be shownin Algorithm 1. h(Ri) =(1, if f(Ri) ¿ 0 0, if f(Ri) ¡=0)

Algorithm 1

Inputs:
(1) $R_1, \dots, R_n$: historical IoH data records;
(2) $q_1, \dots, q_m$: quality dimensions of IoH data.
Output:
(1) $h(R_i)$: Boolean value of $\overrightarrow{R_i}$ after mapping.

```
1: for j = 1,...., m do
2:     v_j = random[−1, 1]
3: end for
4: for i = 1,...., n do
5:     sum = 0
6:     for j = 1,...., m do
7:       sum + = R_i.q_j * v_j
8:     end for
9:     if sum > 0
10:      then f(R_i) = 1
11:    else f(R_i) = 0
12:    end if
13:    return f(R_i)
14: end for
```

2) *Step-2: Creation of hash tables without privacy*

In Step-1 The f(Ri) derived is be regarded as a hash value of Ri through a projection process. But only oneprojection process is not enough to convert Ri into aprivacy-free index. Thus Algorithm 1 is repeated mul-tiple times by projections of f1, . . . , fa, thus we get ana- dimensional hash vector H(Ri) as shown in equation (3).

Thus the mappings of "Ri H(Ri)" (i=1, 2, . . . , n),make a hash table, denoted by "T". by using "T", we can have the index value of Ri , still we cannot know ofreal value of Ri. thus, the privacy of patients stored inRi is secured. H(Ri) = (h1(Ri), . . . , ha(Ri)) ——(3) Considering, the limit of hash table i.e., a single hashtable could not reflect accurately the real index of eachIoH data record, we repeat the creation process of "T"multiple times and get tables b: T1, . . . , Tb. this isshowm in Algorithm 2.

Algorithm 2

Input:
(1) $h(R_1), \dots, h(R_n)$: Boolean values of IoH data records;
(2) $f_1, \dots, f_a$: LSH functions.
Output:
(1) $T_1, \dots, T_b$: b hash tables.

```
1: for x = 1,...., a do
2:     repeat Algorithm 1 based on f_x
3: end for
4: for i = 1,...., n do
5:     H(R_i) = (h_1(R_i), ..., h_a(R_i))
6:     put "R_i → H(R_i)" into T
7: end for
8: return T
9: repeat lines 1-8 b times
```

3) Step-3: Hash Tables-based similar IoH data Searchand Mining

b tables: T1, . . . , Tb are generated instep 2. there are a set of corresponding "Ri → H(Ri)" (i=1, 2, . . . , n) pairs in each table. Also, H(Ri) is regarded as the index of Ri in the table. According to Locality- Sensitive Hashing theory, the IoH data records with the same index would be approximately similar[39]. It means that if two records R1 and R2 share the same index, then R1 and R2 are mostly similar records. This way, we can mine the potential similar IoH data records through check their respective index values without much privacy[39]. However, for two IoH data records R1 and R2, H(R1) H(R2) is a rather rigid constraint condition as each dimensional value of H(R1)should be exactly equal to that of H(R1), this will pro- duce an empty result of similar IoH data records search, which does not make any sense to privacy-free IoH datafusion and mining.

Due to this drawback, the above rigid condition is re- laxed by generating multiple hash tables instead of only one. In concrete, considering the b tables created in Step 2, i.e., T1, . . . , Tb, if H(R1) H(R2) holds in anyTy (y=1, 2, . . . , b), then it is simply conclude that R1 and R2 are probably similar IoH data records[39]. Thus, the similar IoH data records search condition is relaxed accordingly. Therefore, for a specific IoH data record Rx, we can look for its similar record set *Sim$_S$et* (Rx) through the above idea[39]. Details of this step are presentd in Algorithm 3. And finally, we return *Sim$_S$et* (Rx) as the final output of the proposal in this work[39].

Algorithm 3

Inputs:
(1) $T_1, \ldots, T_b$: b hash tables;
(2) $R_1, \ldots, R_n$: historical IoH data records;
(3) R_x: a target IoH data record whose similar records are required.
Output:
Sim_Set (R_x) : similar IoH data records of R_x

```
Sim_Set (Rx) = Φ
for y = 1 to b do
    for i = 1, . . . , n do
        if H(Ri) = H(Rx)
            then put Ri into Sim_Set (Rx)
        end if
    end for
end for
return Sim_Set (Rx)
```

V. RESULTS

To get the result of our solution of privacy-free data mining and fusion, some comparisons is done whichare showed in the form of graphs as bellow:

A. Comparisons

The following values: a=2, 4, 6, 8, 10, b=2, 4, 6, 8, 10are used for the parameters

1) Mean Absolute Error Comparison

The Mean Absolute Error of three methods are mea-sured and compared with following setting:the user vol-ume is 339, item volume is varied from 1000 to 5000,a=b=10.

First, we test the variation trend of Mean Absolute Er-ror for all the three methods by changing the number of items in the used dataset[39]. Second, we test the vari- ation trend of Mean Absolute Error of three methods by changing the number of users in the dataset.

Comparison results are shown in Fig.3. In both Fig(a) and Fig(b), it be can observe that PDFM and UCF compared to had a clear advantage ICF, as UCF isa baseline method and PDFM is an approximate so- lution to UCF. Besides, PDFM achieves an approxi- mate Mean Absolute Error of UCF as the LSH strat- egy adopted in PDFM can promise a good similarity- maintenance property[39]. Moreover, PDFM has an ad-vantage of privacy-preservation capability which is notowned by UCF.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

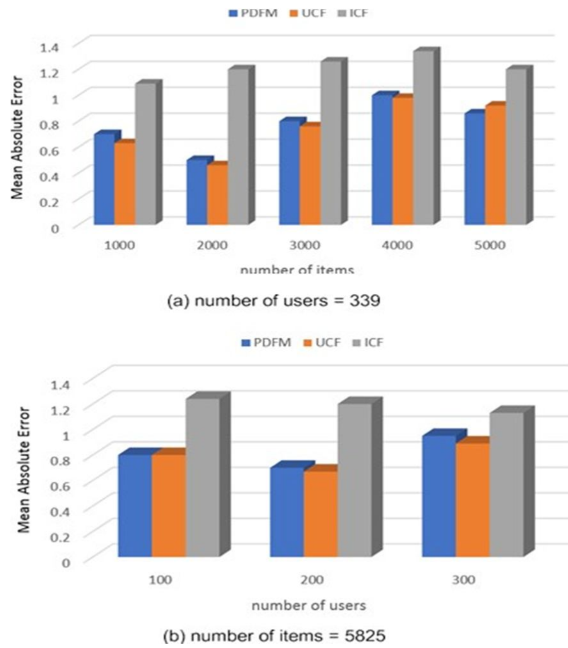


FIGURE 3. Mean absolute error comparison.

2) Computational Time Comparison

We measure and compare the computational time of three methods. The parameter settings are as follows: the user volume is varied from 100 to 300, item volumeis varied from 1000 to 5000, a = b = 10. Compared data are reported in Fig.4 As can be seen from Fig.4, the consumed time of three methods approximately grows when the number of users or the number of items rises[39]. Specifically, UCF and ICF consumes more time than PDFM as heavy-weight user simi- larity calculation or item sim- ilarity calculation is required in UCF and ICF, respec- tively. While in PDFM, the time cost can be dividedinto two parts[34]: (1) hash table creation, which canbe finished offline; as a consequence, the time complex-ity is of O(1)[35]; (2) similar IoH data record retrieval, which needs to be done online and its time complexity is O(1)[36]. As a result, PDFM can often return simi-lar IoH data records within a small response time and hence, our method can be applied to the big IoH data environment.

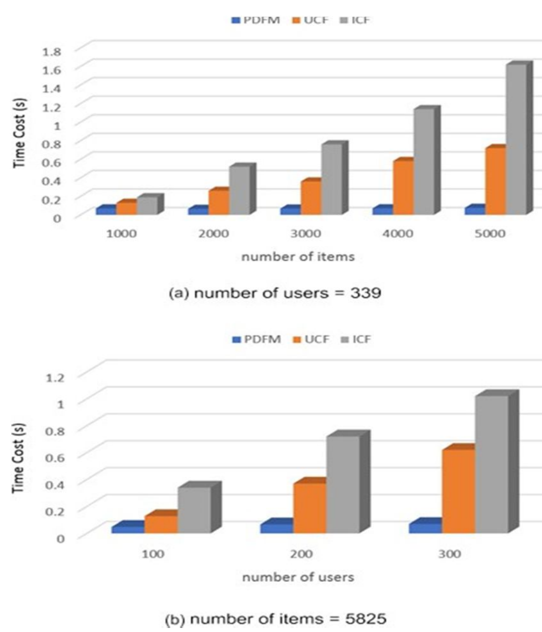


FIGURE 4. Computational time comparison.

3) Mean Absolute Error of PDFM

PDFM method is based on LSH strategy whose performances are often related to some key factorsincluding parameters a and b. [11]Considering this, we observe the performances of PDFM associated with a and b. [16]The parameter settings are as follows: the user volume is 339, item volume is 5825, a 2, 4, 6, 8, 10, b 2, 4, 6, 8, 10. Compared data are reported in Fig.5.
As reported in Fig.5, the Mean Absolute Error of PDFM increases with the rise of parameter b and the decline of parameter a. This is due to the followingreasons: [39](1) when there are more hash tables (i.e., b increases), the similar IoH data record retrieval condition becomes looser; as a result, more similar records are returned and correspondingly, the Mean Absolute Error is rising;[39] (2) when there are more hash functions (i.e., a increases), the similar IoH data record retrieval condition becomes stricter; as a result, less similar records are returned and correspondingly, the Mean Absolute Error is decreased. Moreover, we can observe that more hash functions (i.e., a larger a) and less hash tables (i.e., a smaller b) will bring better prediction accuracy[39].

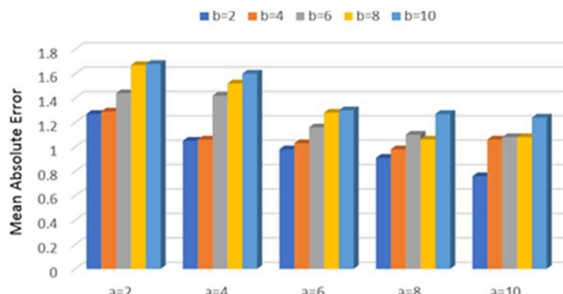


Figure 5. Mean absolute error of PDFM w.r.t. (a, b) pairs.

4) Number of Returned Results of PDFM

As analyzed in the above analysis, PDFM method is based on LSH strategy whose returned result volume is often related to some key factors such as parameters a and b.[27] Considering this, we observe the returned result volume of PDFM associated with a and b. The parameter settings are as follows: the user volume is 339, item volume is 5825, a =2, 4, 6, 8, 10, b=2, 4, 6,8, 10. Compared data are reported in Fig.6.
As reported in Fig.6, the returned result volume of PDFM increases with the rising of parameter b and the dropping of parameter a. This is due to the following reasons: (1) when there are more hash tables (i.e., b increases), the similar IoH data record retrieval condition becomes looser; as a result, more similar records are returned; (2) when there are more hash functions (i.e., a increases), the similar IoH data record retrieval condition becomes stricter; as a result, lesssimilar records are returned[39]. Moreover, we can observe that more hash functions (i.e., a larger a) and less hash tables (i.e., a smaller b) will bring fewer returned results.

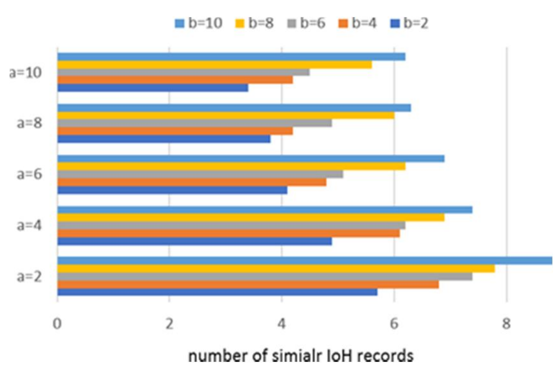


Figure6. Number of returned results of PDFM w.r.t. (a, b) pairs.

VI. CONCLUSION

Effective fusion and analyses of IoH data are of pos- itive significances for scientific disaster diagnosis and medical care services.[25] However, the IoH data pro- duced by patients are often distributed across differ- ent departments and contain partial patient privacy. Therefore, it is often a challenging task to effectively integrate or mine the sensitive IoH data without dis- closing patient privacy. [28]

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IV Apr 2023- Available at www.ijraset.com

To tackle this challenge, we bring forth a novel multi-source medical data integra- tion and min- ing solution for better healthcare ser- vices, named PDFM. Through PDFM, we can search for similar medical records in a time-efficient and privacy- preserving manner, [33]so as to provision patients with better medical and health services. The experiments ona real dataset prove the feasibility of PDFM. In up- coming research, we will update the suggested PDFM method by considering the possible diversity of data types [32]–[34] and data structure [35]–[38]. In addition, how to fuse multiple existing privacy solution for bet- ter perfor- mances is still an open problem that requiresintensive and continuous study.

REFERENCES

[1] S. Din and A. Paul, ”Smart health monitoring and management system: Toward autonomous wearable sensing for Internet of Things using bigdata analytics,” Future Gener. Comput. Syst., vol.111, p. 939, Feb. 2020

[2] N. C. Benda, T. C. Veinot, C. J. Sieck, and J. S. Ancker, “Broadband Internet access is a social determinant of health!,” Amer. J. Pub-lic Health, vol. 110, no. 8, pp. 1123–1125, Aug. 2020.

[3] E. Sillence, J. M. Blythe, P. Briggs, and M. Moss, “A revised model of trust in Internet-based health information and advice: Cross-sectional questionnaire study,” J. Med. Internet Res., vol. 21,no. 11, Nov. 2019, Art. no. e11125.

[4] K. Szulc and M. Duplaga, “The impact of Internet use on mental wellbeing and health be- haviours among persons with disability,” Eur. J.Public Health, vol. 29, no. 4, pp. 185–425, Nov. 2019.

[5] T. Peng, Y. Lin, X. Yao, and W. Zhang, “An efficient ranked multi-keyword search for multiple data owners over encrypted cloud data,” IEEE Access, vol. 6, pp. 21924–21933, 2018.

[6] H. Dai, Y. Ji, G. Yang, H. Huang, and X. Yi,“A privacy-preserving multi-keyword ranked search over encrypted data in hybrid clouds,” IEEE Access,vol. 8, pp. 4895–4907, 2020.

[7] T. V. Xuan Phuong, G. Yang, W. Susilo, F. Guo, and Q. Huang, “Sequence aware functional encryp- tion and its application in searchable encryption,” J. Inf. Secur. Appl., vol. 35, pp. 106–118, Aug. 2017.

[8] Z. Xia, X. Wang, X. Sun, and Q. Wang, “A secure and dynamic multi- keyword ranked search scheme over encrypted cloud data,” IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340–352, Feb. 2016.

[9] M. He, M. Chang, and X. Wu, “A collaborative filtering recommendation method based on differen-tial privacy,” J. Comput. Res. Develop., vol. 54, no.7, pp. 1439–1451, 2017.

[10] T. Wang and S. He, “An improved collaborative filtering recommendation algorithm with differen-tially privacy,” Inf. Secur. Technol., vol. 7, no. 4, pp. 26–28, 2016.

[11] Z. Xian, Q. Li, X. Huang, J. Lu, and L. Li, “Differential privacy protection for collaborativefiltering algorithms with explicit and implicit trust,” Acta Electronica Sinica, vol. 46, no. 12, pp. 3050–3059, 2018.

[12] C. Yin, L. Shi, R. Sun, and J. Wang, “Improved collaborative filter- ing recommendation algorithm based on differential privacy protection,” J. Super-comput., vol. 76, no. 7, pp. 5161–5174, Jul. 2020.

[13] Y. Xiao, L. Xiong, S. Zhang, and Y. Cao, “Lo- cLok: Location cloaking with differential privacy via hidden Markov model,” Proc. VLDB Endowment, vol. 10, no. 12, pp. 1901–1904, Aug. 2017.

[14] S. Yang, J. Xu, X. Yang, and X. Ren, “Bayesian network-based high- dimensional crowdsourced data publication with local differential pri- vacy,” Scientia Sinica Informationis, vol. 49, no. 12, pp. 1586–1605, Dec. 2019.

[15] J. Wang, Z. Cai, Y. Li, D. Yang, J. Li, and H. Gao, “Protecting query privacy with differentially private k-anonymity in location-based services,”Pers. Ubiquitous Comput., vol. 22, no. 3, pp. 453–469, Jun. 2018.

[16] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, “A caching and spatialK-anonymity driven privacy enhancement scheme in continuous location-based services,” Future Gener. Comput. Syst., vol. 94, pp.40–50, May 2019.

[17] F. Casino, J. Domingo-Ferrer, C. Patsakis, D. Puig, and A. Solanas, “A k-anonymous approach to privacy preserving collaborative filtering,” J. Comput. Syst. Sci., vol. 81, no. 6, pp. 1000–1011, Sep. 2015.

[18] P. Zhao, J. Li, F. Zeng, F. Xiao, C. Wang, and H. Jiang, “ILLIA: Enabling k -anonymity-based privacy preserving against location injection attacks in continuous LBS queries,” IEEE Internet ThingsJ., vol. 5, no. 2, pp. 1033–1042, Apr. 2018.

[19] S.-H. Wang, Y. Zhang, Y.-J. Li, W.-J. Jia, F.-Y. Liu, M.-M. Yang, and Y.-D. Zhang, “Single slice based detection for Alzheimer’s disease via wavelet entropy and multilayer perceptron trained by biogeography-based optimization,” Multimedia Tools Appl., vol. 77, no. 9, pp. 10393–10417, May 2018.

[20] S. Wang, J. Sun, I. Mehmood, C. Pan, Y. Chen, and Y. Zhang, “Cerebral micro-bleeding identifi- cation based on a nine-layer convolutional neural network with stochastic pooling,” Concurrency Comput., Pract. Exper., vol. 32, no. 1, Jan. 2020, Art. no. e5130.

[21] Y.-D. Zhang, V. V. Govindaraj, C. Tang, W. Zhu, and J. Sun, “High performance multiple sclerosis classification by data augmentation and AlexNet transfer learning model,” J. Med. Imag. Health Informat., vol. 9, no. 9, pp. 2012–2021, Dec. 2019.

[22] Y. Zhang, S. Wang, Y. Sui, M. Yang, B. Liu, H. Cheng, J. Sun, W. Jia, P. Phillips, and J. M. Gorriz, “Multivariate approach for Alzheimer’s dis-ease detection using stationary wavelet entropy and predator-prey particle swarm optimization,” J. Alzheimer’s Disease, vol. 65, no. 3, pp. 855–869,Sep. 2018.

[23] C. Kang, X. Yu, S.-H. Wang, D. Guttery, H. Pandey, Y. Tian, and Y. Zhang, “A heuristic neural network structure relying on fuzzy logic for imagesscoring,” IEEE Trans. Fuzzy Syst., early access, Jan. 13, 2020, doi:10.1109/TFUZZ.2020.2966163.

[24] S.-H. Wang, Y.-D. Zhang, M. Yang, B. Liu, J. Ramirez, and J. M. Gorriz, “Unilateral sensorineural hearing loss identification based on double-density dual-tree complex wavelet transform and multino- mial logistic regression,” Integr. Comput.-Aided Eng., vol. 26, no. 4, pp. 411–426, Sep. 2019.

[25] S.-H. Wang, J. Sun, P. Phillips, G. Zhao, and Y.-D. Zhang, "Polarimet- ric synthetic aperture radar image segmentation by convolutional neural network using graphical processing units," J. Real- Time Image Process., vol. 15, no. 3, pp. 631–642, Oct. 2018.

[26] S. Wang, C. Tang, J. Sun, and Y. Zhang, "Cere- bral micro-bleeding detec- tion based on densely connected neural network," Frontiers Neurosci., vol.13, p. 422, May 2019.

[27] S.-H. Wang, S. Xie, X. Chen, D. S. Guttery, C. Tang, J. Sun, and Y.-D. Zhang, "Alcoholism identification based on an AlexNet transfer learning model," Frontiers Psychiatry, vol. 10, p. 205, Apr. 2019.

[28] L. Qi, X. Wang, X. Xu, W. Dou, and S. Li, "Privacy-aware cross-platform service recommenda-tion based on enhanced locality-sensitive hashing," IEEE Trans. Netw. Sci. Eng., early access, Jan. 27, 2020, doi: 10.1109/ TNSE.2020.2969489.

[29] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen,and Y. Zhang, "Blockchain empowered arbitrable data auditing scheme for network storage as a service," IEEE Trans. Services Comput., vol. 13, no. 2, pp. 289–300, Mar./Apr. 2019.

[30] L. Qi, C. Hu, X. Zhang, M. R. Khosravi, S. Sharma, S. Pang, and T. Wang, "Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment," IEEE Trans. Ind. Informat., early access, Jul. 28,2020, doi: 10.1109/TII.2020.3012157.

[31] Y. Xu, C. Zhang, G. Wang, Z. Qin, and Q. Zeng, "A blockchain-enabled deduplicatable data auditing mechanism for network storage services," IEEE Trans. Emerg. Topics Comput., early access,Jun. 29, 2020, doi: 10. 1109/TETC.2020.3005610.

[32] W. Zhong, X. Yin, X. Zhang, S. Li, W. Dou, R. Wang, and L. Qi, "Multi-dimensional quality-driven service recommendation with privacy-preservation in mobile edge environment," Comput. Commun.,vol. 157, pp. 116–123, May 2020.

[33] X. Chi, C. Yan, H. Wang, W. Rafique, and L. Qi, "Amplified locality- sensitive hashing-based recommender systems with privacy protection,"Concurrency Comput., Pract. Exper., Feb. 2020,Art. no. e5681, doi: 10. 1002/CPE.5681.

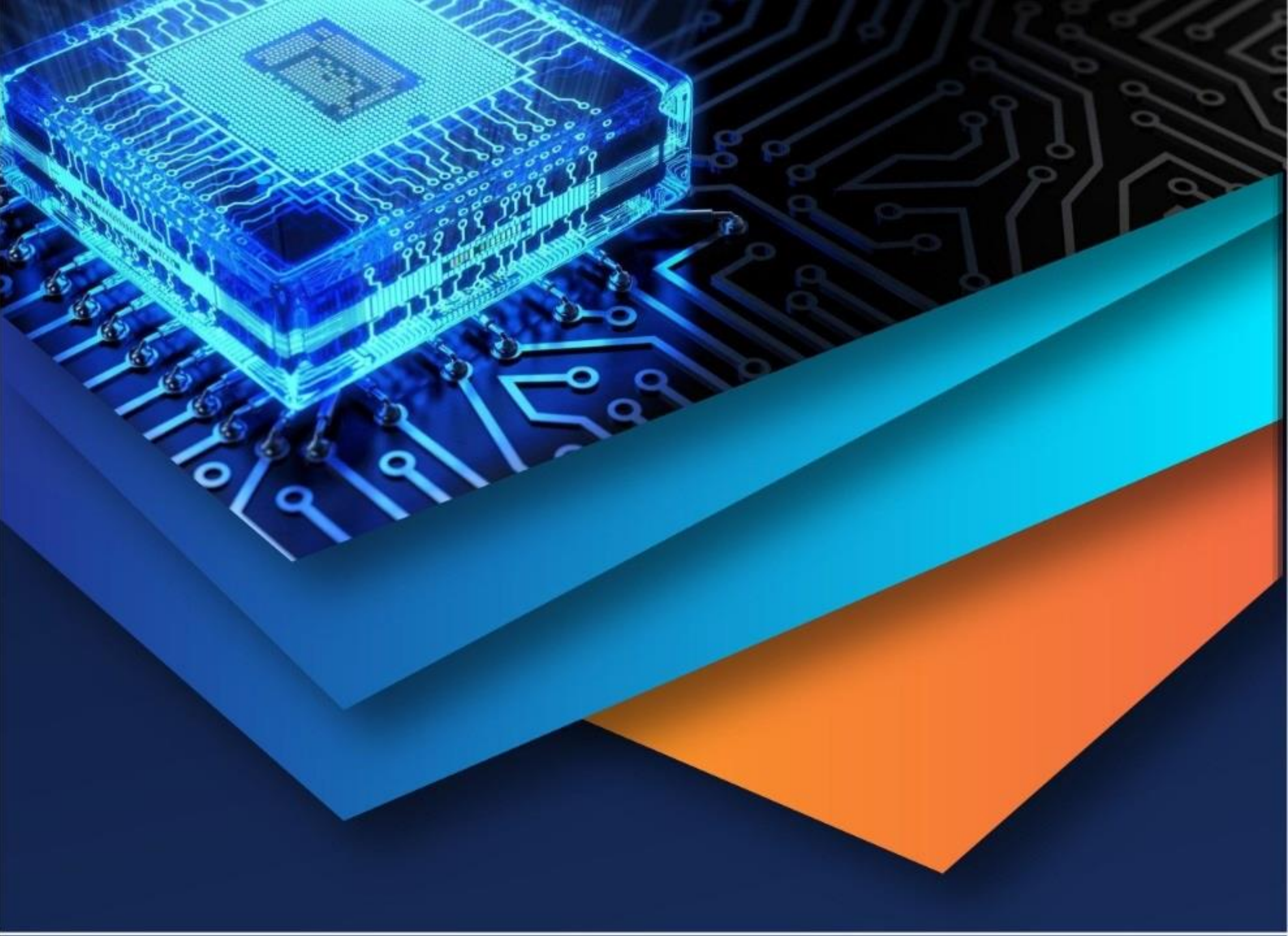
[34] C. Zhou, A. Li, A. Hou, Z. Zhang, Z. Zhang, P. Dai, and F. Wang, "Modeling methodol- ogy for early warning of chronic heart failurebased on real medical big data," Expert Syst. Appl., vol. 151, Aug. 2020, Art. no. 113361, doi: 10.1016/j.eswa.2020.113361.

[35] T. Cai, J. Li, A. S. Mian, R. Li, T. Sellis, and J. X. Yu, "Target-aware holis- tic influence maximization in spatial social networks," IEEETrans. Knowl. Data Eng., early access, Jun. 17, 2020, doi: 10.1109/TKDE.2020.3003047.

[36] L. Qi, Q. He, F. Chen, X. Zhang, W. Dou, and Q. Ni, "Data-driven Web APIs recommendation for building Web applications," IEEE Trans. Big Data, early access, Feb. 24, 2020, doi: 10.1109/TB-DATA.2020.2975587.

[37] H. Liu, H. Kou, C. Yan, and L. Qi, "Keywords- driven and popularity- aware paper recommendation based on undirected paper citation graph," Com- plexity, vol. 2020, pp. 1–15, Apr. 2020.

[38] J. Li, T. Cai, K. Deng, X. Wang, T. Sellis, and F. Xia, "Community- diversified influencemaximization in social networks," Inf. Syst., vol. 92,pp. 1–12, Mar. 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY