Source based Privacy for Confidential Data in Cloud based e-Healthcare Systems

G. Keerthi, P. Sai Kiran

Abstract*: *In cloud computing, Service oriented architecture (SOA) is an emerging concept in e-health care systems. Outsourced consists both sensitive and non-sensitive patient's data like case sheets and others, patients data to be stored in private cloud. Privacy is an aggressive concept to store patient's data in cloud. Conventionally novel cloud computing paradigm based on service oriented architecture is provided for different user's to store their data in heterogeneous cloud environment. To provide customizable data security for e-health records of different patients in e-health care systems. Source based privacy is also a problem in storage of patients data. So that in this paper, we propose and present a Secure Indexing approach for efficient privacy preserving based secure approach to handle privacy in both search hidden data and also check access patterns of human based on redundancy and combine the concept of attribute separation based on authentication with respect to audit ability to prevent source leakage in e-health care systems. Experimental results of proposed approach gives better and efficient authentication time efficiency results on user privacy in cloud related health care systems.

Index Terms*: *Service oriented cloud computing, data privacy, e-health care systems, secure indexing approach and authentication based audit ability.

I. INTRODUCTION

In recent years, storage of personal health records (PHR) has been increased in outsourcing of labeled data to cloud. PHR server enables patient's information to make and control different services performed by the patient in e-health care network systems. Privacy in sharing and recovery of patient's medical data in outside environment is an aggressive concept to share different service related applications Personal health information outsourced in cloud shown in figure 1.

Instances of the previous are relative and companions, while the last can be therapeutic specialists, drug specialists, and analysts, and so forth. We allude to the two classifications of clients as close to home and expert clients, individually. The last has possibly huge scale; should every proprietor herself be straightforwardly in charge of dealing with all the expert clients, she will effortlessly be overpowered by the key administration overhead. Also, since those clients' entrance demands are commonly capricious, it is troublesome for a proprietor to decide a rundown of them. Then again, unique in relation to the single information proprietor situation considered in the greater part of the current works, in a PHR framework, there are various proprietors who may scramble as per their own specific manners, potentially utilizing distinctive arrangements of cryptographic keys. Different types of security related approaches with respect to secure data sharing in e-health care systems.

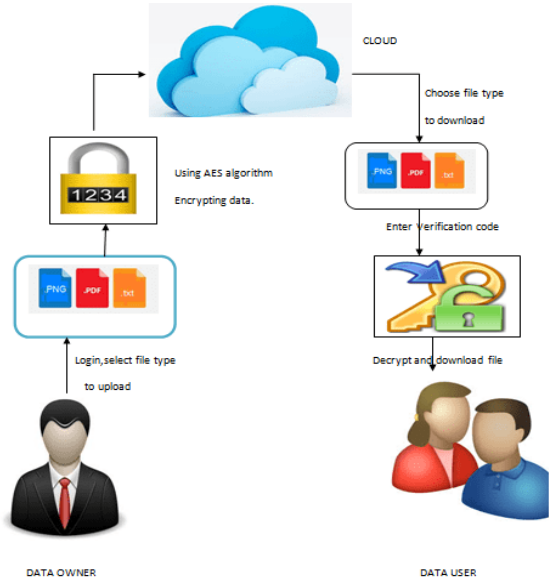

Fig. 1 Cloud computing with respect to e-health data sharing.

.

So that in this paper, we propose a Secure Indexing Method for efficient privacy preserving keyword which describe security for search data and access control policies for data sharing with attribute based encryption and audit the misbehaving activity of different users at emergency situations. Experimental results of proposed approach gives better security related aspects with respect to upload patients data in outsourced cloud in e-health care systems.

II. REVIEW OF LITERATURE

This section describes about different authors opinion regarding secure health data storage and sharing in cloud computing. We demonstrate that the two prerequisites can be fulfilled completely while embracing a novel cloud-based PHR framework design. We explain the job of remote virtual machines in this design and use communication models to reason about security suggestions. At long last, we assess MyPHR Machines, a prototypical usage of the design: we exhibit that the framework empowers the execution of outsider genome investigation benefits on

Revised Manuscript Received on May 07, 2019.

G. Keerthi, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India.

P. Sai Kiran, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India.

patient owned genome information while guaranteeing that (1) such administrations can't vindictively store this information and (2) patients can demonstrate the examination results to specialists without sharing along their full genome.

A novel PHR framework engineering is attractive since protection related prerequisites must be in part fulfilled by business PHR frameworks. We likewise show that the design can be executed. Specifically, we talk about how a complex privacy sensitive use case (in the space of customized prescription) has been acknowledged utilizing our prototypical framework execution. By methods for framework communication models, we elucidate that the engineering alters control contrasted with ordinary web administration designs: while traditionally, information is sent from PHR stages to web administrations running on supplier foundation our engineering expects administrations to be conveyed on a confided in execution stage.

Among the current examples of EHR interoperability, the ISO 13606 standard is an essential thought. It is trusted that the utilization of this standard, related to semantic innovations, may help in the development of a powerful design, remembering the difficulties of semantic interoperability. The target of this paper is to introduce a proposition for an EHR engineering, in view of ISO 13606 and on the usage of semantic advances, for a genuine EHR situation. So as to achieve that, a genuine EHR situation is portrayed, just as its principle interoperability necessities and a competitor design is proposed to fathom the introduced difficulties of interoperability. The capacity of the ISO 13606 EHR reference model to oblige the situation was featured, together with the help given by the utilization of the cosmology particular dialects - RDF and OWL- - in regard to the upkeep of a controlled vocabulary.

III. BASIC PRILIMINARIES USED IN E-HEALTH SYSTEMS

Basic preliminary concepts used in e-Health systems to explore different secure based services as follows:

Symmetric Searchable Encryption: It describes procedure to encrypt different health related documents on remote server accessing data for view and search relevant data from different web sources using searchable encryption.

Based on Curtmola et.al investigation in security aspects in cloud computing, searchable symmetric encryption comprises following calculations

KeyGen(): This function used by the users generate different keys to initiate approach, it takes input as different security attributes relates to users and produces output K.

BuildIdx(): this function builds different indexes for different keys generated by user for collection documents D, for that it takes input as secret key and document d and produces output as I for effective searchable encryption procedure.

Trapdoor (K,w): In this function user compute the trapdoor for keyword for searchable encryption. A searchable encryption encrypted document with proxy id maintenance of each user in real time scenario. This function takes input as secret key and keyword w and returns output as trapdoor Tw.

Search(I,Tw): This function executes by remote server and then search relevant document data based on keyword, because of trapdoor (Tw), remote server explore data with secure index and carried out the specific query without getting knowledge relates to real keyword.

Based on above procedure, we describe the implementation of proposed approach i.e secure index approach.

IV. SYSTEM MODEL AND IMPLEMENTATION

In this section, we propose a secure hash based indexing approach for e-health care systems. Two main concepts present in e-health care systems: accessible encryption, audibility with access control policies. Based on receiving health care data systems, store data into open source cloud with privacy, then data to be accessed with different access control between different user's in cloud based e-health systems

A. Secure Storage Retrieval

Primary component in storage for health care data. Secure index approach describes data in index format store data in searchable encryption format. In encryption, different features are structured for efficient search based data retrieval with authentication of different users in cloud. In our proposed implementation, private, public data storage into cloud server checks user access control in searchable encryption.

In our implementation, check different hash functions relates to different health users store their data into cloud check different authentication based on allocated tasks in distributed healthcare systems.

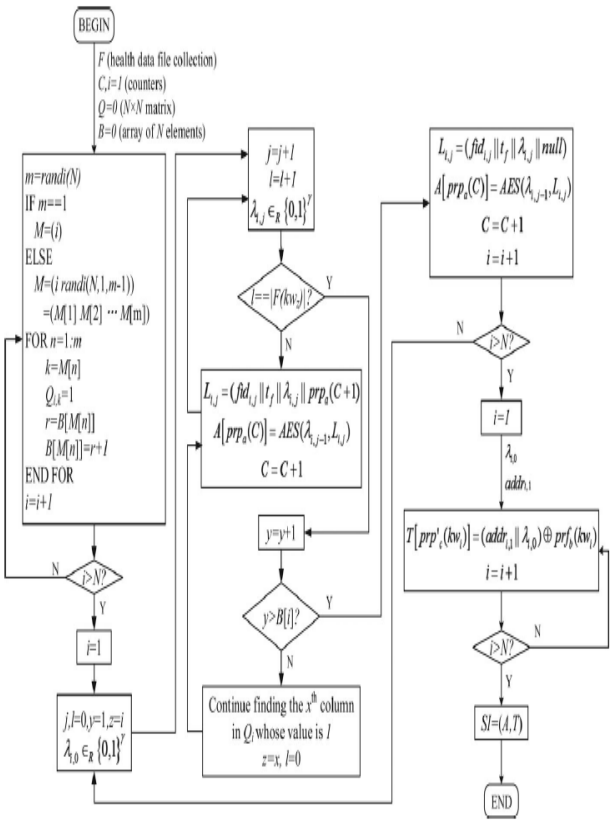

Fig. 2 Proposed approach design

B. Constructing the Secure Index

In private cloud, user receives data from other users for privacy preserving storage as follows: Private cloud secure index for different files stored in figure 2 for index search with sorted index (SI) stored in array index A and lookup table T. A[∗] = d (and similarly T[∗]) denotes the value d stored in A[∗]. With respect to different linked files stored in cloud i.e. L={Li, i=1,....,n} is encrypt and stored in array based on index A. Each linked list consists three fields to perform secure indexing where unique index file with identifier $L_{i,j} = (fid_{i,j} \| \lambda_{i,j} \| ptr)$, unique secret key encrypt into storage system. Ptr expresses address of the encrypted files $L_{i,j+1}(Enc_{\kappa_{i,j}}(L_{i,j+1}))$, Enc describes symmetrically encrypts data using AES with SHA for each file I will be stored in lookup table T in encrypted format.

In our implementation, different files relates to different patients in healthcare systems by assigning privacy to stored data which consist both sensitive and non-sensitive.

C. Audit ability based Access Control Policy

Second segment relates to data access control during storage where different types of data requests appeared through cloud storage system. Proposed approach focused on emergency access control of different services. Emergency access control services mainly based on personal data sharing without loss memory storage and access data any where data store in cloud servers.

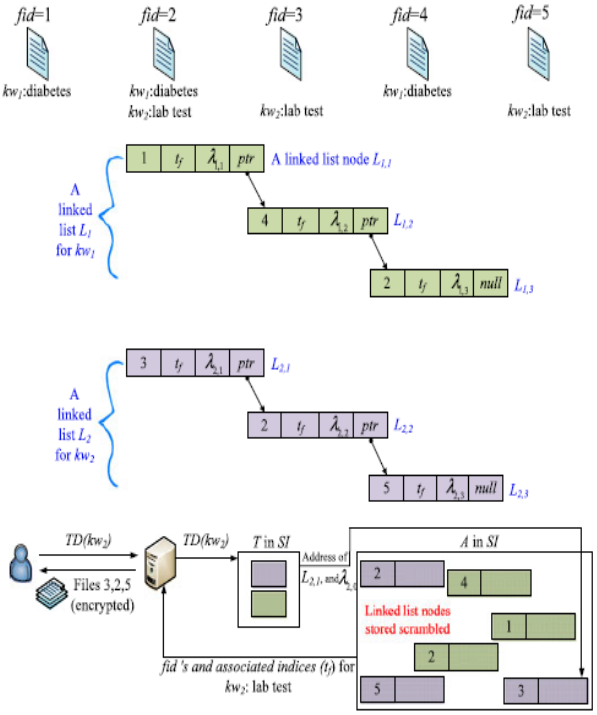

Fig. 3 Secure indexing procedure sorted by keyword search

In our design, users don't store data in encrypted format using attribute based encryption, store data encryption using efficient secure indexing approach in private cloud storage system. In this implementation, users use attribute based encryption to encrypt user's secret data and then share to only authorized author's can decrypt files with authorized file signatures. Based on user's attributes, secure indexing approach every time check the parameters (attributes of user's) for storage and share data to authorized persons only.

V. EXPERIMENTAL EVALLUATION

This section describes the computational efficiency of proposed approach with respect to existing approaches in terms of patient's data storage. For that we use following metrics in implementation of secure cloud storage of patient's data. NETBEANS as IDE and JAVA as programming language and then calculate simulation time.

In security protecting capacity utilizing tolerant cell phones, effective mystery key tasks are basically included which we won't concentrate on in the assessment. In crisis medicinal information get to utilizing EMT cell phones, the most exorbitant continuous calculation incorporates IBE unscrambling and ABE decoding, creating a normal mark on qualities and a fractional edge signature on the entrance demand, and checking the halfway limit with respect to signature verification of each user in cloud.

Comparison w.r.t to Amount of efforts and effort in Key Structure: after set up above reasoning atmosphere in real-time database integration. The performance duration of Installation, KeyGen, Secure in data files upload and download with regard to customer permission are also considered. Time performance with performance assessment as shown in table 1.

Table. 1 Overall values with respect time in cloud health data sharing

No. of Attributes	Setup		KeyGen		Encryption	
	Proposed Approach	DCCSOA	Proposed Approach	DCCSOA	Proposed Approach	DCCSOA
10	4.3	3.8	0.58	0.47	0.052	0.045
30	5.6	4.8	0.78	0.65	0.089	0.065
50	6.4	5.5	0.85	0.75	0.098	0.084
70	7.4	6.4	0.97	0.84	0.15	0.092
100	8.4	7.4	1.24	0.9	0.28	0.14

In comparison mutually the different plan, this point needs an additional initialization of the standard cost, resulting in its slowness. Based on above performance evaluation we shown that our proposed approach gives better results when compare to traditional approaches.

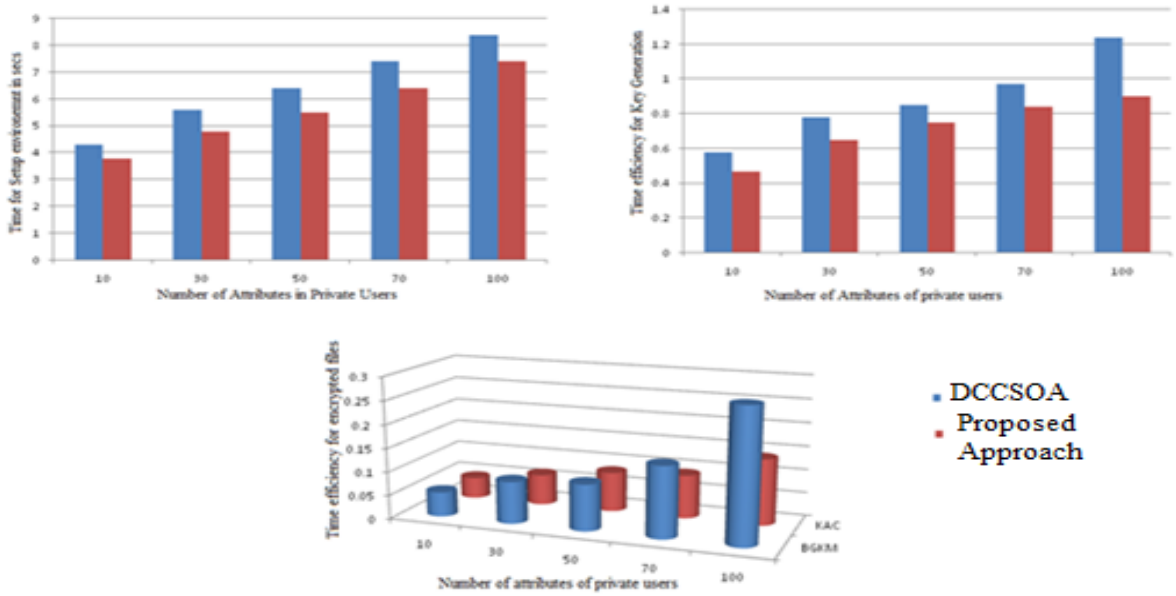

Fig. 4 Overall performance of proposed approach with existing approaches.

VI. CONCLUSION

In this paper, we propose a secure hash based indexing approach to handle privacy preserving keyword based search data. In this approach, discuss search based data extraction and access pattern based data redundancy and also integrate different attributes with encryption to provide access control based data privacy and sharing data to different users in cloud. We also give solution for source based data authentication in data storage into distributed cloud environment. Our method also describes misbehaving activities of administrator using authentication procedure to each user in e-health care systems. Experimental results of proposed approach gives better and efficient secure based performance results with respect to different patient's data in distributed environment.

REFERENCES

1. Mehdi Bahrami and Mukesh Singhal, "A Dynamic Cloud Computing Platform for eHealth Systems", 2015 IEEE 17th International Conference on e-Health Networking, Applications and Services (Healthcom): Short and Demo Papers.
2. Mehdi Bahrami and Mukesh Singhal, "The Role of Cloud Computing Architecture in Big Data", Information Granularity, Big Data, and Computational Intelligence, Vol. 8, pp. 275-295, Chapter 13, Pedrycz and S.-M. Chen (eds.), Springer, 2015 http://goo.gl/4gNW3s
3. Landau, Susan. "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations" Security & Privacy, IEEE 12.1 (2014): 62-64.
4. Mehdi Bahrami and Mukesh Singhal, "DCCSOA: A Dynamic Cloud Computing Service-Oriented Architecture", IEEE International Conference on Information Reuse and Integration (IEEE IRI'15), San Francisco, CA, USA. Aug 2015.
5. Kumar, Karthik, and Yung-Hsiang Lu. "Cloud computing for mobile users: Can offloading computation save energy?" Computer 43.4 (2010): 51-56.
6. Mehdi Bahrami and Mukesh Singhal, "A Light-Weight Permutation based Method for Data Privacy in Mobile Cloud Computing" in 3rd Int. Conf. IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (IEEE Mobile Cloud 2015) San Francisco, IEEE, 2015.
7. Bahrami, Mehdi. "Cloud Computing for Emerging Mobile Cloud Apps" Mobile Cloud Computing, Services, and Engineering (MobileCloud), 3rd IEEE International Conference on. 2015.
8. Harrison, Owen, and John Waldron, "AES encryption implementation and analysis on commodity graphics processing units", Springer Berlin Heidelberg, 2007.
9. Resnick, Steve, Richard Crane, and Chris Bowen, "Essential windows communication foundation: for .Net framework 3.5", Addison-Wesley Professional, 2008.
10. Fan, Lu, et al. "DACAR platform for eHealth services cloud." Cloud Computing (CLOUD), 2011 IEEE International Conference on. IEEE, 2011.
11. Lounis, Ahmed, et al. "Secure and scalable cloud-based architecture for e-health wireless sensor networks." Computer communications and networks (ICCCN), 2012 21st international conference on. IEEE, 2012.
12. Magableh, Basel, and Michela Bertolotto, "A Dynamic Rulebased Approach for Self-adaptive Map Personalisation Services", International Journal of Soft Computing and Software Engineering (JSCSE), vol.3. no.3, 104, March 2013.
13. Yue Tong," Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability", IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. 18, NO. 2, MARCH 2014.
14. E.-J. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.
15. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," presented at the ACM Conf. Comput. Commun. Security, Alexandria, VA, USA, 2006

AUTHORS PROFILE

G. Keerthi, pursuing M.Tech in the Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, completed BTech(CSE) in Lakireddy Balireddy College of engineering, Her research interest mainly in Cloud Computing. Email:keerthireddy6996@gmail.com.

P. Sai Kiran, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India. His research work projects in Data Mining and Cloud Computing. Email:psaikiran@kluniversity.in.