How to Cite:
Rajkumar, M., & Karthika, J. (2022). Consistent sharing of personal health data in cloud using attribute based encryption (ABE). *International Journal of Health Sciences*, *6*(S7), 5217-5224. https://doi.org/10.53730/ijhs.v6nS7.13114

Consistent sharing of personal health data in cloud using attribute based encryption (ABE)

M. Rajkumar*
Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu
* Corresponding author's Email: raj.mylsamy@gmail.com

J. Karthika
Electrical and Electronics Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu

***Abstract*---**Personal Health Record (PHR) is a booming model of patient's health data updating and periodic maintenance. The patients' power over admittance to track their own PHRs is a challenging and recent technology. Attribute based Encryption (ABE) is advanced technologies were rules are framed based on their characteristics rather than identities. It is a secure key of the patient and is dependent on their characteristics .This paper focus on numerous information of the patients and the clients, to fit them in the PHR framework. The decryption of the secure key is done only when the characteristics match with the data base in the cloud. The security access can be a key or a text data. If numerous keys are created the cloud will grant access only when at least one key attribute gets match with the cloud data. This technology provides an additional dynamic tuning of access or record credits, to uphold the skill-ful on-request client/property denial and access under emergency situations. Other than this a Thresh-old Identity Based Encryption (TIBE) conspire is accommodated upgrading solid unscrambling consistency.

***Keywords*---** upgrading solid unscrambling consistency, TIBE, Personal Health Record.

Introduction

Fundamentally, the PHR proprietor ought to conclude encoded records and to permit set of clients to get admittance to each document. A PHR document is just be accessible to the clients com-paring unscrambling key[1]-[4]. Float, the objective of patient-driven security is regularly in strife with adaptability in a PHR

framework. The approved clients may either need to get to the PHR for individual use or expert purposes. Now, attempt to examine the patient driven, PHRs put away in workers, and confounded the testing key issues. So as to secure the personal information put on a worker, receive the strategy called ABE. Using ABE, the access arrangements are linked depending on the qualities of clients, which permits a patient to precisely share their PHR among a bunch of cli-ents, without the need of clients [2],[3].

1. Related Works

2.1 ABE for Fine-grained Data Access Control

To begin with, they typically expect the utilization of a solitary confided in power (TA) in the framework. This not exclusively may make a heap bottleneck, yet in addition experiences the opening entryway for high security. Actually, various associations normally structure their own (sub) spaces and become reasonable specialists to confirm various traits (i.e., gap and rule). Second, there still comes up short on an effective and on-request client renouncement system with dynamic strategy refreshes/changes [5][6]7]. At last, the greater parts of the current works don't separate the individual and public spaces, which have distinctive quality administration necessities and adaptability issues. Actually adroitly for us isolating the framework into two kinds of areas is comparative with that in, float a key distinction is in a solitary TA is as yet expected to administer the entire expert space [8][9]. As of late, key-arrangement to make sure about re-appropriated information in the cloud, where a solitary information proprietor can encode her information and offer with different approved clients, by conveying trait based admittance benefits [10][11]. The strategy of information proprietor to repudiate a client proficiently by assigning the updates of influenced figure writings and client mystery clod worker [12]-[15].

2.2 ABE for Revocation

Our proposing is bound together security structure for understanding driven based multi-space, multi-authority framework with numerous clients. The system captures application level prerequisites of both civic and individual utilization of a patient and disseminates clients' belief to numerous specialists. Additionally, it proposes a set-up of instruments by interestingly joining the technical qualities of both CCMA-ABE and the YWRL-ABE conspire. Utilizing my plan, patients pick, implement their entrance strategy document, and repudiate a client without including overhead.

2. Secure and Scalable PHR Sharing

3.1 Overview of Construction

The proposed system is shown in Fig. 1. The client having various data users in personal and public domain, will store their various files stored in a cloud server.

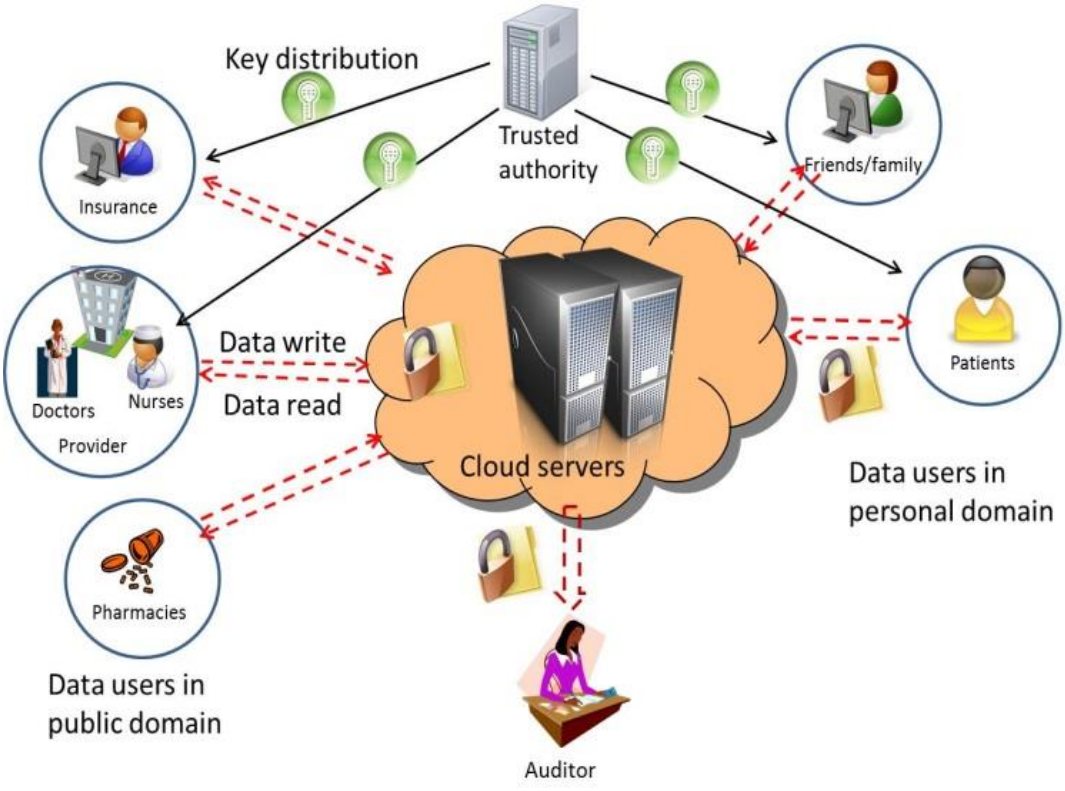

Fig. 1. The proposed methodology.

3.2 System Structure and Key Distribution

The framework initially attributes a typical information ascribes shared by each domain like, "central profile", "clinical history", "sensitivities", and "solutions".

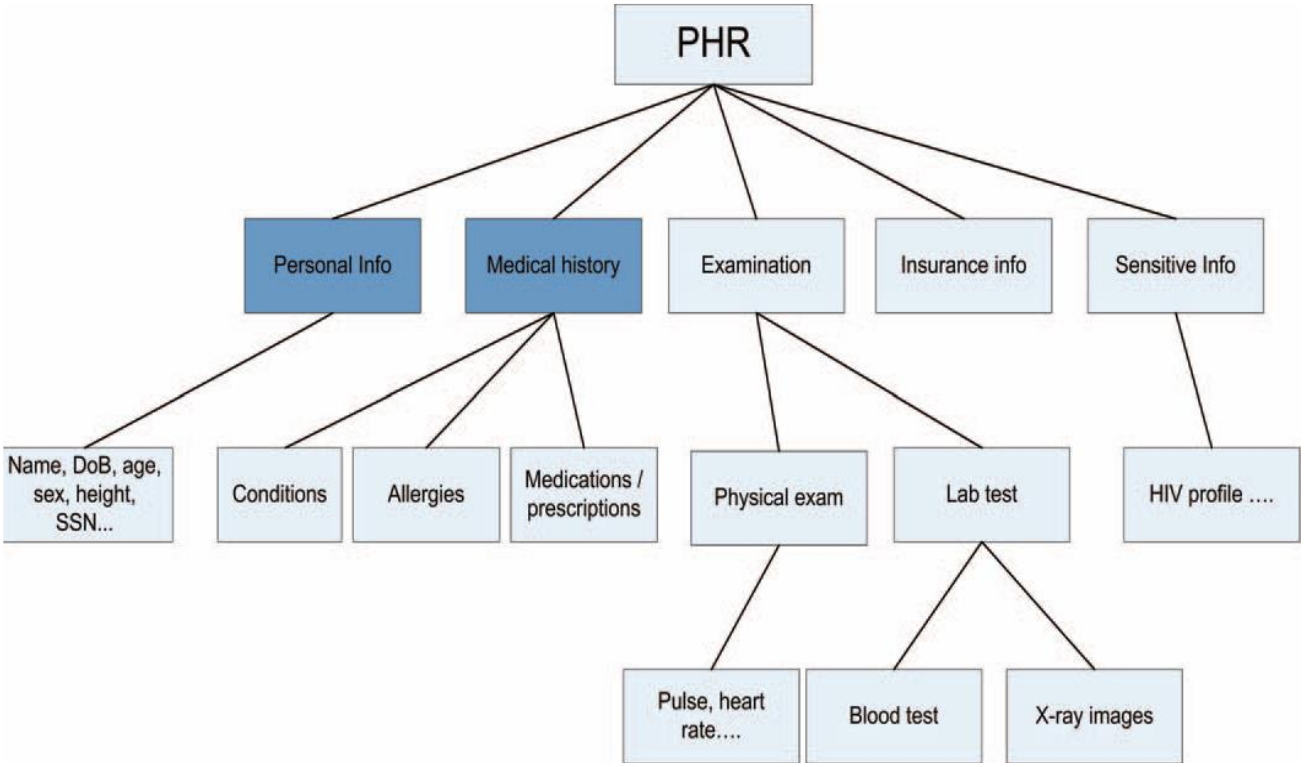

Fig. 2. Hierarchy of files

Each PHR proprietor's produces its comparing ace keys. The public keys can be distributed in an online medical services informal community (HSN). There are two different ways for disseminating mystery keys. First, utilizing the PHR administration, a PHR proprietor can indicate the entrance benefit of an information.

Second, PSD could get the mystery key by sending a solicitation to the PHR proprietor by means of HSN. In view of that, the strategy motor of the application consequently determines entrance structure to create the client mystery that implants entrance structure, see Fig. 2. At point when the client is conceded all the document types under a class, her entrance benefit will be spoken to by that classification all things considered. For the PUDs, the framework characterizes job credits, and a per-user in a PUD gets mystery key from AAs, which ties the client to her guaranteed ascribes/jobs.

3. Proposed issues

4.1 MA_ABE for Public Domain

The system designates key administration capacities and multiple quality specialists. So as to accomplish more grounded security ensure for information

owners, the CCMA_ABE conspire is utilized. It is normal to relate the cipher-text of a PHR report with a proprietor indicated admittance strategy for clients from PUD. Drift, one specialized test is that CCMA_ABE is basically a KP_ABE plot, the entrance strategies are authorized in clients' mystery keys arrangements don't legitimately mean record access approaches from the proprietors' perspectives. By my plan, is concurring upon the configurations of key-approaches and standards of determining which credits are needed in the cipher-text, the CCMA_ABE can actual partner uphold proprietor indicated record access strategies with some level of adaptability i.e., it capacities like CP-ABE2. So as to permit the proprietors to indicate an entrance strategy for each PHR report, I abuse the way that the fundamental CCMA_ABE works like fluffy IBE, where the edge strategies are upheld.

4.2 MA_ABE for User Revocation with Enhancement

To appoint mystery key updates to the worker, a fake trait should be also characterized by every one of (N −1) AAs, which are consistently AND with every client's key approach to keep the worker from getting a handle on the mystery keys. This additionally keeps up the obstruction against up to (N −2) AA plot of MA_ABE. Utilizing lethargic disavowal, the influenced figure writings and client mystery keys are possibly refreshed when an influenced unrevoked client signs into the frame-work. To renounce a client in MA_ABE, one needs to discover an insignificant subset of traits (γ) with the end goal that without it the client's mystery key's entrance structure (Au) will never be ful-filled. Since our MA_ABE conspire requires conjunctive access strategy over the AAs, it does the trick to find insignificant subset by each AAk.

4.3 Write and emergency access control

For specific pieces of information, clinical staffs have to brief access when a crisis happens. The clinical staffs require transitory approval to unscramble the information. Normally they are accomplished by letting every patient agent her crisis key to a crisis office. In particular, first and foremost, every proprietor characterizes an "crisis" quality and incorporates it with the PSD part of the cipher-text of each PHR. At that point it creates a crisis key sk_EM utilizing the hub key-arrangement "crisis", and agents it to the ED. Upon crisis, a clinical staff confirms herself to the ED, demands and gets the relating patient's sk_EM, and afterward decodes the PHR archives utilizing sk_EM.

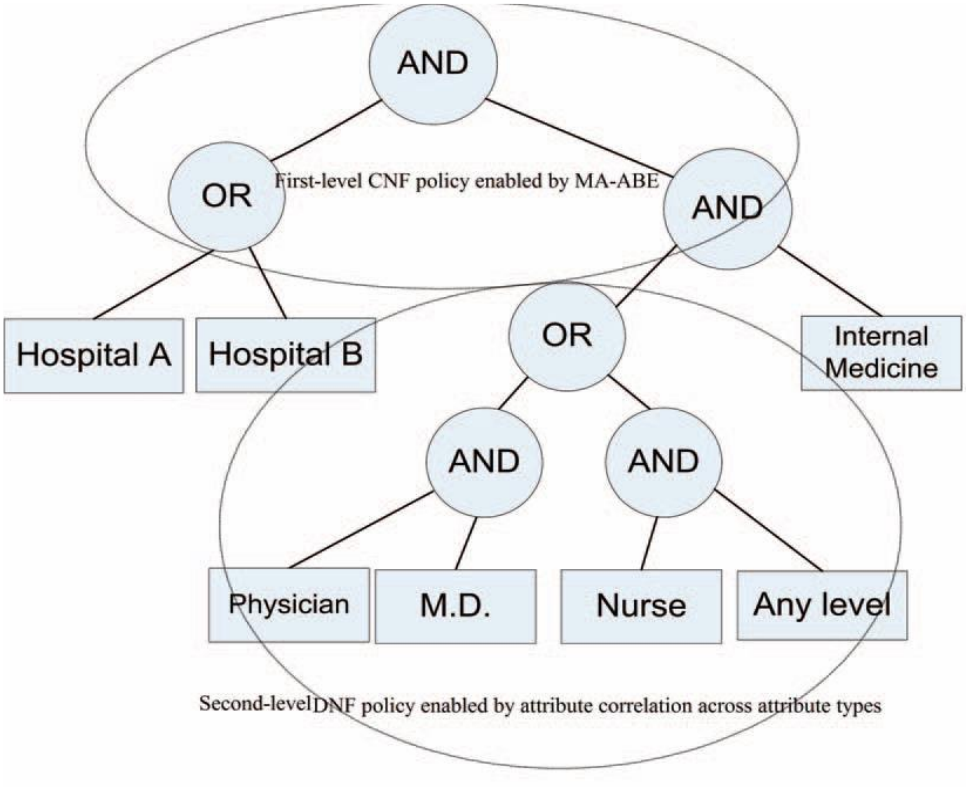

Fig. 3. Framework using MA_ABE

4. Performance Analysis

5.1 Computation Costs

The computational expense of our plan is shown through simulation results. The fig.4. shows the performance of searching operations. Without pre-processing it may took long time to search the file but with pre-processing concept took less time to search the file.

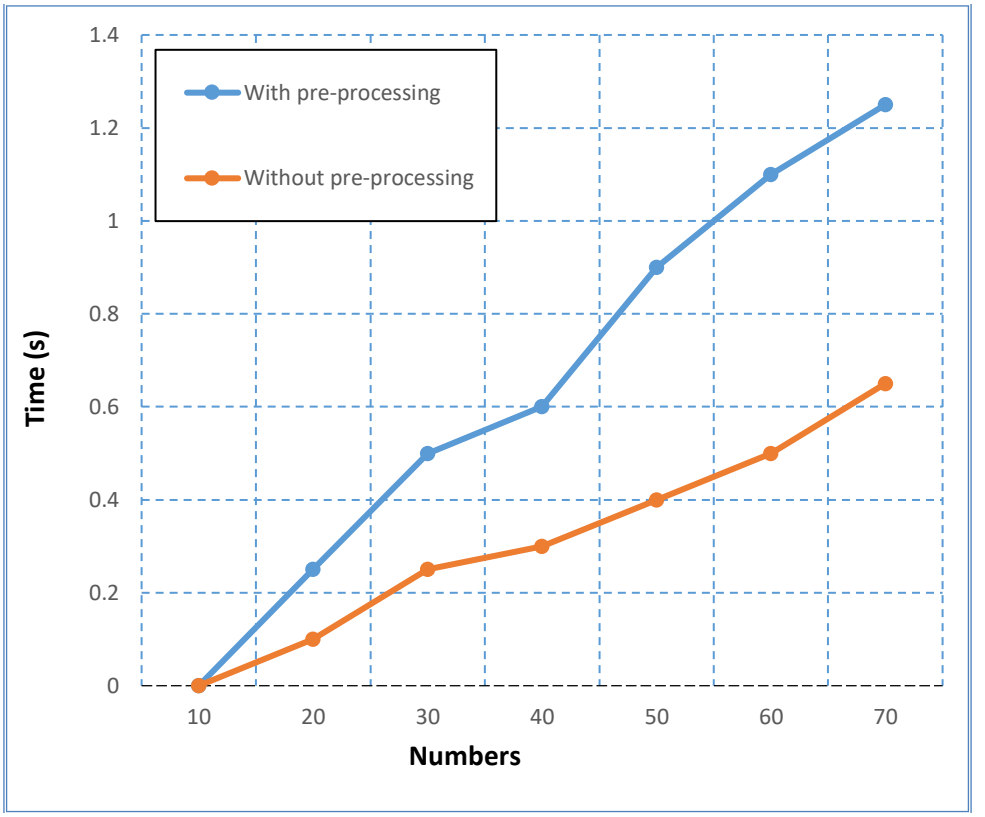

Fig. 4. Pre-Index Search Time (s)

5. Conclusion

The proposed system shows the high secure distribution of individual wellbeing archives in distributed computing. This enhances the clients to build their own PHRs. The structure tends to the one of a kind difficulties brought by different PHR proprietors and clients, in that enormously de-crease the intricacy of key administration while upgrade the protection ensures contrasted and past works. It allows the controlled sharing of health records.

References

[1] Ming Li, Shucheng Yu, Yao Zheng and KuiRen, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", IEEE Transactions on Parallel and Distributed Systems, 24(1),pp. 131- 143 (2013).

[2] J. Feng, L. Liu, and Q. Pei, "Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks," IEEE Transactions on Parallel and Distributed Systems, 2021.

[3] Y. Chen, J. Li, C. Liu, J. Han, Y. Zhang, and P. Yi, "Efficient attribute based server-aided verification signature," IEEE Transactions on Service Computing, 2021.

[4] J. Li, Y. Chen, J. Han, C. Liu, Y. Zhang, and H. Wang, “Decentralized attribute-based server-aid signature in the internet of things,” IEEE Internet of Things Journal, 2021.
[5] L. Liu, M. Zhao, and M. Yu, “Mobility-aware multi-hop task offloading for autonomous driv-ing in vehicular edge computing and networks,” IEEE Transactions on Intelligent Transporta-tion Systems, 2022.
[6] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, “Vehicular edge computing and network-ing: a survey,” Mobile Networks and Applications, vol. 26, no. 3, pp. 1145–1168, 2021.
[7] P. Shi, H. Wang, S. Yang, C. Chen, and W. Yang, “Blockchain-based trusted data sharing among trusted stakeholders in IoT,” Software: Practice and Experience, vol. 51, no. 10, pp. 2051–2064, 2021.
[8] M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal Health records in cloud computing: Pa-tient-centric and fine-grained data access control in multi-ownersettings”, SecureComm’10, pp. 89–106 (2010).
[9] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, “Securing the e-health cloud,” Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI, pp. 220–229 (2010).
[10] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted per-sonal health records in cloud computing,” in ICDCS,(2011).
[11] K. D. Mandl, P. Szolovits, and I. S. Kohane, “Public standards and patients’ control: how to keep electronic medical records accessible but private,” BMJ, 322(7281), pp. 283, (2001).
[12] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient controlled encryption: ensuring privacy of electronic medical records,” in CCSW 09, pp. 103–114 (2009).
[13] VikasVitthalLonare, Prof.J.N.Nandimath., “Ensuring Distributed Accountability for Data Sharing in Cloud Using AES and SHA”, International Journal of Computer Science and In-formation Technologies (IJCSIT),Vol. 6(1), pp.652- 657,(2015).
[14] Y.B.Gurav, ManjiriDeshmukh, "Scalable and Secure Sharing of Personal Health records in Cloud Computing using Attribute Based Encryption", International Journal of Science and Research (IJSR), Vol. 3(7), pp.2319-7064,(2014).
[15] B.SriVarsha, P.S.Suryateja., "Using Advanced Encryption Standard for Secure and Scalable Sharing of personal Health Records in Cloud", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5(6), pp.7745-7747,(2014).