RESEARCH ARTICLE OPEN ACCESS

Incorporated Keyword Search Using Characteristic Based Encryption for Electronic Health Records in Vapours

[1]A.Senthil Kumar, [2]S.Abirami
[1]Asst.professor, Dept.of.Computer Science, Tamil University, Thanjavur-613010.
[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.

----------**********----------

Abstract:

Electronic health (e-health) document frame is a new usage which provide more relieve in healthcare. The fortification shield and safety of the susceptible personal manuscript is the significant matter for the users, these factors major concerns for further evolution of the framework. Users fundamentally have two major concerns related to their personal information like the solitude and safety measures of the susceptible personal information, which might harm or obstruct further enlargement. Re-encryption scheme provides more safety to the records by re-encrypting the encrypted index before uploading them into cloud server. Since the patient's healthcare records consist of susceptible in order, it may be not convenient for the patient when his records are accessed by everybody. The searchable encryption (SE) format is a equipment to have as a feature sanctuary aegis and propitious operability functions together, which can play a consequential role in the e-health record system. This provides the patients to give the access right permission to other users to operate search function on the personal record in limited time period. And then it verifies the user substantiation. Then it allows the user to access the data in a scrupulous time meeting. File access process is over then the meeting is over file convey time is very short time so attackers can't the users file and also user gives request any time so it's very problematical for the attackers to access the user data illegally.

Keywords — **Searchable Encryption; Time Control, Designated Tester, E-health.**

----------**********----------

I. INTRODUCTION

THE ELECTRONIC heath records (EHR) system will make medical records to be computerized with the ability to prevent medical errors. It will facilitate a patient to create his own health information in one hospital and manage or share the information with others in other hospitals. Many practical patient-centric EHR systems have been implemented such as Microsoft Health Vault and Google Health. Given the ambitious prospect to deploy the EHR system ubiquitously, privacy concerns of the patients come up. Healthcare data collected in a data centred may contain private information and vulnerable to potential leakage and disclosure to the individuals or companies who may make profits from them.

1.1. MOTIVATION FOR THE MAKE ENQUIRIES

Data about individuals is considered to be 'sensitive' if exposing it to public knowledge may have adverse affects on the individuals identified. An example is information about a patient being treated for a socially unacceptable illness. On the other hand, the aggregation by governments, businesses and researchers of such data about communities of individuals is needed to support planning, forecasting and budgeting. Over many years, research literature has provided data privatization

techniques for producing meaningful statistical data from aggregated data without revealing information about specific individuals.

Big IT giants like Amazon, Infosys, Cisco, CSC, Sales force and many more are offering health care services through clouds. NIST defines Cloud Computing as "A model for enabling ubiquitous, convenient, on demand network access to shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. IBM, a major player in cloud computing, has defined it as follows, "A cloud is a pool of virtualized computer resources. A cloud can host a variety of different workloads ranging from batch processing jobs to interactive user mode jobs".

1.1.1. Union of cloud computing and health care services:

The health care services provided through electronic medium is called as "e-health". Paper based medical records are improved to Patient Health Records (PHRs) and Electronic Health Records (EHRs). PHRs are maintained by the individuals for their reference and EHRs are maintained by health centers for better analysis and diagnosis of diseases and for further treatment. In addition to the analysis by the doctor, he might share the EHRs to his peers or seniors belonging to other hospitals and health centers for discussion and examination. Electronic Medical Records (EMRs) is another category of health information in electronic version similar to EHRs is maintained and it is not shared to outsiders, kept within the hospital or health centre where the data is generated.

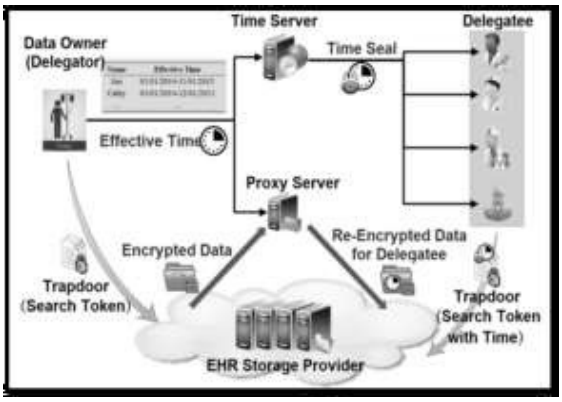
The Conjunctive Multi Keyword Search Security Model with Proxy Re-Encryption Function in E-Health Clouds is proposed which has the following merits.

1) Compared with existing schemes, this system can achieve timing enabled proxy re-encryption with delegation revocation.
2) The proposed system is proven against offline chosen guessing attacks, chosen keyword, chosen time attack.
3) Rather than the random oracle model this scheme works based on standard model.

Shows the proposed system model. There are three types of entities. Data Owner, Data user and Data Center(Authority). Authority is one who owns the data center he provides the private storage space to the data owner to store his EHR files. Data owner extracts the keywords from the EHR files and converts them into secure searchable indices. The EHR files are encrypted to cipher text. A data center provides EHR storage and a server to search. Role of storage provider is to store data and search, add, delete operations are performed by search server as per user request. User uses the trapdoor generated to search the EHR files using his private key and sends it servers to search. The servers on receiving the request interact with the EHR storage provider to find the matched files and returns the result to user in encrypted form.

II. ADVANTAGES OF PROPOSED SYSTEM:

- Secure Sharing Of PHRs Stored.
- Access policies are expressed based on the attributes of users or data
- Flexible treatment details
- Monitoring by admin
- Systematic manner to maintain treatment and Health Records.



III. PERFORMANCE ANALYSIS

There are few important indicators to check whether the scheme is suitable for privacy preserving in EHealth cloud storage. Those indicators are security level, efficiency and utility function. Here we have compared Re-dtPECK proposed system with other SE schemes in terms of functionality, communication and computation overhead.

- **Time control**

In privacy-preserving systems the EHR data owner will be enabled by the time controlled function to spread his access rights to other user in limited time even when EHR data owner is offline

- **Conjuctive Keywords**

Conjuctive Keyword search function when compared with single key word search gives the users with more than requested results and satisfy them with multiple results.

- **Against off-line KG attack**

Till date there is no specific technique to avoid spy attacks over public communication channel. If this is not prevented, then outside attacker can easily implement off-line KG attack by seeing the data transfers between Data center and patient. Existing Systems have not kept an eye on this and not considered. But proposed system is resistant to KG Attacks.

Later to lower computing rate, the proxy server won't re-encrypt the ciphertext till they are acquired and this mechanism is called lazy re-encryption technique. The cloud data server won't recover the similar records except the active time enclosed in the time seal admits with the time in the re-encrypted ciphe rtext, which is different as compared with the classical proxy re-encryption SE schemes.

And generalization is the process of replacing the values of attribute with a border category .e.g. if Joan age is 19 instead of mentioning as 19, it can be replaced by 20<age<=30, which is the border category. And the main advantage is that only the certain users will be able to access certain details, like the doctors can access the full details of patient and the nurse can access the symptoms and the medicine. The chemist can access only the medicine details. In our proposed system if the user requests for the records he gives the query along with his private key to the sever, if the key matches with the severs public key, then an One Time Password will be sent to the users mobile number by the server. If the user enters the correct OTP he will be allowed to search the records. This method is introduced to enhance the security to our proposed system.

We have evaluated the proposed Re-dtPECK scheme by implementing key components on an experimental workbench, including the system global setup, the key generation, the re-encryption key generation, the trapdoor generation and the test algorithms. The pairing-based cryptography (PBC) Library is used. We have elected the type-A elliptic curve parameter, which provides 1024-bit discrete log security strength equivalent to the group order of 160-bit. The experiments have been executed on a PC running Windows7 with an Intel core

CPU at 2.5GHz and a 4.0 GB of the memory.

IV. CONSULTATION

A novel Re-dtPECK scheme to realize the timing enabled privacy-preserving keyword search instrument for the EHR make unclear storage, which could support the mechanical handing over revocation. The tentative grades and security analysis indicate that our scheme holds much higher security than the existing solutions with a rea-sonable overhead for cloud applications. the need and importance behind the union of cloud into health care systems, the design challenges and issues of e-health cloud is reviewed. Then the state of art analysis of security technique is analyzed by classify them into crypto graphical approaches and access control policies. In adding up to security and privacy preserving, there are still more issues for research. Integrity of the medical data stored in cloud, tracking and classification of actions in the health cloud, efficient data search mechanisms, secrecy in multi authority cloud and efficient key management can be considered for research.

V.REFERENCE

[1] W. M. Tierney, J. C. Leventhal, J. A. Cummins, P. H. Schwartz and D. K. Martin,"Designing a system for patients controlling providers' access to their electronic health records: Organizational and technical challenges," *J. General Internal Med.*, vol. 30, no. 1, pp. 17–24, 2015.

[2] Google Inc. *Google Health*. [Online]. Available: https://www.google.com/health, accessed Jan. 1, 2013.

[3]Microsoft. *Microsoft HealthVault*. [Online]. Available: http://www.healthvault.com, accessed May 1, 2015.

[4]. D. Boneh, G. Di Crescenzo, R.Ostrovsky, and G. Persiano, Public key encryption with keyword search, Proc. EUROCRYPT Interlaken, Switzer-land 3027: 506–522 (2004).

[5] P. Liu, J. Wang, H. Ma, H. Nie, "Efficient Verifiable Public Key Encryption with Keyword Search Based on KPABE," In *Proc.* 2014 *Ninth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, IEEE, pp.584-589, 2014.

[6] J. Shao, Z. Cao, X. Liang, H. Lin, "Proxy re-encryption with keyword search," *Information Sciences*, vol. 180, no. 13, pp. 2576-2587, 2010.

[7] W. Yau, R. Phan, S. Heng, B. Goi, "Proxy Re-encryption with Keyword Search: New Definitions and Algorithms," in *Proc. International Conferences on Security Technology, Disaster Recovery and Business Continuity*, Jeju Island, Korea, Dec. 13-15, 2010, vol.122, pp. 149-160, Springer.

[8] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Security models for delegated keyword searching within encrypted contents,"*J. Internet Services Appl.*, vol. 3, no. 2, pp. 233–241, 2012.

[9] K. Emura, A. Miyaji, and K. Omote, "A timed-release proxy re-encryption scheme," *IEICE Trans. Fundam. Electron., Commun.Comput. Sci.*, vol. 94, no. 8, pp. 1682–1695, 2011.

[10] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," *Inf. Sci.*, vol. 258,pp. 355–370, Feb. 2014.