The E-Health Cloud Platform Now Supports A Keyword Search Related To Timer Use And Lab-Enabled Proxy Recoding

G.MOUNIKA
M.Tech Student, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Dr. M. SAMBASIVUDU
Associate Professor, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Abstract: **The delivery of healthcare may be vastly enhanced by the introduction of novel software, such as an electronic health record system. Users' fundamental concerns about the privacy and security of their personal information may be slowing the systems' widespread adoption. The searchable encryption (SE) method is a promising option for the electronic health record system due to its ability to provide strong security without sacrificing usability. Our research introduces a new cryptographic primitive, which we've termed "Re-dtPECK." It's a time-dependent SE approach that combines conjunctive keyword search with a designated tester and a proxy reencryption function that takes time into consideration. Patients may use this function to provide access to their data to carefully chosen researchers for a short period of time. Any allotted period for a delegatee to view and decode their delegator's encrypted papers may be extended if required. It's possible that the delegate's access and search capabilities will expire after a certain period of time has passed. It's also capable of conjunctive keyword searches and resisting assaults based on guessing. Only the authorized tester is allowed to look for the existence of certain keywords in the proposed method. We provide a system model and a security model for the proposed Re-dtPECK approach to prove that it is a safe and effective replacement for the existing standard. Simulations and comparisons with other methods show that it requires very little bandwidth and storage space for data.**

Keywords: **Search And Retrieval Of Information; HR; Encryption; SE*;***

I. INTRODUCTION:

It will make it easier for patients to build their own health records at one hospital, then maintain those records or share them with other patients in other hospitals using the same system. There have been several successful implementations of patient-centric electronic health record systems, such as Google Health and Microsoft Health Vault, among other service providers. It's possible that the health records stored in a data centre include private information about the patient, which makes them susceptible to the risk of leakage and disclosure to persons or businesses that could use the information for their own commercial gain or to further their own interests [1]. Although the service provider may lead the patients to believe that their private information is protected, the electronic health record (EHR) still has the potential to be compromised if the server is broken into or if a member of the staff acts inappropriately. The significant issues about individuals' rights to privacy and safety are the preeminent barrier that prevents widespread implementation of the technology in question. We make an attempt to tackle the issue by implementing a rudimentary technique that was suggested to automatically revoke the delegation immediately after a period of time that was previously defined by the data owner. In the conventional time-release method, the time seal is embedded into the cipher text at the very beginning of the encryption procedure. This is done in order to protect the time seal from being compromised. We developed an online system to collect patients' choices for who might read their electronic health records (including naming all participating clinic providers both individually and categorically, such as doctors, nurses, and other staff) and what data should be redacted (none, all, or by specific categories of sensitive data or patient age). Then, we modified the software that was already being used for data viewing and was being used by a state-wide health information exchange, as well as a large urban health system and its primary care clinics, so that it would allow the preferences of patients to guide the data displays that were being shown to providers. Public key encryption with keyword search, also known as PEKS, is a kind of cryptographic primitive that offers users the ability to search through encrypted data. As a result, this encryption method is suitable for usage in the context of cloud computing. The majority of the existing PEKS schemes are unable to verify the results of the search, and the system does not specify the users who are permitted to make a request for encrypted data files that are stored on the cloud server [2][3]. This is despite the fact that the existing PEKS schemes can enable users to search encrypted data in a confidential manner. Zheng came up with an original cryptographic method not too long ago, and he termed it verifiable attribute-based keyword search (VABKS for short). It makes it possible for a data user, whose credentials fulfill the access control policy of the data owner, to search the encrypted data file and validate the outcome of the search. On the other hand, the approach is predicated on the

 @ 2013-2023 http://www.ijitr.com All rights Reserved.

implausible assumption of a secure channel, much like Boneh's method.

II. PROBLEM STATEMENT:

Proxy re-encryption, also known as PRE, is a process that allows a proxy to transform cipher text that was encrypted using a delegator's public key into a form that can be decrypted using a delegatee's private key. PRE requires that the proxy possess a re-encryption key. The concept of keyword search is new to PRE as a result of the implementation of proxy re-encryption with public keyword search (Re-PEKS). Users that have access to a keyword trapdoor are able to search the encrypted text, even if the proxy does not have access to the concealed keywords. After some time had passed, Wang et al. came up with an enhanced strategy to enable the conjunctive keyword search feature. Under the random oracle model, each of these Re-PEKS techniques has been shown to be safe. Yet, it's possible that a proof in the random oracle model will lead to unsafe schemes. The cost of transmission or processing is too expensive in the existing system. On the other hand, current techniques need an index list of the searched keywords in order to construct a trapdoor. This will cause information to be leaked, which will compromise the secrecy of the query [4]. If an opponent discovers that the encrypted indexes or trapdoors have reduced entropies, it is probable that the adversary will attempt to guess the potential candidate keywords, which will allow the KG attacks to be carried out.

III. PROPOSED METHODOLOGIES:

We are making an effort to remedy the issue by implementing a new technique that has been presented to automatically revoke the delegation immediately after a period of time that was previously set by the data owner. It gives the impression that the time period places restrictions on all users, even the owner of the data. Since the time information is included in the process of re-encryption, the proposed method has the attractive feature of not imposing any time restrictions on the person who owns the data. When the owner of the data delegated some of his responsibilities, he had the ability to specify distinct effective access time periods for each of the users he delegated [5]. A starting time and an ending time are two possible ways to indicate an effective time period that has been specified by the owner of the data. In order to provide users with a time token, the system makes use of a time server, which is responsible for generating the tokens. The time server produces a time seal ST by utilizing both his own private key and the public key of the delegatee. This happens after the time server has been given an effective time period of T by the data owner. The time period denoted by the letter T is therefore encased inside the time symbol denoted by the letter ST. The time interval T will be included in the newly re-encrypted cipher text as a result of the re-encryption method being carried out by the proxy server. The timing-enabled proxy re-encryption function is what this term refers to. The delegatee is responsible for generating a trapdoor for the keywords that are being requested by utilizing his private key and the time seal ST whenever he sends a query request. The cloud service provider will only reply to the search query if the time period contained in the trapdoor coincides with the effective time period that is included in the proxy's re-encrypted cipher text. If you do not provide these details, the search request will be denied. Because of this, the delegatee's access permission will be automatically revoked after a certain amount of time. The owner of the data does not need to perform any extra operations in order to revoke the delegation. To the best of our knowledge, this is the first piece of work that, within the context of a searchable encryption system, permits automated delegation revocation based on temporality. It is suggested to implement a conjunctive keyword search scheme with a specified tester and timed-enabled proxy reencryption function (Re-dtPECK), which has the following desirable qualities: A revolutionary searchable encryption system that supports secure conjunctive keyword search as well as approved delegation functions has been designed by us. As compared to other techniques, the work presented here is capable of achieving timing-enabled proxy re-encryption together with efficient delegation revocation [6]. It has been decided to allow the owner-enforced delegation timing setting. There is the potential for separate access time periods to be established for each delegate. The suggested method has been shown to be safe against chosen-keyword, chosen-time attacks in a formal setting. In addition, it is possible to defend against offline keyword guessing attacks as well. Without the data server's private key, the testing method would not be able to work properly. Listeners in on the conversation were unable to successfully predict any of the keywords due to the testing methodology. Instead of the random oracle model, the standard model is used to determine how the security of the scheme is implemented. This is the first primitive in the standard model to enable the aforementioned functions, and it was very recently added.

IV. ENHANCED SYSTEM:

The proxy re-encryption technique is primarily responsible for the realization of the authority delegation. The cipher text that was encrypted by the delegator's public key is transformed by the proxy server using the re-encryption key into a different form. This new form may be looked for

 @ 2013-2023 http://www.ijitr.com All rights Reserved.

by the delegatee using his own private key. After the allotted amount of time has passed, the delegatee will no longer have any power over the search. A time seal is used to include the previously determined time information into the cipher text that has been re-encrypted. This is done so that the time-controlled access right revocation may be carried out. The delegatee is able to successfully create a legitimate delegation trapdoor using the Trapdoor technique with the assistance of the time seal. In the event that the time information that is concealed within the re-encrypted cipher text differs from that which is included within the delegation trapdoor, the equation that is contained within the Test method will not be valid. Furthermore, the re-dtPeck workflow if the current time is earlier than the time that was specified, the data server will not respond to the search query that was submitted by the delegatee. As compared to the single-keyword search, the conjunctive keyword search function offers customers a greater degree of convenience and the ability to provide accurate results that meet a greater number of the users' needs. Users do not need to do a query on each individual term and instead may depend on a computation of intersection to get the information they want. To the best of our knowledge, there is no current proxy re-encryption searchable encryption system that could give the conjunctive keywords search capacity without needing a random oracle. This is the case even though we have done extensive research on this topic. This previously unsolved issue has been resolved thanks to our plan. The scheme might offer both the conjunctive keyword search and the delegation function. Regrettably, it is demonstrated in the random oracle (RO) paradigm, which significantly lowers the degree of security. In electronic health record systems, the proxy re-encryption technique is usable. The delegation of the patient's rights to search and access will be made simpler as a result. Users were unable to use the searchable encryption feature for proxy re-encryption because the schemes in question were unable to deliver it. The provision of time-controlled revocation capabilities for previously granted access rights is an essential design goal. When the currently observed time falls outside of the range of validity for the specified effective time period, the delegation appointment will be cancelled. It should restrict the authorized user from accessing the data once a certain amount of time has passed.

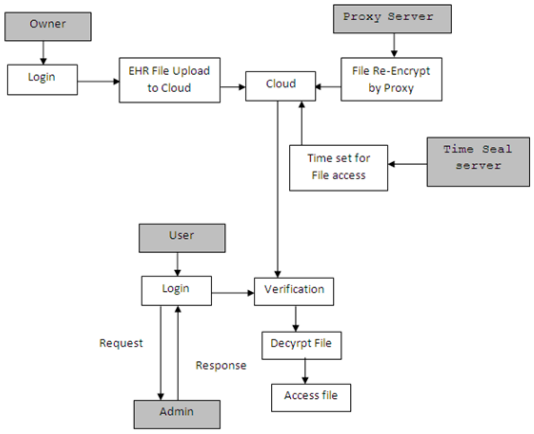

Fig 1: Dataflow of System

V. CONCLUSIONS:

The results of our experiments and our security analysis suggest that our scheme offers far more security than the alternatives that are currently available, all while maintaining a reasonable overhead for cloud applications. To the best of our knowledge, this is the only searchable encryption scheme that has ever been developed with the timing-enabled proxy re-encryption function and the designated tester for the privacy-preserving HER cloud record storage. The method has the potential to safeguard the EHR's secrecy while also providing resilience against KG assaults. It has also been shown to be secure in a formal sense by using the standard model while assuming the difficulty of the truncated decisional ABCDHE issue and the DBDH problem. The efficiency study demonstrates that the suggested method may achieve great compute and storage efficiency, in addition to a higher level of security, when compared with existing traditional searchable encryption systems. The outcomes of our computer simulations have also shown that the suggested solution's communication and computing overhead may be scaled to accommodate any applicable real-world situation.

REFERENCES:

[1] Q. Tang, “Public key encryption schemes supporting equality test with authorization of different granularity,” *Int. J. Appl. Cryptogr.*, vol. 2, no. 4, pp. 304–321, 2012.

[2] P. Liu, J. Wang, H. Ma, and H. Nie, “Efficient verifiable public key encryption with keyword search based on KP-ABE,” in *Proc. IEEE 9th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, Nov. 2014, pp. 584–589.

[3] L. Fang, W. Susilo, C. Ge, and J. Wang, “Public key encryption with keyword search secure against keyword guessing attacks

 @ 2013-2023 http://www.ijitr.com All rights Reserved.

without random oracle," *Inf. Sci.*, vol. 238, pp. 221–241, Jul. 2013.

[4] M.-S. Hwang, S.-T. Hsu, and C.-C. Lee, "A new public key encryption with conjunctive field keyword search scheme," *Inf. Technol. Control*, vol. 43, no. 3, pp. 277–288, 2014.

[5] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Proc. 4th Theory Cryptogr. Conf.*, vol. 4392. Amsterdam, The Netherlands, Feb. 2007, pp. 535–554.

[6] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 262–267, 2011.

[7] J. W. Byun and D. H. Lee, "On a security model of conjunctive keyword search over encrypted relational database," *J. Syst. Softw.*, vol. 84, no. 8, pp. 1364–1372, 2011.

[8] M. Ding, F. Gao, Z. Jin, and H. Zhang, "An efficient public key encryption with conjunctive keyword search scheme based on pairings," in *Proc. 3rd IEEE Int. Conf. Netw. Infrastruct. Digit. Content (IC-NIDC)*, Beijing, China, Sep. 2012, pp. 526–530.

[9] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy re-encryption with keyword search," *Inf. Sci.*, vol. 180, no. 13, pp. 2576–2587, 2010.

[10] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Proxy re-encryption with keyword search: New definitions and algorithms," in *Proc. Int. Conf. Security Technol.*, vol. 122. Jeju Island, Korea, Dec. 2010, pp. 149–160.

 @ 2013-2023 http://www.ijitr.com All rights Reserved.