International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. **05** Issue **02** | **2021**

Multi-Authority Medical Databases to Enabling Authorized Encrypted Search

Abhisha Solanki
Department of Computer Application, Jain University, Bangalore, India

ABSTRACT

Patient's medical records are sensitive and be going to encrypted before outsourcing data from a database through a server. As it is an important aspect of the healthcare system, data retrieval from multi-authorities a comparatively problematic matter of data privacy. Cloud platforms qualify as a scalable and secure solution for huge data storage, but there have been privacy concerns that patients and medical staff collude with third-party access and unauthorized users through cloud servers. The above issue proposed a scheme of multi-authority searchable encryption standards based on the client's access policy. The proposed scheme eases the RSA function, where authorized users can generate requests for secret search tokens to decrypt ciphertexts and send that to the cloud server to allow them the search operations. First, implement front-end security with user names and passwords. Second, store patient's sensitive data in encrypted form to prevent attackers. Third, allow multi-party searchable access for encrypted data according to the policy applied. Experimental results demonstrate a secure, scalable, and efficient scheme.

Keywords: RSA function, authorized searchable encryption, multi-authority attribute-based encryption, multi-authority

1. INTRODUCTION

Medical over the web is stimulated with the advancement of the e-medical framework as of late, where encrypted data outsource to cloud server by the client's side. And selectively provide access for each data search to the user is a challenging task for a multi-party encryption scheme.

Patients are communicating with specialists or experts in distance without visiting physically to the clinic. In the existing system, the most significant issues are security and maintaining the confidentiality of user's sensitive information and health status. Like, the cloud servers sometimes discard qualified results to save computational assets and correspondence overhead. Thus, a well-working and secure query results should provide a mechanism for results confirmation that permits the clients to verify the results.

After laboratory tests and examinations of patients, hospital authorities are responsible for uploading reports and patient's health status to the medical database or cloud to inform doctors which procced to further treatment. In this system, data access for providing to the authorized users using attribute-based encryption. ABE provides various searching abilities with a user access policy for multi-authorities. The various parameter is used for applying policy to access record for preventing a malicious attack, inside attack, and unauthorized users.
The search results for information on ciphertext are positive, on the off chance that 1. The authenticate user enters the system with the specific credential. 2. After if cloud server authorizes the user access by signified parameter to control the operation which they perform. 3. To decryption of report, the user needs to request for secret key allocation on time of interval. This help in securing data from inside attack and third-party leakage.

In the proposed model, the first RSA protocol used for the reconfiguration of non-interactive functionality. Second, integrate attribute-based encryption for multi-party access to realize the fine-grained access control in SE (Searchable Encryption). Last, deploy an encrypted medical database for a searchable encryption system.

2. ARCHITECTURE

The architecture of this scheme consists of three main attributes: Authority, Client, Server. The data outsourced by the owner of the files to the cloud server. The files are stored in encrypted form to assure data privacy in the system. The Admin authorizes or allows the users to access encrypted data stored in a medical database or cloud. The data owner has access to update and manage the encrypted reports. The unique secret search key generates by the admin on client requests for privacy concerns. To decrypt the data, generated token used to access or download the report uploaded to the server. The server executes the search operations and provides the data access on request.

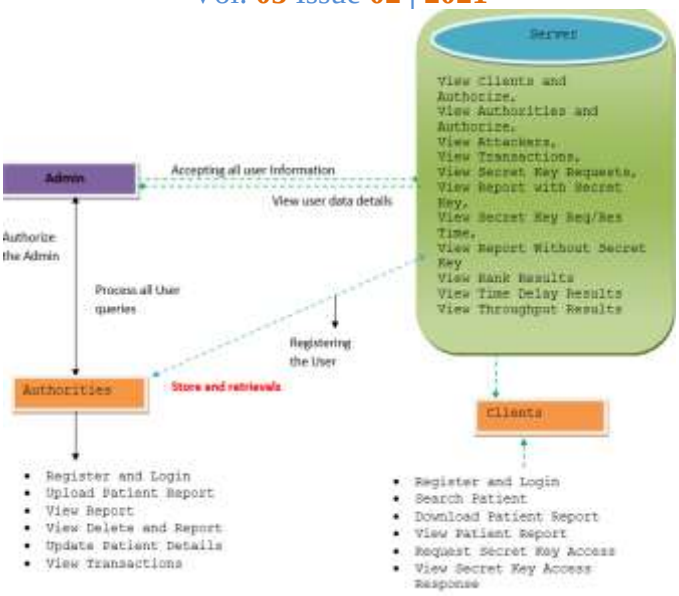

Figure 1: Architectural Diagram

3. SYSTEM FRAMEWORK

The work Involves many users and authorities to access the e-medical database in a very secure manner. The set of events that can take place include a set of people such as a staff of insurance company who help the patients, nurses for filling our medical details, staff of banks to handle the patient's invoices in the hospital and related areas. So, we need these kinds of parties to work together for the same system. They can be defined into various categories such as Authorities, Clients, and Servers.

3.1 Cloud Server

The Cloud server manages which is used to provide data storage service for the Data Owner. Data owners encrypt their files and store them in the server for sharing and manipulation with data consumers. Shared data files are accessed by users and download encrypted files of from the Cloud Server, and then Server will decrypt them. The server will generate the aggregate key if the end-user requests for file authorization to access and performs the following operations as View Clients and Authorize, View Authorities, View Transactions, View Attackers, View Secret Key Requests, View Report with Secret Key, View Secret Key Request Time, View Time Delay Results, View Throughput Results, View Report Without Secret Key, View Rank Results.

- **Servers:** It acts as a medium between the Clients and the Authorities. It gets the data from the authorities and converts them into a non-readable form then provides the information to the clients based on the attributes dependent on the clients. They can be deployed by the cloud service provider. It manages the data from all authorities and supplies search and storage services for encrypted data.

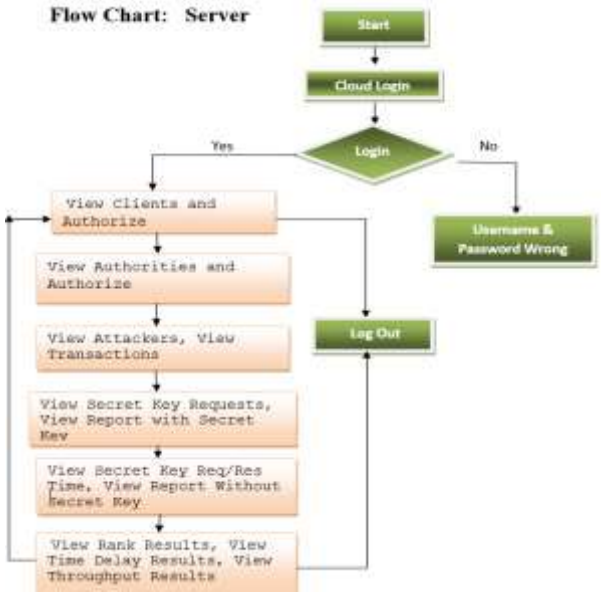

Figure 2: Server Flow Chart

- **Client:** The Clients can be Doctors, Patients, Accounting, Authorities themselves, or authorized to access the encrypted data. The client possesses specific attributes and search capabilities arranged by the authorities. Clients are people who are authorized to access the secured data from the cloud by having attributes that are proposed by the authority.

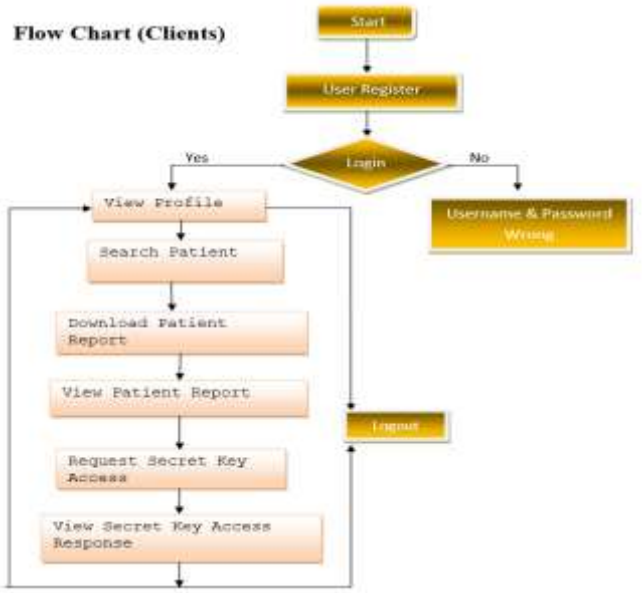

Figure 3:Client Flow Chart

- **Authorities:** The key authority act as a data owner and performs the following operations View Transactions, Update Patient Details, View Report, Upload Patient Report, View Delete, and Report. The authorities always consist of cloud service renters such as the insurance company, hospital, bank, etc. Authorities are the data owners who collect data and upload them to the cloud storage after encrypting them, and it also specifies the search policy for the data and assigns the search capabilities to the client according to their attributes. It provides us information from the data stored in the cloud. Authorities have a specific search pattern and the client who possesses such attributes can get the data.

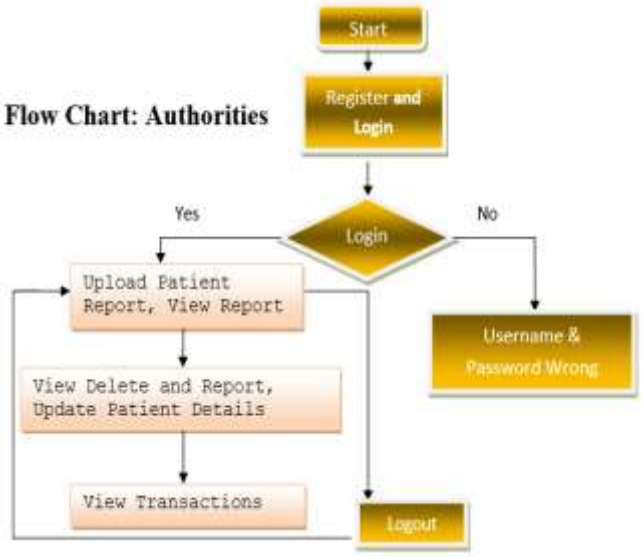

Figure 4:Authority Flow Chart

4. PRILIMINARIES

Searchable Symmetric Encryption: The most important branch of SE is searchable symmetric encryption (SSE). SSE is a way which makes user search and query files without leaking information files stored in the system. For this purpose, we propose a multi-user searchable symmetric encryption scheme with dynamic updates. Some other lines of related works are to target primitive cryptography for encrypted keyword search. First, construction against non-adaptive and adaptive chosen keyword attack. This implemented a dynamic SSE scheme for the large-scale databases to consider I/O efficiency. Recently, efforts given on SSE have focused on the

improvement of the security, which achieves forward privacy and backward privacy. Searchable symmetric encryption (SSE) provides a mechanism to search on encrypted data with acceptable performance and security level. Every SSC existing scheme has a trade-off between performance, security, and functionality. Storage size is consisting of performance, communicational cost, and the communication overhead, which includes interaction in-between the client and the cloud server. The main focus of security is on reducing the leakage of queries, the less leakage, and the better security standards. The main requirement of the SSC scheme is to support query operations (such as construct queries, update operation and delete operation) as many as possible.

Multi -Authority: This supports search capability where all data records are already stored in medical databases. The main aim is to search data that is encrypted at the uploading time. Multi authority is the data record of all authorities which can allocate their searching abilities to the user as well as clients who are supporting various authorities. To improve searching capabilities, we take the help of the accept-based encryption technique. It gives the concept of a multi-user searchable encryption scheme, where a user can authorize multiple users to search encrypted data stored.

Attribute-based: If the attributes that are used for encryption satisfy the access structure on the user's private key, then the ciphertext can be decrypted. In the reverse situation, CP-ABE allows the user private key to be associated with a set of attributes in ciphertext associated with an excess structure. When designing an access control mechanism in a broadcast environment CP-ABE is the preferred choice. Many works have been proposed for more expensive, flexible, and practical versions of the technique since the first construction of CP-ABE. The data user generates the trapdoor independently without relying on always online trusted authority. The encrypted index with the trapdoor on a user ‘s behalf and return a matching result if and only if users' attribute associated with the trapdoor satisfy the access policies embedded in the encrypted indexes can be searched over by the cloud server (CS). Attributes and keywords are differentiated in our design. For search authorization purposes the system only maintains a limited number of attributes. An index containing all the keywords in the files is created by the data owner but encrypts the index with an access structure only based on the attributes of users.

RSA function: the user creates a public key that is based on two large prime numbers, along with an axillary value that is kept secret. Anyone can encrypt a message via the public key but Only be decoded by someone who has the prime number. In RSA, the public key can be generated by multiplying two large prime numbers PP and QQ together, and the private key is generated through a different process. Then a user distributes his public key PQ, and anyone who wishes to send users a message would encrypt their message using the public key. The public key is based on RSA allows shared medical status throughout the e-healthcare system. For online access, the patient's PHI data which is stored in MCS (medical Centre server), doctors and other staff have to take permission from patients. In a simple way, we can achieve group encryption by using RSA, where the whole group is assigned a public key and each member of that group has the corresponding private key.

5. CONCLUSION

An improved cryptographic search scheme is provided by this paper for multi-authority or multiple user e-medical databases to support cloud security. Non-interactive leakage functions are highlighting the proposed framework, and describe who can generate an encrypted database for searchable encrypted data storage with fine-grained access. This method simplifies the control over data accessing for clients. Tokens can only be shared with the particular user for a specific time interval, which grained the security from third-party leakage.

6. RERFERANCE

[1] M. Y. S. Z. Y. R. K. A. L. W. LI, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, pp. 131-143, 2012.

[2] M. H. D. M. M. J. A. S. M. AMERI, “A Key-Policy Attribute-Based Temporary Keyword Search scheme for Secure Cloud Storage,” *IEEE Transactions on Cloud Computing*, vol. 8, no. 3, pp. 660-671, 2020.

[3] Z. Q. J. Z. L. O. Hui Yin and K. Li, “Achieving Secure, Universal, and Fine-Grained Query Results Verification for Secure Search Scheme Over Encrypted Cloud Data,” *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 27 - 39, 2021.

[4] Q. H. S. M. J. S. Hongbo Li and W. Susilo, “Authorized Equality Test on Identity-Based Ciphertexts for Secret Data Sharing via Cloud Storage,” *IEEE Access*, vol. 7, pp. 25409-25421, 2019.

[5] S. Y. W. L. Wenhai Sun and Y. T. Hou, “Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud,” *IEEE*, vol. 27, no. 4, pp. 1187 - 1198, 2016.

[6] X. Y. X. W. C. W. B. L. Yu Guo and X. Jia, “Enabling Encrypted Rich Queries in Distributed Key-value Stores,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 6, pp. 1283 - 1297, 2019.

[7] C. Ma, Y. Gu and H. Li, “Practical Searchable Symmetric Encryption Supporting Conjunctive Queries Without Keyword Pair Result Pattern Leakage,” *IEEE Access*, vol. 8, pp. 107510 - 107526, 2020.

[8] H. S. D. Z. C. J. C. Z. Rui Guo and Z. Wang, "Flexible and Efficient Blockchain-Based ABE Scheme with Multi-Authority for Medical on Demand in Telemedicine System," *IEEE Access,* vol. 7, pp. 88012 - 88025, 2019.
[9] R. X. Rui Zhang and L. Liu, "Searchable Encryption for Healthcare Clouds: A Survey," *IEEE Access,* vol. 7, pp. 88012 - 88025, 2019.
[10] N. L. Kodumru and M. Supriya, "Secure Data Storage in Cloud Using Cryptographic Algorithms," in *Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, 2018.
[11] Q. Tang, "Nothing is for Free: [5] X. Yuan, X. Wang, C. Wang, C. Qian, and J. Lin, "Building an encrypted, distributed, and searchable key-value store," in Proc. Of the 11th ACM on Asia Conf. on Comput. andCommun. Security, 2016, pp. 547–558.
[12] [6] S. Lai, S. Patranabis, A. Sakzad, J. K. Liu, D. Mukhopadhyay, R. Steinfeld, S.-F. Sun, D. Liu, and C. Zuo, "Result pattern hiding searchable encryption for conjunctive queries," in Proc. of the 2018 Conf. on Comput.andCommun. Secur. ACM, 2018, pp. 745–762.
[13] Security in Searching Shared and Encrypted Data," *IEEE*, vol. 9, no. 11, pp. 1943-1954, 2014.
[14] Y. Z. I. S. RASHAD ELHABOB and H. XIONG, "Efficient Certificateless Public Key," *IEEE Access,* vol. 7, pp. 68957 - 68969, 2019.
[15] [1] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute based signcryption," Future Generation Comput. Syst., vol. 52, pp. 67–76, 2015.
[16] [2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Trans. Parallel Distrib. Syst.,vol. 24, no. 1, pp. 131–143, 2013.
[17] [3] Y. Zhang, J. Katz, and C. Papamanthou, "All your queries are belong to us: The power of file-injection attacks on searchable encryption," in Proc. of 25th USENIX Secur. Symp., 2016, pp. 707– 720.
[18] [4] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," in Proc. of 36th Annu. Symp.on Foundations ofComput. Sci., 1995, pp. 41–50.