INTEGRATE AND MINE SEVERAL SOURCES OF MEDICAL DATA FOR HEALTH CARE SERVICES

Mrs. Vijaya Ramineni [1], Mr. Krishna Prasad Chowdam [2]

#1 Associate professor in the department of IT at DVR & DR. HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District.

#2 MCA student in the Department of Computer Applications (DCA) at DVR & DR. HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR District

ABSTRACT_ With the advent of Internet of Health (IoH) age, traditional medical or healthy services are gradually migrating to the Web or Internet and have been producing a considerable amount of medical data associated with patients, doctors, medicine, medical infrastructure and so on. Effective fusion and analyses of these IoH data are of positive significances for the scientific disaster diagnosis and medical care services. However, IoH data are often distributed across different departments and contain partial user privacy. Therefore, it is often a challenging task to effectively integrate or mine the sensitive IoH data, during which user privacy is not disclosed. To overcome the above difficulty, we put forward a novel multi-source medical data integration and mining solution for better healthcare services, named PDFM (Privacy-free Data Fusion and Mining). Through PDFM, we can search for similar medical records in a time-efficient and privacy-preserving manner, so as to offer patients with better medical and health services. A group of experiments are enacted and implemented to demonstrate the feasibility of the proposal in this work.

INDEX TERMS: Cloud Computing, Electronic Health Record, Security, Attribute-based Encryption, Ciphertext policy, Identity Proofing, Authentication, Authorization

1.INTRODUCTION

With the steadily expanding prevalence of Data Innovation and the progressive reception of computerized programming in clinical or solid spaces, different clinical divisions or offices have collected a lot of verifiable information (e.g., patients' clinical records, sound treatment arrangements, etc), which structure a

fundamental wellspring of enormous Web of Wellbeing (IoH) information [1]. The use level of such IoH information is a critical measure to assess and evaluate the data level of clinical or solid units or divisions [2]. By and large, the vast majority of verifiable IoH information records contain significant data particularly for the clinical or sound organizations, for example, the previous illness of a patient at a time point. Mining and examining such verifiable IoH information records can contribute a lot to specialists' logical and sensible finding and treatment choice makings, as well as calamity pattern expectation and safeguard [3]. Thusly, it is of emanant need to gather, coordinate, combine and break down these multisource IoH information records for great medical care administrations reasonable for patients. In any case, verifiable IoH information records from patients frequently contain delicate patient security (e.g., circulatory strain, temperature) as a patient is many times not able to tell others their verifiable fiascos [4]. In this way, the patients or the partners of verifiable IoH information records dare not unveil their IoH information records to general society. Furthermore, they need adequate motivation for IoH information records offering to other people. The over two worries essentially block the use of authentic IoH information records. As a result, albeit numerous clinics or other clinical and sound organizations have gathered a lot of verifiable IoH information records, they only sometimes discharge the information to the outside because of protection concerns. Besides, the verifiable IoH information records are much of the time appropriated across various stages or offices, the joining and combination of which further builds the security divulgence concerns.

2.LITERATURE SURVEY

2.1 Q. Huang, Y. Yang, and M. Shen, ‘‘Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing,’’ Future Gener. Comput. Syst., vol. 72, pp. 239–249, Jul. 2017.

With the expanding pattern of redistributing information to the cloud for productive information stockpiling, secure information coordinated effort administration including information peruse and write in distributed computing is direly required.

Nonetheless, it presents numerous new difficulties toward information security. The key issue is the best approach to bear the cost of secure compose procedure on ciphertext cooperatively, and along these lines different issues remember trouble for key administration and substantial calculation overhead on client since helpful clients may peruse and compose information utilizing any gadget. during this paper, we propose a protected and effective information coordinated effort conspire, during which fine-grained get to control of ciphertext and secure information composing activity are frequently managed bolstered quality based encryption (ABE) and characteristic based mark (ABS) individually. to lighten the property authority from overwhelming key administration trouble, our plan utilizes a full appointment system bolstered progressive characteristic based encryption (HABE). Further, we additionally propose a fractional unscrambling and marking development by designating the majority of the calculation overhead on client to cloud specialist co-op. the wellbeing and execution examination show that our plan is secure and proficient.

2.2 C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, ‘‘Secure integration of IoT and cloud computing,’’ Future Gener. Comput. Syst., vol. 78, pp. 964–975, Jan. 2018.

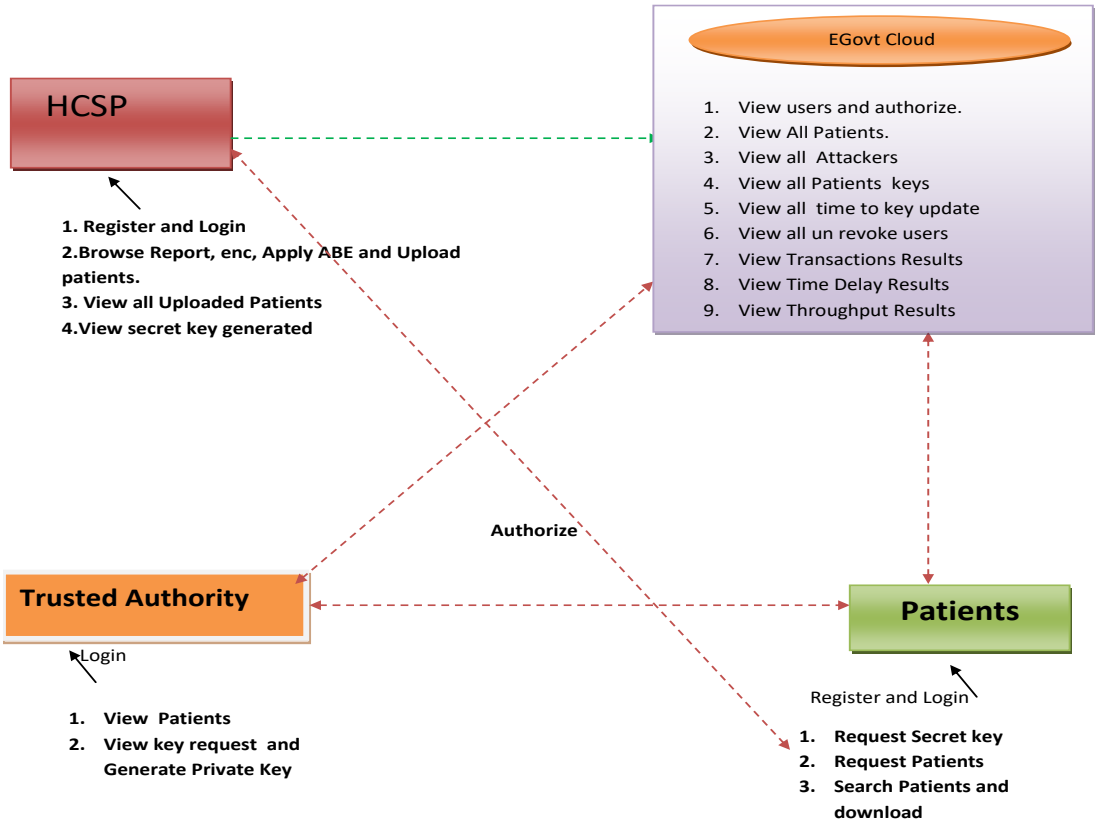
Cloud Computing might be another innovation which alludes to a foundation where the two information stockpiling and preparing work outside of the cell phone. Another ongoing innovation is Internet of Things. Web of Things might be another innovation which is developing quickly inside the field of media communications. All the more explicitly, IoT related with remote media communications. the most objective of the communication and participation among things and articles which sent through the remote systems is to fulfill the objective set to them as a consolidated element. also , there's a fast improvement of the two innovations, Cloud Computing and Internet of Things, respect the segment of remote correspondences. during this paper, we present a study of IoT and Cloud Computing with consideration on the wellbeing issues with the two innovations. In particular, we join the 2 previously mentioned advancements (i.e Cloud Computing and IoT) in

order to take a gander at the regular highlights, thus as to get the benefits of their combination. Finishing up, we present the commitment of Cloud Computing to the IoT innovation. Along these lines, it shows how the Cloud Computing innovation improves the capacity of the IoT. At long last, we review the security difficulties of the blending of IoT and Cloud Computing.

We propose PDFM (Privacy-free Data Fusion and Mining), a revolutionary multi-source medical data integration and mining system for improved healthcare services. In order to provide patients with better medical and health services, we may quickly and privately search for comparable medical records using PDFM. In this paper, a series of tests are conducted to show that the plan is feasible.

3.PROPOSED WORK

Architecture Diagram



3.1 IMPLEMENTATION

- **HCSP**

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the patients details and will do the following operations like Upload Patient Details,View All My Uploaded Patients,View Public Keys,View Transaction Details

- **Patients**

In this module, user logs in by using his/her user name and password. After Login user requests search control to cloud and will Search for Patients based on the index keyword with the Score of the searched Patient and downloads the Patient. User can view the search of the Patients and also do some operations like Search, Request Key, Request File, and View Keys

- **EGovt Cloud Server**

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data Patients and store them in the cloud for sharing with Remote User and will do the following operations like View HSPs and Patients, View Patient Details, View Attackers,View Patient Keys,Un Revoke User ,View Transaction ,View Transactions Results ,View Time Delay Results ,View Throughput Results

- **Trusted Authority**

In this module, TA logs in by using his/her user name and password. After Login he will do some operations like View all Patients, Generate Public Key Requests, key generation

4.RESULTS AND DISCUSSIONS

Fig1: Home Page

Fig2: E-Govt cloud storage

Fig3: Trusted Authority page

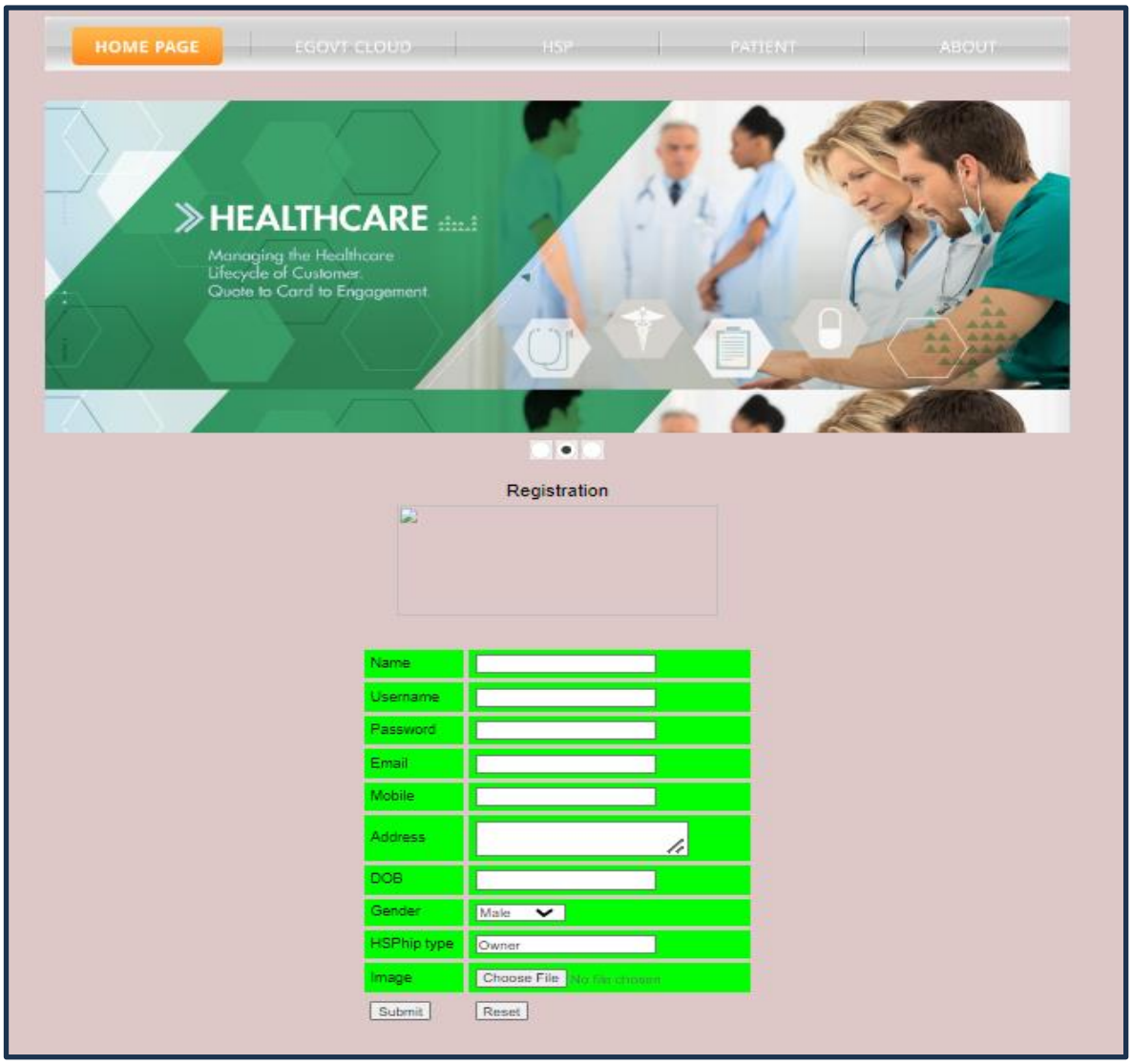


Fig4: HSP registration page

Fig5: Patient registration page

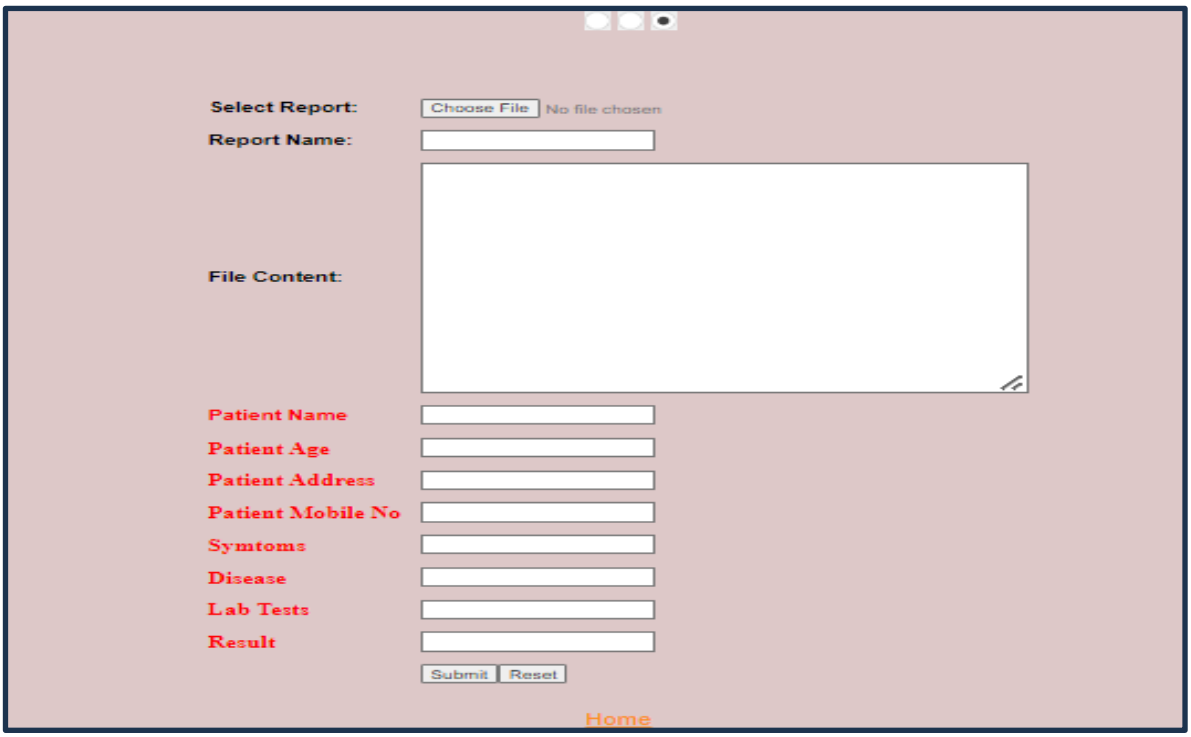


Fig6: HSP can upload patient reports

Fig7:patient can search reports

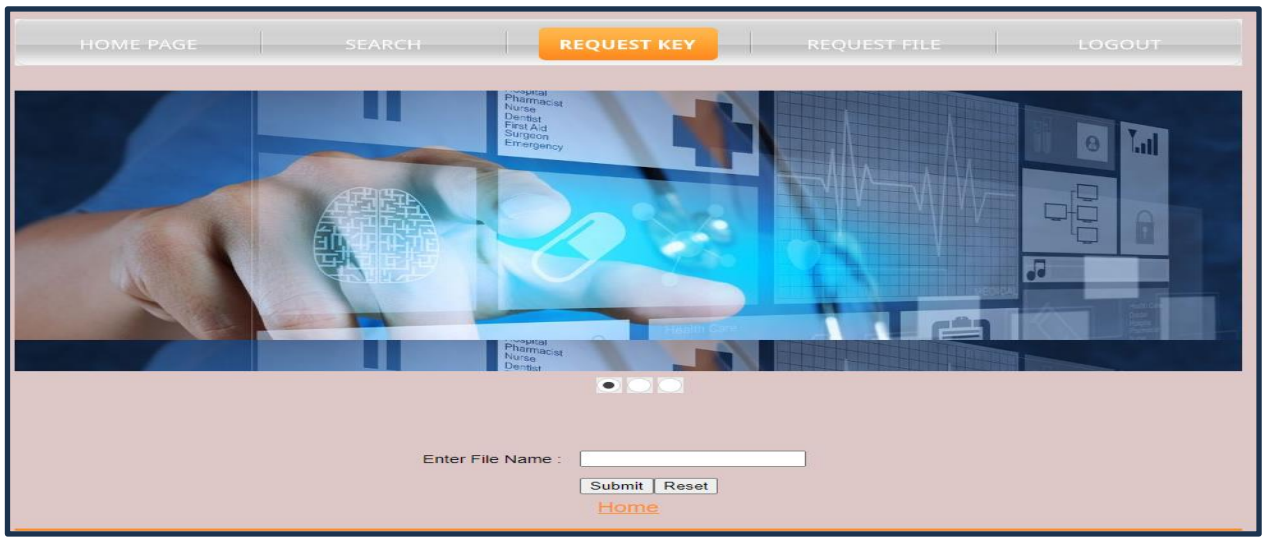


Fig8: Patient can request a key for download a report

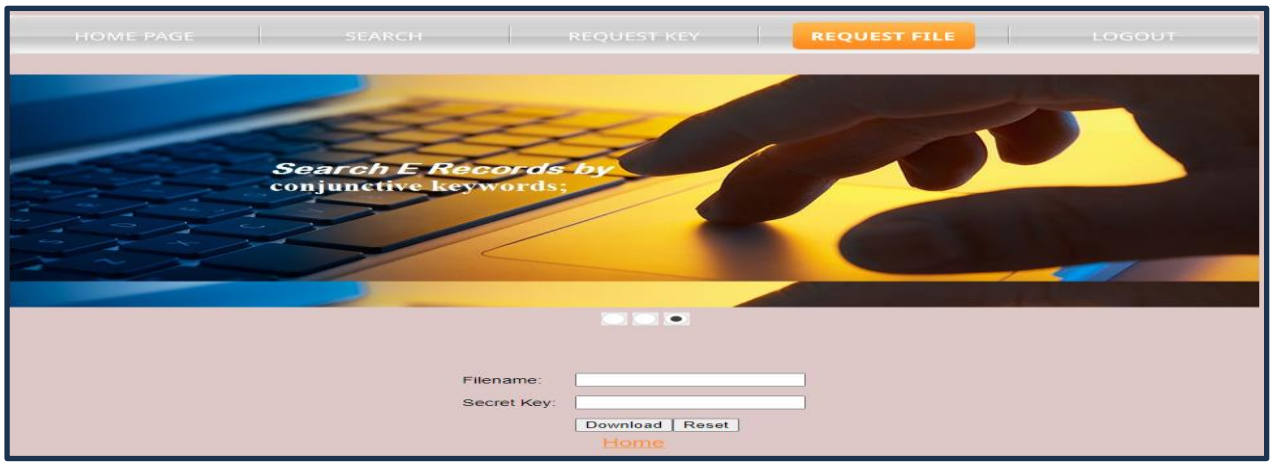


Fig9: Patient can download a report using secret key

5.CONCLUSION

Compelling combination and investigations of IoH information are of positive meanings for logical calamity conclusion and clinical consideration administrations. Be that as it may, the IoH information created by patients are in many cases conveyed across various offices and contain fractional patient security. Consequently, it is much of the time a moving errand to successfully coordinate or mine the delicate IoH information without uncovering patient protection. To handle this test, we deliver a novel multi-source clinical information reconciliation and digging answer for better medical care administrations, named PDFM. Through PDFM, we can look for comparable clinical records in a period effective and protection safeguarding way, to arrangement patients with better clinical and wellbeing administrations. The tests on a genuine dataset demonstrate the plausibility of PDFM. In forthcoming exploration, we will refresh the proposed PDFM technique by considering the conceivable variety of information types [32]-[34] and information structure [35]-[38]. What's more, how to combine various existing security answer for better exhibitions is as yet an open issue that requires concentrated and consistent review.

REFERENCES

[1] S. Din and A. Paul, ‘‘Smart health monitoring and management system: Toward autonomous wearable sensing for Internet of Things using big data 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. Public 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 behaviours 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 encryption 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 multikeyword 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 differential 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 differentially 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 collaborative filtering 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 filtering recommendation algorithm based on differential privacy protection,'' J. Supercomput., vol. 76, no. 7, pp. 5161–5174, Jul. 2020.

[13] Y. Xiao, L. Xiong, S. Zhang, and Y. Cao, ''LocLok: 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 highdimensional crowdsourced data publication with local differential privacy,'' 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 Things J., 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 identification 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

AUTHOR’S PROFILE

Mrs. Vijaya Ramineni completed her Master of Computer Applications (MCA),MTech in (CSE) from Acharya Nagarjuna University. She has published more than 10 papers in indexing Journals, currently working as an Associate Professor in the department of IT at DVR & Dr HS MIC College of Technology (Autonomous), Kanchikacherla, NTR District. Her areas of interest are Data Mining. Cloud Computing and Machine Learning.

Mr. Krishna Prasad Chowdam as MCA student in the department of DCA at DVR & DR . HS MIC COLLEGE OF TECHNOLOGY ,Kanchikacherla ,NTR District .He has completed B.SC(MPCs) in Vignan Degree College From Vikrama Simhapuri University in Nellore .His area of interests are Java ,Python , Machine Learning.