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

I. INTRODUCTION

Cloud Computing is a new technology that has changed the way IT businesses do business. It transports apps and data to centralised data centres from which a large user community can access information on a pay-per-use basis. Data security is jeopardised as a result of this. It's possible that the confidentiality of sensitive data will be compromised. It is therefore necessary to encrypt the data before outsourcing it to a cloud server. Data utilisation becomes challenging as a result of this. Traditional search methods for encrypted data include Boolean searches, which are ineffective when there are a significant number of users and data files stored in the cloud.

They also present two important issues: the post-processing that users must perform in order to locate the relevant document in question, and the network traffic that is generated when all files matching keywords are retrieved in the current scenario. A quest for graded keywords that overcome these issues has been proposed. Cloud processing, as a burgeoning processing model, has prompted many enterprises to seriously consider cloud potential in terms of cost-efficiency, flexibility, and managerial expense offloading. Organizations frequently delegate their computational operations in order to better their data to the cloud. Despite the numerous advantages that the cloud provides, security and comfort concerns in the reasoning are preventing businesses from taking advantage of those advantages.

When information is very sensitive, it must be encoded before it can be freelancing to the cloud. However, when data is encrypted, regardless of the security mechanism in place, performing any information mining operations becomes extremely difficult without first decrypting the data. Furthermore, even if the information is encoded, cloud can collect useful and sensitive information about the genuine information goods by monitoring the information accessible styles. Data is stored in cloud storage in logical pools as digital data. In a multi-owner situation, the same data will have multiple owners. All of the data will be managed by a single server. The cloud may have multiple servers, each of which may be situated in different locations.

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

The primary server or cloud storage providers will be responsible for the security and management of the stored data. Customers will be able to buy or lease storage space from these cloud storage firms. Cloud storage enables network access to dispersed and scalable digital data. In cloud storage, a secure search over encrypted data is a problem that must be addressed. The most difficult task in cloud storage is conducting a secure search on encrypted data. There are numerous search options available. They, on the other hand, either add considerable system overhead or make such strategies difficult to use across large data sets. To prevent unauthenticated access, data will be stored in the cloud in encrypted form.

II. LITERATURE SURVEY

As indicated by [1] Multi-watchword Graded Search Scheme with Fine-grained admittance control, compelling and protection safeguarding (MRSF). By joining coordinate coordinating with Term Frequency-Inverse Document Frequency (TF-IDF) and further developing the safe kNN process, MRSF can perform exceptionally exact ciphertext recovery. Plus, by utilizing the polynomial-based admittance procedure, it can effectively refine the inquiry freedoms of clients. As far as the secrecy of reevaluated information and the protection of files and tokens, formal wellbeing examination shows that MRSF is secure. Moreover, point by point concentrates on show that MRSF accomplishes more prominent pursuit exactness and greater usefulness productively contrasted with current plans.

As indicated by [2] Adopt the Doc2Vec model to accomplish a semantic-mindful multikeyword positioned search plot. Doc2Vec model uses the conveyed portrayal of words and records with an unobtrusive dimensionality of vectors while prepared on a dataset with a couple hundred of millions of words. Archives' appropriated portrayals are removed as reports highlight vector by Doc2Vec model and used as the pursuit record. The elements of the questioned watchwords are additionally removed as the inquiry highlight vector, and the safe internal item activity is taken on to accomplish protection saving semantic hunt with the question include vector and list. Our plan can uphold dynamic update on the archive set with Doc2Vec model. The trial on a genuine world dataset shows that the fixed-length include vector can work on the existence productivity on the semantic-mindful inquiry.

As indicated by [3] The recovery of required records from the encoded cloud turns into an issue which requires looking over the scrambled information. In this paper, we propose an effective multi-catchphrase positioned search plot over encoded information in cloud utilizing the information structure bunch B+ tree. To further develop the question proficiency, we build a B+ tree list structure in light of the gathering of informational collections, which can upgrade the record structure and give productive and quick significance between the inquiry and cloud information. In particular, for the security worry of inquiry information, we utilize the superior KNN-based calculation to encode touchy information; the accessible encryption of this plan accomplishes exactness multi-catchphrase question over scrambled cloud information and returns the most noteworthy important top-k outcomes. Broad trial results on genuine informational collections show that the proposed approach can altogether diminish the file stockpiling and further develop the recovery effectiveness.

As indicated by [4] The safe multi catchphrase positioned search technique is carried out for giving extra security and productivity, which has open tasks like refreshing, cancellation, addition of words. These tasks are utilized to get the documents from cloud server with least recovery time. Information proprietors get together huge volumes of information and store it in cloud servers for future reason; later clients utilize those information. Information proprietors are permitted into the cloud server solely after they are verified effectively and are additionally allowed to make their own site pages. For the capacity and recovery of information from cloud server, Blowfish calculation is for the most part utilized in encryption and unscrambling reason. Sub direct inquiry time and effectiveness is expanded.

As indicated by [5] A clever security persisting accessible encryption plot in light of the Latent Dirichlet Allocation (LDA) subject model. Archives are displayed by LDA, and the idea of points is used to create a report subject importance network and question theme vectors. The lattice is utilized as the list for the proposed conspire. The protected internal item activity is embraced to encode the file and question subject vectors, which gives exact point importance score computation between scrambled file and secret entryways. To work on the effectiveness of our essential plan, we embrace an extraordinary complete paired tree and utilize the "Voracious Depth First Search" calculation. Our assessment results show the viability of our plan.

As indicated by [6] A conjunctive multi-watchword positioned secure quest conspire for quite some time proprietors. To ensure information security and framework adaptability in the numerous information proprietors' climate, we plan a cunning secure question plot that permits every information proprietor to embrace haphazardly picked impermanent keys to construct

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

secure lists for various information documents. An approved information client doesn't have to know these brief keys of developing lists and can rather haphazardly pick one more impermanent inquiry keys to scramble question catchphrases, while the cloud server can accurately perform watchwords matching over encoded information records. To rank the inquiry consequences of a conjunctive multi-catchphrase question, the cloud server figures the closeness scores between the question and its inquiry results as indicated by scrambled significance scores of watchwords without getting any touchy data. Broad tests show the accuracy and reasonableness of the proposed plot

As indicated by [7] Proposed framework examined progressive methodology groups the archives in light of the base importance edge, and afterward segments the subsequent bunches into sub-bunches until the requirement on the most extreme size of group is reached. In the hunt stage, this approach can arrive at a straight computational intricacy against a remarkable size increment of archive assortment. To check the realness of indexed lists, a construction called least hash sub-tree is planned in this methodology. Framework likewise examined ciphertext search in the situation of distributed storage. Framework investigate the issue of keeping up with the semantic connection between various plain reports over the connected encoded archives and give the plan technique to upgrade the presentation of the semantic inquiry

As per [8] This framework center around cloud-helped successive itemset mining arrangement, which is utilized to construct an affiliation rule mining arrangement. Here rethought data sets that permit various information proprietors to proficiently share their information safely without thinking twice about information security and release less data about the crude information than most existing arrangements. In contrast with the main realized arrangement accomplishing a comparable security level as these proposed arrangements, the exhibition of this proposed arrangements is three to five significant degrees higher. In light of this try discoveries utilizing various boundaries and informational collections, framework show that the run time in every one of these arrangements is just one request higher than that in the best non-security safeguarding information mining calculations. Since the two information and processing work are moved to the cloud servers, the asset utilization at the information proprietor end is extremely low. It likewise protection saving re-appropriated continuous itemset digging answer for upward divided data sets. This permits the information proprietors to rethink mining task on their joint information in a security safeguarding way. In light of this arrangement, framework fabricated a protection saving reevaluated affiliation rule parceled data sets. Contrasted and most existing arrangements, this arrangements release less data about the information proprietors' crude information.

As indicated by [9] The proposed k-NN convention safeguards the secrecy of the information, client's feedback question, and information access designs. To the best of this information, this work is quick to foster a protected k-NN classifier over scrambled information under the standard semi-genuine model. In this framework, creator center around tackling the grouping issue over scrambled information. Specifically, propose a safe k-NN classifier over scrambled information in the cloud. The proposed convention safeguards the secrecy of information, protection of client's feedback question, and conceals the information access designs.

As indicated by [10] System proposed a convention of tracking down successive thing in responsible figuring (AC) structure which empowers two gatherings to lead cooperative calculation on their conditional information bases to discover the normal regular things without unveiling their private information to the next party. Their plan was proposed in a solid two-party calculation model against vindictive foes. Framework likewise dissects the execution subtleties of AC-system and recognizes some security shortcomings in their plan. Moreover, framework explains the security necessities for the AC-structure and presents an expanded answer for upgrade security. Framework additionally breaks down the pursuit proficiency and security under two famous danger models. S. L. Bangare et al. [11-17] have worked in the brain tumor detection. N. Shelke et al [18] given LRA-DNN method. Suneet Gupta et al [19] worked for end user system. Gururaj Awate et al. [20] worked on Alzheimers Disease. P. S. Bangare et al [21] worked on the object detection. Kalpana Thakare et al [22-27] have worked on various machine learning algorithms. M. L. Bangare et al. [28-29] worked on the cloud platform. Rajesaheb R. Kadam et al [30] and Sachindra K. Chavan et al. [31] have discussed security issues with cloud.

III. Problem Statement

The system for searching multiple keywords using similarity base technique on encrypted data also classification of document on the basic of weight and query

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

IV. Implementation Details of Module

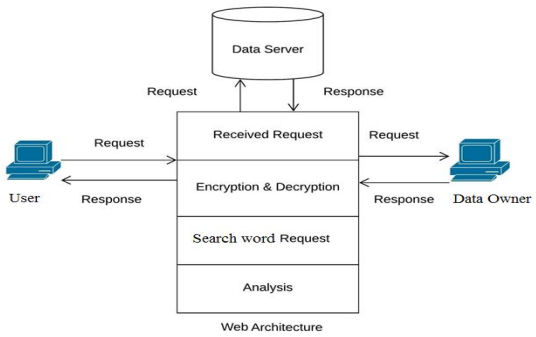

Figure: System Architecture

- **Trusted Authority:** A trusted authority (TA) is a trusted third party. We use it to generate attribute-based encryption (ABE) key to encrypt the medical documents. Patients documents will be encrypted and only some doctors satisfying the corresponding access policy can decrypt them.
- **Patient:** A patient outsources her documents to the cloud server to provide convenient and reliable data access to the corresponding search doctors. To protect the data privacy, the patient encrypts the original documents under an access policy using attribute-based encryption. To improve the search efficiency, she also generates some keyword for each outsourced document. The corresponding index is then generated according to the keywords using the secret key of the secure kNN scheme. After that, the patient sends the encrypted documents, and the corresponding indexes to the cloud server, and submits the secret key to the search doctors.
- **Cloud Server:** A cloud server is an intermediary entity which stores the encrypted documents and the corresponding indexes received from patients, and then provides data access and search services to authorized search doctors. When a search doctor sends a trapdoor to the cloud server, it would return a collection of matching documents based on certain operations.
- **Doctor:** An authorized doctor can obtain the secret key from the patient, where this key can be used to generate trapdoors. When she needs to search the outsourced documents stored in the cloud server, she will generate a search keyword set. Then according to the keyword set, the doctor uses the secret key to generate a trapdoor and sends it to the cloud server. Finally, she receives the matching document collection from the cloud server and decrypts them with the ABE key received from the trusted authority. After getting the health information of the patient, the doctor can also outsource medical report to the cloud server by the same way. For simplicity, we just consider one-way communication in our schemes.

V. Conclusion

The technology provides a rapid data recovery mechanism for encrypted generation in this work. The system also evaluated the protocol's efficiency under various parameter settings. Such runtime objects can be eliminated with the use of the Vector Base Cosine Similarity (VCS) technique. Instead of a linear base search, the encrypted index search technique provides a more accurate search mechanism. Framework has also evaluated the heterogeneous public cloud environment with outcomes evaluation in the cloud environment, which met the aims. Additional privacy and security goals, such as Function Base Access Control, are also included in the framework (RBAC). There are still certain safety challenges to overcome, but future modifications should be made.

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.

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

[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.

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

[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

[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.