IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data

Pallavi S. Bangare[1], Prasad D. Janorkar[2], Vivekanand R. Desai[3], Shubham K. Ingale[4], Uday S. Ahamindrakar[5]
Assistant Professor, Department of Information Technology
UG Scholar, Department of Information[2,3,4,5]
Sinhgad Academy of Engineering, Pune, Maharashtra, India
Savitribai Phule Pune University, Pune, India

Abstract: *In medical cloud computing, a patient can send her medical data to a cloud server from afar. Because medical data is highly sensitive, only authorized doctors are allowed to access it in this case. A frequent solution is to encrypt data before outsourcing it, with the patient simply sending the corresponding encryption key to the authorized doctors. However, due to the difficulties of digging through the encrypted data, the usability of outsourced medical data is severely limited. Over medical cloud data, we propose Secure and Efficient Dynamic Searchable Symmetric Encryption (SEDSSE) schemes. To begin, we propose a dynamic searchable symmetric encryption scheme that uses the secure k-Nearest Neighbor (kNN) and Attribute-Based Encryption (ABE) techniques to achieve two important security features: forward privacy and backward privacy, both of which are difficult to achieve in the field of dynamic searchable symmetric encryption. Then, to address the key sharing problem that plagues the kNN-based searchable encryption strategy, we suggest an improved technique. In terms of storage, search, and update complexity, our solutions outperform prior proposals. Extensive tests show that our approaches are efficient in terms of storage overhead, index building, trapdoor generation, and query.*

Keywords: Health care, Searchable encryption, dynamic updating, Attribute-based encryption

REFERENCES

[1]. Li, Jiayi, et al. "Practical Multi-keyword Ranked Search with Access Control over Encrypted Cloud Data." IEEE Transactions on Cloud Computing (2020).
[2]. Dai, Xuelong, et al. "An efficient and dynamic semantic-aware multikeyword ranked search scheme over encrypted cloud data." IEEE Access 7 (2019): 142855-142865.
[3]. Xu, Jian, et al. "An Efficient Multi-keyword top-k Search Scheme over Encrypted Cloud Data." 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN). IEEE, 2018.
[4]. Brindha, R., and A. Ghousia Samrin. "Efficient privacy-preserving keyword search method for retrieving data from cloud." 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). IEEE, 2017.
[5]. Dai, Hua, et al. "Semantic-aware multi-keyword ranked search scheme over encrypted cloud data." Journal of Network and Computer Applications 147 (2019): 102442.
[6]. Yin, Hui, et al. "Secure conjunctive multi-keyword ranked search over encrypted cloud data for multiple data owners." Future Generation Computer Systems 100 (2019): 689-700.
[7]. Chi Chen at. Al. proposed An Efficient Privacy-Preserving Ranked Keyword Search Method IEEE 2016.
[8]. Lichun Li at. al. Privacy-Preserving-Outsourced Association Rule Mining on Vertically Partitioned Databases in AUGUST 2016.
[9]. Bharath K. Samanthula at. Al. k-Nearest Neighbor Classification over Semantically Secure Encrypted Relational Data MAY 2015.
[10]. Chunhua Su at. al. proposed Analysis and Improvement of Privacy-Preserving Frequent Item Protocol for Accountable Computation Framework IEEE 2012. S. L. Bangare, "Classification of optimal brain tissue using

dynamic region growing and fuzzy min-max neural network in brain magnetic resonance images", Neuroscience Informatics, Volume 2, Issue 3, September 2022, 100019, ISSN 2772-5286, https://doi.org/10.1016/j.neuri.2021.100019 .

[11]. S. L. Bangare, G. Pradeepini, S. T. Patil, "Implementation for brain tumor detection and three dimensional visualization model development for reconstruction", ARPN Journal of Engineering and Applied Sciences (ARPN JEAS), Vol.13, Issue.2, ISSN 1819-6608, pp.467-473. 20/1/2018 http://www.arpnjournals.org/jeas/research_papers/rp_2018/jeas_0118_6691.pdf

[12]. S. L. Bangare, S. T. Patil et al, "Reviewing Otsu's Method for Image Thresholding." International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 9 (2015) pp. 21777-21783, © Research India Publications https://dx.doi.org/10.37622/IJAER/10.9.2015.21777-21783

[13]. S. L. Bangare, G. Pradeepini, S. T. Patil, "Regenerative pixel mode and tumor locus algorithm development for brain tumor analysis: a new computational technique for precise medical imaging", International Journal of Biomedical Engineering and Technology, Inderscience, 2018, Vol.27 No.1/2. https://www.inderscienceonline.com/doi/pdf/10.1504/IJBET.2018.093087

[14]. S. L. Bangare, A. R. Khare, P. S. Bangare, "Quality measurement of modularized object oriented software using metrics", ICWET '11: Proceedings of the International Conference & Workshop on Emerging Trends in Technology, February 2011, pp. 771–774. https://doi.org/10.1145/1980022.1980190.1.

[15]. S. L. Bangare, G. Pradeepini and S. T. Patil, "Brain tumor classification using mixed method approach," 2017 International Conference on Information Communication and Embedded Systems (ICICES), 2017, pp. 1-4, doi: 10.1109/ICICES.2017.8070748.

[16]. S. L. Bangare, S. Prakash, K. Gulati, B. Veeru, G. Dhiman and S. Jaiswal, "The Architecture, Classification, and Unsolved Research Issues of Big Data extraction as well as decomposing the Internet of Vehicles (IoV)," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 566-571, doi: 10.1109/ISPCC53510.2021.9609451.

[17]. S. L. Bangare, G. Pradeepini, S. T. Patil et al, "Neuroendoscopy Adapter Module Development for Better Brain Tumor Image Visualization", International Journal of Electrical and Computer Engineering (IJECE) Vol. 7, No. 6, December 2017, pp. 3643~3654. http://ijece.iaescore.com/index.php/IJECE/article/view/8733/7392

[18]. N. Shelke, S. Chaudhury, S. Chakrabarti, S. L. Bangare et al. "An efficient way of text-based emotion analysis from social media using LRA-DNN", Neuroscience Informatics, Volume 2, Issue 3, September 2022, 100048, ISSN 2772-5286, https://doi.org/10.1016/j.neuri.2022.100048 .

[19]. Suneet Gupta, Sumit Kumar, Sunil L. Bangare, Shibili Nuhmani, Arnold C. Alguno, Issah Abubakari Samori, "Homogeneous Decision Community Extraction Based on End-User Mental Behavior on Social Media", Computational Intelligence and Neuroscience, vol. 2022, Article ID 3490860, 9 pages, 2022. https://doi.org/10.1155/2022/3490860.

[20]. Gururaj Awate, S. L. Bangare, G. Pradeepini and S. T. Patil, "Detection of Alzheimers Disease from MRI using Convolutional Neural Network with Tensorflow",arXiv, https://doi.org/10.48550/arXiv.1806.10170

[21]. P. S. Bangare, S. L. Bangare, R. U. Yawle and S. T. Patil, "Detection of human feature in abandoned object with modern security alert system using Android Application," 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), 2017, pp. 139-144, doi: 10.1109/ETIICT.2017.7977025

[22]. Kalpana S. Thakare, Viraj Varale, "Prediction of Heart Disease using Machine Learning Algorithm", Bioscience Biotechnology Research Communications (Special issue) Volume 13, Issue 12, 2020 (Dec 2020 issue).

[23]. Kalpana S. Thakare, A. M. Rajurkar, "Shot Boundary Detection of MPEG Video using Biorthogonal Wavelet Transform", International Journal of Pure and Applied Mathematics, Volume 118, No. 7, pp. 405-413, ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version), url: http://www.ijpam.eu

[24]. Kalpana S. Thakare, A. M. Rajurkar, R. R. Manthalkar, "Video Partitioning and Secured Key frame Extraction of MPEG Video", Proceedia Computer Science Journal, Volume 78, pp 790-798, Elsevier, 2016. Scopus DOI: htpp://10.1016/j.procs.2016.02.058, www.sciencedirect.com/science/article/pii/S1877050916000600

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

[25]. Kalpana S. Thakare, A. M. Rajurkar and R. R. Manthalkar, "Content based Video Retrieval using Latent Semantic Indexing and Color, Motion and Edge Features", International Journal of Computer Applications 54(12):42-48, September 2012, Published by Foundation of Computer Science, New York, USA. DOI: 10.5120/8621-2486

[26]. Kalpana S. Thakare, Archana M. Rajurkar, R. R. Manthalkar, "A Comprehensive System Based on Spatiotemporal Features Such as motion, Quantized Color and Edge Features", International Journal of Wireless and Microwave Technologies (IJWMT) ISSN 1449 (Print), ISSN: 2076-9539 (Online), Vol.1, No.3, June. 2011, DOI: 10.5815 /ijwmt

[27]. Kalpana S. Thakare, Archana M. Rajurkar, Dr. R. R. Manthalkar, "An effective CBVR system based on Motion, Quantized color and edge density features", International Journal of Computer Science & Information Technology (IJCSIT), ISSN 0975 – 3826, Vol 3, No 2, April 2011 DOI: 10.5121/ijcsit.2011.3206 78.

[28]. M. L. Bangare, "Attribute Based Encryption And Data Integrity For Attack on Cloud Storage", Journal of Analysis and Computation (JAC), (An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861, ICASETMP-2019, pp.1-4. http://www.ijaconline.com/wp-content/uploads/2019/07/ICASETMP67.pdf

[29]. M. L. Bangare, Sarang A. Joshi, "Kernel interpolation-based technique for privacy protection of pluggable data in cloud computing", International Journal of Cloud Computing, Volume 9, Issue 2-3, pp.355-374, Publisher Inderscience Publishers (IEL).

[30]. Rajesaheb R. Kadam and Manoj L. Bangare, "A survey on security issues and solutions in live virtual machine migration", International Journal of Advance Foundation and Research in Computer (IJAFRC), (December, 2012). ISSN (2014), pp.2348-4853.

[31]. Sachindra K. Chavan, Manoj L. Bangare, "Secure Data Storage in Cloud Service using RC5 Algorithm", International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-2, Issue-5 November 2013, pp.139-144.