Implementation of E-Health Cloud System Using Timing Enabled Proxy Re-encryption function (Re-dtPECK)

U.Sarath priyan[1], V.D.Ambeth kumar[2], K.Gunasekaran[3]
Department Of Computer Science And Engineering
Panimalar Engineering College,
Chennai, TamilNadu
Mail Id: sarathpriyancse@gmail.com , vdambethkumar@gmail.com, karguna_it@gmail.com

ABSTRACT:

E-Health record system is a major application which provides great convenience to patients and doctors in the field of health care where patient can no longer use paper prescription and keep it in record for future diagnosis. The major concern is security and sensitive personal information of patients which can be easily misused by the third-party users. Thus, we introduce novel cryptographic primitive named as conjunctive keyword search with designated tester and timing enabled proxy re-encryption function (Re-dtPECK), which is a time-dependent SE scheme. It provides partial access to operate search function to users for limited period of time. Also, the length of the time period can be controlled for the delegatee to search and decrypt delegator's encrypted documents. The major feature is it supports the conjunctive keywords search and resist the keyword guessing attacks. By this, only the designated tester can provide exsistence to certain keywords. Therefore making Re-dtPECK is efficient scheme for standard model.

Keywords: EHR, Encryption, SE, Re-dtPECK.

INTRODUCTION:

Electronic heath records (EHR) system will make medical records which is computerized with the capability to prevent medical errors. It will smooth the process of 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 and other service providers. Health records collected in a data center may contain private information of the patient and therefore leads to vulnerable potential leakage and disclosure to the individuals or companies who may make use for their business and own profits. Even though the service provider can influence the patients to believe that the private information will be safeguarded, the EHR can possibly be exposed if the server is intruded or an inside staff misbehaves. The serious privacy and security concerns are the overriding obstacle that stands in the way of wide adoption of the systems. we make an effort to solve the problem with a primitive mechanism proposed to automatically revoke the delegation right after a period of time designated by the data owner previously. In the traditional time-release system, the time seal is encapsulated in the ciphertext at the very beginning of the encryption algorithm. It implies that all users including data owner are constrained by the time period. The data owner has the right to preset diverse effective access time periods for different users when he appoints his delegation right. An effective time period set by the data owner can be expressed with a beginning and closing time. For example, 1/2/2017 – 12/2/2017.The first work that enables automatic delegation revoking based on timing in a searchable

encryption system. A conjunctive keyword search scheme with designated tester and timing enabled proxy re-encryption function (Re-dtPECK) is proposed, which has the following merits.

1) Designing a novel searchable encryption scheme supporting secure conjunctive keyword search and authorized delegation function. Compared with existing schemes, this work can achieve timing enabled proxy re-encryption with effective delegation revocation.

2) Owner-enforced delegation timing preset is enabled in this system. Distinct access time period can be predefined for various delegatee.

3) The proposed model is formally proved secure against chosen-keyword chosen-time attack. Further, offline keyword guessing attacks can also be resisted . The test algorithm could not function without data server's private key. Third-party could not succeed in guessing keywords by the test algorithm.

4) The security of the scheme works based on the predefined model rather than random oracle model. This is the first novel which supports above functions and is built in the standard model.

LITERATURE SURVEY:

D. Boneh et al. [1] proposed that Public-key system is the major goal for supporting set of queries. For example, payment through credit card which notices a stream of encrypted transactions saying Visa's public key. Flag should be provided for all transactions satisfying a particular predicate P. Storing the secret key on the gateway is not securable for privacy concerns. Therefore, Visa is automized to provide the gateway token TK which tells to identify transactions and enables satisfying P without knowledge of that particular transactions. No information should be saved in the gateway other than predicate value. Still encryption is possible on normal equality queries. Hidden Vector Encryption is the primary tool used for these constructions. This primitive is projected as extreme generalization of Anonymous Identity Based Encryption(AnonIBE). Major advantage of this encryption technique is it supports all types of queries provided by the user. The gateway is not aware of the information other than predicate value. But some open problems are further viewed that provided token is tested by anyone on given ciphertext without the information of plain text. A framework was developed for analyzing security for encrypted data. Then system is developed for comparisons and conjunctive of particular predicates.

In 2008, J.Baek et al. [2] developed Public-key Encryption Keyword Search (PEKS) which allow encryption on keyword search without trailing its confidentiality of novel data. PEKS [2] addresses three major issues which is followed as "refreshing keywords" , "removing secure channel" and "processing multiple keywords". Ineffiency is pointed in original PEKS due to safe channel. Then by efficient PEKS scheme which regrets secure channel. In PEKS, for every keyword a trapdoor is generated, if trapdoor is blocked, the server is in unstable state which PEKS ciphertext encrypts the keyword. For "refreshing keywords" the problem is solved by refreshing the keywords by attaching time period with the encrypted data. The drawback in "removing secure channel" is heavy and high communication load to group a secure channel called Secure Socket Layer (SSL). A user need to

relate multiple keywords to one single message. A problem in designing a PEKS scheme based on primal than BDH problem. The Identity-Based encryption (IBE) is an dependant on Diffie-Hellman inversion problem can buy a PEKS scheme.

In W.C.Yau et al. [3] proposed a new scheme in which PEKS scheme is extended with a designated tester (dPEKS). It ensures that only designated server is responsible for running the test function (dTEST). In 2010 [3] , a new proposal for searchable proxy re-encryption scheme (Re-PEKS). It is a significant contribution to Re-dPEKS where the proxy encryption is done by the searchable content. This allows a proxy with re-encyption key to change the keyword under public key A into the particular keyword encrypted using different public key B. the pros and cons of Re-dPEKS defines the security models, construction ans secure proofs of encryption schemes. The open problem is as follows: It is hard to find an efficient Re-dPEKS schemes in a model. Constructing a secure single-directional scheme in proposed model. Thus, in this paper, we constructed a scheme and proved its security in a random oracle.

B.Zhang et al. [4] proposed a idea and led to construction of Public Key Encryption with Conjunctive subset Keyword Search (PECSK) Scheme. When compared with other scheme, Efficiency plays a major role will be presented and also list of security requirements of the scheme which provide security analysis. The development of Public key Encryption Keyword Search (PEKS) which led to many extensive developments. In this, Conjunctive Keyword search is also an extension but cannot solve subset keywords search which means the receiver can develop a query the subset embedded in cipher text. It improves confidentiality because it encrypt keyword data.

In the year 2012, L.fang et al. [5] proposed a innovative cryptographic method called Conditional Proxy Re-encryption with Keyword Search (C-PRES) which is a combination of C-PRE and PEKS. By combining the sublets of these two concepts a more secure scheme is achieved. The open problem in this PRES scheme is how to design an effectual single-directional PRES scheme. By using C-PRES scheme it provides CCA-Security. Both communication and computation has overall efficiency in this scheme. Anonymity and non-interactivity is also an advantage. Therefore, in this C-PRES scheme rely on ROM because first level CCA security for Fujisaki-Okamoto transformation.

Tang et al. [6] proposed a design for authorization mechanism called PKEET which specifies the user to perform a plaintext equality test from their ciphertexts. A new primitive called AoN-PKEET in which individual user can scamper an authorization algorithm independently and issue those tokens to half-trusted proxies. The major challenge is to develop a mechanism which does parallel to achieve proposed business idea and offer high level privacy and assure confidentiality on sensitive information. In PKEET, it prevents offline data recovery but it is high of cost to process the text because an interactive procedure between two proxies. All the concepts of PKEET, AoN-PKEET, their capabilities are discussed to authorize users to perform equality tests in their respective ciphertexts and available security assurance. Offline recovery attack of data is a major concern on all models, also semi-proxies can transmit the attack in AoN-PKEET.

In the year 2013 [7], Fang et al. proposed SCF-PEKS proposal without random oracle. In this scheme, the receiver is chosen by the server(designated tester) which can perform a test to verify the

relationship between cipher text and trapdoor. The issue proposed in this paper is PEKS secure keywords attack is under random oracle, which does not provide security in real case scenario. There is no complete that capture free PEKS scheme even though these ideas seem to be more practical of PRES models. Some of the advantages are incomplete security and provides a SCF-PEKS secure against guessing attacks. The open problems are on how to achieve an efficient system SCF-PEKS without random oracle is desirable. SCF-PEKS model is proposed in this paper. Furthermore, chosen keyword and ciphertexts attacks are models are discussed on SCF-PEKS model.

Jarecki et al. [8] proposed a new primitive called MC-OXT which searches data on various databases. The problem proposed in this paper is a data source located in a remote server in encrypted form such that it can search the data while hiding data of database and queries. A leakage is detected when queries is limited to minimum to make strategy decision. The conclusion is that a policy manager authorizes a query enforcing them to learn without their policy, only Boolean and query attributes is learned.

Cash et al. [9] developed Searchable Symmetric Encryption (SSE) which permits a user to store data at an untrusted server and shortly search the information for the respective records which coincides with the given keyword simultaneously maintaining privacy. The issue aroused in this paper as it supports one word searches and provides optimal index server size. The development showed several factors disclosed by previous theoretical performance including low space and I/O parallelism and efficient throughput. The advantages are effective CPU parallelism during searching because path amount of I/O code path is in parallel kernel threads. It has some open problems which includes suffering of large index and does not automatically translates I/O into different characteristics of different systems. This paper led to the conclusion which led to the tension between security and performance for SSE non-trivial outcomes for both encryption design and data structures.

Leventhal et al. [10] proposed Electronic Health Records (EHR) which developed a online system for taking patients preferences for an individual for view their EHR. The issue addressed in this paper is to apply fair information practices and balancing the patients personal details wth data providers which needs to deliver safe. The advantages are patients can allow or restrict information to be displayed in different categories. The conclusion is given where the patients information can be restricted for third party viewers and applying them in clinical practices which makes choices to overcome technical and organizational challenges.

PROPOSED SYSTEM :

In Fig 1. Explains there are three types of entities: an information owner, users and data center. The data owners also called as patient or delegator uploads the e-health record files or EHR files into the cloud server where all data services are provided. The EHR files are encrypted by a symmetric encryption algorithm and a symmetric key in encapsulated with the delegator's public key pk_A by key encapsulation mechanism.

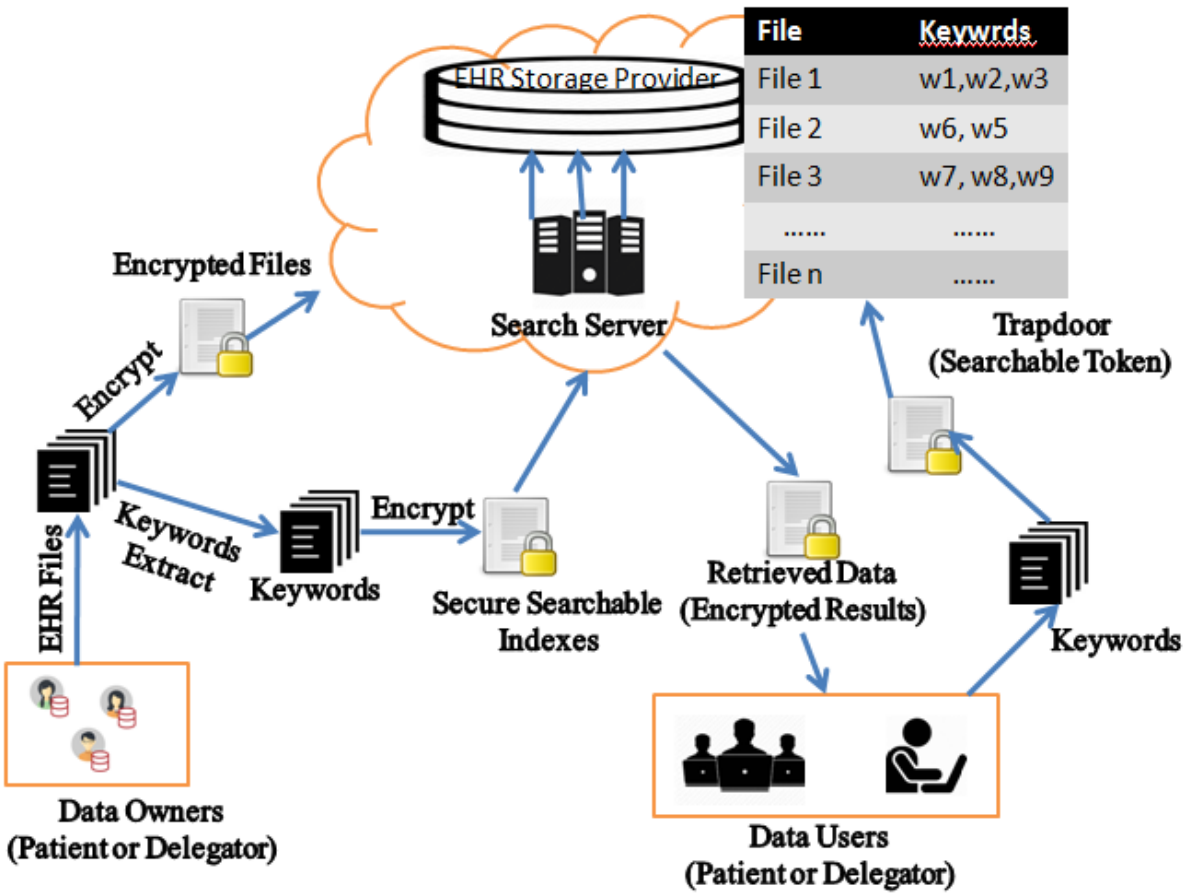

Fig 1. PROPOSED MODEL

The algorithms in the following focus on the searchable keywords encryption and the timing controlled delegation function. From the records, certain words are taken as keywords for the delegatee to open the file by using the keywords. The keywords are once again encrypted and stored as secure searchable indexes and directly stored in the cloud server for retrieval purpose by the doctor or patient. If the data users want to retrieve the information from the cloud. The delegatee should enter the keywords to search the particular file. The data owner wants to store his private EHR files on a third-party database. He extracts keywords from the EHR files and encrypts those plaintext keywords into the secure searchable indices. The EHR files are encrypted to ciphertext. Then, those information are outsourced to the data center . A data center consists of an EHR storage provider and a search server. The storage provider is responsible for storing data and search server performs search/add/delete operations according to users' requests. A user generates a trapdoor to search the EHR files using his private key and sends it to the search servers. After receiving the request, the search servers interact with the EHR storage provider to find the matched files and returns those retrieved information to the user in an encrypted form.

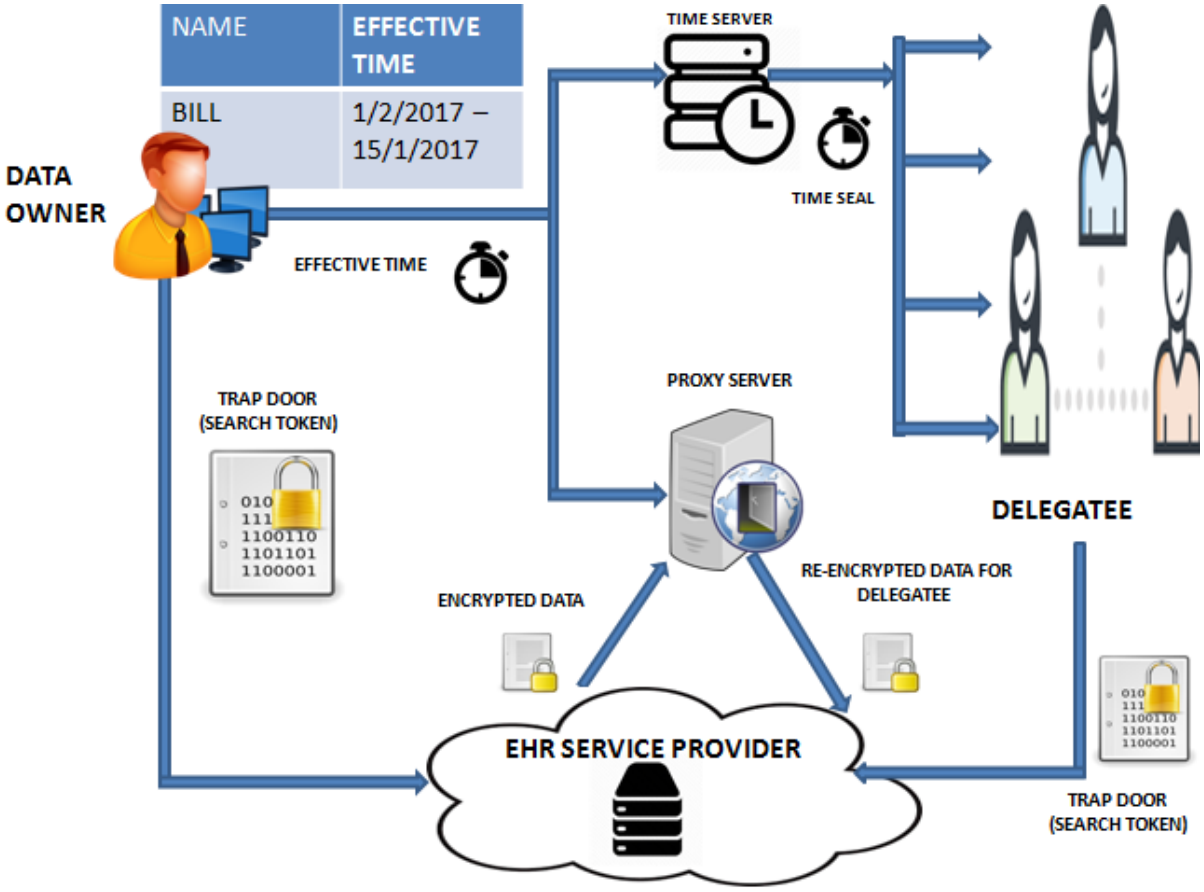

Fig 2. Timing Enabled Proxy Encryption

In Fig. 2, Explains the timing enabled proxy re-encryption searchable encryption model. In this module, we highlight the operation of the time controlled function. The data owner acts as a delegator sends a list of delegation effective time periods for his delegatees to the time server and the proxy server. The entry list consists of identity of each delegatee and the effective time period, such as "bill, 01/02/2017 – 15/02/2017". It indicates that the delegatee bill is authorized to issue queries and perform decryption operations on the encrypted data of the data owner from feb. 1st, 2017 to feb. 15th, 2017. After receiving the list, the time server generates a time seal for each delegatee, which is transmitted to individuals. The time seal is a trapdoor of an effective time period and concealed by the private key of the time server. In the re-encryption operation, the proxy server will encapsulate the effective time into the re-encrypted ciphertext. In order to reduce computing cost, the proxy server will not re-encrypt the ciphertext until they are accessed, which is so called lazy re-encryption mechanism. In the query phase, the data owner can conduct ordinary search operations with his own private key. However, the delegatee has to generate a keywords trapdoor with the help of the time seal. The cloud data server will not return the matched files unless the effective time encapsulated in the time seal accords with the time in the re-encrypted ciphertext, which is different from traditional proxy re-encryption SE schemes.

4.3 MODULE DESCRIPTION

There are 5 modules in the project

1. Authorisation Delegation
2. EHR Storage Provider
3. Time Stamp
4. File Retrieval

Authorisation Delegation

The patient or delegator should register to provide file synchronization to the cloud server where the doctor can view the encrypted file by using some of the decryption algorithms. The authorization and URS provides a user registration service allowing users to self-register, free of charge. The user needs to set up a profile that includes a user ID, password, and provide a small amount of additional information, including affiliation, country, and a valid e-mail address. This information is never provided to any application without a user's explicit permission. A login, logging in or logging on is the entering of identifier information into a system by a user in order to access that system (e.g., a computer or a website). It is an integral part of computer security procedures. A login generally requires the user to enter two pieces of information, first a user name and then a password. This information is entered into a login window on a GUI(graphical user interface) or on the command line in a console (i.e., an all-text mode screen), depending on the system and situation. A user name, also referred to as an account name, is a string (i.e., sequence of characters) that uniquely identifies a user. User names can be the same as or related to the real names of users, or they can be completely arbitrary.

EHR Storage Provider

The data owner wants to store his private EHR files on a third-party database. He extracts keywords from the EHR files and encrypts those plaintext keywords into the secure searchable indices. The EHR files are encrypted to ciphertext. Then, those information are outsourced to the data center. A data center consists of an EHR storage provider and a search server. The storage provider is responsible for storing data and search server performs search/add/delete operations according to users' requests. A user generates a trapdoor to search the EHR files using his private key and sends it to the search servers. After receiving the request, the search servers interact with the EHR storage provider to find the matched files and returns those retrieved information to the user in an encrypted form. The EHR data server is deemed as semi-trusted, who is honest to search information for the benefits of users but curious to spy out the private information of the patients. On the other hand, malicious outside attacker could eavesdrop and analyze the information transferred in public channel, such as the encrypted indexes and trapdoors.

Time Stamp

The timing enabled proxy re-encryption searchable encryption model is shown. In this model, we highlight the implementation of the time controlled function. The data owner acting as a delegator

sends a list of delegation effective time periods for his delegatees to the time server and the proxy server. The entry of the list contains the identity of each delegatee and the effective time period, such as “bill, 01/02/2017 – 15/02/2017”. It indicates that the delegatee Bill is authorized to issue queries and perform decryption operations on the encrypted data of the data owner from Feb. 1st, 2017 to Feb. 15th, 2017. After receiving the list, the time server generates a time seal for each delegatee, which is transmitted to individuals. The time seal is a trapdoor of an effective time period and concealed by the private key of the time server. In the re-encryption operation, the proxy server will encapsulate the effective time into the re-encrypted ciphertext.

File Retrieval

In the query phase, the data owner can conduct ordinary search operations with his own private key. However, the delegatee has to generate a keywords trapdoor with the help of the time seal. The cloud data server will not return the matched files unless the effective time encapsulated in the time seal accords with the time in the re-encrypted ciphertext, which is different from traditional proxy re-encryption SE schemes.

CONCLUSION :

In this paper, we have proposed a primitive Re-dtPECK scheme to recognise the timing enabled privacy-preserving keyword search mechanism for the EHR cloud storage, which could support the automatic delegation revocation. The experimental results and security analysis indicate that the scheme holds high effective security than the existing solutions with a reasonable overhead for cloud applications. To the best of our scenarios, until now this is the first searchable encryption scheme with the timing enabled proxy re-encryption function and the designated tester for the privacy–preserving EHR cloud record storage. The solution could ensure the confidentiality of the EHR and the resistance to the KG attacks. It has also been formally proved secure based on the standard model under the hardness assumption of the truncated decisional l-ABDHE problem and the DBDH problem. Compared with other classical searchable encryption schemes, the efficiency analysis shows that our proposed scheme can achieve high computation and storage efficiency besides its higher security.

REFERENCES :

[1] 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.

[2] J. Baek, R. Safavi-Naini, and W. Susilo, “Public key encryption with keyword search revisited,” in Proc. Int. Conf. ICCSA, vol. 5072. Perugia, Italy, Jun./Jul. 2008, pp. 1249–1259.

[3] 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

[4] 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.

[5] L. Fang, W. Susilo, C. Ge, and J. Wang, "Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search," Theoretical Comput. Sci., vol. 462, pp. 39–58, Nov. 2012.

[6] Q. Tang, "Public key encryption schemes supporting equality test with authorisation of different granularity," Int. J. Appl. Cryptogr., vol. 2, no. 4, pp. 304–321, 2012

[7] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Inf. Sci., vol. 238, pp. 221–241, Jul. 2013.

[8] S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Outsourced symmetric private information retrieval," in Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2013, pp. 875–888.

[9] D. Cash et al., "Dynamic searchable encryption in very-large databases: Data structures and implementation," in Proc. Netw. Distrib. Syst. Security Symp. (NDSS), Feb. 2014, pp. 1–32

[10] J. C. Leventhal, J. A. Cummins, P. H. Schwartz, D. K. Martin, and W. M. Tierney, "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.